This bulletin provides a summary of new or updated vulnerabilities, exploits, trends and viruses identified between July 21 and August 3, 2004.

Bugs, Holes, & Patches

The table below summarizes vulnerabilities that have been identified, even if they are not being exploited. Updates to items appearing in previous bulletins are listed in bold. Complete details about patches or workarounds are available from the source of the information or from the URL provided in the section. CVE numbers are listed where applicable.

Vulnerabilities that affect **both** Windows and Unix Operating Systems are included in the Multiple Operating Systems section.

Note: All the information included in the following tables has been discussed in newsgroups and on web sites.

Risk is defined as follows:

- **High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.
- **Medium** - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.
- **Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Windows Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
Layton Technology HelpBox 3.0.1	An input verification vulnerability exists that could allow an attacker to conduct SQL injection attacks. Various scripts fail to verify input passed to certain parameters properly before it is used in a SQL query. No solution is available at this time. A Proof of Concept exploit has been published.	Layton HelpBox Multiple SQL Injection Vulnerabilities	High	Secunia, SA12118, July 22, 2004 SecuriTeam, July 21, 2004

Microsoft
MS Windows NT Workstation 4.0 SP 6a;
MS Windows NT Server 4.0 SP 6a;
MS Windows NT Server 4.0 Terminal Server Edition SP 6;
MS Windows 2000 SP2, SP3, SP4;
MS Windows XP / XP SP1;
MS Windows XP 64-Bit Edition SP1;
MS Windows XP 64-Bit Edition Version 2003;
MS Windows Server 2003 / 2003 64-Bit Edition;
MS Windows 98, 98 SE, and Me
Internet Explorer 5.01 SP2, 3, 4
Internet Explorer 5.5 SP2
Internet Explorer 6, SP1, SP1 (64-Bit Edition), Windows Server 2003, Windows Server 2003 (64-Bit
	Cross-site scripting and remote code execution vulnerabilities exist. This security patch fixes three vulnerabilities:
	• A double-free vulnerability in the processing of GIF files
	• An integer overflow in the processing of bitmap files
	• Internet Explorer does not adequately validate the security context of a frame that has been redirected by a web server.
	An attacker can use malicious images on a web page or in HTML-formatted email messages. If the attacker can convince a user to visit the web page, open the message, or otherwise view the image, the attacker may be able to gain control of the user's machine. An attacker also may be able to take advantage of frames to redirect users to a malicious web site.
	Verify Windows is updated and download updates at:
	http://v4.windowsupdate.microsoft.com/en/default.asp
	We are not aware of any exploits for this vulnerability.
		Cumulative Security Update for Internet Explorer (867801)
		CVE Name:
		CAN-2004-0549
		CAN-2004-0566
		CAN-2003-1048
			High	Microsoft Security Bulletin MS04-025, July 30, 2004
				US-CERT Cyber Security Alert SA04-212A, July 30, 2004
				US-CERT VU#685364 and VU#266926, July 30, 2004

Edition)				
NetSupport DNA Helpdesk 1.01	An input verification vulnerability exists which could allow an attacker to conduct SQL injection attacks. The script "problist.asp" fails to verify input passed to the "where" parameter properly before it is used in a SQL query. No solution is available at this time. A working exploit has been published.	DNA HelpDesk SQL Injection Vulnerability	High	Secunia, SA12119, July 22, 2004
OllyDbg version 1.10	A Denial of Service vulnerability exists that could allow an attacker to crash OllyDbg and execute machine code. This vulnerability is due to a format string bug in the code that handles Debugger Messages. No solution is available at this time. A working exploit has been published.	OllyDbg Format String Bug	High	SecuriTeam, July 20, 2004
SapporoWorks BlackJumboDog FTP Server 3.6.1	A buffer overflow vulnerability exists in which a remote user can execute arbitrary code on the target system. A remote user can send a specially crafted FTP command with a long parameter string to trigger the flaw. The USER, PASS, RETR, CWD, XMKD, XRMD, and other commands are affected. The software reportedly copies the user-supplied parameter string to a 256 byte buffer. Update to version 3.6.2, available at: http://homepage2.nifty.com/spw/software/bjd/ We are not aware of any exploits for this vulnerability.	BlackJumboDog Has Buffer Overflow in the FTP Service	High	US-CERT VU#714584, August 3, 2004
Webcam Corp. Webcam Watchdog 4.0.1a	An input validation vulnerability exists that could allow an attacker to conduct cross-site scripting attacks. 'sresult.exe' does not properly filter HTML code from user-supplied input in the 'cam' variable before displaying the input. A remote user can access the target user's cookies (including authentication cookies), if any, associated with the site running the Watchdog software, access data recently submitted by the target user via web form to the site, or take actions on the site acting as the target user. No solution is available at this time. A Proof of Concept exploit has been published.	Webcam Watchdog Input Validation Hole in 'sresult.exe' Permits Cross-Site Scripting Attacks	High	SecurityTracker Alert ID: 1010824, July 30, 2004
Whisper Technology Limited FTP Surfer 1.0.7	A buffer overflow vulnerability exists due to a boundary error when handling filenames that could allow an attacker to execute arbitrary code. This can be exploited to cause a buffer overflow, which is triggered when the application is closed, by tricking a user into opening a file with an overly long filename from a malicious FTP server. No solution is available at this time. We are not aware of any exploits for this vulnerability.	FTP Surfer File Handling Buffer Overflow Vulnerability	High	Secunia, SA12107, July 27, 2004
XLineSoft ASPRunner 2.4 and prior	Multiple vulnerabilities exist in ASPRunner due to improper input validation. A remote user can inject SQL commands, conduct cross-site scripting attacks, and download the underlying database. Several scripts do not properly filter HTML code from user-supplied input before displaying the input. A remote user can create a specially crafted HTTP POST request that, when loaded by a target user, will cause arbitrary scripting code to be executed by the target user's browser. The code will originate from the site running the ASPRunner scripts and will run in the security context of that site. As a result, the code will be able to access the target user's cookies (including authentication cookies), if any, associated with the site, access data recently submitted by the target user via web form to the site, or take actions on the site acting as the target user. No solution is available at this time. A Proof of Concept exploit has been published.	ASPRunner Input Validation Holes Permit SQL Injection and Cross-Site Scripting Attacks	High	SecurityTracker Alert ID: 1010777, July 26, 2004 SecuriTeam, July 27, 2004
Innovative Technology Consulting FTP GLIDE 2.43	A vulnerability exists in the FTP GLIDE client software in which a local user can view passwords. FTP GLIDE client stores usernames and passwords in clear text. No solution is available at this time. No exploit code required.	FTP GLIDE Discloses Passwords to Local Users	Medium	SecurityTracker Alert ID: 1010776, July 26, 2004
Leigh Business Enterprises Ltd. LBE Web HelpDesk 4.0.80	An input verification vulnerability exists in the "jobedit.asp" script that an attacker could use to manipulate SQL queries. Update to version 4.0.0.81 available at: http://www.lbehelpdesk.com/helpdesk-latest.htm A working exploit has been published.	LBE Web HelpDesk SQL Injection	Medium	Secunia, SA12123, July 22, 2004 SecuriTeam, July 21, 2004
Microsoft Microsoft Systems Management Server (SMS) 2.50.2726.0	A Denial of Service vulnerability exists due to an error within the client SMS Remote Control service when processing specially crafted packets containing the string "RCH0####RCHE" followed by about 130 characters. Successful exploitation crashes the service. Restrict access to ports 2701/TCP and 2702/TCP. A working exploit has been published.	Microsoft Systems Management Server Remote Control Service Vulnerability	Medium	Secunia, SA11814, July 27, 2004
NET2SOFT Inc. Flash FTP Server 1.0 (banner version 2.1)	A vulnerability exists in the Flash FTP Server which could allow a remote user can view files on the target system that are located outside of the FTP root directory. A remote authenticated user, including an anonymous user, can generate a 'CWD ...' command followed by a 'CWD /' command to gain access to the root directory on the target system. No solution is available at this time.	Flash FTP Server Lets Remote Users Traverse the Directory With CWD Command	Medium	SecurityTracker Alert, 1010750, July 21, 2004

