Department of Homeland Security
Information Analysis and Infrastructure Protection Directorate
CyberNotes

Issue #2003-20 *October 6, 2003*

CyberNotes is published every two weeks by the Department of Homeland Security/Information Analysis and Infrastructure Protection (IAIP) Directorate. 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 Department of Homeland Security Information Analysis Infrastructure Protection Directorate Web site at http://www.nipc.gov.

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

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between September 18 and October 3, 2003. 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
Alan Ward[1]	Windows	A-Cart 2.0, PRO 2.0	A Cross-Site Scripting vulnerability exists in the 'signin.asp' script due to insufficient filtering of HTML from user-supplied input in the 'msg' variable, which could let a remote malicious user execute arbitrary HTML or script code.	No workaround or patch available at time of publishing.	A-Cart Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[1] Zone-h Security Team Advisory, ZH2003-29SA, September 27, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Apache Software Founda-tion[2]	MacOS X 10.x, Unix	Apache 2.0a9, 2.0, 2.0.28, 2.0.32, 2.0.35-2.0.47	A Denial of Service vulnerability exists because the 'mod_cgi' doesn't handle output to STDERR correctly.	**Mandrake:** http://www.mandrakesecure.net/en/ftp.php	Apache2 MOD_CGI Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Apache Software Founda-tion[3] ***RedHat issues advisories[4]***	**Windows, OS2, Unix**	**Apache 1.3.1, 1.3.3, 1.3.4, 1.3.6, 1.3.9, 1.3.11, 1.3.12, 1.3.14, 1.3.17-1.3.20, 1.3.22-1.3.27**	**Multiple vulnerabilities exist: a vulnerability exists in the 'rotatelogs' support program because special control characters received over the pipe are not ignored, which could let a malicious user cause the program to quit logging; a Denial of Service vulnerability exists because a malicious user can make the server enter infinite loops; and a vulnerability exists because several file descriptors can be leaked to child processes, such as CGI scripts, which could let a malicious user obtain sensitive information.**	**Upgrades available at: http://httpd.apache.org/download.cgi** **Conectiva: ftp://atualizacoes.conectiva.com.br/** ***RedHat:*** **ftp://updates.redhat.com/**	**Apache HTTP Server Multiple Vulnerabil-ities** **CVE Name: CAN-2003-0460**	**Low/ Medium** **(Medium is sensitive informa-tion can be obtained)**	**Bug discussed in newsgroups and websites.**
Apache Software Founda-tion[5, 6] ***More updates issued[7, 8]*** ***More updates issued[9]***	**Windows, MacOS X 10.x, Unix**	**Apache 2.0, 2.0.28, 2.0.32, 2.0.35-2.0.46**	**A remote vulnerability exists when the 'SSLCipherSuite' directive is used to upgrade a cipher suite, which could cause a weaker cipher suite being used.**	**Apache Software Foundation: http://httpd.apache.org/download.cgi** **Trustix: ftp://ftp.trustix.net/pub/Trustix/updates/2.0/RPMS/** ***Conectiva:*** **ftp://atualizacoes.conectiva.com.br** ***Hewlett Packard:*** **http://www.software.hp.com/** ***Mandrake:*** **http://www.mandrakesecure.net/en/ftp.php** ***RedHat:*** **ftp://updates.redhat.com/**	**Apache Web Server SSLCipher Suite Weak Cipher Suite** **CVE Name: CAN-2003-0192**	**Medium**	**Bug discussed in newsgroups and websites.** **Vulnerability has appeared in the press and other public media.**

