SecurityCenter 4

TENABLE NETWORK SECURITY

PVS Plugin Family

March 13, 2012 at 3:04pm CDT

Dave Breslin [dlbreslin]

TENABLE

Network Security®

Table of Contents

Plugin Family Summary

Plugin Family Severity Counts

Family	Total	Info	Low	Med.	High	Crit.
Port scanners	9852	0	9852	0	0	0
Generic [Passive]	530	0	65	0	465	0
CGI [Passive]	525	0	0	0	525	0
SMTP Servers [Passive]	477	0	0	0	477	0
Mobile Devices [Passive]	473	0	208	54	211	0
SCADA [Passive]	473	0	259	97	117	0
Web Servers [Passive]	470	0	18	0	452	0
Data Leakage [Passive]	467	0	467	0	0	0
RPC [Passive]	462	0	462	0	0	0
Samba [Passive]	450	0	53	181	216	0
POP Server [Passive]	444	0	0	72	372	0
FTP Servers [Passive]	437	0	0	0	437	0
Policy [Passive]	435	0	0	383	52	0
Internet Messengers [Passive]	434	0	0	0	434	0
SNMP Traps [Passive]	431	0	0	0	431	0
IMAP Servers [Passive]	431	0	0	36	395	0
SSH [Passive]	428	0	0	0	428	0
Web Clients [Passive]	408	0	5	0	403	0
DNS Servers [Passive]	387	0	0	189	198	0
Peer-To-Peer File Sharing [Passive]	387	0	46	298	43	0
SMTP Clients [Passive]	373	0	0	0	373	0
Backdoors [Passive]	366	0	0	0	366	0
Database [Passive]	364	0	0	0	364	0
Operating System Detection [Passive]	360	0	170	34	156	0
IRC Clients [Passive]	358	0	46	197	115	0
Internet Services [Passive]	349	0	349	0	0	0
FTP Clients [Passive]	115	0	74	0	41	0
Finger [Passive]	83	0	15	35	33	0
IRC Servers [Passive]	83	0	10	14	59	0

Backdoors

Top 25 Most Common Plugin Results

Plugin	Total	Severity	Plugin Name
1919	28	High	SETI@HOME Client Detection
1915	27	High	EvilFTP Backdoor Detection
1918	26	High	SyGate Backdoor Detection
4477	25	High	Trojan Horse Client Detection
1921	25	High	GnoCatan Remote Overflow
1917	24	High	SubSeven Backdoor Detection
1910	23	High	DeepThroat Backdoor Detection
5357	22	High	Arugizer Backdoor Activity Detection
4479	20	High	Trojan Horse Client Detection
5841	18	High	SSL revoked certificate in use
1912	17	High	GateCrasher Backdoor Detection
5840	14	High	SSL revoked certificate in use
4478	14	High	Trojan Horse Client Detection
4480	12	High	Trojan Horse Client Detection
3164	12	High	Zotob Worm Infection
1911	12	High	NetSphere Backdoor Detection
5738	10	High	Stuxnet infected host detection
2815	9	High	Hydrogen Server Detection
4471	7	High	Malware Payload Code Detection
5835	6	High	SSL revoked certificate in use
1916	4	High	Phase Zero Backdoor Detection
4476	3	High	Trojan Horse Client Detection
5838	2	High	SSL revoked certificate in use
5834	2	High	SSL revoked certificate in use
4481	2	High	Trojan Horse Client Detection

CGI

Top 25 Most Common Plugin Results

Plugin	Total	Severity	Plugin Name
5629	28	High	SquirrelMail < 1.4.21 Multiple Vulnerabilities
5991	26	High	Symantec Web Gateway forget.php Blind SQL Injection (SYM11-008)
5618	26	High	Piwik 0.6 < 0.6.4 Remote File Include Vulnerability
5295	26	High	Novell iManager < 2.7 SP3 eDirectory Plugin Buffer Overflow Vulnerability
5504	25	High	Moodle < 1.8.12 / 1.9.8 Multiple Vulnerabilities
5330	25	High	Symantec Altiris Notification Server 6.0 < SP3 R12 Static Encryption Key
5285	25	High	OpenX < 2.8.3 Authentication-Bypass
5522	24	High	MODx < 1.0.3 Multiple Vulnerabilities
5714	23	High	FreeNAS < 0.7.2 Revision 5543 Command Execution Vulnerability
5209	23	High	phpMyAdmin < 2.11.9.6 / 3.2.2.1 Multiple Vulnerabilities
5304	21	High	phpMyAdmin < 2.11.10 Multiple Vulnerabilities
5208	21	High	Achievo < 1.4.0 Multiple Vulnerabilities
5210	20	High	MapServer < 4.10.5/5.2.3/5.4.2 Integer Overflow Vulnerability
5990	19	High	Symantec Web Gateway login.php Blind SQL Injection (SYM11-001)
5257	18	High	Moodle < 1.8.11 / 1.9.7 Multiple Vulnerabilities
5506	17	High	AjaXplorer < 2.6 Multiple Vulnerabilities
5513	16	High	MyBB < 1.4.12 Multiple Vulnerabilities
5365	16	High	eGroupWare < 1.6.003
5324	15	High	HP Power Manager < 4.2.10 Multiple Vulnerabilities
5611	14	High	MapServer < 5.6.4 / 4.10.6 Multiple Vulnerabilities

Plugin	Total	Severity	Plugin Name
5545	14	High	PHPGroupWare < 0.9.16.016
5263	14	High	Piwik < 0.5 unserialize() PHP Code Execution Vulnerability
6113	12	High	HP Managed Printing Administration < 2.6.4 Multiple Vulnerabilities
5736	12	High	HP Power Manager < 4.3.2 Buffer Overflow Vulnerability
5575	12	High	Moodle < 1.8.13 / 1.9.9 Multiple Vulnerabilities

Data Leakage

Top 25 Most Common Plugin Results

Plugin	Total	Severity	Plugin Name
4781	28	Low	Web Server Allows Download of .ini Files
4671	27	Low	Possible Social Security Number in Cookie
4065	26	Low	FTP Server Zipped .pst File Uploaded
5286	25	Low	.torrent file detection
4711	25	Low	'.dll' File Detection
4063	23	Low	FTP Server Zipped .mpg File Uploaded
4067	22	Low	FTP Server Zipped .uni File Uploaded
4948	21	Low	Microsoft Office .xlsx Files Detection
4949	19	Low	Microsoft Office .pptx Files Detection
4061	19	Low	FTP Server Zipped .wma File Uploaded
4060	19	Low	FTP Server Zipped .ogg File Uploaded
4059	19	Low	FTP Server Zipped .wav File Uploaded
4663	18	Low	Possible Social Security Number in Cookie
4672	17	Low	Possible User ID and Password Sent Within a Web Form (POST)
5214	16	Low	Possible userID and password sent within an XML request
4068	16	Low	FTP Server Zipped .pdf File Uploaded
4968	15	Low	Mac .dmg File Detection
4665	15	Low	'.conf' File Detection
4947	13	Low	Microsoft Office .docx File Detection
4062	13	Low	FTP Server Zipped .avi File Uploaded
4064	12	Low	FTP Server Zipped .divx File Uploaded
4673	11	Low	Possible User ID and Password Sent Within a Web Form (GET)