	A working exploit has been published.			
Opera Software Opera 7.53	A spoofing vulnerability exists that could be exploited by an attacker to conduct phishing attacks against a user. Opera fails to update the address bar if a web page is opened using the "window.open" function and then "replaced" using the "location.replace" function. This causes Opera to display the URL of the first website while loading the content of the second website. Workaround: Do not follow links from untrusted websites. A Proof of Concept exploit has been published.	Opera Browser Spoofing Vulnerability	Medium	Secunia, SA12162, July 27, 2004
Polar Polar HelpDesk 3.0	An authentication vulnerability exists because the system does not verify if a user is logged on. It only checks if a cookie with the appropriate "UserId" and "UserType" is set. An attacker could log on as any user with arbitrary privileges. Solution: Restrict access using a different authentication mechanism or upgrade to latest version. A working exploit has been published.	Polar HelpDesk Authentication Bypass and Inadequate Security Checks	Medium	Secunia, SA12120, July 22, 2004 SecuriTeam, July 21, 2004

[back to top]

UNIX Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
Citadel/UX Citadel/UX 6.23 and prior	Citadel/UX "USER" Command Buffer Overflow Vulnerability A buffer overflow vulnerability exists in Citadel/UX, which could allow a Denial of Service attack or remote code execution. The vulnerability is caused due to a boundary error within the citadel service when processing "USER" commands. This can be exploited to cause a stack-based buffer overflow by passing an overly long argument (about 94 bytes) to the "USER" command. A patch is available in the CVS repository available at: http://www.citadel.org/cvs.php A Proof of Concept exploit has been published.	Citadel/UX Remote Buffer Overflow Vulnerability	High	No System Group - Advisory #04 - July 28, 2004
Debian libapache-mod-ssl, courier (sqwebmail), mailreader	Multiple vulnerabilities including cross-site scripting exist in Linux modules. Debian has issued updates for libapache-mod-ssl, courier, and mailreader. This fixes Denial of Service and other vulnerabilities. Update to Debian GNU/Linux 3.0 alias woody. Details available at: http://lists.debian.org/debian-security-announce/debian-security-announce-2004/msg00134.html http://lists.debian.org/debian-security-announce/debian-security-announce-2004/msg00136.html http://lists.debian.org/debian-security-announce/debian-security-announce-2004/msg00135.html We are not aware of any exploits for this vulnerability.	Debian updates for libapache-mod-ssl , courier, and mailreader	High	Debian Security Advisories: DSA 532-1, DSA 533-1, DSA 534-1, July 22, 2004
GNU / GPL Conectiva Gentoo Mandrake RedHat SuSE Trustix Samba 3.0.0 - 3.0.4 and 2.2.9 and prior	Multiple buffer overflow vulnerabilities exist in Samba that could allow a remote user to execute arbitrary code on the target system. These are caused by boundary errors when decoding base64 data and when handling "mangling method = hash". Upgrade to version 3.0.5 or 2.2.10 available at: http://us2.samba.org/samba/ftp/ Conectiva: ftp://atualizacoes.conectiva.com.br RedHat: RedHat Enterprise Linux AS 3, ES 3, WS 3: http://rhn.redhat.com/ Gentoo: http://security.gentoo.org/glsa/glsa-200407-21.xml Mandrakesoft: Mandrake Multi Network Firewall 8.x, 9.x; Mandrake Corporate Server 2.x http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:071 SuSE: SuSE Linux, Email, Database, and Enterprise Servers http://www.suse.de/de/security/2004_22_samba.html Trustix: http://http.trustix.org/pub/trustix/updates/ A working exploit has been published.	Samba Buffer Overflow Vulnerabilities CVE Names: CAN-2004-0600 CAN-2004-0686	High	Samba Release Notes 3.0.5, July 20, 2004 Gentoo, RedHat, Mandrakesoft, SuSE, Trustix, Conectiva Advisories
Internet Software Sciences Web+Center 4.0.1	An input verification vulnerability exists that could allow an attacker to conduct SQL injection attacks. Various scripts fail to verify input passed to certain parameters through cookies properly, before it is used in a SQL query. No solution is available at this time. A working exploit has been published.	Web+Center SQL Injection Vulnerability	High	Secunia, SA12121, July 22, 2004 SecuriTeam, July 21, 2004

Oracle Oracle 8i, 9i Multiple Implementations	A privilege escalation vulnerability exists in the default library directory. This is due to a default configuration error that could allow an attacker to replace libraries required by setuid root applications with arbitrary code. This issue would allow an Oracle software owner to execute code as the superuser, taking control of the entire system. No solution is available at this time. An untested workaround is available at: http://www.securityfocus.com/bid/10829/solution/ A Proof of Concept exploit has been published.	Oracle Database Default Library Directory Privilege Escalation Vulnerability	High	Security Focus ID 10829, July 30, 2004
PHP Group **Debian** **Slackware** **Fedora** pp 4.3.7 and prior	Updates to fix multiple vulnerabilities with php4 which could allow remote code execution. **Debian:** **Update to Debian GNU/Linux 3.0 alias woody at http://www.debian.org/releases/stable/** **Slackware: http://www.slackware.com/security/viewer.php?l=slackware-security&y=2004&m=slackware-security.406480** **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/**	PHP 'memory_limit' and strip_tags() Remote Vulnerabilities CVE Name: CAN-2004-0594 CAN-2004-0595	High	Secunia, SA12113 and SA12116, July 21, 2004 Debian, Slackware, and Fedora Security Advisories
phpBB Group phpBB 2.0.9 and prior	Multiple vulnerabilities including cross-site scripting and full path disclosure exist due to improper input sanitization in the search.php, privmsg.php, and login.php scripts and uninitialized arrays. Upgrade to version 2.0.10 available at: http://www.phpbb.com/downloads.php A Proof of Concept exploit has been published.	phpBB Cross Site Scripting, Full Path, and XSS Vulnerabilities	High	Secunia, SA12114, July 22, 2004 SecuriTeam, July 22, 2004
SCO UnixWare 7.1.3 / Open UNIX 8.0.0:	A buffer overflow exists in ReadFontAlias from dirfile.c of Xsco that may allow local users and remote attackers to execute arbitrary code via a font alias file with a long token. There are also multiple vulnerabilities reading font files. Apply updated packages available at: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2004.2/erg712546.pkg.Z We are not aware of any exploits for this vulnerability.	UnixWare / Open UNIX Xsco Buffer Overflow Vulnerabilities CVE Name: CAN-2004-0083 CAN-2004-0106	High	SCO Security Advisory, SCOSA-2004.2, July 29, 2004
SCO SCO OpenServer 5.0.6 and 5.0.7	A buffer overflow exists in ReadFontAlias from dirfile.c of Xsco that may allow local users and remote attackers to execute arbitrary code via a font alias file with a long token. There are also multiple vulnerabilities reading font files. Apply updated packages available at: ftp://ftp.sco.com/pub/updates/OpenServer/SCOSA-2004.3/VOL.000.000 ftp://ftp.sco.com/pub/openserver5/507/mp/mp3/507mp3_vol.tar We are not aware of any exploits for this vulnerability.	OpenServer Xsco Buffer Overflow Vulnerabilities CVE Name: CAN-2004-0083 CAN-2004-0106	High	SCO Security Advisory, SCOSA-2004.3, July 29, 2004
Sourceforge.net Gentoo Linux Pavuk 0.x	Multiple vulnerabilities exist which could allow an attacker to run arbitrary code. The vulnerabilities are caused due to boundary errors within the handling of digest authentication. Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200407-19.xml We are not aware of any exploits for this vulnerability.	Pavuk Digest Authentication Buffer Overflow Vulnerabilities	High	Gentoo Security Advisory, GLSA 200407-19 / Pavuk Release Date July 26, 2004
sox.sourceforge.net Fedora Mandrakesoft Gentoo Conectiva RedHat SoX 12.17.4, 12.17.3, and 12.17.2	Multiple vulnerabilities exist that could allow a remote attacker to execute arbitrary code This is due to boundary errors within the "st_wavstartread()" function when processing ".WAV" file headers and can be exploited to cause stack-based buffer overflows. Successful exploitation requires that a user is tricked into playing a malicious ".WAV" file with a large value in a length field. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/ http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Mandrakesoft: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:076 Gentoo: http://security.gentoo.org/glsa/glsa-200407-23.xml Conectiva: ftp://atualizacoes.conectiva.com.br RedHat: http://rhn.redhat.com/errata/RHSA-2004-409.html A working exploit has been published.	SoX ".WAV" File Processing Buffer Overflow Vulnerabilities CVE Name: CAN-2004-0557	High	Secunia, SA12175, 12176, 12180, July 29, 2004 SecurityTracker Alerts 1010800 and 1010801, July 28/29, 2004 Mandrakesoft Security Advisory MDKSA-2004:076, July 28, 2004

