National Infrastructure Protection Center CyberNotes

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 5905, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between June 27 and July 11, 2002. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
AnalogX[1]	Multiple	Proxy 4.0, 4.0.1-4.0 7	Multiple vulnerabilities exist: a buffer overflow vulnerability exists when malformed SOCKS4A requests are handled, which could let a remote malicious user execute arbitrary code and a buffer overflow vulnerability exists when malformed HTTP proxy requests are handled, which could let a malicious user potentially execute arbitrary instructions.	No workaround or patch available at time of publishing.	Proxy Socks4A Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

---

[1] Foundstone Security Advisory, FS-070102-23-AXPR, July 1, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Apache Software Foundation[2]	Multiple	Tomcat 4.0.3	Several Cross-Site Scripting vulnerabilities exist: a Cross-Site Scripting vulnerability exists when a request is made for a DOS device file name, which could let a malicious user cause a Denial of Service; and a Cross-Site Scripting vulnerability exists when using the /servlet/ mapping to invoke various servlets/classes, which could let a malicious user cause a Denial of Service.	Upgrading to v4.1.3 beta resolves the DOS device vulnerability. No workaround or patch available at time of publishing for the servlet mapping vulnerability.	Tomcat Multiple Cross-Site Scripting	Low	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.
Apple[3]	MacOS X 10.1x	MacOS X 10.1x	A vulnerability exists in SoftwareUpdate because no authentication is required for updates, which could let a malicious user compromise root.	No workaround or patch available at time of publishing.	MacOS X Software Update Arbitrary Package Installation	High	Bug discussed in newsgroups and websites. Exploit script has been published. Vulnerability has appeared in the press and other public media.
Apple[4]	MacOS X 10.x	MacOS X 10.0-10.0.4, 10.1-10.1.5, MacOS X Server 1.0	A vulnerability exists in the 'local.nidump' file because it is created world-readable, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	MacOS X World Readable Local.NIDump	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
ArGoSoft[5]	Windows NT 4.0/2000, XP	Mail Server Plus 1.8.1.5, Pro 1.8.1.5,	A Directory Traversal vulnerability exists when a specially crafted request is submitted, which could let a remote malicious user obtain sensitive information.	Upgrade available at: http://www.argosoft.com/files/apps/msplus.exe	Mail Server Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
BBC Education[6]	Multiple	Betsie 1.5-1.5.11	A Cross-Site Scripting vulnerability exists in the 'parserl.pl' script because URL input is not properly validated and filtered, which could let a malicious user execute arbitrary script code.	Upgrade available at: http://www.bbc.co.uk/education/betsie/download.html	Betsie 'Parserl.pl' Cross-Site Scripting	High	Bug discussed in newsgroups and websites.
Bea Systems[7]	Windows NT 4.0/2000	WebLogic Server and Express 5.1.x, 6.0.x, 6.1.x and 7.0	A vulnerability exists in 'NTDLL.DLL' due to a race condition, which could let a remote malicious user cause a Denial of Service.	Patch available at: ftp://ftpna.bea.com/pub/releases/security/	WebLogic Server & Express Remote Denial of Service	Low	Bug discussed in newsgroups and websites.

[2] Westpoint Security Advisory, wp-02-0008, July 10, 2002.
[3] Bugtraq, July 7, 2002.
[4] SecurityFocus, June 28, 2002.
[5] Team N.finity Security Advisory, July 3, 2002.
[6] PenTest Limited Security Advisory, ptl-2002-03, July 1, 2002.
[7] KPMG-2002029, July 8, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Blackboard Inc.[8]	Multiple	Blackboard 5.0	A Cross-Site Scripting vulnerability exists in the 'login.pl' script because HTML tags are not properly filtered from CGI parameters, which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	Blackboard Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Exploit has been published.
Epic Games[9]	Multiple	Unreal Tourna-ment Server 436.0	A remote Denial of Service vulnerability exists when a malicious user transmits multiple spoofed UDP connections.	No workaround or patch available at time of publishing.	Unreal Tournament Server Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Ethereal Group[10, 11]	Windows 95/98/ME /NT 4.0/2000, XP, Unix	Ethereal 0.8.18, 0.9.0-0.9.4	Multiple vulnerabilities exist: a vulnerability exists in the LMP dissector which could let a malicious user cause a Denial of Service; a vulnerability exists in the AFS dissector mechanism when AFS data is analyzed, which could let a malicious user cause a Denial of Service; a vulnerability exists in the SOCKS dissector when malformed SOCKS data is injected, which could let a malicious user cause a Denial of Service; a vulnerability exists in the RSVP dissector when malformed RSVP data is injected, which could let a malicious user cause a Denial of Service; a buffer overflow vulnerability exists in the WCP (Wellfleet Compression Protocol) dissector due to insufficient bounds checking of framesizes, which could let a malicious user execute arbitrary code; and a buffer overflow vulnerability exists in the Ethereal BGP dissector mechanism, which could let a malicious user execute arbitrary code.	**Ethereal Group**: ftp://ftp.ethereal.com/pub/ethereal/ethereal-0.9.5.tar.gz **Conectiva:** ftp://atualizacoes.conectiva.com.br/	Ethereal Multiple Vulnerabilities	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites.

---

[8] Bugtraq, July 1, 2002.
[9] Bugtraq, July 3, 2002.
[10] Ethereal Advisory, enpa-sa-00005, June 28, 2002.
[11] Conectiva Linux Security Announcement, CLA-2002:505, July 4, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
GoAhead Software[12]	Windows 95/98/ME /NT 4.0, Unix	GoAhead WebServer 2.1, (Windows) 2.1	Several vulnerabilities exist: a Cross-Site Scripting vulnerability exists because unsantized requested URLs are included when a 404 error page is displayed, which could let a malicious user execute arbitrary script code; and a Directory Traversal vulnerability exists when URL encoded substitutions are used for the '/' character, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	GoAhead WebServer Cross-Site Scripting & Directory Traversal	Medium/ High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Proof of Concept exploits have been published.
Hewlett Packard Company[13]	Unix	Advanced Server/ 9000 B.04.05-B.04.09	A Denial of Service vulnerability exists when a malformed UDP packet is received on port 139.	Patch available at: http://itrc.hp.com PHNE_26988	Advanced Server/9000 Denial of Service	Low	Bug discussed in newsgroups and websites.
Hewlett Packard Company[14]	Unix	HP-UX 11.11	A remote Denial of Service vulnerability exists in the DCED and RPCD services when a malicious user modifies certain internal data.	Patches available at: http://itrc.hp.com PHSS_27258 PHSS_27259	HP-UX DCED & RPCD Services Remote Denial of Service	Low	Bug discussed in newsgroups and websites.
Icecast[15]	Unix	Icecast 1.3.12	A Directory Traversal vulnerability exists in list_directory() because requests are not constrained to the static directory, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Icecast Server Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Inktomi[16]	Unix	Media-IXT 3.0.4, Traffic Edge 1.1.2, 1.5.0, Traffic Server 4.0.18, 4.0.20, 5.1.3, 5.2.0-R, 5.2.1, 5.2.2	A buffer overflow vulnerability exists in the 'traffic_manager' binary when an excessively long commandline argument is sent, which could let a remote malicious obtain root or superuser privileges.	Inktomi is aware of the issue and have specific instructions on how to reconfigure the products, instructions are available at: http://support.inktomi.com/kb/070202-003.html	Traffic Server Remote Buffer Overflow	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

---

[12] Westpoint Security Advisory, wp-02-0001, July 10, 2002.
[13] Hewlett-Packard Company Security Bulletin, HPSBUX0207-198, July 10, 2002.
[14] Hewlett-Packard Company Security Bulletin, HPSBUX0207-196, July 2, 2002.
[15] SecurityFocus, July 9, 2002.
[16] Core Security Technologies Vulnerability Report, CORE-20020620, July 2, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
iPlanet & Netscape[17]	Windows NT 4.0/2000, Unix	iPlanet E-Commerce Solutions, iPlanet Web Server 4.1, 4.1SP1-9, 6.0, 6.0SP1&2; Enterprise Edition 4.1, 4.1SP1-9, 6.0, 6.0SP1&2; Netscape Enterprise Server 3.6	A buffer overflow vulnerability exists in the 'NS-rel-doc-name' parameter when an overly long value is supplied for the saved return address, which could let a remote malicious user execute arbitrary code.	Users of iPlanet Web Server 6 should install Service Pack 3 and users of iPlanet Web Server 4.1 should install Service Pack 10.	iPlanet Web Server Search Component	High	Bug discussed in newsgroups and websites. Exploit has been published. Vulnerability has appeared in the press and other public media.
Key Focus[18]	Windows 95/98/ME /NT 4.0/2000, XP	KF Web Server 1.0.2	A vulnerability exists if the requested URL contains a certain character, which could let a remote malicious user obtain sensitive information.	Upgrade available at: http://www.keyfocus.net/kf ws/download/kfws10.exe	KF Web Server Directory Contents Disclosure	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploits have been published.
Kim Storm[19]	Unix	NN 6.6.0-6.6.3	A format string vulnerability exists in the nn_exitmsg() function, which could let a remote malicious user execute arbitrary code.	Upgrade available at: ftp://ftp.nndev.org/pub/nn-6.6/nn-6.6.4.tar.Z	NN Format String	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Leung Eric[20]	Unix	E-Guest 1.1	A vulnerability exists because user-supplied input and script code is not properly filtered in guest book entries, which could let a remote malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	E-Guest Guest Book Script Injection	High	Bug discussed in newsgroups and websites. There is no exploit code required.
Lotus[21]	Unix	Domino R4 (version 4.x)	A vulnerability exists because the server allows downloading of files in the web root directory, which could let an unauthorized malicious user obtain access to files in the web root directory.	**Workaround:** Create a separate directory for the web site files (do not put them in the web root created during installation). In addition, the permissions on these files should be appropriately applied.	Domino File Retrieval	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Macro-media[22]	Multiple	Sitespring 1.2.0	A Denial of Service vulnerability exists when a malicious user sends a malformed request to the database engine.	No workaround or patch available at time of publishing.	Sitespring Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.