[2] Mandrake Linux Security Update Advisory, MDKSA-2003:096, September 26, 2003.
[3] SecurityFocus, July 24, 2003.
[4] Red Hat Security Advisory, RHSA-2003:243-01 & RHSA-2003:244-01, September 22, 2003.
[5] Apache Security Announcement, July 9, 2003.
[6] Trustix Secure Linux Security Advisory, 2003-0025, July 11, 2003.
[7] Conectiva Linux Security Announcement, CLA-2003:698, July 21, 2003.
[8] Mandrake Linux Security Update Advisory, MDKSA-2003:075, July 21, 2003.
[9] Red Hat Security Advisory, RHSA-2003:243-01 & RHSA-2003:244-01, September 22, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
ArGoSoft [10]	Windows 95/98/NT 4.0	FTP Server 1.4.1 .1	A buffer overflow vulnerability exists in the 'XCWD' command due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.argosoft.com/applications/ftpserver/download.asp	FTP Server 'XCWD' Command Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Atrise Software Company [11]	Windows	Atrise Everyfind 5.0.2	A Cross-Site Scripting vulnerability exists in the 'search.html' page due to insufficient filtering of HTML code, which could let a remote malicious user execute arbitrary code.	Update available at: http://www.atrise.com/everyfind/version.html	Atrise Everyfind 'search.html' Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Blaine R. Southam[12]	Windows	Web Weaver 0.49 beta-0.52 beta, 0.60 beta-0.63 beta, 1.0 1-1.0 6	A remote Denial of Service vulnerability exists due to a failure to log the IP address of HTTP requests that contain a long hostname.	No workaround or patch available at time of publishing.	WebWeaver Long URL Request Remote Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Brian Bassett[13]	Unix	ipmasq 3.5.10	A vulnerability exists due to use of certain improper filtering rules, which could let a remote malicious user send traffic to systems that should be restricted by the firewall.	Patches available at: http://security.debian.org/pool/updates/main/i/ipmasq/	ipmasq Incorrect Filtering Rules CVE Name: CAN-2003-0785	Medium	Bug discussed in newsgroups and websites.
DCP-Portal Com-munity[14]	Multiple	DCP-Portal 5.5	Multiple SQL Injection vulnerabilities exist due to insufficient sanitization of user-supplied URI parameters, which could let a malicious user bypass authentication, manipulate data and extract arbitrary data.	No workaround or patch available at time of publishing.	Multiple DCP-Portal SQL Injection	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Flying Dog Software[15]	Unix	Powerslave 4.3	A vulnerability exists in the 'sql_id' parameter due to insufficient validation, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Powerslave Information Disclosure	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
GameSpy [16]	Multiple	GameSpy 3D 2.62, 3D 2.63 015	A buffer overflow vulnerability exists when a 'NICK' or 'USER' command is submitted to the IRC server due to a failure to handle large replies, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	GameSpy 3d IRC Client Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[10] Securiteam, September 29, 2003.
[11] Secunia Advisory , SA9913, October 2, 2003.
[12] Bugtraq, September 24, 2003.
[13] Debian Security Advisory, DSA 389-1, September 20, 2003.
[14] Bugtraq, October 1, 2003.
[15] H Zero Seven Security Advisory, September 19, 2003.
[16] Bugtraq, September 30, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Geeklog[17]	Unix	Geeklog 1.3, 1.3.5, sr1&sr2, 1.3.7, sr1&sr2, 1.3.8, rc1&rc2 1.3.8–1	Multiple vulnerabilities exist: a vulnerability exists because several scripts do not properly validate user-supplied input, which could let a malicious user obtain unauthorized access and sensitive information; a vulnerability exists because various parameters such as 't' in 'faqman/index.php' and 'lid' in 'filemgmt/brokenfile.php' aren't properly validated, which could let a malicious user execute arbitrary HTML or script code; and a Cross-Site Scripting vulnerability due to improper validation, which could let a remote malicious user execute arbitrary code.	Workaround available at: http://www.geeklog.net/article.php?story=2003092804362257	Multiple Geeklog Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Exploit has been published.
Gnome Develop-ment Team[18]	Unix	Midnight Com-mander 4.5.52, 4.5.55, 4.6	A buffer overflow vulnerability exists because 'vfs/direntry.c' uses an uninitialized buffer for processing symbolic links in compressed archives, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Midnight Commander Symlink Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
GNU[19]	Unix	Cfengine 2.0.0-2.0.6, 2.0.7, p1-p3, 2.1.0a6, 2.1.0a8, 2.1.0a9	A buffer overflow vulnerability exists in the 'cfservd' daemon due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.cfengine.org/mirrors.html	CFServD Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Guardian Digital[20]	Unix	EnGarde Secure Community 2.0, Secure Profes-sional 1.5	A vulnerability exists in the /var/log/userpass.log file when the user creates an SSH key using WebTool-userpass, which could let a malicious user obtain sensitive information.	Update available at: http://www.linuxsecurity.com/advisories/engarde_advisory-3680.html	EnGarde WebTool Password Disclosure	Medium	Bug discussed in newsgroups and websites.
GuppY[21]	Windows, Unix	GuppY 2.4	A Cross-Site Scripting vulnerability exists in the 'postguest.php' file due to insufficient filtering of user-supplied HTML code, which could let a remote malicious user execute arbitrary code.	Patch and update available at: http://www.freeguppy.org/file/guppy_patch2.zip http://www.freeguppy.org/file/guppy.zip	GuppY Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[17] SecurityTracker Alert, 1007828, September 28, 2003.
[18] Bugtraq, September 19, 2003.
[19] Securiteam, September 29, 2003.
[20] Guardian Digital Security Advisory, ESA-20030924-026, September 24, 2003.
[21] ECHU.ORG Alert #4, September 29, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Gus! & Psilord[22]	Unix	freesweep 0.88, 0.90	A buffer overflow vulnerability exists when processing several environment variables, which could let a malicious user execute arbitrary code.	**Debian:** http://security.debian.org/pool/updates/main/f/freesweep/	freesweep Environment Variable Buffer Overflow CVE Name: CAN-2003-0828	**High**	Bug discussed in newsgroups and websites.
Hewlett Packard Company[23]	Unix	HP-UX 11.0	A Denial of Service vulnerability exists due to an unspecified error in the socket programs.	Patch available at: ftp://ftp.itrc.hp.com/export/patches/hp-ux_patch_matrix/	HP Socket Implementation Denial of Service	Low	Bug discussed in newsgroups and websites.
IBM[24]	Unix	AIX 5.1, 5.2	A local/remote Denial of Service vulnerability exists because the 'getipnodebyname()' API does not close sockets.	Patch available at: https://techsupport.services.ibm.com/server/aix.fdc	IBM AIX GetIPNodeByName API Socket Denial of Service CVE Name: CAN-2003-0697	Low	Bug discussed in newsgroups and websites.
IBM[25]	Windows, Unix	DB2 Universal Database for AIX 7.1, 7.2, HP-UX 7.1, 7.2, Linux 7.1, 7.2, Solaris 7.1, 7.2, Windows 7.1,7.2	A Denial of Service vulnerability exists in the Discover Service when a malicious user submits a UDP packet larger than 20 bytes.	Fixpack 10a for IBM DB2 version 7 on various platforms is available at: http://www-3.ibm.com/cgi-bin/db2www/data/db2/udb/winos2unix/support/download.d2w/report	DB2 Discovery Service UDP Denial of Service CVE Name: CAN-2003-0827	Low	Bug discussed in newsgroups and websites. Vulnerability can be exploited with any number of available packet shaping tools.
IBM[26]	Windows, Unix	DB2 Universal Database for Linux 7.2, 8.1, DB2 Universal Database for Windows 7.2, 8.1	A buffer overflow vulnerability exists when handling the LOAD command due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code.	Patch available at: http://www-3.ibm.com/cgi-bin/db2www/data/db2/udb/winos2unix/support/download.d2w/report	DB2 Remote LOAD Command Buffer Overrun CVE Name: CAN-2003-0836	**High**	Bug discussed in newsgroups and websites.