SquirrelMail Project Team SquirrelMail 1.4.2	An input validation vulnerability was reported in SquirrelMail. A remote user may be able to execute SQL statements on the target system. The flaw resides in 'abook_database.php' where the $alias variable is not properly filtered. Update to version 1.4.3 RC1 and later versions, available at: http://www.squirrelmail.org/download.php We are not aware of any exploits for this vulnerability.	SquirrelMail Input Validation Flaw in 'abook_database.php' CVE Name: CAN-2004-0521	High	SecurityTracker Alert ID: 1010842, August 3, 2004
Team OpenFTPD OpenFTPD 0.30.2 prior to July 16, 2004, and prior versions	A vulnerability exists that could allow a remote attacker to execute arbitrary code on the target system. A remote authenticated user can send a specially crafted message to another FTP user to trigger a format string flaw and execute arbitrary code on the FTP server due to a flaw in 'misc/msg.c'. Update available at: http://www.openftpd.org:9673/openftpd/download_page.html A Proof of Concept exploit has been published.	OpenFTPD Format String Flaw Lets Remote Authenticated Users Execute Arbitrary Code	High	VSA0402 - openftpd - void.at security notice, July 31, 2004
Apple Computer Panther 10.3.4 - Internet Connect 1.3	A privilege and Denial of Service vulnerability exist which could allow a local user to can gain root privileges. An attacker could also render the machine unusable by corrupting important system files.The application creates a log file in an unsafe manner and a local user can create a symbolic link (symlink) from a critical file on the system to the temporary file. When Internet Connect is run the symlinked file will be written to with 'root' user privileges. Workaround: Ensure that the temporary file already exists (preventing the creation of a symlink) with the following commands: /usr/bin/touch /tmp/ppp.log echo '/usr/bin/touch /tmp/ppp.log' >> /etc/daily echo '/usr/bin/touch /tmp/ppp.log' >> /etc/rc.common Proof of Concepts have been published.	Apple 'Internet Connect.app' Uses and Unsafe Temporary File That Lets Local Users Gain Root Privileges	Medium	SecurityTracker Alert ID: 1010771, July 25, 2004 SecuriTeam, July 27, 2004
eSeSIX Computer GmbH Thintune OS 2.4.38	Multiple vulnerabilities exist that could allow a remote attacker to gain system access and local users to escalate their privileges. A process is listening on port 25702/TCP allowing an attacker to connect using a certain password. The process provides access to certain administrative functionality including a root shell. Certain usernames and passwords used for connecting to remote servers are stored incorrectly. It is possible to open a local root shell "lshell" on the client by pressing a certain keystroke combination and password. The Phoenix browser is executed as "root". Update to Thintune OS version 2.4.39. No exploit code required.	Thintune Client Multiple Vulnerabilities	Medium	Secunia, SA12154, July 26, 2004 SecuriTeam, July 25, 2004
Hewlett-Packard HP-UX B.11.23 HP-UX B.11.22 HP-UX B.11.11 HP-UX B.11.00	A vulnerability exists in HP-UX when running xfs and stmkfont. A a remote user can gain 'bin' group privileges. Updates to the following patches available at: http://itrc.hp.com PHSS_31181 - B.11.23 PHSS_31180 - B.11.22 PHSS_31179 - B.11.11 PHSS_31178 - B.11.00 We are not aware of any exploits for this vulnerability.	HP-UX Unspecified Flaw in Xfs and stmkfont May Grant Access to Remote Users	Medium	HP Security Bulletin, HPSBUX01061, July 21, 2004
Jamie Cameron **Mandrakesoft** Webmin 1.140 Usermin	A vulnerability exists in the account lockout mechanism due to insufficient validation of user supplied input and improper parsing of certain characters, which could let a remote attacker attempt to guess IDs and passwords continuously and prevent legitimate users from logging on. Usermin: http://www.webmin.com/udownload.html Webmin: http://prdownloads.sourceforge.net/webadmin/webmin-1.150.tar.gz **Mandrakesoft:** **http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:074** There is no exploit code required.	Webmin & Usermin Account Lockout Bypass CVE Name: CAN-2004-0582 CAN-2004-0583	Medium	US-CERT Cyber Security Bulletin SB04-173, July 23, 2004 **Mandrakesoft Security Advisory, MDKSA-2004:074, July 27, 2004**
Nessus prior to version 2.0.12	A vulnerability exists in the 'nessus-adduser' function which may allow a local user to gain elevated privileges. There is a race condition that can be exploited when the TMPDIR variable has not been specified. Update to version 2.0.12, available at: http://nessus.org/download.html We are not aware of any exploit for this vulnerability.	Nessus Race Condition in 'nessus-adduser' May Let Local Users Gain Elevated Privileges	Medium	SecurityTracker Alert ID: 1010758, July 22 2004
Polar HelpDesk 3.0	An authentication vulnerability exists because the the system does not verify if a user is logged on. It merely checks if a cookie with the appropriate "UserId" and "UserType" is set. This could allow an attacker to log on as any user with arbitrary privileges. No solution is available at this time. A working exploit has been published.	Polar HelpDesk Authentication Bypass	Medium	Secunia, SA12120, July 22, 2004