[17] NGSSoftware Insight Security Research Advisory, NISR09072002, July 9, 2002.
[18] Securiteinfo.com, July 7, 2002.
[19] Securiteam, July 6, 2002.
[20] DownBload Security Research Lab Advisory, June 28, 2002.
[21] Digisec.org Security Advisory, July 2, 2002.
[22] KPMG-2002028, July 1, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Macro-media[23]	Windows	ColdFusion Server MX Profes-sional, Enterprise, Developer	A buffer overflow vulnerability exists in `jrun.dll' when malformed HTTP requests are received, which could let a malicious user cause a Denial of Service.	Patch available at: http://www.macromedia.com/v1/handlers/index.cfm?ID=23161	ColdFusion MX jrun.dll Denial of Service	Low	Bug discussed in newsgroups and websites.
Macro-media[24]	Windows 95/98/NT 4.0/2000, Unix	JRun 3.0, 3.1, 4.0	A vulnerability exists in the HTML login form, which could let a remote malicious user bypass admin server authentication.	Patches available at: http://www.macromedia.com/v1/handlers/index.cfm?ID=23164	JRun Authentication Bypass	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Macro-media[25]	Windows 95/98/NT 4.0/2000, Unix	JRun 3.0, 3.1, 4.0	Multiple source disclosure vulnerabilities exist due to improper handling of null characters, which could let a malicious user obtain sensitive information.	http://www.macromedia.com/v1/handlers/index.cfm?ID=23164	Macromedia JRun Source Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Mark Hanson[26]	Windows	XiRCON 1.0 Beta 4	A remote Denial of Service vulnerability exists due to the way unusually large amounts of data are handled.	This application is no longer being maintained.	XiRCON Remote Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Microsoft[27]	Windows	SQL Server 2000 all editions, Desktop Engine (MSDE) 2000	Multiple vulnerabilities exist: a buffer overflow vulnerability exists in a procedure used to encrypt SQL Server credential information, which could let a malicious user gain significant control over the database and possibly the server; a buffer overflow vulnerability exists in a procedure that relates to the bulk inserting of data in SQL Server tables, which could let a malicious user gain significant control over the database and possibly the server itself; and a privilege elevation vulnerability exists due to incorrect permissions on the Registry key that stores the SQL Server service account information, which could let a malicious user obtain elevated privileges.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-034.asp	Multiple SQL Server Vulnerabilities CVE Names: CVE-CAN-2002-0624, CVE-CAN-2002-0641, CVE-CAN-2002-0642	High	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.

---

[23] Macromedia Security Bulletin, MPSB02-05, June 27, 2002.
[24] Westpoint Security Advisory, WP-02-0009, June 28, 2002.
[25] KPMG-2002026, July 1, 2002.
[26] Securiteam, July 7, 2002.
[27] Microsoft Security Bulletin, MS02-034, July 10, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[28] *Revised patch issued[29]*	Windows NT 4.0/2000, XP	Windows 2000 Advanced Server, 2000 Advanced Server SP1&2, 2000 Datacenter Server, 2000 Datacenter Server SP1&2, 2000 Profes-sional, 2000 Profes-sional SP1&2, 2000 Server, 2000 Server SP1&2, NT Enterprise Server 4.0, NT Enterprise Server 4.0 SP1-6a, NT Server 4.0, NT Server 4.0 SP1-6a, NT Terminal Server 4.0, NT Terminal Server 4.0 SP1-6a, NT Work-station 4.0, NT Work-station 4.0 SP1-6a, XP 64-bit Edition, XP Home, XP Profes-sional	A buffer overflow vulnerability exists in the Remote Access Server (RAS) Phonebook service when a specially malformed phonebook entry is sent, which could let a malicious user obtain elevated privileges, and gain complete control over the machine. *Although the original patch completely eliminated the vulnerability, it had the side effect of preventing non-administrative users from making VPN connections in some cases. The revised patch correctly handles VPN connections.*	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/ technet/treeview/default.as p?url=/technet/security/bu lletin/MS02-029.asp	Windows 2000 Remote Access Service Buffer Overflow **CVE Name: CAN-2002-0366**	**High**	Bug discussed in newsgroups and websites. *Vulnerability has appeared in the press and other public media.*

[28] Microsoft Security Bulletin, MS02-029, June 12, 2002.
[29] Microsoft Security Bulletin, MS02-029 V2.0, July 2, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[30] *Microsoft updates bulletin[31]*	Windows NT 4.0/2000	IIS 4.0, 5.0	A buffer overflow vulnerability exists because of an arithmetic error in the ISAPI extension that implements the HTR functionality, which could let a remote malicious user execute arbitrary code. *Bulletin was updated to revise the severity rating to "critical," due to a significant change in the threat environment because of an increased focus on chunked encoding vulnerabilities in general, and the discovery of hostile code attempting to exploit similar vulnerabilities on other platforms.*	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-028.asp *Customers who have not disabled HTR should do so as soon as possible. Alternately, customers who cannot disable HTR should apply the patch immediately.*	Microsoft IIS ISAPI Extension Buffer Overflow CVE Name: CAN-2002-0364	High	Bug discussed in newsgroups and websites. *Exploit scripts have been published.* *Vulnerability has appeared in the press and other public media.*
Microsoft[32]	Windows NT 4.0/2000	SQL Server 7, including Microsoft Data Engine 1.0 (MSDE 1.0), SQL Server 2000	A vulnerability exists in the 'setup.iss' file because passwords are stored insecurely, which could let a malicious user obtain sensitive information and elevated privileges.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-035.asp	SQL Server Installation Process Password Storage CVE Name: CAN-2002-0643	Medium	Bug discussed in newsgroups and websites.
Microsoft[33]	Windows 95/98/ME/NT 4.0/2000	Internet Explorer 5.5, 5.5 SP1&2, 6.0	A vulnerability exists because the object property of embedded WebBrowser controls is not subject to the Cross-Domain security checks, which could let a malicious user obtain elevated privileges, steal arbitrary cookies, or execute arbitrary commands.	No workaround or patch available at time of publishing.	Internet Explorer Universal Cross Domain Scripting	Medium/ High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Exploits have been published. Vulnerability has appeared in the press and other public media.

---

[30] Microsoft Security Bulletin, MS02-028, June 12, 2002.
[31] Microsoft Security Bulletin, MS02-028 V2.0, July 1, 2002.
[32] Microsoft Security Bulletin, MS02-035, July 10, 2002.
[33] Thor Larholm, PivX, Security Advisory, TL#003, July 10, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
mod_ssl[34] *Vendors issue patches*[35, 36, 37, 38]	**Multiple**	**mod_ssl 2.8.5-2.8.9**	**A buffer overflow vulnerability exists when handling certain types of long entries in an '.htacess' file, which could let a malicious user cause a Denial of Service or execute arbitrary code.**	**Upgrade available at:** **http://www.modssl.org/source/mod_ssl-2.8.10-1.3.26.tar.gz** **OpenBSD:** **ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.1/common/008_mod_ssl.patch'** ***Trustix:*** http://www.trustix.net/pub/Trustix/updates/ ***Caldera:*** ftp://ftp.caldera.com/pub/updates/OpenServer/CSSA-2002-SCO.32 ***Engarde:*** http://ftp.engardelinux.org/pub/engarde/stable/updates/ ***Conectiva:*** ftp://atualizacoes.conectiva.com.br/	**Mod_SSL HTAccess Buffer Overflow**	**Low/High** **(High if arbitrary code can be executed)**	**Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.**
Multiple Vendors[39]	Windows 95/98/ME/NT 4.0/2000, XP	Microsoft Foundation Class Library 7.0; Working Resources Inc. BadBlue Personal Edition 1.7.3	A buffer overflow vulnerability exists in the Microsoft Foundation Class Library (MFC) ISAPI framework, which could let a malicious user cause a Denial of Service.	No workaround or patch available at time of publishing.	Microsoft Foundation Class Library ISAPI Buffer Overflow	Low	Bug discussed in newsgroups and websites.
Multiple Vendors[40]	Unix	Mandrake Soft Linux Mandrake 7.1, 8.0, 8.0 ppc; RedHat Linux 6.2 sparc, i386, alpha, 7.0 sparc, i386, alpha, 7.1 ia64, i386, alpha; Slackware Linux 8.0	A buffer overflow vulnerability exists in the EFSTool program due to improper bounds checking, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	EFSTool Commandline Argument Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published.