[22] Debian Security Advisory, DSA 391-1, September 28, 2003.
[23] Hewlett-Packard Company Security Bulletin, HPSBUX0309-283, September 29, 2003.
[24] SecurityTracker Alert, 1007849, October 1, 2003.
[25] AppSecInc Security Alert, September 19, 2003.
[26] Pentest Limited Security Advisory, October 1, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
IBM[27] ***Proof of Concept exploit published***[28]	**Unix**	**DB2 Universal Database for Linux 7.2**	**Several vulnerabilities exist: a buffer overflow vulnerability exists in the 'db2dart' utility because long strings are not handled properly, which could let a malicious user execute arbitrary code; and a buffer overflow vulnerability exists in the 'db2licm' utility because long strings are not handled properly, which could let a malicious user execute arbitrary code.**	**Patch available at: ftp://ftp.software.ibm.com/ps/products/db2/fixes/english-us/db2linuxv7/FP10a_U49517**	**DB2 'db2dart' & 'db2licm' Buffer Overflows** **CVE Names: CAN-2003-0758, CAN-2003-0759**	**High**	**Bug discussed in newsgroups and websites.** ***Proof of Concept exploit has been published.***
IBM[29]	Windows,	DB2 Universal Database for Windows 7.2	A buffer overflow vulnerability exists when specific queries are passed to the INVOKE stored procedure, which could let a remote malicious user execute arbitrary code.	Patch available at: http://www-3.ibm.com/cgi-bin/db2www/data/db2/udb/winos2unix/support/download.d2w/report	DB2 Invoke Stored Procedure Buffer Overflow CVE Name: CAN-2003-0837	**High**	Bug discussed in newsgroups and websites.
Imatix[30]	Windows NT 4.0	Xitami 2.4 d9, 2.5 b4	A remote Denial of Service vulnerability exists when a malicious user requests a .shtm file that contains an overly long HTTP header. It also may be possible for a remote malicious user to execute arbitrary code.	No workaround or patch available at time of publishing.	Xitami Long Header Remote Denial of Service	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required, however a Proof of Concept exploit script has been published.
Ingate Systems[31]	Multiple	Firewall 3.2, SIParator 3.2	A vulnerability exists because a SYN+RST packet can be sent through the firewall in the reply (return) direction when TCP packet filtering is used, which could let a remote malicious user bypass packet-filtering rules.	Upgrade available at: http://www.ingate.com/upgrades/	Ingate Firewall/ SIParator Packet Filter Rule Bypass	Medium	Bug discussed in newsgroups and websites.
Invision Power Services[32]	Windows, Unix	Invision Board 1.1.1, 1.1.2	A vulnerability exists due to incorrect permissions on folders during the installation process, which could let a malicious user modify files and execute arbitrary code.	No workaround or patch available at time of publishing.	Invision Power Board Insecure Permissions	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.

[27] Core Security Technologies Advisory, CORE-2003-0531, September 18, 2003.
[28] SecurityFocus, September 26, 2003.
[29] Pentest Limited Security Advisory, October 1, 2003.
[30] Bugtraq, September 22, 2003.
[31] SecurityFocus, September 23, 2003.
[32] SecurityTracker Alert, 1007827, September 28, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
John Walker[33]	Windows	Speak Freely 7.1, 7.5, 7.6 a, 7.6	Several vulnerabilities exist: a vulnerability exists in the 'Show Your Face' feature when processing malformed GIF images which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code; and a remote Denial of Service vulnerability exists when a malicious user submits UDP packets that contain spoofed source addresses.	The vendor has issued an 'End of Life' Announcement for Speak Freely, indicating that version 7.6a will be the last release of the product.	Speak Freely Spoofed Packet & Malformed GIF	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. 'Show Your Face' feature vulnerability may be exploited with a hex-editor or other tool that allows GIF header data to be manipulated. Spoofed UDP vulnerability may be exploited using a packet-crafting tool. A Proof of Concept exploit has been published for both vulnerabilities..
Khaled Mardam[34]	Windows	mIRC 6.01-6.03, 6.1	A buffer overflow vulnerability exists in the 'USERHOST' request due to insufficient boundary checking, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	mIRC USERHOST Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Knox Software[35]	Unix	Arkeia Pro 5.1.12 & prior	A buffer overflow vulnerability exists due to a failure to handle long specially crafted packets sent to port 617/tcp, which could let a remote malicious user obtain root privileges and execute arbitrary code.	Upgrade available at: http://www.arkeia.com/download.html	Arkeia Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Lincoln D. Stein[36]	Unix	sbox 1.0.4	A path disclosure vulnerability exists in the 'cgi-bin' script when a HTTP request is made for a nonexistent resource, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	SBox Path Disclosure	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[33] Securiteam, September 23, 2003.
[34] Securiteam, September 29, 2003.
[35] Securiteam, September 21, 2003.
[36] EightOne Research Facility Security Advisory, EORF2003-04, September 25, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Macro-media[37]	Windows NT 4.0/2000, XP, Unix	ColdFusion 5.0, MX 6.0, 6.1, MX J2EE 6.0, 6.1	A Cross-Site Scripting vulnerability exists due to missing input validation by the default 'Site-Wide Error Handler' and 'Missing Template Handler' pages, which could let a remote malicious user execute arbitrary HTML or script code.	Upgrade & patches available at: http://www.macromedia.com/devnet/security/security_zone/mpsb03-06.html	ColdFusion MX Error Handler Pages Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites.
Mah-Jong[38]	Unix	Mah-Jong 1.4	A buffer overflow vulnerability exists when large requests are handled that contain certain flags, which could let a malicious user obtain elevated privileges.	No workaround or patch available at time of publishing.	Mah-Jong Buffer Overflow	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
man[39]	Unix	man 2.3.19	A vulnerability exists in the man utility due to insufficient sanity checks before executing a user-defined compression program, which could let a malicious user execute arbitrary code.	**Conectiva:** ftp://ul.conectiva.com.br/updates	Man Utility Local Compression Program	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Mega-computing[40]	Multiple	Personal-WebServer Profes-sional 5.3.42	Several vulnerabilities exist: a Directory Traversal vulnerability exists due to the way requests for files are handled, which could let a malicious user obtain sensitive information; and a Denial of Service vulnerability exists when a malicious user submits an excessively long request.	No workaround or patch available at time of publishing.	Personal-WebServer Professional Remote Directory Traversal	Low/ Medium (Medium if sensitive informa-tion can be obtained)	Bug discussed in newsgroups and websites. Vulnerabilities may be exploited via a web browser.
Michael Speck[41]	Unix	marbles 1.0.1	A buffer overflow vulnerability exists when processing the HOME variable, which could let a malicious user execute arbitrary code.	**Debian:** http://security.debian.org/pool/updates/main/m/marbles/	Marbles Local Home Environment Variable Buffer Overflow CVE Name: CAN-2003-0830	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.