SERENA Software, Inc. Serena TeamTrack 6.1.1 and prior	Cross Site Scripting vulnerabilities exists due to improper input validation that an attacker could use to view sensitive information without authentication. Workaround: Restrict access using a different authentication mechanism such as ".htaccess" or similar. A working exploit has been published.	Serena TeamTrack Multiple Vulnerabilities	Medium	Secunia, SA12122, July 22, 2004
Opera **Gentoo** Opera 5.x, 6.x, 7.x	Due to a race condition in Opera it is possible to spoof the contents of the address bar using a specially crafted HTML page. Solution: Disable support for Javascript or update as follows: **Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200407-15.xml** A Proof of Concept exploit has been published.	Opera Address Bar Spoofing Condition	High	SecuriTeam, July 11, 2004 **Gentoo Linux Security Advisory, GLSA 200407-15 / opera, July 20, 2004**
PostgreSQL Global Development Group Mandrakesoft PostgreSQL	A buffer overflow vulnerability exists in the ODBC driver of PostgreSQL. It is possible to exploit this problem and crash the surrounding application. Mandrakesoft: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:072 We are not aware of any exploits for this vulnerability.	Updated postgresql Packages Fix Buffer Overflow	Low	Mandrakesoft Security Advisory, MDKSA-2004:072, July 27, 2004
Tigris.org Fedora Gentoo Subversion 1.0.5 and prior	A vulnerability exists in Subversion that could allow an attacker to read protected files. This is because the Apache module "mod_authz_svn" allows users to copy files from a read protected part of the repo into a part which the user can read. Update to version 1.0.6 available at: http://subversion.tigris.org/servlets/ProjectDocumentList?folderID=260 Fedora Core 2: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200407-20.xml We are not aware of any exploits for this vulnerability.	Subversion File Restriction Bypass	Low	Tigris.org Advisory: mod_authz_svn-copy-advisory.txt Gentoo and Fedora Security Advisories

[back to top]

Multiple Operating Systems - Windows / UNIX / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source

Check Point Software Technologies
Check Point VPN-1/FireWall-1 VSX NG;
Check Point VPN-1/FireWall-1 NG with Application Intelligence (AI);
Check Point VPN-1/Firewall-1 NG;
Check Point VPN-1 SecuRemote;
Check Point VPN-1 SecureClient;
Check Point SSL Network Extender;
Check Point Provider-1;
Check Point FireWall-1 GX 2.x
	A vulnerability exists in in various Check Point VPN-1 products, which an attacker can exploit to execute arbitrary code. The vulnerability is caused due to a boundary error in the ASN.1 decoding library during setup of the initial encrypted connection. This can be exploited to cause a heap overflow by establishing a VPN connection and sending a malicious packet containing specially crafted fields.
	Updates available at:
	http://www.checkpoint.com/techsupport/alerts/asn1.html
	We are not aware of any exploits for this vulnerability.
		Check Point VPN-1 ASN.1 Decoding Heap Overflow Vulnerability	High	Check Point ASN.1 Alert, July 28, 2004
				US-CERT VU#435358

Cisco Cisco ONS 15327, 15454, and 15454 SDH; prior to 4.6(2) Cisco ONS 15600	Multiple vulnerabilities exist on Cisco control cards that could allow a remote user to gain access to an account on the system or cause the cards to reset. Cisco reported that if an account on the system has a blank password, then a remote user can login to the device with an arbitrary password that is longer than 10 characters. This authentication vulnerability only affects the TL1 login interface. A Denial of Service vulnerability also exists. A remote user can send malformed SNMP, UDP, TCP, ICMP, or IP packets to potentially cause the XTC, TCC/TCC+/TCC2 and TCCi/TCC2 control cards to reset. A detailed patch matrix is available at: www.cisco.com/warp/public/707/cisco-sa-20040721-ons.shtml No exploit script required.	Cisco ONS Control Cards Malformed Packet Vulnerabilities	High	SecurityTracker, 1010748 and 1010749, July 21, 2004 Cisco Security Advisory: Document ID: 60322, Revision 1.0, July 21, 2004
Cisco ServletExec 3.x, 2.x Cisco Collaboration Server (CSS) 3.x, 4.x	A vulnerability exists in the ServletExec subcomponent that could allow an attacker to upload and execute arbitrary files.The vulnerability affects CCS (prior to 5.0) using a ServletExec version prior to 3.0E. Update instructions available at: http://www.cisco.com/warp/public/707/cisco-sa-20040630-CCS.shtml We are not aware of any exploits for this vulnerability.	Cisco Collaboration Server ServletExec Arbitrary File Upload Vulnerability	High	US-CERT VU#718896

Comersus Open Technologies Comersus Shopping Cart 5.098	Input validation vulnerabilities exist in Comersus that could allow an attacker to conduct SQL injection and cross-site scripting attacks. Comersus fails to verify input passed to the "email" parameter properly before it is used in a SQL query. Also, input passed to the "message" parameter in "comersus_message.asp" and "comersus_backoffice_message.asp" is not properly sanitized before being returned to the user. Workaround: Edit the source code to ensure that input is properly sanitized. We are not aware of any exploits for this vulnerability.	Comersus SQL Injection and Cross-Site Scripting Vulnerabilities	High	Secunia, SA12183, August 3, 2004
GNU 0.75-RC3 and 0.726PostNuke-3 with Xanthia module	Full path disclosure and cross site scripting vulnerabilities exists in PostNuke's Xanthia module due to an unvalidated input error and an error in the showcontent() function. No solution is available at this time. A Proof of Concept exploit is available.	PostNuke Multiple Vulnerabilities In Xanthia Module	High	Securiteam, July 27, 2004
GNU / GPL Nucleus prior to 3.0.1	An input validation vulnerability exists because the input used to include files isn't properly validated. This may allow an attacker to include arbitrary files from local and external resources if "register_globals" is set to "On" and gain system access. Upgrade to Nucleus 3.0.1 available at: http://nucleuscms.org/ A Proof of Concept exploit has been published.	Nucleus Inclusion of Arbitrary Files	High	SecurityTracker Alert, 1010746, July 21, 2004 Secunia, SA12097, July 20, 2004
GNU / GPL AntiBoard 0.7.2 and prior	Multiple vulnerabilities exist that could allow an attacker to conduct cross-site scripting and SQL injection attacks. The vulnerabilities are caused due to missing validation of various parameters in the "antiboard.php" script. No updates available. Edit the source code to ensure that user input is properly sanitized. We are not aware of any exploits for this vulnerability.	AntiBoard Cross-Site Scripting and SQL Injection Vulnerabilities	High	Secunia, SA12137, July 29, 2004 SecurityTracker Alert ID: 1010803, July 29, 2004
GNU / GPL BLOG:CMS prior to 3.1.4	An input validation vulnerability in BLOG:CMS exists because the input used to include files isn't properly validated. This may allow an attacker to include arbitrary files from local and external resources if "register_globals" is set to "On" and gain system access. Upgrade to BLOG:CMS 3.1.4 available at: http://forum.blogcms.com/viewtopic.php?id=324 A Proof of Concept exploit has been published.	BLOG:CMS Inclusion of Arbitrary Files	High	SecurityTracker Alert, 1010746, July 21, 2004 Secunia, SA12097, July 20, 2004
GNU / GPL PunBB prior to 1.1.5	An input validation vulnerability exists because the input used to include files isn't properly validated. This may allow an attacker to include arbitrary files from local and external resources if "register_globals" is set to "On" and gain system access. Upgrade to PunBB 1.1.5 available at: http://www.punbb.org/ A Proof of Concept exploit has been published.	PunBB Inclusion of Arbitrary Files	High	Secunia, SA12097, July 20, 2004
GNU / GPL Nucleus 3.01	An input verification vulnerability exists that could allow an attacker to conduct SQL injection attacks. Nucleus fails to verify input passed to the "itemid" parameter properly before it is used in SQL queries. No updates available. Edit the source code to ensure that input is properly sanitized. We are not aware of any exploits for this vulnerability.	Nucleus "itemid" SQL Injection Vulnerability	High	Secunia, SA12166, July 28, 2004
Hewlett-Packard dced	A buffer overflow vulnerability exists in HP's DCED implementation that listens by default on TCP port 135. Successful exploitation of this vulnerability may allow an attacker to execute arbitrary commands on the targeted system with the privileges of the DCED process which is typically run as the root user. Disable dced or update as follows: OS: HP HP-UX 11 update available at: http://itrc.hp.com OS: HP Tru64 update available at: http://support.entegrity.com/private/patches/dce/ssrt4741.asp OS: HP OpenVMS update available at: http://www2.itrc.hp.com/service/patch/mainPage.do We are not aware of any exploits for this vulnerability.	HP dced Remote Command Execution CVE Name: CAN-2004-0716	High	atstake.com, July 22, 2004 SecuriTeam, July 25, 2004 HP Bulletins: HPSBUX0311-299, HPSBUX0311-299: SSRT3660 DCE (Rev.01), SSRT4741 rev.0 DCE
Hitachi Web Page Generator 1.x, 2.x, 3.x, 4.x	Multiple vulnerabilities exist in Web Page Generator, which could allow an attacker to cause a Denial of Service, disclose content of directories, or conduct cross-site scripting attacks. These are due to an unspecified error which can stop the website service by accessing the website "improperly" multiple times (Windows platforms only) and errors in the error transactions of the Web Page Generator templates.	Hitachi Web Page Generator Multiple Vulnerabilities	High	Hitachi Vulnerability Notice HS04-002 and HS04-003, July 28, 2004