[34] Bugtraq, June 24, 2002.
[35] Trustix Secure Linux Security Advisory, TSL-2002-0058, June 28, 2002.
[36] Caldera International, Inc. Security Advisory, CSSA-2002-SCO.32, July 1, 2002.
[37] EnGarde Secure Linux Security Advisory, ESA-20020702-017, July 2, 2002.
[38] Conectiva Linux Security Announcement, CLA-2002:504, July 2, 2002.
[39] Bugtraq, July 11, 2002.
[40] Ptrace Networks Security, June 28, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[41]	Windows 95/98/NT 4.0/2000, Unix	HP Application Server 8.0; jo! jo Webserver 1.0 rc1; Macro-media JRun 3.0, 3.1, 4.0; Oracle 9i Application Server 1.0.2 .2, 9.0.2; Orion Application Server 1.5.3; Pramati Server 3.0; Sybase Enterprise Application Server 4.0	A vulnerability exists when a malformed request is submitted to the WEB-INF directory, which could let a remote malicious user obtain sensitive information.	**jo! jo Webserver:** http://unc.dl.sourceforge.net/ sourceforge/tagtraum-jo/jo1_0b7.zip **Orion:** http://www.orionserver.com /mirrordownload.jsp?file=or ion1.5.4.zip **Macromedia JRun:**; http://www.macromedia.co m/v1/handlers/index.cfm?ID =23164 **Oracle:** http://otn.oracle.com/softwa re/products/ias/devuse.html	Multiple Vendor WEB-INF Directory Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Multiple Vendors[42]	Unix	Linux kernel 2.4.1-2.4.19 -pre6	A Denial of Service vulnerability exists when a malicious user opens all system file descriptors.	No workaround or patch available at time of publishing.	Linux Kernel File Descriptor Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Multiple Vendors[43, 44]	Unix	FreeBSD 4.0-4.6, 4.1.1–STABLE-4.5 –STABLE, 4.1.1 –RELEASE-4.6 –RELEASE; OpenBSD 3.0, 3.1	A vulnerability exists in multiple BSD kernels that may allow local users to trace setuid/setgid processes using the ktrace function, which could let a malicious user obtain sensitive information.	**FreeBSD:** ftp://ftp.FreeBSD.org/pub/Fr eeBSD/CERT/patches/SA-02:30/ **OpenBSD:** ftp://ftp.openbsd.org/pub/Op enBSD/patches/3.0/common /026_ktrace.patch ftp://ftp.openbsd.org/pub/Op enBSD/patches/3.1/common /009_ktrace.patch	Multiple Vendor KTrace SUID/SGID Process Tracing	Medium	Bug discussed in newsgroups and websites.

[41] Westpoint Security Advisory, wp-02-0002, June 28, 2002.
[42] Bugtraq, July 7, 2002.
[43] OpenBSD Security Advisory, June 27, 2002.
[44] FreeBSD Security Advisory, FreeBSD-SA-02:30, July 12, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[45, 46, 47]	Unix	Solaris 2.5.1 2.6 7.0, 8.0, 9.0; HP-UX 10.10 10.20 11.00 11.11; Compaq Tru64 4.0f, 4.0g, 5.0a, 5.1, 5.1a; Xi Graphics deXtop CDE 2.1; IBM AIX 4.3.3, 5.1.0; Caldera OpenUnix, 8.0, UnixWare 7.1.1; SGI IRIX 5.2, 5.3, 6.0, 6.0.1, 6.1-6.5.16	Two vulnerabilities exist in the Common Desktop Environment (CDE) ToolTalk RPC database server: a vulnerability exists in 'rpc.ttdbserverd' because the file descriptor argument _TT_ISCLOSE() is not properly validated, which could let a remote malicious user delete arbitrary files, cause a Denial of Service, or possibly execute arbitrary code; and a vulnerability exists in 'rpc.ttdbserverd' because file operations are not properly validated, which could let a malicious user overwrite arbitrary files, obtain elevated privileges or cause a Denial of Service.	For workaround and patches see: http://www.cert.org/advisories/CA-2002-20.html **Caldera:** ftp://ftp.caldera.com/pub/updates/UnixWare/CSSA-2001-SCO.28/erg711831b.Z **HP-UX:** ftp://hprc.external.hp.com Patch rpc.ttdbserver	Multiple CDE ToolTalk Vulnerabilities CVE Names: CAN-2002-0677, CAN-2002-0678	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.

---

[45] Core Security Technologies, CORE-20020528, July 10, 2002.
[46] CERT® Advisory, CA-2002-20, July 11, 2002.
[47] Caldera International, Inc. Security Advisory, CSSA-2002-SCO.28, July 11, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[48, 49, 50, 51, 52, 53, 54, 55, 56] *More vendors issue updates[57, 58, 59]*	Windows 95/98/NT 4.0/2000, XP, MacOS X 10.0-10.0.3, Unix	Apache Software Foundation Apache 1.0-1.0.3, 1.0.5, 1.1, 1.1.1, 1.2, 1.2.5, 1.3, 1.3.1, 1.3.3, 1.3.4, 1.3.9, 1.3.11-1.3.14, 1.3.11 win32-1.3.20 win32, 1.3.14 Mac, 1.3.17-1.3.20, 1.3.22-1.3.24, 1.3.22 win32-1.3.24 win32, 2.0. 2.0.28, 2.0.32, 2.0.35, 2.0.36	A vulnerability exists when invalid requests are coded with the 'Chunked Encoding' mechanism, which could let a remote malicious user cause a Denial of Service and in some cases execute arbitrary code. This can facilitate the further exploitation of vulnerabilities unrelated to Apache on the local system, potentially allowing the intruder root access. *Note: The impact of this vulnerability is dependent upon the software version and the hardware platform the server is running on.*	*More vendors have released updates regarding this vulnerability. For a complete list of current updates, see CERT® Advisory CA-2002-17 located at:* http://www.cert.org/advisories/CA-2002-17.html *Caldera:* http://www.caldera.com/support/security/index.html	Multiple Vendor Apache Chunked-Encoding Memory Corruption **CVE Name: CAN-2002-0392**	Low/High (High if arbitrary code can be executed or if root access is obtained)	Bug discussed in newsgroups and websites. Exploit scripts have been published. *Note: There is an Internet worm that uses the Chunked Encoding vulnerability.* Vulnerability has appeared in the press and other public media. *New Internet worm which exploits this vulnerability has been published.*

---

[48] CERT Advisory CA-2002-17, June 17, 2002.
[49] SuSE Security Announcement, SuSE-SA:2002:022, June 18, 2002.
[50] EnGarde Secure Linux Security Advisory, ESA-20020619-014, June 19, 2002.
[51] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:103-13, June 19, 2002.
[52] OpenPKG Security Advisory, OpenPKG-SA-2002.004, June 19, 2002.
[53] Debian Security Advisory DSA-131-2, June 19, 2002.
[54] Slackware Security Team, June 19, 2002.
[55] Trustix Secure Linux Security Advisory, TSLSA-2002-0056, June 20, 2002.
[56] Mandrake Linux Security Update Advisory, MDKSA-2002:039-2, June 22, 2002.
[57] Caldera International, Inc. Security Advisory, CSSA-2002-SCO.31, July 1, 2002.
[58] Caldera International, Inc. Security Advisory, CSSA-2002-SCO.32, July 1, 2002.
[59] CERT® Advisory CA-2002-17, updated July 8, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[60], [61, 62, 63, 64, 65, 66, 67, 68, 69] *Vendors' updates issued and exploit scripts published.* [70, 71, 72, 73, 74, 75]	Unix	HP HP-UX Secure Shell A.03.10; OpenSSH 1.2.2, 1.2.3, 2.1, 2.1.1, 2.3, 2.5, 2.5.1, 2.5.2, 2.9, 2.9 p1&2, 2.9.9, 3.0, 3.0 p1, 3.0.1, 3.0.1 p1, 3.0.2, 3.0.2 p1, 3.1, 3.1 p1, 3.2, 3.2.2 p1, 3.2.3 p1, 3.3, 3.3 p1	Two vulnerabilities exist when the OpenSSH server is configured at compile-time to support the 'BSD_AUTH' or 'SKEY' authentication, which could let an unauthenticated remote malicious user execute arbitrary code with root privileges. The first vulnerability affects OpenSSH versions 2.9.9 through 3.3 that have the challenge response option enabled and use 'SKEY' or 'BSD_AUTH' authentication and the second vulnerability affects PAM modules which use the interactive keyboard authentication in OpenSSH versions 2.3.1p1 through 3.3, regardless of the challenge response option setting. *Numerous vendors have released new updates regarding these vulnerabilities. Please check your vendor site for new updates.*	**OpenSSH:** ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH **Conectiva:** ftp://atualizacoes.conectiva.com.br/ **Debian:** http://security.debian.org/pool/updates/main/o/ **EnGarde:** http://ftp.engardelinux.org/pub/engarde/stable/updates/ **Mandrake:** ftp://ftp.nmt.edu/pub/linux/mandrake/updates/ ftp://mirrors.secsup.org/pub/linux/mandrake/Mandrake/updates/ **SuSE:** ftp://ftp.suse.com/pub/suse **OpenPKG:** ftp://ftp.openpkg.org/release/1.0/UPD/openssh-3.0.2p1-1.0.3.src.rpm **Trustix:** http://www.trustix.net/pub/Trustix/updates/ For more information on patches and workarounds see CERT® Advisory CA-2002-18 available at: http://www.cert.org/advisories/CA-2002-18.html *RedHat:* ftp://updates.redhat.com/	OpenSSH 'BSD_AUTH' or 'SKEY' Authentication	High	**Bug discussed in newsgroups and websites.** *Note: It has been reported that malicious individuals or organizations may be developing, or have developed functional exploit code.* **Vulnerability has appeared in the press and other public media.** *Exploit scripts have been published.*
MyWeb Server[76]	Windows 95/98/ME /NT 4.0/2000	MyWeb Server 1.0.1, 1.0.2	A buffer overflow vulnerability exists when a GET request is sent that contains a certain number of characters, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	MyWebServer GET Request Buffer Overflow	High	Bug discussed in newsgroups and websites.