[37] Macromedia Security Bulletin, MPSB03-06, September 18, 2003.
[38] SecurityFocus, September 29, 2003.
[39] Conectiva Linux Announcement, CLSA-2003:745, September 19, 2003.
[40] SecurityFocus, September 29, 2003.
[41] Debian Security Advisory, DSA 390-1, September 26, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [42]	Windows 2000, 2003, XP	BizTalk Server 2000 Developer Edition, SP1& SP2, 2000 Enterprise Edition, SP1&SP2, 2000 Standard Edition, SP1& SP2, 2002 Developer Edition, 2002 Enterprise Edition, 2002 Partner Edition	A vulnerability exists due to a configuration error in the 'BizTalkServerDocs' and 'BizTalkServerRepository' virtual directories, which could let a remote malicious user execute arbitrary code.	Microsoft has released a knowledge base article (824935) in order to address this issue available at: http://support.microsoft.com/default.aspx?scid=kb;en-us;824935	BizTalk Server Documentation /WebDAV Weak Permissions	**High**	Bug discussed in newsgroups and websites.
Microsoft [43] ***Microsoft issued bulletin[44]***	**Windows 95/98/SE/ NT 4.0/2000, 2003**	**Internet Explorer 5.0.1, SP1-SP3, 5.5, SP1&SP2, 6.0, SP1**	**A vulnerability exists because object types are not handled properly when rendering malicious popup windows, which could let a malicious user execute arbitrary code.**	***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/MS03-040.asp**	**Internet Explorer Browser Popup Window** **CVE Name: CAN-2003-0838**	**High**	**Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.**
Microsoft [45] ***Microsoft issued bulletin[46]***	**Windows 95/98/SE/ NT. 40/2000, 2003**	**Internet Explorer 5.0.1. SP1-SP3, 5.5, SP1&SP2, 6.0, SP1**	**A vulnerability exists when rendering XML based web sites due to a failure to properly handle object types, which could let a malicious user execute arbitrary code.**	***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/MS03-040.asp**	**Internet Explorer XML Page Object Type Validation** **CVE Name: CAN-2003-0809**	**High**	**Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.**
Mondo Soft[47]	Windows NT 4.0/2000	Mondo Search 4.4, 5.0, 5.1	A vulnerability exists in the 'MsmSetup.exe' module, which could let a remote malicious user execute arbitrary code.	Workaround and patch available at: http://www.mondosoft.com/security/	MondoSearch MsmSetup.exe Remote Code Execution	**High**	Bug discussed in newsgroups and websites. Vulnerability may be exploited via a web browser.