Plugin	Total	Severity	Plugin Name
4662	10	Low	'.cnf' File Detection
4661	9	Low	Java '.class' File Detection
4066	7	Low	FTP Server Zipped .ost File Uploaded

Database

Top 25 Most Common Plugin Results

Plugin	Total	Severity	Plugin Name
4680	29	High	DB2 < 8 FixPak 17 Multiple Vulnerabilities
4638	29	High	DB2 < 9.5 Fix Pack 2 Multiple Vulnerabilities
4612	28	High	DB2 < 9.5 Fix Pack 1 Multiple Vulnerabilities
4230	27	High	Firebird Database Multiple Stack-based Overflows
4239	23	High	IBM DB2 < 9 FixPak 3 / 8 FixPak 15 Multiple Vulnerabilities
5750	19	High	DB2 9.5 < Fix Pack 7 Multiple Vulnerabilities
5150	19	High	Sybase SQL-Anywhere database server default credentials
4536	18	High	DB2 < 9 Fix Pack 5
5906	17	High	IBM Solid Database < 4.5.182 / 6.0.1069 / 6.3.49 / 6.5.0.4 Denial of Service Vulnerability
5749	16	High	DB2 9.1 < Fix Pack 10 Multiple Vulnerabilities
4927	14	High	Vulnerability in Microsoft SQL Server Could Allow Remote Code Execution (959420)
4423	14	High	Informix Dynamic Server Multiple Remote Overflows
5599	13	High	IBM Solid Database < 6.5 Service Pack 2 Handshake Request Username Field Remote Code Execution
4615	13	High	Ingres Database Multiple Local Vulnerabilities
4358	13	High	DB2 < 8.1 FixPak 16 Multiple Vulnerabilities
5751	12	High	DB2 9.7 < Fix Pack 3 Multiple Vulnerabilities
3901	12	High	PostgreSQL Multiple Vulnerabilities
3632	11	High	PostgreSQL SQL Injection
4494	8	High	SAP MaxDB Multiple Vulnerabilities

Plugin	Total	Severity	Plugin Name
4337	6	High	SAP DB / MaxDB Cons Program Arbitrary Command Execution
3921	6	High	IBM DB2 Multiple Local Vulnerabilities
4511	5	High	Firebird Default Credentials
4333	4	High	PostgreSQL Multiple Vulnerabilities
5588	3	High	MySQL Community Server 5.1 < 5.1.48 Denial of Service Vulnerability
5157	2	High	Sybase ASE (Adaptive Server Enterprise) database server default credentials

DNS Servers

Top 25 Most Common Plugin Results

Plugin	Total	Severity	Plugin Name
5933	28	Medium	ISC BIND 9 Large RRSIG RRsets Negative Caching Remote DoS
5107	28	Medium	ISC BIND Dynamic Update Message Handling Remote DoS
1011	28	High	ISC BIND < 4.9.11 Multiple Remote Vulnerabilities
1001	28	High	ISC BIND rdataset Parameter Malformed DNS Packet DoS
5323	27	Medium	BIND 9 DNSSEC Bogus NXDOMAIN Response Remote Cache Poisoning
4578	26	Medium	ISC BIND DNS Query ID Field Prediction Cache Poisoning
1004	26	High	ISC BIND < 8.2.3 Multiple Remote Vulnerabilities
5243	19	Medium	BIND 9 DNSSEC Query Response Remote Cache Poisoning
1008	19	High	ISC BIND < 4.9.5 Multiple DNS Resolver Functions Remote Overflow
3978	16	High	ISC BIND query.c query_addsoa Function Unspecified Recursive Query DoS
1007	16	High	ISC BIND < 4.9.7 Inverse-Query Remote Overflow
5040	15	Medium	NSD packet.c Off-By-One Buffer Overflow
1009	15	High	ISC BIND < 8.2.7 Multiple Remote Vulnerabilities
5909	14	Medium	Bind9 9.8.0 RRSIG Query Type Remote Denial of Service Vulnerability
4601	11	Medium	DNS Server Source Port 53 Query Usage
1012	11	High	ISC BIND < 8.2.2-P5 Multiple Remote Vulnerabilities
2771	10	High	dnsmasq < 2.21 Multiple Remote Vulnerabilities
5601	9	Medium	BIND 9.7.1 < 9.7.1 P2 'RRSIG' Record Type Remote DoS

Plugin	Total	Severity	Plugin Name
1006	9	High	ISC BIND < 8.3.4 Multiple Remote Vulnerabilities
1005	8	High	ISC BIND < 4.9.2 Multiple Remote Vulnerabilities
5718	6	Medium	BIND 9.4-ESV < 9.4-ESV-R4 / 9.6.2 < 9.6.2-P3, 9.6-ESV < 9.6-ESV-R3 / 9.7.x < 9.7.2-P3 Multiple Vulnerabilities
1013	4	High	ISC BIND Compressed ZXFR Name Service Query DoS
6093	3	High	ISC BIND 9 Query.c Logging Resolver Denial of Service
5981	2	Medium	ISC BIND Response Policy Zones (RPZ) DNAME / CNAME Parsing Remote DoS
5803	2	High	BIND 9.7.1-9.7.2-P3 IXFR / DDNS Update Combinded with High Query Rate DoS

Finger

Top 25 Most Common Plugin Results

Plugin	Total	Severity	Plugin Name
1276	22	Medium	Finger Service Detection
1281	16	High	FreeBSD 4.1.1 Finger Arbitrary File Access
1278	15	Low	cfingerd Detection
1279	12	High	cfingerd Multiple Vulnerabilities
1280	7	Medium	Solaris in.fingerd Crafted Request Information Disclosure
1277	6	Medium	Finger Service Detection
1282	5	High	in.fingerd Remote Command Execution

FTP Clients

Top 25 Most Common Plugin Results

Plugin	Total	Severity	Plugin Name
3838	28	Low	Kaspersky Antivirus Client Detection
5702	27	High	SmartFTP Directory Traversal Vulnerability
3377	17	Low	FTP Client Detection
1195	13	Low	FTP Based ZIP File Download Detection
5703	12	High	SmartFTP filename Unspecified Vulnerability
3375	12	Low	FTP Client Detection (PORT)
3376	4	Low	FTP Client Detection (PASV)
3841	2	High	Kaspersky Antivirus Client MIME-encoded Scan Bypass