---

[60] CERT® Advisory, CA-2002-18, June 25, 2002.
[61] Conectiva Linux Security Announcement, CLA-2002:500, June 25, 2002.
[62] EnGarde Secure Linux Security Advisory, ESA-20020625-015, June 25, 2002.
[63] SuSE Security Announcement, SuSE-SA:2002:023, June 25, 2002.
[64] OpenPKG Security Advisory, OpenPKG-SA-2002.005, June 26, 2002.
[65] NetBSD Security Advisory, 2002-005, June 27, 2002.
[66] Caldera International, Inc. Security Advisory, CSSA-2002-030.0, June 27, 2002.
[67] Debian Security Advisory, DSA-134-4, June 27, 2002.
[68] Mandrake Linux Security Update Advisory, MDKSA-2002:040, June 24, 2002.
[69] Trustix Secure Linux Security Advisory, 2002-0059, June 28, 2002.
[70] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:127-18, June 27, 2002.
[71] Conectiva Linux Security Announcement, CLA-2002:502, June 28, 2002.
[72] Revised OpenSSH Security Advisory, July 2, 2002.
[73] EnGarde Secure Linux Security Advisory, ESA-20020702-016, July 2, 2002.
[74] SuSE Security Announcement, SuSE-SA:2002:024, July 2, 2002.
[75] Mandrake Linux Security Update Advisory, MDKSA-2002:040-1, July 2, 2002.
[76] Foundstone Advisory, FS-070302-24-MWSX, July 8, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
National Science Foundation[77], [78, 79, 80]	Unix	Squid-2.x up to and including 2.4. STABLE6	Multiple vulnerabilities exist: a buffer overflow vulnerability exists in the MSNT auth helper component when msnt_auth is configured to use denyusers or allowusers access control files, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; several buffer overflow vulnerabilities exist due to the way FTP directory listings are parsed, which could let a remote malicious cause a Denial of Service or execute arbitrary code (This condition is only present in configurations that allow proxying of FTP requests); and multiple buffer overflow vulnerabilities exist when gopher URLs are parsed by the gopher proxy, which could let a remote malicious user execute arbitrary code.	**National Science Foundation:** ftp://ftp.squid-cache.org/pub/squid-2/STABLE/ or http://www.squid-cache.org/Versions/v2/2.4/ **RedHat:** ftp://updates.redhat.com/6.2/en/os/ **Conectiva:** ftp://atualizacoes.conectiva.com.br/ **SuSE:** ftp://ftp.suse.com/pub/suse/	Squid Multiple Vulnerabilities	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
NEC[81]	Windows 95/98/ME /NT 4.0/2000, XP, Unix	Socks4 4.2, 4.2.1, 4.2.2, 4.3 .beta2, 4.3 .beta.p1	A buffer overflow vulnerability exists due to improper bounds checking of user names, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.	No workaround or patch available at time of publishing.	Socks4 User Name Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
NEC[82]	Windows 95/98/ME /NT 4.0/2000, XP, Unix	Socks5 1.0 r5-1.0 r10	A vulnerability exists because user names are handled in an unsafe manner, which could let a malicious user cause a Denial of Service and potentially execute arbitrary code.	No workaround or patch available at time of publishing.	Socks5 User Name Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
NEC[83]	Windows 95/98/ME /NT 4.0/2000, XP, Unix	Socks5 1.0r5-1.0r11,	A buffer overflow vulnerability exists due to an 'off-by-one' error in the code that handles hostnames, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.	No workaround or patch available at time of publishing.	Socks5 Off-By-One Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.

---

[77] Squid Security Update Advisory, SQUID-2002:3, July 3, 2002.
[78] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:051-16, July 2, 2002.
[79] Conectiva Linux Security Announcement, CLA-2002:506, July 5, 2002.
[80] SuSE Security Announcement, SuSE-SA:2002:025, July 9, 2002.
[81] ISS Security Alert Summary, AS02-27, July 8, 2002.
[82] Bugtraq, July 3, 2002.
[83] ISS Security Alert Summary, AS02-27, July 8, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Network Associates[84]	Windows 95/98/ME /NT 4.0/2000, MacOS 9.0	Desktop Security 7.0.4, PGP Freeware 7.0.3, PGP Personal Security 7.0.3	A vulnerability exists in the message decoding functionality when a specially crafted e-mail is sent, which could let a remote malicious user execute arbitrary code.	Patch available at: http://download.nai.com/products/licensed/pgp/desktop_security/windows/version_7.04/hotfix/PGPOutlookPluginHotfix	PGP Outlook Plug-In Heap Corruption	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
NullSoft Inc.[85]	Windows 95/98/ME /NT 4.0/2000, XP	Winamp 2.50, 2.60 (lite), (full), 2.61 (full), 2.62 (standard), 2.64 (standard), 2.65, 2.70, 2.70 (full), 2.71, 2.72, 2.73-2.80, 2.73 (full),	A buffer overflow vulnerability exists when checking for updated versions, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Winamp Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Omnicron Technologies Corpora-tion[86]	Windows 95/98/NT 4.0/2000, XXP	Omni HTTPD 2.0 9	A buffer overflow vulnerability exists due to the way requests are handled that contain overly long headers, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.	No workaround or patch available at time of publishing.	OmniHTTPD Long Request Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Exploit script has been published.
Pacific Software[87]	Multiple	Carello 1.3	A vulnerability exists due to the way 'Carello.dll' accepts HTTP requests, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	Carello Shopping Cart Remote File Execution	**High**	Bug discussed in newsgroups and websites.
PHP Auction[88]	Multiple	PHP Auction 1.2, 1.3, 2.0, 2.1	A vulnerability exists in '/admin/login.php' when authentication credentials are submitted via 'login.php,' which could let a malicious user obtain elevated privileges.	No workaround or patch available at time of publishing.	PHPAuction Unauthorized Administrative Access	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Sendmail Consortium[89]	Unix	Sendmail 8.11-8.11.6, 8.12-8.12.4	A buffer overflow vulnerability exists due to the way code is handled by DNS, which could let a malicious user potentially execute arbitrary code.	Upgrade available at: ftp://ftp.sendmail.org/pub/sendmail/sendmail.8.12.5.tar.gz	Sendmail DNS Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

[84] eEye Digital Security Advisory, July 10, 2002.
[85] Security Advisory Número Dos, July 5, 2002.
[86] Bugtraq, July 1, 2002.
[87] Westpoint Security Advisory, wp-02-0012, July 10, 2002.
[88] Bugtraq, July 2, 2002.
[89] SecurityFocus, June 28, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Sharp Electronics[90]	Unix	Zaurus SL-5000D, SL-5500	Multiple vulnerabilities exist: a vulnerability exists because the FTP daemon used to sync does not require authentication, which could let a remote malicious user obtain root access; and a vulnerability exists in the passcode function, which could let a remote malicious user obtain sensitive information and unauthorized access.	No workaround or patch available at time of publishing.	Zaurus Multiple Vulnerabilities	Medium/ **High** **(High if root access is obtained)**	Bug discussed in newsgroups and websites. FTP authentication vulnerability may be exploited with an FTP client. Vulnerability has appeared in the press and other public media.
Simple WAIS[91]	Unix	Simple WAIS 1.11	A vulnerability exists due to insufficient santization of user-supplied input, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	Simple WAIS Interface Arbitrary Command Execution	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Sun Micro-systems, Inc.[92]	Unix	SunPCi II Driver Software 2.3	A vulnerability exists due to a weakness in the authentication scheme used by the VNC client, which could let a malicious user obtain user passwords.	No workaround or patch available at time of publishing.	SunPCi II Weak Authentication Scheme	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Sun Micro-systems, Inc.[93]	Unix	Solaris 2.5.1, 2.5.1 _x86, 2.6, 2.6 _x86, 7.0, 7.0_x86	A vulnerability exists because data from the serial console is not sufficiently secured, which could let a malicious user obtain sensitive information.	Patches available at: http://sunsolve.sun.com Patch 103641-40, Patch 103640-40, Patch 105182-32, Patch 105181-32, Patch 106542-20, Patch 106541-21	Solaris Serial Console Keystroke Interception	Medium	Bug discussed in newsgroups and websites.
Sun Micro-systems, Inc.[94]	Unix	Solaris 2.5.1, 2.6, 7.0, 8.0	A vulnerability exists because the'pkgadd' command will erroneously install some files with the suid/sguid bit set. The files may also have the owner set to root meaning that a set-uid root shell could be installed without the system administrator being aware of it.	Patches available at: http://sunsolve.sun.com/pub -cgi	Sun Solaris pkgadd Inappropriate File Permissions	**High**	Bug discussed in newsgroups and websites.
Sun Micro-systems, Inc.[95]	Unix	Solaris 8.0, 8.0 _x86	A Denial of Service vulnerability exists when a program uses the /dev/poll device.	Patches available at: http://sunsolve.sun.com Patch 108529-15, Patch 108528-15	Solaris /dev/poll Denial of Service	Low	Bug discussed in newsgroups and websites.