[42] NTBugtraq, September 18, 2003.
[43] SecurityFocus, September 9, 2003.
[44] Microsoft Security Bulletin MS03-040, October 3, 2003.
[45] SecurityFocus, September 8, 2003.
[46] Microsoft Security Bulletin MS03-040, October 3, 2003.
[47] PROTEGO Security Advisory, PSA200302, September 24, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
mpg123[48]	Unix	mpg123 0.59s, 0.59r	A buffer overflow vulnerability exists in the 'readstring()' function in 'httpget.c' which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	MPG123 Remote Buffer Overflow CVE Name: CAN-2003-0577	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
MPlayer[49]	Unix	MPlayer 0.9 0rc4, 9.1, 0.90 rc series, 0.90 pre series, 0.90, 0.91, 9.2, 1.0 pre1	A buffer overflow vulnerability exists in 'asf_http_request() due to a boundary error when parsing ASX Headers, which could let a remote malicious user execute arbitrary code.	**Mandrake:** http://www.mandrakesecure.net/en/mlist.php	MPlayer Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
Multiple Vendors[50]	Unix	Olaf Titz CIPE 1.0.1, 1.1-1.3, 1.4.5, 1.4.6, 1.5.2-1.5.4; tinc 1.0 pre3-pre5, 1.0, 1.0.1; VTun 2.0-2.6	Multiple VPN implementations contain security vulnerabilities, which could let a remote malicious user perform a man-in-the-middle attack, decrypt VPN communications or abuse trust relationships.	No workaround or patch available at time of publishing.	Multiple Vendor VPN Implementation Vulnerabilities	Medium	Bug discussed in newsgroups and websites.
Multiple Vendors[51] ***Ingate releases upgrade[52]***	**Unix**	**Linux kernel 2.4.20, 2.4.21, pre7, pre4, pre1**	**A remote Denial of Service vulnerability exists due to an error when the system performs NAT (Network Address Translation) if the modules 'ip_nat_ftp' or 'ip_nat_irc' are loaded, or 'CONFIG_IP_NF_NAT_FTP' or 'CONFIG_IP_NF_NAT _IRC' is enabled.**	**Patch available at: http://downloads.securityfocus.com/vulnerabilities/patches/netfilter-ircftp-nat.patch** ***Ingate:*** **http://www.ingate.com/relnote-321.php**	**Netfilter NAT Remote Denial of Service** **CVE Name: CAN-2003-0467**	**Low**	**Bug discussed in newsgroups and websites.**

[48] Securiteam, September 24, 2003.
[49] Mandrake Linux Security Update Advisory, MDKSA-2003:097, September 30, 2003.
[50] Bugtraq, September 25, 2003.
[51] Netfilter Core Team Security Advisory, August 2, 2003.
[52] SecurityFocus, September 19, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[53]	MacOS X 10.x, Unix	OpenSSL 0.9.x	There are multiple vulnerabilities in different implementations of the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols. These vulnerabilities occur primarily in Abstract Syntax Notation One (ASN.1) parsing code, which could let a remote malicious user cause a Denial of Service or execute arbitrary code. For more information, see CERT Advisor, CA-2003-26 located at: http://www.cert.org/advisories/CA-2003-26.html.	http://www.openssl.org/news/secadv_20030930.txt **Apple:** http://docs.info.apple.com/article.html?artnum=61798 **BlueCoat:** http://www.bluecoat.com/support/knowledge/advisory_openSSL_ASN_vulnerability.html **Cisco:** http://www.cisco.com/warp/public/707/cisco-sa-20030930-ssl.shtml **Conectiva:** ftp://atualizacoes.conectiva.com.br/ **Debian:** http://security.debian.org/pool/updates/main/o/openssl/ **Engarde:** http://www.linuxsecurity.com/advisories/engarde_advisory-3693.html **F-Secure:** http://www.f-secure.com/support/technical/ssh/ssh2_digital_certificates_tech.shtml **Hewlett Packard:** ftp://hprc.external.hp.com **Immunix:** http://download.immunix.org/ImmunixOS/7+/Updates/ **Mandrake:** http://www.mandrakesecure.net/en/ftp.php **Novell:** http://support.novell.com/servlet/tidfinder/10087450 **OpenPKG:** ftp.openpkg.org **RedHat:** ftp://updates.redhat.com/ **SCO:** ftp://ftp.sco.com/pub/updates/UnixWare/ **SGI:** ftp://patches.sgi.com/support/free/security/patches/ **SmoothWall:** http://www.smoothwall.org/home/news/item/20031001.01.html **SuSE:** Ftp://ftp.suse.com/pub/suse **Tawie Server Linux:** http://http.tawie.org/pub/tawie/updates/ **TurboLinux:** ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/	Multiple Remote OpenSSL ASN.1 Parsing CVE Names: CAN-2003-0543, CAN-2003-0544, CAN-2003-0545	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.

[53] CERT Advisory CA-2003-26, October 1, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[54, 55, 56, 57] ***More updates issued***[58, 59] ***RedHat issues advisory***[60]	**Unix**	**CGI.pm 2.73-2.79, 2.93, 2.751, 2.753; Debian Linux 3.0, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; Mandrake Soft Corporate Server 2.1, 8.2, ppc, 9.0, 9.1, ppc, Single Network Firewall 7.2; OpenPKG Current, 1.2, 1.3**	**A Cross-Site Scripting vulnerability exists in the 'start_form()' function (or other functions that use this function) due to insufficient sanitization of user-supplied HTML and script, which could let a remote malicious user execute arbitrary code.**	**Conectiva:** **ftp://atualizacoes.conectiva.com.br/** **Debian:** **http://security.debian.org/pool/updates/main/p/perl/** **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** **OpenPKG:** **http://pgp.openpkg.org** ***TurboLinux:*** **http://www.turbolinux.com/update** ***SOT Linux:*** **ftp://ftp.sot.com/updates/2003** ***RedHat:*** **ftp://updates.redhat.com/**	**Multiple Vendor CGI.pm 'Start_Form' Cross-Site Scripting** **CVE Name: CAN-2003-0615**	**High**	**Bug discussed in newsgroups and websites. There is no exploit code required.**
Multiple Vendors[61, 62]	Unix	Apple MacOS X 10.2-10.2.7, MacOS X Server 10.2-10.2.7; FreeBSD 4.0-5.1	A remote Denial of Service vulnerability exists in the 'arplookup()' function because unnecessary cache ARP entries are not deleted when responding to requests.	**Apple:** http://www.info.apple.com/kbnum/ **FreeBSD:** ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-03:14/arp.patch	BSD Kernel ARP Cache Remote Denial of Service CVE Name: CAN-2003-0804	Low	Bug discussed in newsgroups and websites.