	Update to Web Page Generator Enterprise version 03-03-/D or 04-02-/L, and set the "DEBUG_MODE" property to "off". We are not aware of any exploits for this vulnerability.			
Invision Power Services Invision Power Board 2.0	Cross site scripting and input validation vulnerabilities exists because the URL (QUERY_STRING) is used in "index.php" and isn't properly sanitized 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 a vulnerable site. No updates available. Edit the source code to ensure that input is properly sanitized. We are not aware of any exploits for this vulnerability.	Invision Power Board "index.php" Cross Site Scripting Vulnerability	High	Secunia, SA12105, July 20, 2004
l2tpd.org Debian **Gentoo** l2tpd 0.62 0.69	A buffer overflow vulnerability exists in the 'write_packet()' function due to a failure of the application to properly validate user supplied string lengths, which could let a remote malicious user cause a Denial of Service and potentially execute arbitrary code. **Debian:** **http://www.debian.org/security/2004/dsa-530** **Gentoo:** **http://www.gentoo.org/security/en/glsa/glsa-200407-17.xml** We are not aware of any exploits for this vulnerability.	L2TPD Buffer Overflow	High	Gentoo Linux Security Advisory, GLSA 200407-17 / net-dialup/l2tpd, July, 22, 2004
Mateo & Mewis AG EasyIns Stadtportal 4 and prior	A vulnerability was reported in EasyIns Stadtportal. A remote user can supply a URL with a specially crafted 'site' parameter to cause the target system to include and execute PHP code from a remote site. No solution is available at this time. A working exploit has been published.	EasyIns Stadtportal Include File Bug Lets Remote Users Execute Arbitrary Code	High	SecurityTracker Alert ID: 1010769, July 24, 2004
Matt Johnston Dropbear SSH Server 0.42	A vulnerability exists that could allow a remote attacker to execute arbitrary code. This vulnerability is caused due to freeing of uninitialized variables in the DSS verification code. Update to version 0.43 available at: http://matt.ucc.asn.au/dropbear/ We are not aware of any exploits for this vulnerability.	Dropbear SSH Server DSS Verification Vulnerability	High	Secunia, SA12153, July 26, 2004 Dropbear Security Update
mod SSL Project Gentoo Slackware Mandrake mod_ssl 2.x	A vulnerability exists in mod_ssl, which may allow an attacker to compromise a vulnerable system. The vulnerability is reportedly due to a "ssl_log()" related format string error within the "mod_proxy" hook functions. Update to version 2.8.19-1.3.31 available at: http://www.modssl.org/source/mod_ssl-2.8.19-1.3.31.tar.gz OpenPKG: ftp://ftp.openpkg.org/release/1.3/UPD/apache-1.3.28-1.3.6.src.rpm **Gentoo:** http://www.gentoo.org/security/en/glsa/glsa-200407-18.xml **Slackware: http://www.slackware.com/security/viewer.php?l=slackware-security&y=2004&m=slackware-security.419544** **Mandrakesoft:** **http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:075** We are not aware of any exploits for this vulnerability.	mod_proxy" Hook Functions Format String Vulnerability in mod_ssl	High	modSSL Notice, July 16, 2004 Secunia, SA12077, July 19, 2004 **Gentoo, Mandrakesoft and Slackware Security Advisories**
Mozilla Organization Mozilla 1.6 and prior Netscape 7.0, 7.1, and prior	A input validation vulnerability exists in the SOAPParameter object constructor in Netscape and Mozilla which allows execution of arbitrary code. The SOAPParameter object's constructor contains an integer overflow which allows controllable heap corruption. A web page can be constructed to leverage this into remote execution of arbitrary code. Upgrade to Mozilla 1.7.1 available at: http://www.mozilla.org/products/mozilla1.x/ We are not aware of any exploits for this vulnerability.	Netscape/Mozilla SOAPParameter Constructor Integer Overflow Vulnerability CVE Name: CAN-2004-0722	High	iDEFENSE Security Advisory, August 2, 2004 Bugzilla Bug 236618
MyServer.org MyServer 0.6.2	Multiple vulnerabilities exist in the math_sum.mscgi sample script. A remote user may be able to conduct arbitrary code or conduct cross-site scripting attacks. This is because the 'a' and 'b' parameters are not filtered to remove HTML code from user-supplied input before the input is displayed. A remote user can access the target user's cookies (including authentication cookies), if any, associated with the site running the MyServer software, access data recently submitted by the target user via web form to the site, or take actions on the site acting as the target user. Workaround: Remove the math_sum.mscgi sample script. A working exploit is available.	MyServer Bugs in math_sum.mscgi May Let Remote Users Execute Arbitrary Code and Conduct Cross-Site Scripting Attacks	High	SecurityTracker Alert ID: 1010808, July 29, 2004