---

[90] Syracuse University Security Advisory, SURUAZ-2002-07-07, July 10, 2002.
[91] Securiteam, July 1, 2002.
[92] Trust Factory Security Advisory, TF20020601, July 3, 2002.
[93] SecurityFocus, July 4, 2002.
[94] Sun(sm) Alert Notification, 45693, July 10, 2002.
[95] SecurityFocus, July 5, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Sun Micro-systems, Inc.[96]	Unix	Solaris 7.0, 7.0 _x86, 8.0, 8.0_x86	A buffer overflow vulnerability exists in the Kodak Color Management System (KCMS) package when an overly long string on the command-line is passed, which could let a malicious user execute arbitrary code as root. *Note: This is an old vulnerability but a new exploit script has been published.*	Patch available at: http://sunsolve.Sun.COM/pub-cgi/retrieve.pl?doc=fpatches/111400	Solaris 7/8 KCMS Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Watch Guard[97]	Multiple	Firebox Firmware 5.0	A remote Denial of Service vulnerability exists in the Dynamic VPN Configuration Protocol (DVCP) service when a malicious user submits a malformed packet.	Upgrade to firmware version 6.x, available at the livesecurity website. If you are not a subscriber to the livesecurity service, please contact Watchguard support further assistance.	Firebox DVCP Remote Denial Of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Watch-guard[98]	Multiple	Soho Firewall, firmware 5.0.35a	A vulnerability exists because the FTP service is enabled by default and only requires a password for access, which could let a malicious user obtain sensitive information and full control over the firewall configuration.	No workaround or patch available at time of publishing.	Soho FTP Authentication	Medium/ **High** **(High if firewall control can be obtained)**	Bug discussed in newsgroups and websites.
Working Resources Inc.[99]	Windows 95/98/ME /NT 4.0/2000, XP	BadBlue Personal Edition 1.7.3	A Cross-Site Scripting vulnerability exists in the 'cleanSearchString' function because user input is not properly sanitized, which could let a malicious user execute arbitrary script code.	Upgrade available at: http://www.badblue.com/down.htm	BadBlue cleanSearch String() Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Working Resources Inc.[100]	Windows 95/98/ME /NT 4.0/2000, XP	BadBlue Personal Edition 1.7.3	Two vulnerabilities exist: a Denial of Service vulnerability exists when a malformed GET request is sent by a malicious user; and a remote Denial of Service vulnerability exists due to a heap overflow in an ISAPI that ships with the product.	No workaround or patch available at time of publishing.	BadBlue Denial of Service Vulnerabilities	Low	Bug discussed in newsgroups and websites.
WorldSpan [101]	Windows 95/98	Res Manager 4.1	A Denial of Service vulnerability exists when a malicious user sends a malformed packet via TCP port 17990.	No workaround or patch available at time of publishing.	Res Manager Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.

---

[96] Bugtraq, July 7, 2002.
[97] KPMG-2002030, July 9, 2002.
[98] KPMG-2002027, July 1, 2002.
[99] Securiteam, July 9, 2002.
[100] SecurITeam News, July 8, 2002.
[101] Bugtraq, July 4, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Zap Book[102]	Unix	Zap Book 1.0.3	A vulnerability exists because user-supplied input and script code is not properly filtered in guest book entries, which could let a remote malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	Zap Book Server Side Include Arbitrary Command Execution & Script Injection	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Zoltan Milosevic[103]	Multiple	Fluid Dynamics Search Engine 2.0.0.0050-2.0.0.0054	A Cross-Site Scripting vulnerability exists because an URL can be constructed that will cause scripting code to be embedded in a search results page, which could let a malicious user execute arbitrary script code.	Upgrade available at: http://www.xav.com/scripts/search/download/fdse.beta.zip	Fluid Dynamics Search Engine Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

*"Risk" is defined by CyberNotes in the following manner:

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.*

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between June 28 and July 12, 2002, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing**. During this period, 33 scripts, programs, and net-news messages containing holes or exploits were identified. *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 12, 2002	Nmap-2.54beta37.tgz	A utility for port scanning large networks.
July 12, 2002	Nn-expl.pl	Perl script which exploits the NN Format String vulnerability.
July 12, 2002	Ntop-2.1.tar.gz	An Unix / Windows network sniffing tool that shows the network usage.

---

[102] DownBload Security Research Lab Advisory, June 28, 2002.
[103] SecurityFocus, July 10, 2002.

Date of Script (Reverse Chronological Order)	Script name	Script Description
July 10, 2002	**Wp-02-0001.txt**	**Exploit URLs for the GoAhead WebServer Cross-Site Scripting & Directory Traversal vulnerabilities.**
July 9, 2002	0x4553artsd.c	Script which exploits the KDT ARTSD buffer overflow vulnerability.
July 9, 2002	Driftnet-0.1.6.tar.gz	Program which sniffs network traffic and picks out images from TCP streams it observes.
July 9, 2002	Flawfinder-1.20.tar.gz	Flawfinder searches through source code for potential security flaws, listing potential security flaws sorted by risk, with the most potentially dangerous flaws shown first.
July 7, 2002	2fax.c	Script which exploits the Linux bpcx vulnerability.
July 7, 2002	Bigeye-0.3.tar.gz	A network utility dump that can be run in multiple modes: sniffer, logging connections, and even emulating protocols such as HTTP or FTP.
July 7, 2002	Burndump.c	A LKM that strips off the Teso burneye protection from encrypted executables.
July 7, 2002	**Fddos.c**	**Script which exploits the Linux Kernel File Descriptor Denial of Service vulnerability.**
July 7, 2002	IeEn030.zip	A tool that remotely controls Internet Explorer using The Distributed Component Object Model (DCOM) and exposes traffic between an IE user and any server that is contacted, including logins and passwords over HTTPS.
July 7, 2002	Kcms_sparc.c	Script which exploits the Solaris 7/8 KCMS Buffer Overflow vulnerability.
July 7, 2002	Lcrzoex-4.11-src.tgz	A toolbox for network administrators and network malicious users that contains over 200 functionalities using network library lcrzo.
July 7, 2002	**Phantomupdate-0.7.tgz.tar**	**Exploit for the MacOS X Software Update Arbitrary Package Installation vulnerability.**
July 6, 2002	Dla-25-06-2002.txt	Proof of Concept exploit for the Microsoft Internet Information Server 5.0 Administration Web Site redirect vulnerability.
July 6, 2002	Elfsh-0.43b-Portable.tgz	An automated reverse engineering tool for the ELF format that has a sophisticated output with cross references using .got, .ctors, .dtors, .symtab, .dynsym, .dynamic, .rel.* and many other with an integrated hexdump.
July 6, 2002	Examiner-0.4.tar.gz	A tool to analyze foreign binary executable which was designed for forensic purposes but could be used for basic reverse-engineering goals as well.
July 6, 2002	Psreal.c	Psreal.c for Linux kernel 2.4.x finds processes hidden even if a LKM is used.
July 6, 2002	Safemode-adv-nn.txt	Exploit for the NN Format String vulnerability.
July 5, 2002	**Wampexp.c**	**Script which exploits the Winamp Buffer Overflow vulnerability.**
July 4, 2002	Argospill.sh	Exploit for the ArGoSoft Mail Server Directory Traversal vulnerability.
July 4, 2002	**Worldspan.pl**	**Perl script which exploits the Res Manager Denial of Service vulnerability.**
July 3, 2002	**Apache-worm.c**	**An Internet worm based on the GOBBLES exploit for the Apache chunked encoding vulnerability.**
July 3, 2002	Ettercap-0.6.7.tar.gz	A network sniffer/interceptor/logger for switched LANs that uses ARP poisoning and the man-in-the-middle technique to sniff all the connections between two hosts.
July 3, 2002	**Omni-overflow.c**	**Script which exploits the OmniHTTPD Long Request Buffer Overflow vulnerability.**
July 3, 2002	Sshutup-theo.tar.gz	Remote root exploit for the default install of OpenBSD 3.x. vulnerability.
July 3, 2002	**Ut.tgz**	**Exploit for the Unreal Tournament Server Remote Denial of Service vulnerability.**

Date of Script (Reverse Chronological Order)	Script name	Script Description
July 3, 2002	**Vncsunpci.c**	**Script which exploits the SunPCi II Weak Authentication Scheme vulnerability.**
July 2, 2002	Evil-sshconnect2.c	Script which exploits the OpenSSH 'BSD_AUTH' or 'SKEY' Authentication vulnerability.
July 2, 2002	Sshutup-theo.tar.gz.sig	Script which exploits the OpenSSH 'BSD_AUTH' or 'SKEY' Authentication vulnerability.
June 28, 2002	**Efs.pl**	**Perl script which exploits the EFSTool Commandline Argument Buffer Overflow vulnerability.**
June 28, 2002	**Efstool.pl**	**Perl script which exploits the EFSTool Commandline Argument Buffer Overflow vulnerability.**

Trends

- **There has been an increase in scanning for the Apache Chunk Encoding Vulnerability and direct reports of exploitation have been received by CERT/CC. For more information see** http://www.cert.org/current/current_activity.html#Apache**.**
- **A warning has been issued by NIPC regarding a potential vulnerability in numerous versions of the open-source Apache Web Server Software. This vulnerability can allow remote access to the system and gives an intruder the ability to take control of the system and execute root level commands. NIPC considers this to be a significant threat due to the large installed base of Apache Servers, the potential for remote compromise, and the level of access granted by this vulnerability. For more information, see "Bugs, Holes, and Patches" table and NIPC Advisory 02-005, located at:** http://www.nipc.gov/warnings/advisories/2002/02-005.1.htm
- **BSD/Scalper.worm is an Internet Worm that spreads over Apache web servers on FreeBSD by using the Chunked Encoding exploit. For more information, see Virus Section. Also see the "Bugs, Holes, and Patches" table for more information regarding the vulnerability.**
- **Numerous exploit scripts exist which exploit the Apache Chunked-Encoding Memory Corruption vulnerability. For more information, see "Recent Exploit Scripts and Techniques" table.**

Viruses

The following virus descriptions encompass new viruses and variations of previously encountered viruses that have been discovered in the last two weeks. The viruses are listed alphabetically by their common name. While these viruses might not all be in wide circulation, it is highly recommended that users update anti-virus programs as often as updates become available. *NOTE: At times, viruses may contain names or content that may be considered offensive.*

BAT_ARICA.B (Alias: ARICA.B) (Batch File Worm): This batch file worm propagates via Internet Relay Chat (mIRC) and e-mail. It drops and executes a Visual Basic script and an IRC script, which are responsible for its propagation.