FTP Servers

Top 25 Most Common Plugin Results

Plugin	Total	Severity	Plugin Name
4979	28	High	Serv-U < 8.0.0.1 Multiple Vulnerabilities (DoS, Traversal)
2861	27	High	NetTerm FTP Server USER Command Remote Overflow
3165	26	High	Zotob Worm Infection
2667	23	High	Golden FTP Server < 1.93 USER Remote Overflow
5237	21	High	Serv-U < 9.1.0.0 TEA Decoder Remote Stack Buffer Overflow
4361	21	High	WS_FTP Server < 6.1.1 Multiple Vulnerabilities
3902	21	High	WinProxy < 6.1 R1c HTTP CONNECT Request Overflow
2941	21	High	Hummingbird Inetd Multiple Remote Overflows
4699	20	High	Serv-U < 7.3.0.1 Multiple Remote Vulnerabilities
2115	20	High	Serv-U FTP Server Default Account
1840	20	High	GuildFTPd Traversal Arbitrary File Enumeration
1844	19	High	ProFTPd ASCII Newline Character Overflow
1836	19	High	FTP Server 'glob' Function Overflow
4981	15	High	Xlight FTP Server Authentication SQL Injection
1854	15	High	TNFTPD Multiple Signal Handler Remote Superuser Privilege Escalation
1843	13	High	ProFTPd < 1.2.0pre6 mkdir Command Overflow
6101	12	High	ProFTPD < 1.3.3g / 1.3.4 Response Pool Use-After-Free Code Execution
4930	12	High	ProFTPD Username Variable Substitution SQL Injection
3534	12	High	Gene6 FTP Server < 3.8.0.34 Multiple Command Remote Overflows
3040	12	High	Inframail FTP Server < 7.12 NLST Command Remote Overflow

Plugin	Total	Severity	Plugin Name
4624	11	High	HP-UX ftpd Remote Privileged Access Authentication Bypass
3836	11	High	TNFTPD < 20040811 Globbing Overflow
2746	9	High	WU-FTPD FTP Server File Globbing Remote DoS
3344	8	High	WinProxy < 6.1a Multiple Vulnerabilities
2738	7	High	FileZilla FTP Server < 0.9.6 Multiple DoS

Generic

Top 25 Most Common Plugin Results

Plugin	Total	Severity	Plugin Name
5689	28	High	Winamp < 5.59 Build 3033 Multiple Vulnerabilities
5741	27	High	Rocket Software UniVerse < 10.3.9 Remote Code Execution Vulnerability
5597	27	High	Winamp < 5.58 Multiple Vulnerabilities
5570	27	High	Novell eDirectory < 8.8 SP5 Patch 4 Multiple Vulnerabilities
6039	26	High	Mac OS X 10.7 < 10.7.2 Multiple Vulnerabilities
5745	26	High	OpenOffice < 3.3 Multiple Vulnerabilities
5267	25	High	Winamp < 5.57 Multiple Vulnerabilities
5705	23	High	Mac OS X 10.6 < 10.6.5 Multiple Vulnerabilities
5984	22	High	HP Intelligent Management Center Endpoint Admission Defense < 5.0 E0101P03 Code Execution Vulnerability
5927	22	High	HP Intelligent Management Center < 5.0 E0101-L02 Multiple Vulnerabilities
5227	22	High	Mac OS X 10.6 < 10.6.2
5826	21	High	Mac OS X 10.6 < 10.6.7 Multiple Vulnerabilities
6303	19	High	Mac OS X 10.7 < 10.7.3 Multiple Vulnerabilities
5726	18	High	Winamp < 5.601 MIDI Timestamp Stack Buffer Overflow
5270	17	High	Zabbix < 1.6.8 Multiple Vulnerabilities
5968	15	High	Mac OS X 10.6 < 10.6.8 Multiple Vulnerabilities
5907	14	High	Novell File Reporter Agent XML Parsing Remote Code Execution
5489	13	High	Mac OS X < 10.6.3 Multiple Vulnerabilities
5739	12	High	Mac OS X 10.6 < 10.6.6 Multiple Vulnerabilities

Plugin	Total	Severity	Plugin Name
5564	12	High	OpenOffice < 3.2.1 Multiple Vulnerabilities
5511	12	High	RealNetworks Helix Server 11.x / 12.x / 13.x Multiple Vulnerabilities
5251	12	High	eDirectory < 8.8.5.2/8.7.3.10 ftf2 'NDS Verb 0x1' Buffer Overflow
12	12	Low	Host TTL discovered
4716	8	Low	DHCP Client Detection
7034	7	Low	Web server vhost detection

IMAP Servers

Top 25 Most Common Plugin Results

Plugin	Total	Severity	Plugin Name
3937	29	High	Ipswitch IMail Server < 2006.2 Multiple Overflows
1095	29	High	Mozilla IMAP Client literal_size Remote Overflow
3814	28	High	WorldMail <= 6.1.22.0 Multiple Vulnerabilities
1094	28	High	MDaemon IMAP Service CREATE Command Mailbox Name Handling Overflow
2425	27	High	Cyrus IMAPD < 2.2.10 Multiple Vulnerabilities
2310	27	High	Alt-N MDaemon Multiple Buffer Overflows
1099	26	High	Pine c-client IMAP Client literal_size Remote Overflow
1093	24	High	UoW imapd (UW-IMAP) Multiple Command Remote Overflows
1210	23	High	Courier IMAP Server < 3.0.7 Multiple Vulnerabilities
3068	22	High	MailEnable IMAP STATUS Command Remote Overflow
1101	22	High	UoW imapd (UW-IMAP) AUTHENTICATE Command Remote Overflow
5184	21	Medium	Ability Mail Server < 2.70 Remote Denial of Service
3383	18	High	Mercury Mail Transport System < 4.01b ph Service Buffer Overflow
3906	15	High	AXIGEN Mail Server IMAP Server Multiple Authentication Methods DoS
2438	14	High	Mercury Mail Remote IMAP Stack Buffer Overflow
4730	11	High	UW-IMAP < 2007d.404 Multiple Utility Mailbox Name Overflow
3958	11	High	Lotus Domino IMAP Server < 6.5.6 / 7.0.2 FP1 CRAM-MD5 Authentication Overflow
4798	9	Medium	UW-IMAP < 2007e c-client Library Overflow

Plugin	Total	Severity	Plugin Name
1092	9	High	Netscape Messaging Server IMAP LIST Command Remote Overflow
2645	7	High	Cyrus IMAPD < 2.2.12 Multiple Remote Overflows
2158	5	High	Merak Mail Server < 7.5.2 Web Mail Module Multiple Issues
1085	5	High	Cyrus IMAP Server login Command Remote Overflow
3483	4	High	MailEnable Multiple Products POP3 Authentication Bypass
1090	4	High	Ipswitch IMail 5.0 Multiple Remote Overflows
4290	3	Medium	Ability Mail Server < 2.61 Multiple Vulnerabilities

Internet Services

Top 25 Most Common Plugin Results

Plugin	Total	Severity	Plugin Name
3414	29	Low	ReadNotify Email Tracker Application Detection
4467	27	Low	MarketFirst Software Detection
4157	27	Low	SendThisFile Client Detection
5948	24	Low	Box.net client detection
5200	24	Low	Pandora version detection
4164	23	Low	Mediamax File Sharing Detection
6100	20	Low	Sony Blu-Ray player detection
6124	19	Low	BingToolbar Installed
5817	18	Low	Facebook Chat Client Detection
6112	17	Low	Shavlik software management detection
5679	17	Low	iDisk user enumeration
5274	15	Low	classmates.com usage detection
4156	14	Low	YouSendIt Client Detection
5875	12	Low	Wikipedia 'edit' detection
6339	11	Low	Evernote Client detection
6090	11	Low	Google music client detection
4161	11	Low	Box.net File Sharing Detection
3939	9	Low	MySpaceIM Chat Detection
5276	7	Low	XM Radio usage detection
3217	4	Low	Google Talk Detection
2488	4	Low	"Google Hacking" via Google API
6128	3	Low	Spotify Installed
5695	3	Low	YouSendIt client detection