[54] Conectiva Linux Security Announcement, CLA-2003:713, July 29, 2003.
[55] OpenPKG Security Advisory, OpenPKG-SA-2003.036, August 6, 2003.
[56] Debian Security Advisory, DSA 371-1, August 12, 2003.
[57] Mandrake Linux Security Update Advisory, MDKSA-2003:084, August 20, 2003.
[58] Turbolinux Security Announcement, TLSA-2003-08-27, August 27, 2003.
[59] SOT Linux Security Advisory, SLSA-2003:38, August 27, 2003.
[60] Red Hat Security Advisory, RHSA-2003:256-01 & RHSA-2003:256-02, September 22, & October 3, 2003
[61] Apple Security Advisory, APPLE-SA-2003-09-22, September 23, 2003.
[62] FreeBSD Security Advisory, FreeBSD-SA-03:14.arp, September 23, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [63, 64, 65, 66, 67] ***Conectiva issues advisory***[68]	**Unix**	**KDE Konqueror 2.1.1, 2.2.2, 3.0-3.0.3, 3.0.5, 3.1, 3.1.1, Konqueror Embedded 0.1**	**A vulnerability exists in the 'user:password@host' form because authentication credentials are not removed from URLs in the HTTP-Referrer header, which could let a remote malicious user obtain sensitive information.**	**KDE:** **http://ftp.kde.org/pub/kde/security_patches** **Debian:** **http://security.debian.org/pool/updates/main/k/kdelibs/** **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** **RedHat:** **http://rhn.redhat.com/errata/RHSA-2003-236.html** **Slackware:** **ftp://ftp.slackware.com/pub/slackware/slackware-9.0/patches/packages/kde/*.tgz** **ftp://ftp.slackware.com/pub/slackware/slackware-9.0/patches/packages/kdei/*.tgz** ***Conectiva:*** **ftp://atualizacoes.conectiva.com.br/**	**Konqueror HTTP REFERER Authentication Disclosure** **CVE Name: CAN-2003-0459**	**Medium**	**Bug discussed in newsgroups and websites. There is no exploit code required.**

[63] Turbolinux Security Advisory, TLSA-2003-45, July 30, 2003.
[64] RedHat Security Advisories, RHSA-2003:236-08 & RHSA-2003:235-01, July 30, & August 11, 2003.
[65] Mandrake Linux Security Update Advisory, MDKSA-2003:079, July 31, 2003.
[66] Debian Security Advisories, DSA 361-1 & DSA 361-2, August 1 & 11, 2003.
[67] Slackware Security Advisory, SSA:2003-213-01, August 3, 2003.
[68] Conectiva Linux Security Announcement, CLA-2003:747, September 19, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [69, 70, 71] ***Hewlett Packard issues another advisory***[72] ***SGI issues advisory***[73]	**Windows, OpenVMS, Unix**	**Compaq OpenVMS 7.1 Alpha, 7.1 -2 Alpha, 7.1 VAX, 7.2 -2 Alpha, 7.2 -1H2 Alpha, 7.2 -1H1 Alpha, 7.2 VAX, 7.2 Alpha, 7.2.1 Alpha, 7.3 VAX, Alpha, Tru64 5.0 a, 5.1 a, 5.1; Cray UNICOS 6.0 E, 6.0, 6.1, 7.0, 8.0, 8.3, 9.0, 9.0.2.5, 9.2.4 , 9.2, UNICOS MAX 1.3.5, 1.3, UNICOS/ mk 1.5, 1.5.1, 2.0.5.54; Entegrity DCE/DFS for Linux 2.1, DCE/DFS for Tru64 Unix 4.1.6, 4.2.2, PC-DCE for Windows 4.0.8, 5.0.1; HP HP-UX 10.20, 11.0; IBM DCE 2.2 for Windows, 3.1 for Solaris, AIX, 3.2 for Solaris, AIX**	**A remote Denial of Service vulnerability exists in multiple vendor OSF DCE (Distributed Computer Environment) implementations.**	**Entegrity:** **http://support.entegrity.com/private/patches/dce/rpcattacks.shtml** **Hewlett Packard:** **http://itrc.hp.com** **Patch PHSS_19739, Patch PHSS_17810** **IBM:** **ftp://ftp.software.ibm.com/software/network/dce/support/ifixes/** ***SGI:*** ftp://patches.sgi.com/support/free/security/advisories/20030902-01-P.asc	**Multiple Vendor OSF Distributed Computing Environment Remote Denial of Service**	**Low**	**Bug discussed in newsgroups and websites. There is no exploit code required.**

[69] CERT/CC Vulnerability Note, VU#377804, August 8, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [74, 75, 76, 77, 78, 79, 80, 81] ***More advisories issued***[82, 83]	**Unix**	**Sendmail 8.12.9 & prior**	**A buffer overflow vulnerability exists when parsing non-standard rulesets, which could possibly let a remote malicious user execute arbitrary code.**	**SendMail:** ftp://ftp.sendmail.org/pub/sendmail/ **Conectiva:** ftp://atualizacoes.conectiva.com.br/ **Debian:** http://security.debian.org/pool/updates/main/s/sendmail/ **Immunix:** http://download.immunix.org/ImmunixOS/7+/Updates/RPMS/ **OpenPKG:** ftp://ftp.openpkg.org/release/ **RedHat:** ftp://updates.redhat.com/ **Slackware:** ftp://ftp.slackware.com/pub/slackware/ **TurboLinux:** Ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ **YellowDog:** ftp://ftp.yellowdoglinux.com/pub/yellowdog/updates/yellowdog-3.0/ ***Hewlett Packard:*** ftp://hprc.external.hp.com ***Sun:*** http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F56922	**Sendmail Ruleset Parsing Buffer Overflow** **CVE Name: CAN-2003-0681**	**High**	**Bug discussed in newsgroups and websites.**