Netav (Alias: I-Worm.Netav) (Internet Worm): This is a worm that spreads via e-mail messages. E-mail addresses are collected from the users' Address Book and HTML files located in the Temporary Internet Files folder. Every Tuesday the worm searches for *.DOC files in the Documents folder and, if there are several files there, picks one randomly and sends it out. It does not spread on Tuesday and only sends *.DOC files out. Every Thursday, the worm regenerates a new address list. The worm contains randomly selected subject lines and bodies. The following names are given to the worm's attachment:
- HGAME.EXE
- MININET.EXE
- NETAV.EXE

When the worm is first started, it shows a fake error message:

- "This file does not work on this system"

It then installs itself to your system and copies itself to the Windows System Directory as "NETAV.EXE" file. Next, it adds the path of that file to the System Registry:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\NETAV Agent

This way the worm starts during all Windows sessions.

PE_WEIRD.D (Aliases: PE_ZYTZMXZY, W95/Kuang.f, W32.Weird.d, W32/Weird.d) (File Infector): Upon execution, this file infector infects Windows executable files in the Windows, the Program Files, and the root directory. Their code reveal that it specifically targets the critical Windows application, "EXPLORER.EXE," which is actually Windows Explorer.

VBS_LUBUS.A (Aliases: I-Worm.Lubus, VBS.Loveletter.CV@mm, VBS/LoveLetter@MM) (Visual Basic Script Worm): This destructive, mass-mailing worm propagates via e-mail using Microsoft Outlook, sending a copy of itself to all addresses in the Microsoft Outlook address book. It sends an e-mail message with the following details:

- Subject: ANGEL1
- Message Body: %Recipient% Eres algo especial…escribeme
- Attachment: ANGEL1.PPT.vbs
  *where %Recipient% is the name of the target recipient.

This worm deletes files with certain file extensions.

VBS_SLIP.A (Aliases: I-Worm.Ley, VBS.Slip@mm) (Visual Basic Script Malware): This Visual Basic Script Malware is a variant of VBS_SLIP.B and propagates via e-mail using Microsoft Outlook. It sends the following e-mail message to all addresses listed in the Microsoft Outlook address book:

- Subject: hola quieres ver todos los videos de slipknot
- Message Body: con este programa vas a poder ver todo el video slipknot y sus mejores videos
- Attachment: %Malware file%
  *where %Malware file% is the name of the Malware file on the infected system.

VBS_SLIP.B (Alias: VBS.SLIP.B@MM) (Visual Basic Script Malware): This Malware sends e-mail messages with a copy of itself as attachment. It carries a destructive payload by overwriting the contents of some files on the infected system.

VBS.Slip.C@mm (Alias: VBS.Patch@mm) (Visual Basic Script Worm): This is a mass-mailing worm that uses Microsoft Outlook to send itself to all contacts in the Microsoft Outlook Address Book. When VBS.Slip.C@mm runs, it will open 20,000 instances of WordPad. This is done in an attempt to mask the e-mailing activity. The e-mail message has the following characteristics:

- Subject: Actualizacion de Windows urgente
- Message: Actulizacion critica contra agujeros de seguridad este parche cerrara los puertos abiertos para que no entren hackers a su computadora.
- Attachment: The name of the attachment varies.

After the worm sends itself, it adds the value, "system_windows" = "startup," to the registry key:

- HKEY_CURRENT_USER\Software

to avoid sending itself again the next time that it runs.

W32/Bajar-B (Aliases: W32.ZVM@mm, VBS.ZVM@mm, VBS.Bajar.B@mm) (Win32 worm): This is a mass mailing worm that e-mails itself to all entries in all Windows address books. It arrives in an e-mail with the following characteristics:

- Subject line: Nuevo programa para bajar musica gratis
- Message body: con este programa vas a poder bajar cualquier tipo de musica las mejores canciones

The attached filename can be anything. On execution, the worm displays a message box containing the text "Instalando ZVmusic." The worm checks the registry entry, "HKCU\Software\mp3_sent," and if it is not

set to "yea" then it changes the setting so the mass mailing routine can be executed. Finally W32/Bajar-B deletes the following:

- C:\windows\rundll.exe
- C:\windows\system\vshield.vxd
- C:\autoexec.bat
- C:\windows\regedit.exe
- C:\windows\regedit.com

W32.Dalbug.Worm (Win32 Worm): This worm will only replicate under NT/2000/XP systems. It spreads by attacking computers that have open user accounts and shares, installing itself remotely as a service on the victim's computer.

W32/Datom-A (Alias: W32.Datom.worm) (Win32 worm): This worm has been reported in the wild. It is a virus disguised as "copyrighted Microsoft code" and claiming to be a Windows update. It can also spread through open network shares. The actual worm itself consists of three components: "MSVXD.exe," "MSVXD16.dll," and "MSVXD32.dll," created using Borland C++. "MSVXD.exe" is the executable component of the worm, which loads the two DLL files. "MSVXD32.dll" contains the code to spread the worm. It enumerates network shares and attempts to copy itself onto remote machines. If the worm is successful copied, it attempts to change the win.ini file so that the worm file "MSVXD.exe" is run on Windows startup. W32/Datom-A changes the registry value:

- \HKLM\Software\Microsoft\Windows\CurrentVersion\Run\MSVXD

so that the worm file "MSVXD.exe" is run on Windows startup

W32/Duni-A (Aliases: W32.Duni.Worm, I-Worm.Duni, W32/Dadinu, WORM_DANDI.A, UNIDAD.A, W32/Duni.worm.b, I-Worm.Kitro.c, Win32/Kitro.C@mm, Win32.Kitro.B worm) (Win32 worm): This worm has been reported in the wild. It is an e-mail worm that uses a wide range of subject lines and attachment names. The worm finds addresses to send itself to in the user's MSN Messenger contact list using the server mail.hotmail.com. It also attempts to use the KaZaA peer-to-peer network to spread. The worm copies itself to the user's KaZaA download area using a variety of filenames. When the worm is run, it will create copies of itself in the root folder and the Windows folder. These copies will have a name consisting of a random number and the extension .CPL. The worm then adds the following registry entry so that the copy in the Windows folder is run each time Windows is started:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run

W32/Duni-A attempts to interfere with anti-virus software by deleting the files C:\archiv~1\perav\pav.dll, C:\archiv~1\perav\per.dll, C:\program files\perav\pav.dll and C:\program files\perav\per.dll and the files PAV.EXE, \bases\avp.set, system\vshield.vxd, \system32\vshield.vxd and \vshield.vxd from the Windows folder. It also modifies the following registry entries:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Pav.exe
- HKLM\Software\KasperskyLab\SharedFiles\Folder.

W32/Eversaw.bat@MM (Win32 Worm): This Internet worm is written in Batch script. It attempts to spread via a number of mechanisms: mass mailing itself to the Outlook contacts list, via mIRC and pIRCh, and via KaZaA file sharing. The worm is an MS-DOS batch file. When executed, it attempts to copy itself to A:\ (will only succeed on Win9x), and drops a sequence of other files:

- An encrypted batch file, "RUN.BAT"
- A debug script to create a VBS script (CR.VBS) to decrypt the above batch file
- A debug script to create a JPEG image file (C:\SOULCONTROL.JPG - 32,966 bytes).

Subsequently "RUN.BAT" is decrypted and executed. This batch file can perform the following various actions:

- Attempts to delete certain AV signature files and mIRC/pIRCh ini files
- Modifies win.ini to run a copy of the worm (C:\BAT.SOULCONTROL.BAT) at system startup
- Modifies mIRC/pIRCh ini files to attempt to spread via these channels
- Modifies Registry keys to alter KaZaA file sharing configuration (shares C:\):
  HKCU\Software\Kazaa\LocalContent "Dir0" = 012345:C:\,
  HKCU\Software\Kazaa\LocalContent "DisableSharing" = 00 00 00 00

- Drops and executes a VBS script (OL.VBS) which mails a copy of the worm to all addresses in the Outlook contacts list
- Modifies a Registry key to run a dropped BAT file (C:\PL.BAT) at system startup, which displays the dropped JPEG image.

W32/Grade.A (Win32 Worm): This is a worm that spreads via e-mail, by sending itself out to every address in the Outlook Address Book. The message that is it used to spread has variable characteristics. It is very dangerous, as it deletes files that are necessary for the correct functioning of the computer. It is programmed in Borland Delphi and gets into systems in a file compressed with UPX 169,984 bytes in size.