Internet Messengers

Top 25 Most Common Plugin Results

Plugin	Total	Severity	Plugin Name
4103	29	High	AOL Instant Messenger <= 6.1.32.1 SIP INVITE Message DoS
2894	29	High	Gaim < 1.3.0 Multiple Vulnerabilities
4197	27	High	Windows Live Messenger < 8.1.0178 Video Processing Overflow
3772	27	High	Skype Technologies < 1.5.0.80 NSRRunAlertPanel Function Format String (Mac OS X)
1274	26	High	AOL Instant Messenger aim:goaway URI Handler goaway Function Away Message Handling Remote Overflow
2630	24	High	Yahoo! Messenger < 6.0.0.1750 Detection
4210	23	High	Vulnerability in Microsoft MSN Messenger and Windows Live Messenger Could Allow Remote Code Execution (942099)
4144	22	High	Trillian < 3.1.7.0 Multiple Vulnerabilities
3008	20	High	AOL Instant Messenger Remote Malformed GIF DoS
4102	19	High	Trillian < 3.1.6.0 Multiple Vulnerabilities
5137	18	High	Pidgin < 2.5.9 Buffer Overflow vulnerability
4199	18	High	Yahoo! Messenger < 8.1.0.419 YVerInfo ActiveX Buffer Overflow
5032	16	High	Pidgin < 2.5.6 Multiple Buffer Overflow Vulnerabilities
4405	15	High	ICQ 6 HTML Code Generation Remote Format String
3268	15	High	Skype Technologies Multiple Buffer Overflows
3199	14	High	IndiaTimes Instant Messenger ActiveX RenameGroup Function Overflow
1266	13	High	Yahoo! Messenger Message Field Remote Overflow

Plugin	Total	Severity	Plugin Name
2749	12	High	Trillian HTTP-parsing Remote Overflow
4778	10	High	Trillian < 3.1.12.0 Multiple Vulnerabilities
4310	10	High	Skype Technologies < 3.6.0.216 skype4com URI Handler Remote Heap Corruption
4515	9	High	Trillian < 3.1.10.0 Multiple Vulnerabilities
4211	9	High	Vulnerability in Microsoft MSN Messenger and Windows Live Messenger Could Allow Remote Code Execution (942099)
1271	8	High	Yahoo! Messenger Download Feature Long Filename Overflow
4531	6	High	Skype Technologies URI Handler remote code execution
2405	6	High	Skype < 1.0.0.100 CallTo URI Buffer Remote Overflow

IRC Clients

Top 25 Most Common Plugin Results

Plugin	Total	Severity	Plugin Name
1872	26	Medium	Trillian IRC JOIN Remote Overflow
1863	26	Medium	mIRC < 6.03 Scripting $asctime Overflow
1855	26	High	BitchX IRC Client "/INVITE" Command Format String DoS
1876	24	Medium	XChat Client URL Metacharacter Command Execution
1873	23	High	XChat Malformed Nickname Remote Format String
1862	21	Low	mIRC < 6.1 DCC Server Protocol Nickname Disclosure
1870	20	High	Trillian IRC Module Channel Name Format String
1867	20	High	Trillian IRC Module DCC Length Remote Overflow
1865	20	Medium	Trillian IRC PART Message Remote DoS
2547	19	Medium	Konversation IRC Client < 0.15.1 Multiple Remote Vulnerabilities
1868	19	Medium	Trillian IRC Oversized Data Block Remote Overflow DoS
1878	15	Low	IRC Client Detection
3101	10	Low	IRC Client Detection
1874	10	Medium	XChat /dns Reverse Lookup Response Arbitrary Command Execution
1864	10	Medium	mIRC DCC Get Dialog File Spoofing Weakness
1875	9	Medium	XChat CTCP Ping Arbitrary Remote IRC Command Execution
1871	9	Medium	Trillian IRC Server Response Remote Overflow
1861	9	High	mIRC < 6.0 Long Nickname Buffer Overflow
1859	9	High	BitchX Trojaned Distribution Authentication Bypass
1856	9	Medium	BitchX IRC Clent DNS Response Remote Overflow

Plugin	Total	Severity	Plugin Name
1866	8	High	Trillian IRC User Mode Numeric Remote Overflow
1857	7	Medium	BitchX IRC Client Malformed RPL_NAMEREPLY Message DoS
1877	6	Medium	mIRC Minimized Dialogue Window DoS
1869	3	Medium	Trillian IRC Raw Message DoS

IRC Servers

Top 25 Most Common Plugin Results

Plugin	Total	Severity	Plugin Name
2403	26	High	BNC < 2.9.1 getnickuserhost IRC Server Response Buffer Overflow
2919	24	High	ignitionServer < 0.3.6p1 Channel Locking Remote DoS
2153	10	Low	Unreal IRCD < 3.2.1 Cloak IP Address Disclosure
2404	9	High	BNC IRC Server < 2.9.1 Authentication Bypass
2154	7	Medium	Unreal IRCD OperServ Raw Message Channel Join DoS
2152	7	Medium	ignitionServer < 0.3.2 SERVER Command Remote DoS

Mobile Devices

Top 25 Most Common Plugin Results

Plugin	Total	Severity	Plugin Name
5715	27	High	Apple iPhone/iPad iOS < 4.2 Multiple Vulnerabilities
5889	26	High	Apple iPhone/iPad OS 4.2.5 / 4.2.6 Multiple Vulnerabilities
5110	26	High	Apple iPhone 3.x detection
6079	25	Low	Samsung mobile device version detection
6084	24	Low	PalmOS mobile device version detection
6082	24	Low	Samsung mobile device version detection
6077	24	Low	Nokia mobile device version detection
6041	24	High	Apple iOS 3.0 through 4.3.5 Multiple Vulnerabilities
6114	23	Low	Kindle mobile device detection
5993	22	Medium	Apple iOS < 4.2.10 / 4.3.5 Data Security Certificate Verification Vulnerability
5578	21	High	Apple iPhone/iPad OS < 4.0 Multiple Vulnerabilities
6297	19	Medium	Android 2.3 < 2.3.6 Information Disclosure
6080	18	Low	Samsung mobile device version detection
5814	17	High	Apple iPhone/iPad OS < 4.3 Multiple Vulnerabilities
4425	17	High	Apple iPhone < 1.1.4 Detection
6085	16	Low	Symbian mobile device version detection
5160	14	High	Apple iPhone < 3.1 Multiple Vulnerabilities
6081	13	Low	Samsung mobile device version detection
5986	13	High	Apple iPhone/iPad iOS < 4.3.4 and iOS 4.2.5 through 4.2.9 Multiple Vulnerabilities
5189	12	Medium	BlackBerry Dialog Box Certificate Mismatch
5337	11	High	Apple iPhone OS < 3.1.3 Multiple Vulnerabilities
5737	10	High	Android < 2.3 Multiple Vulnerabilities