powerportal.sourceforge.net PowerPortal 1.3	A cross-site scripting vulnerability exists in the private_messages module that could allow a remote user to execute arbitrary code. T the private_messages module does not properly filter HTML code from user-supplied input in the message title field. Cookies and passwords are also vulnerable as they are stored in clear text. No solution is available at this time. A Proof of Concept exploit has been published.	PowerPortal Input Validation Hole in Private Message Title Permits Cross-Site Scripting Attacks	High	SecurityTracker Alert ID: 1010802, July 29, 2004
Sourceforge.net Jaws 0.4	An input validation vulnerability exists which could allow an attacker to can gain administrative access to the application. This is because 'config.php' disables magic quotes and 'controlpanel.php' contains an input validation error, allowing a remote user to inject SQL commands via the "crypted_password" variable. Replace the 'gadgets/controlpanel.php' file with this file: http://jaws.com.mx/files/controlpanel.php.txt A working exploit has been published.	Jaws 'controlpanel.php' Input Validation Error	High	SecurityTracker Alert ID: 1010815, July 30, 2004
U.S. Robotics Wireless Router Model 8054	A Denial of Service vulnerability exists in U.S. Robotics wireless router (model 8054). A remote user can cause the router to crash and may be able to execute arbitrary code on the router by connecting to the router's web administration port and issuing a specially crafted HTTP GET request to trigger an overflow and cause the device to crash. No solution is available at this time. A Proof of Concept exploit has been published.	U.S. Robotics Wireless Router Can Be Crashed By Remote Users	High	SecurityTracker Alert ID: 1010839, August 2, 2004
4D Portal 1.5	A configuration vulnerability exists that could allow a remote attacker to gain access to the system if the default password has not been changed. Solution: Change the "super-user" default username and password. No exploit script required.	4D Portal Default Password May Let Remote Users Access the System	Medium	SecurityTracker Alert, 1010747, July 21, 2004
artmedic webdesign artmedic kleinanzeigen	An input verification vulnerability exists in artmedic kleinanzeigen because the "id" parameter isn't properly verified in "index.php" before it is used to include a file. This could allow an attacker to supply arbitrary paths to local and external resources. Upgrade to the latest release available at: http://www.artmedic.de/index.php A working exploit has been published.	artmedic kleinanzeigen Inclusion of Arbitrary Files	Medium	Secunia, SA12099, July 21, 2004
Dom Lachowicz Fedora AbiWord 2.0.7 and prior	A vulnerability exists in the "wv" library of AbiWord, which could be exploited by an attacker to compromise a user's system. Update to version 2.0.8 or later available at: http://www.abisource.com/download/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/ http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ We are not aware of any exploits for this vulnerability.	AbiWord "wv" Library Buffer Overflow Vulnerability	Medium	AbiWord 2.0.7-2.0.9 Changes Secunia, SA12136 and SA12146, July 26, 2004
EasyWeb FileManager 1.0 RC-1 for PostNuke	An input validation vulnerability exists that could allow an attacker to retrieve arbitrary files. An input validation error in the "ew_filemanager" module can be exploited to access directories outside the web root via the "../" directory traversal character sequence using the "pathext" parameter. No solution is available at this time. A Proof of Concept exploit has been published.	EasyWeb FileManager "pathext" Directory Traversal	Medium	cirt.net, CIRT-200404: EasyWeb (EW) FileManager Directory Traversal, July 23, 2004
Fusion News 3.6.1 and prior	A vulnerability exists that could allow a remote attacker to create a specially crafted URL that, when loaded by a target administrator, will cause a user account to be added to Fusion News. The malicious URL can be placed in a BBCode image tag within a comment and then executed when the target administrator views the comment, for example. No solution is available at this time. A Proof of Concept exploit has been published.	Fusion News Lets Remote Users Add User Accounts on the Application	Medium	SecurityTracker Alert ID: 1010829, July 31, 2004
GNU PostNuke 0.73x - 0.75 GOLD	An installation vulnerability exists that could allow a remote user to determine the administrator's username and password on affected sites. PostNuke does not remove the 'install.php' file after installation. A remote user can request the file and accept the terms to view the password information. Workaround: Rename or delete the 'install.php' file. A Proof of Concept exploit has been published.	PostNuke 'install.php' Discloses Administrator Password to Remote Users	Medium	SecurityTracker Alert ID: 1010755, July 22, 2004
Hewlett-Packard HP-UX B.11.00, B.11.11, B.11.22, and B.11.23 with CIFS Server A.01.11.01	A buffer overflow vulnerability exists which could be exploited by an attacker to gain root access. Set "mangling method = hash2" or "mangled names = no" in the "smb.conf" configuration file. We are not aware of any exploits for this vulnerability.	HP-UX CIFS Server Buffer Overflow Vulnerability CVE Name: CAN-2004-0686	Medium	Secunia, SA12168, July 28, 2004 HP SECURITY BULLETIN,

installed				HPSBUX01062, July 26, 2004
IBM IBM Directory Server 4.1 and prior	An input verification vulnerability exists in the IBM Directory Server in 'ldacgi.exe'. A remote user can view files on the target system with the privileges of the web service. The script does not properly validate user-supplied input in the 'Template' parameter. A remote user can supply a path containing directory traversal characters ('../') to view arbitrary files on the target system. Update to 3.2.2 Fix Pack 4 available at: http://www-1.ibm.com/support/docview.wss?rs=0&uid=swg24006917 or 4.1 Fix Pack 3 available at: http://www-1.ibm.com/support/docview.wss?rs=0&q1=directory+server&uid=swg24006667&loc=en_US&cs=utf-8&cc=us〈=en A Proof of Concept exploit has been published.	IBM Directory Server 'ldacgi' Discloses Files to Remote Users	Medium	SecurityTracker Alert ID: 1010834, August 2, 2004 IBM APAR IR52692 and IR 53631
Mozilla Organization Mozilla Firefox 0.9.2 and Mozilla 1.7.1 on Windows Mozilla Firefox 0.9.2 on Linux	A spoofing vulnerability exists that could allow malicious sites to abuse SSL certificates of other sites. An attacker could make the browser load a valid certificate from a trusted website by using a specially crafted "onunload" event. The problem is that Mozilla loads the certificate from a trusted website and shows the "secure padlock" while actually displaying the content of the malicious website. The URL shown in the address bar correctly reads that of the malicious website. An additional cause has been noted due to Mozilla not restricting websites from including arbitrary, remote XUL (XML User Interface Language) files. Workaround: Do not follow links from untrusted websites and verify the correct URL in the address bar with the one in the SSL certificate. A Proof of Concept exploit has been published.	Mozilla / Mozilla Firefox "onunload" SSL Certificate Spoofing	Medium	Cipher.org, July 25, 2004 Secunia, SA12160, July 26, 2004; SA12180, July 30, 2004
Open Source Development Network OpenDocMan 1.x	An authentication vulnerability exists which can be exploited by an attacker to bypass certain security restrictions and make unauthorized changes. The vulnerability is caused due to a missing authentication check in "commitchange.php" when committing changes. Update to version 1.2-Final available at: http://prdownloads.sourceforge.net/opendocman/opendocman-1.2.tar.gz?download No exploit code required.	OpenDocMan "commitchange.php" Unauthorized Commitment of Changes	Medium	Secunia, SA12159, July 26, 2004 OpenDocMan 1.2 Final Release Notes
QualiTeam Litecommerce 2.0.0	A configuration vulnerability exists in Litecommerce. A remote user can invoke the installation script to gain administrative access on some sites. By default, the software leaves the 'install.php' installation file on the server after installation. A remote user can load the file to change the administrative password. On some systems, this requires authentication but on other systems, authentication is not required. Workaround: Remove the 'install.php' script manually after installation. A working exploit is available.	Litecommerce Installation Script May Let Remote Users Gain Administrative Access	Medium	SecurityTracker Alert ID: 1010778, July 26, 2004
Sun Microsystems Sun Java System Portal Server 6.2	An authentication vulnerability exists which may allow an attacker to gain administrative credentials. The problem arises if the user changes the display options to a non-default view. This only affects the Calendar server. As a workaround, Sun indicates that you can prohibit end users from editing the calendar channels "calendar" or "view" display profile properties when Admin Proxy Authentication is enabled. SPARC updates: http://sunsolve.sun.com/pub-cgi/findPatch.pl?patchId=116856&rev=10 X86 Platform updates: http://sunsolve.sun.com/pub-cgi/findPatch.pl?patchId=117757&rev=09 We are not aware of any exploits for this vulnerability.	Sun Java System Portal Server Proxy Authentication Failure	Medium	Sun Alert ID: 57586, July 21, 2004 US-CERT Vulnerability Note VU#881254 , July 23, 2004
Sun Microsystems SDK and JRE 1.4.2_04 or earlier; 1.4.1_07 or earlier; 1.4.0_04 or earlier	A vulnerability exists in Sun Java JRE/SDK that could allow an attacker to gain escalated privileges on a vulnerable system. The vulnerability is caused due to an error within the XSLT processor. This allows applets to read data from other applets being processed or gain escalated privileges. Update to version 1.4.2_05 or later available at: http://java.sun.com/j2se/ We are not aware of any exploits for this vulnerability.	Sun Java JRE/SDK XSLT Processor Vulnerability	Medium	Sun Alert ID: 57613, August 2, 2004
Conceptronic CADSLR1 Router with firmware version 3.04n	A Denial of Service vulnerability exists in the router because the device fails to handle HTTP requests with a long username (65535 characters). This causes the device to reboot. Solution: Filter access to the device or disable the HTTP service. We are not aware of any exploits for this vulnerability.	Conceptronic CADSLR1 Router Denial of Service Vulnerability	Low	Secunia, SA12110, July 21, 2004