W32/Gunsan-A (Win32 worm): This is a worm that spreads via e-mail, on local drives and in local shares. It also has backdoor capabilities and allows unauthorized access to the user's computer via IRC. When run, W32/Gunsan-A drops itself into the Windows system folder as "explorer16.exe" and sets the following registry entry so that this file is run when Windows starts up:
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\Explorer = <system folder>\explorer16.exe

Under Win9x, the worm runs as a service process. If the worm detects the ZoneAlarm personal firewall on the user's computer, it creates C:\noalarm.bat. This file deletes ZoneAlarm related files when the computer is restarted (via a line added to autoexec.bat to execute C:\noalarm.bat on startup). It also blocks access to the following websites by modifying the <Windows folder>\Hosts file:
- www.mcafee.com
- www.mcaffee.com
- www.norton.com
- www.theregister.co.uk
- www.zdnet.com
- www.sophos.com
- www.zonelabs.com
- www.zonealarm.com

The worm opens a random TCP port (<5000) and listens on this port for web connections (the random port number is recorded in C:\skyliner.dat). After detecting an Internet connection by connecting to www.microsoft.com, the worm retrieves the name of the SMTP server from the default mail account (or from the first account if the default account does not exist). Next it opens up a backdoor by connecting to one of the following IRC servers: irc.dal.net, typhoon.va.us.dal.net, or liberty.nj.us.dal.net. The worm then scans all local drives and network shares and does the following:
- Collects e-mail addresses from DBX, MBX, IDX, HTM and HTML files;
- Adds IFRAME blocks to HTM/HTML files. These IFRAME blocks point to the random port opened on the local machine;
- Searches for files with a KIX extension. If any are found, then the worm creates a copy of itself with a random name based on the computer name in the given folder and adds the line run "<random name>.exe" to the KIX file;
- Searches for files with the extension MP3, ISO, AVI, or MPG. If any are found, then the worm creates a copy of itself in the given folder using the same filename with the double extension .mp3.exe, .iso.exe, avi.exe, or .mpg.exe respectively;
- Searches for "winrar.exe." If this file is found, then the worm adds itself to RAR and ZIP archives;
- Deletes all files whose file path contains any of the following strings: McAfee, Softice, Numega, antivirus, anti-virus, win32dasm, Sophos, catsclaw, claw95, lockdown, Symantec, firewall, virusscan, virus-scan, FProt, F-Prot, Zone labs, or Atguard.

W32/Gunsan-A sends itself as an attachment to e-mail addresses collected during the scanning process. The worm sends two e-mails to every e-mail address. The first e-mail contains an IFRAME block referencing the server the worm opened up on the random port. This e-mail has no attachment. The second e-mail contains the worm as an attachment and has the following characteristics:
- Subject line: <a single space character>
- Attached file: tast.exe

This second e-mail makes use of two exploits to run the attachment automatically on unpatched versions of Microsoft Outlook and Outlook Express.

W32/Metrion-B (Aliases: Win32-HLLP-Metrion32704-B, Win32.Metrion.37204) (Win32 executable file virus): W32/Metrion-B will infect several EXE files at a time. When an infected file is run, two processes are created: one for the virus and one for the host file. The host will behave as expected and the virus will only start infecting when the host program has terminated. The viral process will terminate when infection has completed. BAT files are overwritten with a two line batch script that is designed to run the virus. Since this action may affect batch files that are executed when Windows starts up, the virus is likely to be run at this time. CPP files are overwritten with a few lines of C++ code that will print the output "Tagged by Metrion Cascade II" when compiled. VBS files are overwritten with a single line of VBScript that displays the same output as the compiled C++ code would. HTM files are overwritten with several lines of HTML that will display a page containing the text "Metrion Cascade II -icarus."

W32/Nahata-F (Alias: I-Worm.Nahata.e) (Win32 worm): This is a worm that tries to spread via e-mail, mIRC, and pIRCH. The worm drops itself into the root folder of drive C: and also attempts to drop the file C:\info.vbs. This file is meant to send the worm to e-mail addresses found in the Outlook address book and overwrite script.ini and events.ini when the computer is restarted. However, this functionality does not work properly.

W32.Supova.Worm (Alias: W32.Kitty.Worm) (Win32 Worm): This worm comes disguised as a popular software file. It spreads across KaZaA file-sharing networks by tricking KaZaA users into downloading and running the program.

W32/Tinit-B (Win32 Executable File Virus): W32/Tinit-B may infect files on open Windows network shares.

W97M.Zacry.A@mm (Word 97 Macro Virus): This is a Microsoft Word macro virus. It spreads by infecting the global template, Normal.dot, and the currently active document. Also, it attempts to replicate itself to all contacts in the Microsoft Windows Address Book using Microsoft Outlook. The e-mail message will have the following characteristics:
- Subject: Re: Send to me
- Attachment: [A Word document, infected with W97M.Zacry.A@mm]

WORM_ARGEN.A (Aliases: ARGEN.A, VBS_LEOLE.A, W32.Banegra.int, W32.Kitro.D.Worm) (Win32 Worm): This destructive worm drops a Visual Basic Script (VBScript) file. This VBScript file sends WORM_ARGEN.A to all e-mail addresses in the infected user's Microsoft Outlook address book. The worm deletes all non-hidden files found in the root directory of Drive C:\ and drops several copies of itself.

Worm/BWG.H (Internet Worm): This is an Internet worm that spreads through e-mail by using addresses it collects in the Microsoft Outlook Address Book, as well as, through the use of the Internet Rely Chat (IRC) network. The worm arrives through e-mail in the following format:
- Subject: As a friend, and you BETRAY me!!
- Body: How could you do that? Read the attachment for the evidence!!
- Attachment: chick.vbs

However, due to a programming error in the VBS Script, the virus does not correctly replicate itself nor does it properly register itself correctly into the Registry. If executed, the worm copies itself in the directory under which it is run using the filename "chick.bat." Once the spreading routine is finished, these files are then deleted. Additionally, the file "system.ini" file gets modified. Numerous files are created in the \windows\ and root directories. So that it can spread through IRC, the following file gets modified, "script.ini." It will also try to delete various antivirus software applications, including avp32.exe, antivir.vdf, tc.exe, scan.dat, tbav.dat, fpw32.dll, and various Norton applications.

WORM_CRAZYBOX.A (Internet Worm): This worm sends copies of itself as a file attachment in e-mail messages. It does not have a destructive payload.

WORM_LIAC.A (Aliases: W32.Liac.A@mm, W32/Calil-A, Lilac) (Win32 Worm): The worm is written in Visual Basic and compressed with Petite file compressor. When the worm's file is started, it shows a fake error message:

- Error54: Media Player not installed correctly

The worm copies itself to TEMP folder of Windows, adds a startup key for that file into System Registry, and sends itself to all recipients of Outlook Address Book and Windows Address Book with the following message:

- Subject: FW:FW: LILAC project video attach
- Body: Things that the govt. dont want you to know
- Attachment: LILAC_WHAT_A_WONDERFULNAME.avi.exe

The worm has bugs in its code and can fail to send its attachment. In this case, recipients will get an empty EXE file. Also the worm changes Windows owner information to 'xEnOcrAtEs' and sets logon text to 'Owned by: xEnOcrAtEs'. The worm can display a message:

- 'Your PC is infected with LILAC virus by: xEnOcrAtEs'

WM97/Marker-KR (Word 97 Macro Virus): This virus has been reported in the wild. It is a corrupted but working variant of the WM97/Marker family of viruses. It will attempt to append confidential data to the end of the macro code.

X97M.Hail.A (Excel 97 Macro Virus): This is a macro virus that infects Microsoft Excel workbooks. It infects files that have been recently used by Microsoft Excel. The virus activates when an infected file is opened and performs the following actions:

- It changes a Microsoft Excel security option so that when a macro is run, Excel will not display any prompts or alert messages.
- X97M.Hail.A opens a collection of files that have been used recently by Excel and infects them with the macro virus.
- It adds instructions to the C:\Autoexec.bat file to delete the files from the C drive

XM97/Momac-A (Alias: X97M/Momac.C) (Excel 97 Macro Virus): This virus has been reported in the wild. It does not create an infected workbook in the XLSTART directory. Instead, it copies itself directly from one open file to another.

XM.ZePast.A (Excel 95 Macro Virus): This is a Microsoft Excel 95 macro virus that will only replicate if Excel is installed in the C:\Msoffice\Excel folder. This virus contains, among other text messages, the comment: "Macro recorded at zome time in ze past by ze germanz." Once activated, this virus will change the following attributes in the active workbook:

- Title: ""
- Subject: ""
- Author: "The nicer virus"
- Keywords: ""
- Comments: "ha ha ha"

It then attempts to save it as C:\Msoffice\Excel\Xl2.xls. It also tries to save a copy of itself as C:\Msoffice\Excel\Xlstart\BOOK.xlt.