Plugin	Total	Severity	Plugin Name
6075	9	Low	Kindle mobile device version detection
6086	7	Low	Motorola mobile device version detection
6078	7	Low	Nook mobile device version detection

Operating System Detection

Top 25 Most Common Plugin Results

Plugin	Total	Severity	Plugin Name
6122	28	Low	Windows OS version info
6118	27	Low	Windows OS version info
6117	27	Low	Windows OS version info
3947	25	High	Mac OS X < 10.4.9 / Security Update 2007-003
2751	25	High	Windows 2000 Server Detection (No Service Pack)
2753	23	High	Windows 2000 SP2 Detection
6119	21	Low	Windows OS version info
2766	21	High	Mac OS X 10.1 Detection
2752	20	High	Windows 2000 SP1 Detection
6120	19	Low	Windows OS version info
3010	19	Medium	Mac OS X 10.4.1 Detection
2765	16	High	Mac OS X 10.0 Detection
6121	12	Low	Windows OS version info
6123	11	Low	Windows OS version info
3502	8	Medium	Mac OS X < 10.4.6 Multiple Vulnerabilities
2756	8	High	Windows XP (No Service Pack) Detection
6296	7	Low	CentOS version detection
6116	7	Low	Windows OS version info
4284	7	High	Mac OS X < 10.4.11 Multiple Vulnerabilities / Security Update 2007-008
2934	7	Medium	Mac OS X 10.4.0 Detection
6115	5	Low	Windows OS version info
4373	5	High	Mac OS X < 10.5.2 Multiple Vulnerabilities
2767	4	High	Mac OS X 10.2 Detection
6127	3	Low	Windows OS version info
6125	3	Low	Windows OS version info

Peer-To-Peer File Sharing

Top 25 Most Common Plugin Results

Plugin	Total	Severity	Plugin Name
2062	27	Medium	KazaaClient Detection
4550	26	Medium	JXTA P2P Server Detection
2872	23	Medium	BitTorrent Client Detection
2813	23	Medium	DC++ < 0.674 File Content Manipulation
4942	22	Low	Manolito Peer-to-Peer Server Detection
2710	21	Medium	LimeWire < 4.8.0 Directory Traversal Arbitrary File Access
2057	19	Medium	Xolox Detection
3991	18	Medium	BitTorrent Server Detection
2063	18	Medium	Trillian Detection
5034	17	Low	SoulSeek version detection
3385	17	High	Shareaza P2P Fileshare Client Integer Overflow
2868	17	Medium	ICUII Peer-To-Peer Client Detection
2577	16	Medium	BitTorrent P2P Client Detection
2056	16	Medium	WinMX Detection
2060	15	Medium	Edonkey2k Detection
2347	13	High	Vypress < 4.0 First Message Field Overflow
2327	13	Medium	Zinf .pls File Overflow
2058	13	High	Kazaa Detection
3920	12	Medium	BitTorrent Client Detection
5292	7	Medium	Transmission Client Detection
4941	7	Low	Manolito Peer-to-Peer Client Detection
4551	5	Medium	JXTA P2P Client Detection
2434	5	Medium	Open DC Hub RedirectAll Value Remote Buffer Overflow
2053	5	Medium	Blubster Detection.
2051	4	Medium	BearShare Detection

Policy

Top 25 Most Common Plugin Results

Plugin	Total	Severity	Plugin Name
5866	29	Medium	Webserver serving pornographic materials
5863	28	Medium	Webserver serving pornographic materials
5876	26	Medium	.NET verbose error reporting
5723	26	High	JavaScript eval() usage on Web Server
4527	26	High	Dell Printer administrative web console detection
3686	25	Medium	WebInspect Detection
5869	24	Medium	Webserver serving pornographic materials
3813	24	Medium	Tivoli Network Services Auditor (NSA) Scanner Detection
5871	23	Medium	Webserver serving pornographic materials
5862	23	Medium	Webserver serving pornographic materials
3660	23	Medium	GFI Languard Scanner Detection
5868	22	Medium	Webserver serving pornographic materials
3909	22	Medium	Sensepost Wikto Detection
3806	17	Medium	MetaSploit Server Detection
3685	15	Medium	MetaSploit Shell Detection
5864	13	Medium	Webserver serving pornographic materials
5874	9	Medium	Webserver serving pornographic materials
5865	9	Medium	Webserver serving pornographic materials
3807	9	Medium	Brutus Password Scanning Tool Detection
5873	8	Medium	Webserver serving pornographic materials
5861	8	Medium	Webserver serving pornographic materials
4558	8	Medium	Kismet Server Information Disclosure
4138	6	Medium	IBM AppScan Detection
5867	5	Medium	Webserver serving pornographic materials

Plugin	Total	Severity	Plugin Name
3683	4	Medium	MetaSploit Detection

POP Server

Top 25 Most Common Plugin Results

Plugin	Total	Severity	Plugin Name
5186	28	Medium	Ability Mail Server < 2.70 Remote Denial of Service
4260	28	High	Delegate < 9.7.5 Multiple Vulnerabilities
1801	28	High	XMail < 2.4 (Build 0530) APOP Remote Format String
1790	27	High	ZetaMail Remote DoS
2156	26	High	Merak Mail Server < 7.5.1 Web Mail Module Multiple Issues
2938	25	High	GNU Mailutils Multiple IMAP Vulnerabilities
1799	25	High	Xtramail < 1.12 Control Server Overflow Denial of Service
1796	23	High	Computalynx CMail < 2.4.10 HELO Command Overflow
2413	22	High	Digital Mappings Systems POP3 Server Remote Buffer Overflow
1800	21	High	XMail < 0.59 APOP Overflow DoS
4765	18	Medium	MDaemon WorldClient < 10.0.2 Script Injection
3655	18	High	MERCUR < 2005 SP4 Multiple Remote DoS
1794	16	High	Qualcomm Qpopper Username Remote Overflow
3034	15	High	True North eMailServer < 5.3.4 Build 2019 LIST Command Remote DoS
3300	13	High	Winmail Server <= 4.2 Multiple Vulnerabilities
1791	13	High	Delegate Multiple Function Remote Overflows
4292	12	Medium	Ability Mail Server < 2.61 Multiple Vulnerabilities
5517	11	Medium	Alt-N MDaemon < 11.0.1 Multiple Remote DoS Vulnerabilities
2935	10	High	Qualcomm Qpopper < 4.0.5 Multiple Local Privilege Escalation
1798	10	High	Xtramail < 1.12 POP3 Overflow

Plugin	Total	Severity	Plugin Name
1792	10	High	Qualcomm Qpopper Remote Overflow DoS
1789	10	High	qpopper Options File Buffer Overflow
1785	9	High	qpopper < 4.0 PASS Command Remote Overflow
1793	8	High	Qualcomm Qpopper Remote Overflows
3938	6	High	Ipswitch IMail Server < 2006.2 Multiple Overflows