[70] Hewlett-Packard Company Security Bulletin, HPSBUX0308-273, August 13, 2003.
[71] Hewlett-Packard Company Software Security Response Team, SSRT3608, August 15, 2003.
[72] Hewlett-Packard Company Security Bulletins, HPSBUX0308-274 & HPSBUX0309-276, August 26, Sept 2, 2003.
[73] SGI Security Advisory, 20030902-01-P, September 26, 2003.
[74] Debian Security Advisory. DSA 384-1, September 17, 2003.
[75] Immunix Secured OS Security Advisory, IMNX-2003-7+-021-01, September 17, 2003.
[76] Yellow Dog Linux Security Announcement, YDU-20030917-2, September 17, 2003.
[77] Slackware Security Advisory, SSA:2003-260-02, September 17, 2003.
[78] Conectiva Linux Security Announcement, CLA-2003:742 , September 18, 2003.
[79] TurboLinux Security Advisor, TLSA-2003-52, September 18, 2003.
[80] Red Hat Security Advisory, RHSA-2003:283-01, September 18, 2003.
[81] OpenPKG Security Advisory, OpenPKG-SA-2003.041, September 19, 2003.
[82] Hewlett-Packard Company Security Bulletin, HPSBUX0309-281, September 29, 2003.
[83] Sun(sm) Alert Notification, 56922, September 30, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [84, 85, 86, 87, 88, 89, 90, 91, 92, 93] ***More advisories issued***[94, 95, 96, 97]	**Windows NT 4.0/2000, MacOS X 10.x, Unix**	**Systems running open-source SendMail versions prior to 8.12.10, Com-mercial releases of Sendmail including Sendmail Switch, Advanced Message Server (SAMS), & Sendmail for NT**	**A buffer overflow vulnerability exists in the 'prescan()' function, which could let local/remote malicious user execute arbitrary code.**	**SendMail:** **ftp://ftp.sendmail.org/pub/sendmail/** **Conectiva:** **ftp://atualizacoes.conectiva.com.br/** **Debian:** **http://security.debian.org/pool/updates/main/s/sendmail/** **FreeBSD:** **ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-03:13/sendmail.patch** **Immunix:** **http://download.immunix.org/ImmunixOS/7+/Updates/RPMS/** **OpenPKG:** **ftp://ftp.openpkg.org/** **RedHat:** **ftp://updates.redhat.com** **Slackware:** **Ftp://ftp.slackware.com/pub/slackware/slackware-9.0/patches/packages/** **SuSE:** **ftp://ftp.suse.com/pub/suse** **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** **YellowDog:** **ftp://ftp.yellowdoglinux.com/pub/yellowdog/updates/yellowdog-3.0/** ***Hewlett Packard:*** **Ftp://hprc.external.hp.com** ***IBM:*** **ftp://aix.software.ibm.com/aix/efixes/security/sendmail_4_efix.tar.Z** ***SGI:*** **ftp://patches.sgi.com/support/free/security/advisories/20030903-01-P.asc** ***Sun:*** **http://sunsolve.sun.com/pub-cgi/**	**Sendmail Prescan() Buffer Overflow** **CVE Name: CAN-2003-0694**	**High**	**Bug discussed in newsgroups and websites.**

[84] Debian Security Advisory, DSA 384-1, September 17, 2003.
[85] FreeBSD Security Advisory, FreeBSD-SA-03:13, September 17, 2003.
[86] Slackware Security Advisory, SSA:2003-260-02, September 17, 2003.
[87] Yellow Dog Linux Security Announcement, YDU-20030917-2, September 17, 2003.
[88] Conectiva Linux Security Announcement, CLA-2003:742, September 18, 2003.
[89] Immunix Secured OS Security Advisory, IMNX-2003-7+-021-01, September 18, 2003.
[90] Red Hat Security AdvisoryRHSA-2003:283-01, September 18, 2003.
[91] TurboLinux Security Advisory, TLSA-2003-52, September 18, 2003.
[92] OpenPKG Security Advisory, OpenPKG-SA-2003.041, September 19, 2003.
[93] SuSE Security Announcement, SuSE-SA:2003:040, September 20, 2003.
[94] SGI Security Advisory, 20030903-01-P, September 29, 2003.
[95] Hewlett-Packard Company Security Bulletin, HPSBUX0309-281, September 29, 2003.
[96] IBM, MSS-OAR-E01-2003:1235.1, September 28, 2003.
[97] Sun(sm) Alert Notification, 56860 & 56922, September 30, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Mutant Penguin Software[98]	Windows	MPNews Pro 2.1 .0.18	A Directory Traversal vulnerability exists due to a failure to filter specific dot-dot-slash sequences, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	MPNews PRO Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
MyPHP Nuke[99]	Unix	MyPHP Nuke 1.8.8	A vulnerability exists in the 'auth.in.php' module due to insufficient sanitization of user-supplied data, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	myPHPNuke 'auth.inc.php' SQL Injection	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
myServer [100]	Windows	myServer 0.4.3	A Directory Traversal vulnerability exists which could let a remote malicious user obtain sensitive information.	Upgrade available at: http://sourceforge.net/project/showfiles.php?group_id=63119	myServer Information Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability may be exploited via a web browser.
MySQL AB[101, 102, 103] ***More advisories issued[104, 105, 106, 107]***	**Unix**	**MySQL 3.23 .x, 3.23.2-3.23.5, 3.23.8-3.23.10, 3.23.22-3.23.34, 3.23.36-3.23.56, 4.0.0-4.0.14. 4.1.0-alpha, 4.1 .0-0**	**A buffer overflow vulnerability exists when handling user passwords of excessive size due to insufficient bounds checking, which could let a malicious user execute arbitrary code.**	**Patch available at: http://www.mysql.com/downloads/mysql-4.0.html** **Debian: http://security.debian.org/pool/updates/main/m/mysql/** **OpenPKG: Ftp://ftp.openpkg.org/release/** **Trustix: http://www.trustix.net/pub/Trustix/updates/** ***Conectiva:*** **ftp://atualizacoes.conectiva.com.br/** ***Engarde:*** **http://www.linuxsecurity.com/advisories/engarde_advisory-3650.html** ***Mandrake:*** **http://www.mandrakesecure.net/en/ftp.php** ***SuSE:*** **ftp://ftp.suse.com/pub/suse**	**MySQL Password Handler Buffer Overflow** **CVE Name: CAN-2003-0780**	**High**	**Bug discussed in newsgroups and websites. Proof of Concept exploit has been published. An exploit script has also been published.**