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table starts with Trojans discussed in CyberNotes #2002-01, and items will be added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on Trojans and Trojan variants that anti-virus software detects. *Note: At times, Trojans may contain names or content that may be considered offensive.*

Trojan	Version	CyberNotes Issue #
APStrojan.sl	N/A	CyberNotes-2002-03
Arial	N/A	CyberNotes-2002-08
Backdoor.Anakha	N/A	CyberNotes-2002-13
Backdoor.AntiLam	N/A	CyberNotes-2002-12
Backdoor.Assasin	**N/A**	**Current Issue**
Backdoor.Crat	N/A	CyberNotes-2002-12
Backdoor.EggHead	N/A	CyberNotes-2002-04
Backdoor.Evilbot	N/A	CyberNotes-2002-09
Backdoor.FTP_Bmail	N/A	CyberNotes-2002-12
Backdoor.G_Door.Client	N/A	CyberNotes-2002-05
Backdoor.GRM	N/A	CyberNotes-2002-13
Backdoor.GSpot	N/A	CyberNotes-2002-12
Backdoor.IISCrack.dll	N/A	CyberNotes-2002-04
Backdoor.Latinus	N/A	CyberNotes-2002-12
Backdoor.Mirab	N/A	CyberNotes-2002-13
Backdoor.NetControle	N/A	CyberNotes-2002-13
Backdoor.NetDevil	N/A	CyberNotes-2002-04
Backdoor.Nota	N/A	CyberNotes-2002-12
Backdoor.Omed.B	N/A	CyberNotes-2002-11
Backdoor.Palukka	N/A	CyberNotes-2002-01
Backdoor.RemoteNC	N/A	CyberNotes-2002-09
Backdoor.Sazo	N/A	CyberNotes-2002-13
Backdoor.Sparta	N/A	CyberNotes-2002-13
Backdoor.Subwoofer	N/A	CyberNotes-2002-04
Backdoor.Surgeon	N/A	CyberNotes-2002-04
Backdoor.Systsec	N/A	CyberNotes-2002-04
Backdoor.Tron	N/A	CyberNotes-2002-12
Backdoor.Ultor	N/A	CyberNotes-2002-13
BackDoor-AAB	N/A	CyberNotes-2002-02
BackDoor-ABH	N/A	CyberNotes-2002-06
BackDoor-ABN	N/A	CyberNotes-2002-06
BackDoor-FB.svr.gen	N/A	CyberNotes-2002-03
Bck/Litmus.201	**N/A**	**Current Issue**
BDS/ConLoader	N/A	CyberNotes-2002-12
BDS/Osiris	N/A	CyberNotes-2002-06
BKDR_EMULBOX.A	N/A	CyberNotes-2002-10
BKDR_INTRUZZO.A	N/A	CyberNotes-2002-09
BKDR_LITMUS.C	N/A	CyberNotes-2002-09
BKDR_SMALLFEG.A	N/A	CyberNotes-2002-04
BKDR_WARHOME.A	N/A	CyberNotes-2002-06
Dewin	N/A	CyberNotes-2002-08
DlDer	N/A	CyberNotes-2002-01
DoS-Winlock	N/A	CyberNotes-2002-03
Downloader-W	N/A	CyberNotes-2002-08
Fortnight	N/A	CyberNotes-2002-10

Trojan	Version	CyberNotes Issue #
Hacktool.IPStealer	N/A	CyberNotes-2002-02
Irc-Smallfeg	N/A	CyberNotes-2002-03
IRC-Smev	N/A	CyberNotes-2002-08
JS/NoClose	N/A	CyberNotes-2002-11
JS/Seeker-E	N/A	CyberNotes-2002-01
JS_EXCEPTION.GEN	N/A	CyberNotes-2002-01
Liquid.Trojan	**N/A**	**Current Issue**
mIRC/Gif	N/A	CyberNotes-2002-08
Multidropper-CX	N/A	CyberNotes-2002-08
QDel227	N/A	CyberNotes-2002-09
QDel234	N/A	CyberNotes-2002-11
RCServ	N/A	CyberNotes-2002-10
SecHole.Trojan	N/A	CyberNotes-2002-01
Swporta.Trojan	N/A	CyberNotes-2002-13
TR/Win32.Rewin	N/A	CyberNotes-2002-12
Tr/WiNet	N/A	CyberNotes-2002-10
TR/Zirko	N/A	CyberNotes-2002-10
Troj/Diablo	N/A	CyberNotes-2002-09
Troj/Download-A	N/A	CyberNotes-2002-01
Troj/DSS-A	N/A	CyberNotes-2002-12
Troj/Flood-O	**N/A**	**Current Issue**
Troj/ICQBomb-A	N/A	CyberNotes-2002-05
Troj/Kbman	N/A	CyberNotes-2002-10
Troj/Momma-B	N/A	CyberNotes-2002-11
Troj/Msstake-A	N/A	CyberNotes-2002-03
Troj/Optix-03-C	N/A	CyberNotes-2002-01
Troj/Sub7-21-I	N/A	CyberNotes-2002-01
Troj/WebDL-E	N/A	CyberNotes-2002-01
TROJ_CYN12.B	N/A	CyberNotes-2002-02
TROJ_DANSCHL.A	N/A	CyberNotes-2002-01
TROJ_DOAL.A	**N/A**	**Current Issue**
TROJ_DSNX.A	N/A	CyberNotes-2002-03
TROJ_FRAG.CLI.A	N/A	CyberNotes-2002-02
TROJ_ICONLIB.A	N/A	CyberNotes-2002-03
TROJ_JUNTADOR.B	N/A	CyberNotes-2002-06
TROJ_JUNTADOR.G	N/A	CyberNotes-2002-10
TROJ_OPENME.B	N/A	CyberNotes-2002-09
TROJ_SMALL.J	N/A	CyberNotes-2002-10
TROJ_SMALLFEG.DR	N/A	CyberNotes-2002-04
TROJ_SQLSPIDA.B	N/A	CyberNotes-2002-11
TROJ_WORTRON.10B	N/A	CyberNotes-2002-12
Trojan.Allclicks.A	N/A	CyberNotes-2002-13
Trojan.Badcon	N/A	CyberNotes-2002-02
Trojan.Fatkill	N/A	CyberNotes-2002-09
Trojan.Prova	N/A	CyberNotes-2002-10

Trojan	Version	CyberNotes Issue #
Trojan.PSW.CrazyBilets	N/A	CyberNotes-2002-12
Trojan.PSW.M2	N/A	CyberNotes-2002-13
Trojan.StartPage	N/A	CyberNotes-2002-02
Trojan.Suffer	N/A	CyberNotes-2002-02
VBS.Gascript	N/A	CyberNotes-2002-04
VBS_CHICK.B	N/A	CyberNotes-2002-07
VBS_THEGAME.A	N/A	CyberNotes-2002-03
W32.Alerta.Trojan	N/A	CyberNotes-2002-05
W32.Delalot.B.Trojan	N/A	CyberNotes-2002-06
W32.DSS.Trojan	N/A	CyberNotes-2002-09
W32.Estrella	N/A	CyberNotes-2002-13
W32.Evala.Worm	**N/A**	**Current Issue**
W32.IRCBot	**N/A**	**Current Issue**
W32.Libi	N/A	CyberNotes-2002-10
W32.Maldal.J	N/A	CyberNotes-2002-07
W32.Tendoolf	N/A	CyberNotes-2002-09
WbeCheck	N/A	CyberNotes-2002-09

Backdoor.Assasin (Alias: Backdoor.Assasin.10): This is a Trojan horse that allows unauthorized access to the infected computer. The Trojan also attempts to terminate the processes of many executables, including various firewall and antivirus programs.

Bck/Litmus.201: This Trojan allows malicious users to gain remote access to affected computers through an IP connection. The IP connection could be either the Internet or an Intranet. It consists of two parts, a client and a server. The client is a program that must be installed on the attacking computers, and the server installs itself (in the background) on the computer under attack. Once the client-server connection has been established, the computer under attack will be accessible form the attacking computer.

Liquid.Trojan: This Trojan comes in the form of the executable file, "Mp3 Liquid Burn.exe." When it is executed, it creates numerous text files in the \Program Files folder and the root of the C drive. The file names will be "You suckxxxx.txt" (where xxxx is a number from 1 upwards). All files contain this text: "you suck." After inserting the files, Liquid.Trojan reboots the computer.

TROJ_DOAL.A (Alias: W32.Doal.Trojan): This destructive malware comes disguised as a Windows XP Home Edition Key Generator. It drops a file named "load.exe" that is executed on every system reboot. This program prompts the user with a message that the system does not have enough disk space on the installation drive, and asks whether the user wishes to continue. If the infected user clicks Yes, it parses Drive C:\ and deletes files.

Troj/Flood-O: Troj/Flood-O is an attempt to create an IRC backdoor and flooder Trojan. The Trojan is derived from a legitimate mIRC32 client that has been intentionally manipulated to change the characteristics of the original client. The original client has a standard mIRC32 program icon while the Trojan file has no icon at all. The title in the Trojan window title bar is "Taskmon" instead of "mIRC32" and the Trojan file does not have the original client's menu information. The Trojan may attempt to flood IRC channels once connected to an IRC server.

W32.Evala.Worm (Alias: W32.Warcraft): This is a Backdoor Trojan that allows a malicious user to gain access to the infected system. It is also capable of spreading across KaZaA, Grokster, and Morpheus file sharing networks. It listens for connections on TCP ports 69 and 70.

W32.IRCBot (Alias: Backdoor.Sdbot): This Trojan contains backdoor capabilities that allows a malicious user to control your computer remotely using Internet Relay Chat (IRC). It also has the ability to download and execute other files of the malicious user's choice. When this Trojan is executed, it copies itself to "%windir%\Winapii\Winapii.exe" and sets itself to run as a service. Next it locates the \Windows folder (by default this is C:\Windows or C:\Winnt) and copies itself to that location. It also adds the value, "winapii %windir%\Winapii\Winapii.exe" to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

This Trojan contains its own Internet Relay Chat (IRC) client. This allows it to connect to an IRC channel that was hardcoded into the Trojan. Using the IRC channel, the Trojan listens for commands from the malicious user. The malicious user accesses the Trojan by using a password-protected authorization. The commands allow the following actions to be performed:

- Manage the installation of the Trojan
- Control the IRC client on the compromised computer
- Update the installed Trojan
- Send the Trojan to other IRC channels
- Download and execute files
- Perform DoS attacks against a target defined by the malicious user
- Uninstall itself completely by removing the relevant registry entries