RPC

Top 25 Most Common Plugin Results

Plugin	Total	Severity	Plugin Name
1071	29	Low	RPC traffic Service In Use
1083	28	Low	Superflous NFS Daemon Detection
1081	28	Low	RPC fypxfrd Service In Use
1078	28	Low	RPC amd Service In Use
1080	27	Low	RPC bwnfsd Service In use
1061	27	Low	RPC hostmem Service In Use
1068	25	Low	RPC iproutes Service In Use
1059	24	Low	RPC hostperf Service In Use
1065	21	Low	RPC NFS (na.rpcnfs) Service In Use
1064	20	Low	RPC ping Service In Use
1056	20	Low	RPC SunNet Manager event Service In Use
1067	19	Low	RPC etherif Service In Use
1084	18	Low	RPC status Service In Use
1082	16	Low	RPC portmapper Service In Use
1077	16	Low	RPC pcnfsd Service In Use
1060	16	Low	RPC SunNet Manager activity Service In Use
1066	15	Low	RPC hostif Service In Use
1072	13	Low	RPC nfs_acl Service In Use
1076	11	Low	RPC ufsd Service In Use
1073	11	Low	RPC sadmind Service In Use
1074	8	Low	RPC nisd Service In Use
1058	8	Low	RPC SunNet sync Service In Use
1070	7	Low	RPC snmp Service In Use
1069	7	Low	RPC layers Service In Use
1063	7	Low	RPC x25 Service In Use

Samba

Top 25 Most Common Plugin Results

Plugin	Total	Severity	Plugin Name
1337	29	Low	Samba Version Detection
5194	27	Medium	Samba < 3.0.37 / 3.2.15 / 3.3.8 / 3.4.2 Multiple Vulnerabilities
2337	26	Medium	Samba < 2.2.11 Remote Arbitrary File Access
3499	24	Low	Samba < 3.0.22 Local File Permissions Credentials Disclosure
1341	24	High	Samba-TNG < 0.3.1 multiple flaws
5663	23	High	Samba 3.x < 3.5.5 / 3.4.9 / 3.3.14 sid_parse Buffer Overflow
3988	23	High	Samba < 3.0.25 NDR MS-RPC Request Heap-Based Overflow
4774	21	Medium	Samba 3.0.29 - 3.2.4 Potential Memory Disclosure
1338	21	High	Samba < 2.0.10 Remote Arbitrary File Overwrite
5572	18	High	Samba 3.x < 3.3.13 SMB1 Packet Chaining Memory Corruption
2463	18	Medium	Samba < 3.0.10 Directory Access Control List Remote Integer Overflow
2338	17	Medium	Samba < 3.0.6 Remote Arbitrary File Access
1342	17	High	Samba < 2.2.8a trans2.c trans2open() Function Overflow
4522	16	High	Samba < 3.0.30 receive_smb_raw Buffer Overflow Vulnerability
3682	16	Medium	Samba < 3.0.23 smdb Share Remote DoS
3905	15	Medium	Samba < 3.0.24 nss_winbind.so.1 Multiple Function Overflow
1343	14	High	Samba < 2.2.7 Unicode Encrypted Password Decryption Overflow
6299	13	Medium	Samba 3.6.x < 3.6.3 Denial of Service

Plugin	Total	Severity	Plugin Name
3990	13	High	Samba < 3.0.25 Multiple Vulnerabilities
4285	12	High	Samba < 3.0.27 Multiple Vulnerabilities
5087	10	High	Samba Format String and Security Bypass Vulnerabilities
5360	9	Medium	Samba 3.3.11 / 3.4.6 / 3.5.0 Security Bypass Vulnerability
5534	8	High	Samba Denial of Service in versions < 3.5.2/3.4.8
2397	8	Medium	Samba < 3.0.8 Remote Wild Card DoS and QFILEPATHINFO Remote Overflow
1340	8	High	Samba < 2.2.5 Multiple Overflows

SMTP Clients

Top 25 Most Common Plugin Results

Plugin	Total	Severity	Plugin Name
5692	29	High	Mozilla Thunderbird 3.0.x < 3.0.10 Buffer Overflow Vulnerability
4762	28	High	Mozilla Thunderbird < 2.0.0.18 Multiple Vulnerabilities
6010	27	High	Mozilla Thunderbird 5 Multiple Vulnerabilities
6110	24	High	Mozilla Thunderbird 8 Multiple Vulnerabilities
5966	21	High	Mozilla Thunderbird 3.1.x < 3.1.11 Multiple Vulnerabilities
5730	21	High	Mozilla Thunderbird 3.1.x < 3.1.7 Multiple Vulnerabilities
5483	21	High	Mozilla Thunderbird Unsupported Version Detection
5729	19	High	Mozilla Thunderbird 3.0.x < 3.0.11 Multiple Vulnerabilities
4609	18	High	Mozilla Thunderbird < 2.0.0.16 Multiple Vulnerabilities
5693	17	High	Mozilla Thunderbird 3.1.x < 3.1.6 Buffer Overflow Vulnerability
5480	16	High	Mozilla Thunderbird < 2.0.0.24 Multiple Vulnerabilities
5355	15	High	Mozilla Thunderbird < 3.0.2 Multiple Vulnerabilities
4696	15	High	Mozilla Thunderbird < 2.0.0.17 Multiple Vulnerabilities
4806	12	High	Mozilla Thunderbird < 2.0.0.19 Multiple Vulnerabilities
5684	11	High	Mozilla Thunderbird 3.1.x < 3.1.5 Multiple Vulnerabilities
5582	9	High	Mozilla Thunderbird < 3.0.5 Multiple Vulnerabilities
5903	8	High	Mozilla Thunderbird 3.1.x < 3.1.10 Multiple Vulnerabilities
5608	8	High	Thunderbird 3.0.x < 3.0.6 Multiple Vulnerabilities
5001	8	High	Mozilla Thunderbird < 2.0.0.21 Multiple Vulnerabilities
4964	8	High	Mozilla Thunderbird < 2.0.0.21 Multiple Vulnerabilities

Plugin	Total	Severity	Plugin Name
5658	7	High	Thunderbird < 3.0.x < 3.0.7 Multiple Vulnerabilities
6029	6	High	Mozilla Thunderbird 6 Multiple Vulnerabilities
5683	6	High	Mozilla Thunderbird 3.0.x < 3.0.9 Multiple Vulnerabilities
4497	6	High	Mozilla Thunderbird < 2.0.0.14 Multiple Vulnerabilities
5354	5	High	Mozilla Thunderbird < 3.0.1 Multiple Vulnerabilities