phpMyFAQ Team phpMyFAQ 1.4.0	A user validation vulnerability exists in phpMyFaq, which could allow an attacker to upload or delete arbitrary images. The security issue is caused due to a missing user authentication check in the ImageManager plugin, which allows anyone to access the plugin's functionality. Update to version 1.4.0a available at: http://www.phpmyfaq.de/download.php We are not aware of any exploits for this vulnerability.	phpMyFaq ImageManager Plugin Missing User Authentication	Low	phpMyFAQ Security Advisory, July 27, 2004
Sun Microsystems Solaris 9	A Denial of Service vulnerability exists in the Sun Solaris Volume Manager (SVM) that could allow a local user to cause a denial-of-service condition. There is a vulnerability in the way the Sun Volume Manager handles certain types of probe requests. By supplying an incorrectly formed probe request, a local user could cause a denial-of-service condition on a Solaris 9 system with this service configured. Update available at: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/57598 We are not aware of any exploits for this vulnerability.	Sun Solaris Volume Manager (SVM) fails to properly handle malformed probe requests	Low	US-CERT Vulnerability Note VU#390742 Sun Alert ID: 57598, July 16, 2004
Sun Sun Java System Web Server (Sun ONE/iPlanet) 6.x	A Cross-Site Scripting vulnerability exists in the the sample application "webapps-simple". Sample scripts should not be installed on production systems. Update to Sun Java System Web Server 6.1 Service Pack 2 and later. We are not aware of any exploits for this vulnerability.	Sun Java System Web Server Cross Site Scripting Vulnerability	Low	Sun Alert ID: 57605, July 21, 2004
WWW File Share Pro 2.60	A Denial of Service vulnerability exists due to an unspecified error during the handling of HTTP GET requests. This can be exploited to crash the process by sending an overly long request. Solution: Filter requests using a firewall or proxy server. A working exploit has been published.	WWW File Share Pro HTTP Request Denial of Service Vulnerability	Low	Secunia, SA12111, July 21, 2004

[back to top]

Recent Exploit Scripts/Techniques

The table below contains a sample of exploit scripts and "how to" guides identified during this period.

Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script name	Script Description
July 31, 2004	fusionphp.net	A specially crafted URL that, when loaded by a target administrator, will cause a user account to be added. The malicious URL can be placed in a BBCode image tag within a comment and then executed when the target administrator views the comment.
July 30, 2004	controlpanel.php	An SQL injection vulnerability allowing a remote user administrative access.
July 29, 2004	antiboard072txt	SQL Injection and cross site scripting vulnerabilities exist in AntiBoard versions 0.7.2 and below due to a lack of input validation of various variables.
July 29, 2004	citadel-advisory-04.txt	Citadel/UX versions 6.23 and below are vulnerable to a buffer overflow that occurs when more than 97 bytes are sent with the USER directive to port 504.
July 29, 2004	IRM-009.txt	IRM Security Advisory 009 - RiSearch version 1.0.01 and RiSearch Pro 3.2.06 are susceptible to open FTP/HTTP proxying, directory listings, and file disclosure vulnerabilities.
July 28,2004	bitlanceOpera.txt	A vulnerability in the Opera 7.x series allows phishing attacks due to not updating the address bar if a web page is opened using the window.open function and then replaced using the location.replace function.
July 27, 2004	taskShed.C	Microsoft Windows 2K/XP Task Scheduler local exploit that will spawn notepad.exe.
July 27, 2004	nucleusCMSSQL.txt	Nucleus CMS version 3.01 addcoment/itemid SQL Injection Proof of Concept PHP exploit that dumps the username and md5 hash of the password for the administrator user.
July 26, 2004	eSeSix.txt	eSeSIX Thintune with a firmware equal to or below 2.4.38 is susceptible to multiple vulnerabilities. These include having a backdoored service on a high port with an embedded password giving a remote root shell, various other passwords being stored locally in clear text, and a local root shell vulnerability.
July 26, 2004	ew_file_manager.txt	The EasyWeb FileManager Module for PostNuke is vulnerable to a directory traversal problem which allows retrieval of arbitrary files from the remote system. Versions affected: EasyWeb FileManager 1.0 RC-1.
July 26, 2004	Mozilla_Firefox_25-07-2004.txt	Mozilla FireFox versions 0.9.1 and 0.9.2 has a flaw where it is possible to make a browser load a valid certificate from a trusted website by using a specially crafted onunload event
July 25, 2004	applePanther.txt	Apple OSX Panther 10.3.4 with Internet Connect version 1.3 by default appends to ppp.log in /tmp if the file already exists. If a symbolic link is made to any file on the system, it automatically writes to it as root allowing for an easy local compromise. Detailed exploitation given.
July 24, 2004	wgetusr.c	Exploit that makes use of the mod_userdir vulnerability in various Apache 1.3 and 2.x servers.

July 24, 2004	sambaPoC.txt	Proof of concept exploit code for the Samba 3.x swat preauthentication buffer overflow vulnerability.
July 24, 2004	httpdDoS.pl	Denial of service test exploit for the flaw in Apache httpd 2.0.49.
July 23, 2004	OpteronMicrocode.txt	This document details the procedure for performing microcode updates on the AMD K8 processors. It also gives background information on the K8 microcode design and provides information on altering the microcode and loading the altered update for those who are interested in microcode hacking. Source code is included for a simple Linux microcode update driver for those who want to update their K8's microcode without waiting for the motherboard vendor to add it to the BIOS. The latest microcode update blocks are included in the driver.
July 23, 2004	FlashFTPtraverse.txt	Flash FTP Server version 1.0 (and possibly 2.1) for Windows is susceptible to a directory traversal attack.
July 20, 2004	unrealdecloak.tar.gz	Unreal Decloak Toolkit version 0.1 illustrates the weak hashing system vulnerability in Unreal ircd 3.2 and previous versions.

[back to top]

Trends

Six months since the W32/MyDoom mass-mailing virus first appeared on the Internet, US-CERT continues to see new variants appearing and many variants (new and old) continuing to spread. Many variants of W32/MyDoom are known to open a backdoor and use its own SMTP engine to spread through email. US-CERT strongly encourages users to install and maintain anti-virus software and exercise caution when handling attachments. Anti-virus software may not be able to scan password protected archive files so users must use discretion when opening archive files and should scan files once extracted from an archive. See US-CERT Cyber Security Alert SA04-208A.

Microsoft has reported two vulnerabilities in the way Internet Explorer processes certain types of images. Attackers may be able to gain control of your machine if you view a malicious image, visit a web page, or open an email message that contains these images. Microsoft has also published an update to address the cross-domain vulnerability discussed in SA04-163A. This vulnerability may allow an attacker to alter a web site to point to a different location. If the attacker can convince you to visit the site, they may be able to gain control of your machine. See US-CERT Cyber Security Alert SA04-212A.

[back to top]

Viruses/Trojans

New Viruses / Trojans

Viruses or Trojans Considered to be a High Level of Threat

- **MyDoom.M / MyDoom.N**: New variants of the MyDoom worm surfaced and produced a tremendous amount of e-mail traffic as well as drastically slowing access to major search engines. After a PC is infected, the virus searches for e-mail addresses on the hard drive, and then it looks for more by running queries on search engines.