SMTP Servers

Top 25 Most Common Plugin Results

Plugin	Total	Severity	Plugin Name
4207	29	High	Hexamail < 3.0.1.004 POP3 Service USER Command Overflow
4141	29	High	Ipswitch IMail Server < 2006.21 Multiple Vulnerabilities
4555	28	High	SurgeMail < 3.9g2-2 IMAP Command Handling Unspecified DoS
3322	27	High	Courier Mail Server < 0.52.2 Deactivated Account Authentication Bypass
4077	25	High	Lotus Domino Web Server Multiple Vulnerabilities
4431	23	High	NetWin SurgeMail <= 3.8k4-4 IMAP LIST Command Remote Overflow
3646	22	High	Courier Mail Server < 0.53.2 Crafted Username Encoding DoS
5600	21	High	Ipswitch IMail Server < 11.02 Multiple Vulnerabilities
3484	21	High	Sendmail < 8.13.6 Unspecified Overflow
3317	21	High	Ipswitch IMail Format String and 'LIST' Command DoS
5752	19	High	Exim < 4.74 Local Privilege Escalation Vulnerability
3039	18	High	Inframail SMTP Server < 7.12 MAIL FROM Command Remote Overflow
3029	18	High	Sendmail < 8.13.4 Multiple Vulnerabilities
4517	17	High	Lotus Domino < 8.0.1 / 7.0.3 FP1 Multiple Vulnerabilities
3106	17	High	GoodTech SMTP Server < 5.17 'RCPT TO' Command Remote Overflow
4148	16	High	Kerio MailServer < 6.4.1 Attachment Filter Unspecified Issue
5293	15	High	Sendmail < 8.14.4 SSL Certificate NULL Character Spoofing

Plugin	Total	Severity	Plugin Name
4381	15	High	Kerio MailServer < 6.5.0 Multiple Vulnerabilities
4203	15	High	MailMarshal <= 6.2.1 tar Archive Traversal Arbitrary File Overwrite
3659	15	High	Clearswift MAILsweeper for SMTP < 4.3.20 Multiple Vulnerabilities
5910	14	High	Exim < 4.70 string_format Function Remote Overflow
3738	13	High	Ipswitch IMail Server RCPT String Remote Overflow
3155	13	High	BusinessMail SMTP < 4.7 Multiple Command Remote Overflows
4339	6	High	Lotus Domino < 7.0.2 FP3 Unspecified DoS
4261	6	High	Lotus Domino Multiple Vulnerabilities

SNMP Traps

Top 25 Most Common Plugin Results

Plugin	Total	Severity	Plugin Name
2209	29	High	Cisco PPTP Authentication Bypass / DoS (Bug ID CSCdt56514)
2244	27	High	Cisco TFTP Server Long Filename DoS (Bug ID CSCdy03429)
2240	27	High	Cisco Multiple DoS (Bug ID CSCdx92043)
2228	26	High	Cisco VPN Concentrator HTML Source Certificate Password Disclosure (Bug ID CSCdw50657)
2222	26	High	Cisco VPN Concentrator PPTP Multiple Issues (Bug ID CSCdv66718)
2245	24	High	Cisco TFTP Server Long Filename DoS (Bug ID CSCdy03429)
2223	24	High	Cisco VPN Concentrator PPTP Multiple Issues (Bug ID CSCdv66718)
2233	23	High	Cisco VPN Concentrator ACL Bypass / DoS (Bug ID CSCdx07754, CSCdx24622, CSCdx24632)
2229	22	High	Cisco VPN Concentrator HTML Source Certificate Password Disclosure (Bug ID CSCdw50657)
2219	20	High	Cisco VPN Concentrator Invalid Login DoS (Bug ID CSCdu82823)
2208	20	High	Cisco PPTP Authentication Bypass / DoS (Bug ID CSCdt56514)
2251	18	High	Cisco IOS SIP Packet Remote DoS (Bug ID CSCdz39284, CSCdz41124)
2231	18	High	Cisco VPN Concentrator ACL Bypass / DoS (Bug ID CSCdx07754, CSCdx24622, CSCdx24632)
2220	16	High	Cisco VPN Concentrator Invalid Login DoS (Bug ID CSCdu82823)

Plugin	Total	Severity	Plugin Name
3750	15	High	SNMP 'cable-docsis' Community String
2227	13	High	Cisco VPN Concentrator HTML Source Cleartext Password Disclosure (Bug ID CSCdv88230, CSCdw22408)
2225	13	High	Cisco VPN Concentrator HTML Source Cleartext Password Disclosure (Bug ID CSCdv88230, CSCdw22408)
2203	12	High	Cisco IOS OSPF Neighbor Announcement Overflow DoS (Bug ID CSCdp58462)
2242	10	High	Cisco Multiple DoS (Bug ID CSCdx92043)
3749	9	High	SNMP 'cable-docsis' Community String
2249	8	High	Cisco IOS SIP Packet Remote DoS (Bug ID CSCdz39284, CSCdz41124)
2232	7	High	Cisco VPN Concentrator ACL Bypass / DoS (Bug ID CSCdx07754, CSCdx24622, CSCdx24632)
2250	5	High	Cisco IOS SIP Packet DoS (Bug ID CSCdz39284, CSCdz41124)
2241	5	High	Cisco Multiple DoS (Bug ID CSCdx92043)
2230	5	High	Cisco VPN Concentrator HTML Source Certificate Password Disclosure (Bug ID CSCdw50657)

SCADA

Top 25 Most Common Plugin Results

Plugin	Total	Severity	Plugin Name
3852	29	High	Modicon Modbus/TCP Programming Function Code Access (SCADA)
6284	28	Low	Rockwell Automation PLC HTTP Server Detection (SCADA)
3851	28	High	Modicon PLC Default FTP Password (SCADA)
6323	27	Low	7T-IGSS Server login attempt detected (SCADA).
3555	27	Low	COTP Client Detection (SCADA)
6282	26	High	GE PLC telnet Server Default Account/Password (SCADA)
6317	25	Medium	InduSoft WebStudio Server detection Version 6 (SCADA)
6330	24	Low	7T-IGSS Server detected (SCADA).
6313	24	Low	ClearSCADA Management Server Detection (SCADA)
3855	23	Medium	Modicon PLC CPU Type Default Credentials (SCADA)
6316	22	Low	InduSoft WebStudio Server detection (SCADA)
6314	22	Low	ClearSCADA Management Server Detection (SCADA)
6281	22	Low	GE PLC telnet Server Detection (SCADA)
6285	21	Medium	Rockwell Automation PLC HTTP Server Administrator Access Detection (SCADA)
6286	19	Low	Rockwell Automation PLC - Micrologix Controller Version Detection (SCADA)
3854	18	High	Modicon PLC Telnet Server Detection (SCADA)
6318	17	Medium	InduSoft WebStudio Server detection Version 7 (SCADA)
3556	17	Low	MODBUS Server Detection (SCADA)
3850	12	Low	Modicon PLC Embedded HTTP Server Detection (SCADA)

Plugin	Total	Severity	Plugin Name
3849	11	Medium	MODBUS Server Diagnostic Mode (SCADA)
3553	8	Low	Distributed Network Protocol v3 Server Detection
3853	7	High	Modicon PLC HTTP Server Default Username/Password (SCADA)
6283	5	High	GE PLC telnet Server Default Account/Password (SCADA)
6287	4	High	Modicon PLC HTTP Default Account/Password Detection (SCADA)
3557	4	Low	MODBUS Client Detection (SCADA)