The following table provides, in alphabetical order, a list of new viruses, variations of previously encountered viruses, and Trojans that have been discovered during the period covered by this bulletin. This information has been compiled from the following anti-virus vendors and security related web sites: Sophos, Trend Micro, Symantec, McAfee, Network Associates, Central Command, F-Secure, Kaspersky Labs, MessageLabs, and The WildList Organization International. Users should keep anti-virus software up to date and should contact their anti-virus vendors to obtain specific information on the Trojans and Trojan variants that anti-virus software detects.

NOTE: At times, viruses and Trojans may contain names or content that may be considered offensive.

Name	Aliases	Type
Backdoor.Agent.B	BackDoor-CFB TROJ_AGENT.AC Troj/Agent-AC Agent.E Backdoor.Agent.ac	Trojan: Backdoor
Backdoor.Berbew.I	Berbew.I TrojanSpy.Win32.Qukart.gen W32/Berbew.G	Trojan: Backdoor
Backdoor.Moonlit		Trojan: Backdoor
Backdoor.Xordoor		Trojan: Backdoor
Backdoor.Zincite.A		Trojan: Backdoor
BackDoor-CHI		Trojan: Backdoor
Downloader-MY		Trojan: Downloader
Downloader-NE.dr		Trojan: Downloader
Downloader-NK		Trojan: Downloader
HTML.Phishbank.AI	HTML/Phishbank.AI.Worm	E-mail Scam

Kol.D	BackDoor-CGP Backdoor.Delf.nm Keylogger.Trojan Win32.Kol.D Win32/Kol.D.1.Trojan	Trojan - Keylogging
Lovgate.AT	W32/Lovgate.AT.worm	Win32 Worm
Mabutu.B	W32/Mabutu.B.worm W32/Mabutu.b@MM	Win32 Worm
MultiDropper-LA	Neblso Neblso.A W32/MultiDropper-LA	Trojan: Dropper
Mydoom.M	I-Worm.Mydoom.M I-Worm.Mydoom.R MyDoom.M Mydoom.M@MM Mydoom.O W32.Mydoom.M@mm W32/Mydoom-O W32/Mydoom.L W32/Mydoom.M.worm W32/Mydoom.N.worm W32/Mydoom.o@MM Win32.Mydoom.O Win32/MyDoom.O.Worm WORM_MYDOOM.M ZIP.Mydoom.O	Win32 Worm
Mydoom.N	I-Worm.Mydoom.n W32.Mydoom.N@mm W32/Mydoom.p@MM WORM_MYDOOM.N	Win32 Worm
Mydoom.P	Win32.Mydoom.P Win32/Mydoom.P.Worm	Win32 Worm
OF97/Toraja-I	O97M.Toraja.Gen X97M/Toraja O97M_TORAJA.I	MS Word Virus
Protoride.I	W32.Protoride.Worm W32/Protoride.J Win32.Protoride.I Win32/Protoride.G Win32/Protoride.I.Worm Worm.Win32.Protoride.j	Win32 Worm
PWSteal.Ldpinch.B	Backdoor-CEX Ldpinch.W Multidropper-KN	Trojan
Rbot.H	Backdoor.SdBot.jg Backdoor/SDBot W32.Randex.gen W32/Sdbot.worm.gen.i Win32.Rbot.H	Win32 Worm
Secdrop.A	Trojan.Win32.Small.q Win32.Secdrop.A Win32/LowSec.Trojan	Trojan
Troj/CmjSpy-Z		Trojan: Keylogging
Troj/Delf-DU	New Malware.b	Trojan
Troj/Dluca-CQ	TrojanDownloader.Win32.Dyfuca.cq	Trojan: Adware
Troj/PatchLs-A	Trojan.Win32.PatchLs.a Win32/PatchLs.A	Trojan
Troj/Psyme-AI	TrojanDownloader.VBS.Iwill.v JS/Exploit-InjScript JS/SillyDownloader.C Exploit.HTML.InjScript	Trojan
Troj/Small-AO		Trojan: Backdoor
Trojan.Download.Inor.C		Trojan: Downloader
Trojan.Exruntel		Trojan
W32.Beagle.AH@mm		Win32 Worm
W32.Bugbros.C@mm	Bloodhound.W32.VBWORM I-Worm.generic W32/Generic.a@MM	Win32 Worm
W32.Gaobot.BAJ		Win32 Worm
W32.Korgo.AD	W32/Korgo.worm.gen	Win32 Worm
W32.Mits.A@mm	Mits.A Trojan.Win32.Smith	Trojan
W32.Rotor		Win32 Worm

W32/Agobot-LL	Gaobot Nortonbot Phatbot Polybot Backdoor.Agobot.gen	Win32 Worm
W32/Agobot-LM		Win32 Worm
W32/Atak-C	Atak-C I-Worm.Agist.a	Win32 Worm
W32/Bagle.aj!proxy	Trojan.Mitglieder.M	Win32 Proxy Virus
W32/Bagle.ak!proxy		Win32 Proxy Virus
W32/Mydoom.o@MM!zip		Win32 Worm
W32/Rbot-EK	Backdoor.Rbot.gen W32/Sdbot.worm.gen.h	Win32 Worm
W32/Rbot-EP	Backdoor.Rbot.gen W32/Sdbot.worm.gen	Win32 Worm
W32/Rbot-EQ		Win32 Worm
W32/Rbot-ET	Backdoor.Rbot.gen	Win32 Worm
W32/Rbot-EW	Backdoor.Rbot.gen	Win32 Worm
W32/Rbot-FC	Backdoor.Rbot.gen	Win32 Worm
W32/Scaner-A	Exploit-DcomRpc.gen Win32.Agent.Z Win32.Dcom.db	Win32 Worm
W32/Sdbot-KM		Trojan: Backdoor
W32/Sdbot-KU	W32/Sdbot.worm.gen Backdoor.SdBot.np BKDR_SDBOT.GEN	Win32 Worm
W32/Spybot-CZ	W32.Spybot.worm.gen.a Backdoor.Spyboter.gen	Win32 Worm
W32/Stewon-A	Worm.P2P.Stewon	Win32 Worm
W32/Tompai-A		Win32 Worm
W97M.Diperis.A	W97M/Diperis.A Word97Macro/Diperis.A	MS Word Virus
W97M.Kuna		MS Word Virus
W97M.Seliuq.D	Macro.Word97.Seliuq.c W97M/Assilem.g.gen W97M_SELIUQ.C WM97/Seliuq-A	MS Word Virus
Win32.Dluca.H	Downloader-DC TrojanDownloader.Win32.Dluca.y Win32/Dluca.H.Trojan	Win32 Worm
Win32.Glieder	Troj/Dload-AO Trojan.Mitglieder.M TrojanClicker.Win32.Small.ak TrojanClicker.Win32.Small.al W32/Bagle.am!proxy W32/Bagle.dll.gen Win32.Glieder Win32.Glieder.C Win32/Glieder.DLL.Trojan	
Win32.Rbot.H	Backdoor.SdBot.jg Backdoor/SDBot W32.Randex.gen W32/Sdbot.worm.gen.i	Win32 Worm
WinCE/Duts.1520.dr	WinCE/Duts.1536.dr	WinCE Virus
WORM_KORGO.AC	Korgo.AC	Win32 Worm
Zindos.A	W32.Zindos.A W32/Zindos-A W32/Zindos.A W32/Zindos.A.worm W32/Zindos.worm Win32.Zindos.A Win32/Zindos.A.Trojan Win32/Zindos.A.worm Worm.Win32.Zindos.A WORM_ZINDOS.A Zindos	Win32 Worm

[back to top]