SSH

Top 25 Most Common Plugin Results

Plugin	Total	Severity	Plugin Name
3929	28	High	Dropbear < 0.49 Hostkey Host Spoofing Vulnerability
3329	27	High	SSH Tectia Server < 5.0.1 Host Authentication Authorization Bypass
1994	26	High	OpenSSH < 3.7 buffer_append_space Function Overflow
1991	26	High	OpenSSH < 2.1.1 UseLogin Local Privilege Escalation
1989	26	High	OpenSSH < 3.2.1 AFS/ Kerberos Ticket/Token Passing Overflow
1974	25	High	SSH Multiple Vulnerabilities
1990	22	High	OpenSSH < 3.1 Channel Code Off by One Privilege Escalation
1996	21	High	Portable OpenSSH < 3.7.1p2 Multiple PAM Issues
1981	21	High	SSH-1 < 1.2.31 SSH Daemon Account Login Attempt Logging Failure
1987	19	High	OpenSSH < 3.4 Multiple Remote Overflows
1973	18	High	SSH Multiple Vulnerabilities
3648	17	High	WinSCP < 3.8.2 Arbitrary Command Insertion
4214	15	High	WinSCP < 4.0.4 URL Protocol Handler Arbitrary File Transfer
1995	15	High	LSH < 1.5 lshd Daemon Remote Overflow
1980	15	High	SSH1 CRC-32 detect_attack Function Overflow
3754	14	High	OpenBSD Portable OpenSSH < 4.4.p1 GSSAPI Authentication Overflow
3620	14	High	FortressSSH < 0.47 SSH_MSG_KEXINIT Logging Remote Overflow
1975	14	High	SSH Multiple Vulnerabilities
4209	13	High	OpenSSH < 4.7 Trusted X11 Cookie Connection Policy Bypass
4335	12	High	SSH Tectia Server < 5.2.4 / 5.3.6 Local Privilege Escalation

Plugin	Total	Severity	Plugin Name
2637	11	High	PuTTY < 0.57 SFTP Remote Buffer Overflow
1986	11	High	OpenSSH < 3.0.1 Multiple Issues
3751	10	High	OpenSSH < 4.4 Multiple GSSAPI Vulnerabilities
1993	3	High	Dropbear SSH Server Format String
6338	1	High	Dropbear SSH Server Channel Concurrency Use-after-free Remote Code Execution

Web Clients

Top 25 Most Common Plugin Results

Plugin	Total	Severity	Plugin Name
6322	28	High	Google Chrome < 17.0.963.56 Multiple Vulnerabilities
6097	28	High	Flash Player < 10.3.183.11 / 11.1.102.55 Multiple Vulnerabilities (APSB11-26)
6052	26	High	QuickTime < 7.7.1 Multiple Vulnerabilities
6327	25	High	Mozilla Thunderbird 10.x < 10.0.2 'png_decompress_chunk' Integer Overflow
6310	25	High	Mozilla SeaMonkey 2.x < 2.7.0 Multiple Vulnerabilities
6262	25	High	Google Chrome < 16.0.912.75 Multiple Vulnerabilities
6307	23	High	Mozilla Firefox 3.6.x < 3.6.26 Multiple Vulnerabilities
6054	20	High	Novell iPrint Client < 5.72 Code Execution Vulnerability
6329	18	High	Mozilla SeaMonkey 2.x < 2.7.2 'png_decompress_chunk' Integer Overflow
6053	18	High	Opera < 11.52 Multiple Vulnerabilities
6308	17	High	Mozilla Thunderbird 9.0 Multiple Vulnerabilities
6098	17	High	iTunes < 10.5.1 Update Authenticity Verification Weakness
6095	17	High	Google Chrome < 15.0.874.121 Code Execution Vulnerability
6315	15	High	Novell iPrint Client < 5.78 Multiple Code Execution Vulnerabilities
6328	13	High	Mozilla SeaMonkey 2.x < 2.7.1 Memory Corruption
6312	11	High	Google Chrome < 17.0.963.46 Multiple Vulnerabilities
6295	11	High	Opera < 11.61 Multiple Vulnerabilities
6311	10	High	Real Networks RealPlayer < 15.0.2.72 Multiple Vulnerabilities

Plugin	Total	Severity	Plugin Name
6309	9	High	Mozilla Thunderbird 3.1.x Multiple Vulnerabilities
6325	8	High	Mozilla Firefox 10.x < 10.0.2 'png_decompress_chunk' Integer Overflow
6326	6	High	Mozilla Thunderbird 10.x < 10.0.1 Memory Corruption
6324	6	High	Mozilla Firefox 10.x < 10.0.1 Memory Corruption
6094	6	High	Google Chrome < 15.0.874.120 Multiple Vulnerabilities
6050	5	High	Google Chrome < 15.0.874.102 Multiple Vulnerabilities
6306	4	High	Mozilla Firefox 9.0 Multiple Vulnerabilities

Web Servers

Top 25 Most Common Plugin Results

Plugin	Total	Severity	Plugin Name
6129	28	High	OpenSSL 0.9.8 < 0.9.8s / 1.x < 1.0.0f Multiple Vulnerabilities
5704	27	High	Adobe Flash Media server < 3.0.7 / 3.5.5 / 4.0.1 Multiple Vulnerabilities (APSB10-27)
5732	26	High	PHP 5.3 < 5.3.4 Multiple Vulnerabilities
5649	26	High	Linksys WAP default credentials
5574	26	High	CUPS < 1.4.4 Multiple Vulnerabilities
6332	25	High	Apache Tomcat 6.0.x < 6.0.35 Multiple Vulnerabilities
5824	25	High	PHP 5.3 < 5.3.6 String To Double Conversion DoS
5358	24	High	OpenSSL < 0.9.8m Multiple Vulnerabilities
5537	22	High	Drupal Services module < 6.x-2.1
5624	21	High	Adobe Flash Media server < 3.0.6 / 3.5.4 Multiple Vulnerabilities (APSB10-19)
5733	20	High	PHP 5.2.x < 5.2.15 Multiple Vulnerabilities
5615	19	High	Apache 2.2 < 2.2.16 Multiple Vulnerabilities
5583	19	High	EvoCam < 3.6.8 GET Request Buffer Overflow
5356	19	High	Apache < 2.2.15 Multiple Vulnerabilities
5932	16	High	IBM Tivoli Management Framework Endpoint '/addr' Remote Buffer Overflow
6302	15	High	Apache 2.2 < 2.2.22 Multiple Vulnerabilities
5616	13	High	PHP < 5.3.3 / 5.2.14 Multiple Vulnerabilities
6003	11	High	Adobe Flash Media Server Unsupported Version Detection
6304	10	High	PHP 5.3.9 php_register_variable_ex() Code Execution

Plugin	Total	Severity	Plugin Name
6002	9	High	Adobe Flash Media server < 3.5.7 / 4.0.3 Multiple Vulnerabilities (APSB11-20)
1442	9	Low	Web Server Detection
6062	8	High	Apache 2.2 < 2.2.21 mod_proxy_ajp DoS
5559	8	High	OpenSSL < 0.9.8o / 1.0.0a Multiple Vulnerabilities
3830	8	Low	Web Server Detection on Port Other Than TCP/80
6021	7	High	Apache 2.2 < 2.2.20 Multiple Vulnerabilities