[98] SecurityFocus, October 1, 2003.
[99] Bugtraq, September 20, 2003.
[100] SecurityTracker Alert, 1007816, September 26, 2003.
[101] Debian Security Advisory, DSA 381-1, September 14, 2003.
[102] OpenPKG Security Advisory, OpenPKG-SA-2003.038, September 15, 2003.
[103] Trustix Secure Linux Security Advisory, TSLSA-2003-09-17, September 17, 2003.
[104] Conectiva Linux Security Announcement, CLA-2003:743, September 18, 2003.
[105] Guardian Digital Security Advisory, ESA-20030918-025, September 18, 2003.
[106] Mandrake Linux Security Update Advisory, MDKSA-2003:094, September 18, 2003.
[107] SuSE Security Announcement, SuSE-SA:2003:042, October 1, 2003

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
NetUP Systems [108]	Windows NT 4.0/2000, XP, Unix	NetUp UTM 3.0, 4.0	Multiple vulnerabilities exist: a vulnerability exists in the 'admin' and 'utm_stat' scripts due to insufficient validation of the user-supplies 'sid' parameter, which could let a remote malicious user execute arbitrary code; a vulnerability exists due to a failure to properly verify the 'lang' parameter, which could let a remote malicious user modify sensitive information; a vulnerability exists due to a failure to verify parameters that are passed to executables such as 'ipchains' or 'ipfw,' which could let a malicious user execute arbitrary code; a vulnerability exists in the 'dict' table because the configuration settings can be altered, which could let a remote malicious user modify sensitive information; and a vulnerability exists in the '/bin/mv' utility, which could let a remote malicious user obtain root privileges.	No workaround or patch available at time of publishing.	NetUP UTM Multiple Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed or root privileges obtained)**	Bug discussed in newsgroups and websites. There is no exploit code required.
Niels Moller[109]	Unix	GNU LSH 1.4, 1.4.1, 1.4.2	A buffer overflow vulnerability exists due to a boundary error in 'read_line.c' when checking for errors, which could let a remote malicious user execute arbitrary code.	Upgrade available at: Http://www.lysator.liu.se/~nisse/archive/	LSH Remote Buffer Overflow CVE Name: CAN-2003-0826	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
Novell[110]	Multiple	NetWare 5.1, SP1-SP6	A vulnerability exists due to a lack of user authentication when accessing the Broker, which could let a malicious user obtain sensitive information.	Workaround available at: http://support.novell.com/cgi-bin/search/searchtid.cgi?/10087316.htm	NetWare Broker Information Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[108] Secunia Advisory, SA9831, September 24, 2003.
[109] Bugtraq, September 19, 2003.
[110] Novell Technical Information Document, TID10087316, September 26, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
NullLogic [111]	Windows, Unix	Null HTTPd 0.5.1	Two vulnerabilities exist: a Cross-Site Scripting vulnerability exists when displaying error pages, which could let a remote malicious user execute arbitrary HTML or script code; and a remote Denial of Service vulnerability exists when a malicious user submits multiple HTTP POST requests that contain less data than specified in the "Content-Length."	No workaround or patch available at time of publishing.	Null HTTPd Cross-Site Scripting & Denial of Service	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.
OmniCom [112]	Windows	winShadow 2.0	Several vulnerabilities exist: a vulnerability exists because the server can't handle long usernames or passwords, which could let a remote malicious user cause a Denial of Service or possibly execute arbitrary code; and a buffer overflow vulnerability exists when handling the 'hostname' parameter in session files, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	winShadow Remote Denial of Service & Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Exploits have been published.
OpenSSH [113, 114, 115, 116]	Unix	OpenSSH 3.7 p1, 3.7.1 p1	Multiple vulnerabilities exist in the Portable OpenSSH PAM support implementation: a vulnerability exists when Privilege Separation is disabled due to insufficient authentication checking, which could let a remote malicious user obtain root access; and a vulnerability exists because an array of structures is interpreted as an array of pointers, which could let a remote malicious user obtain elevated privileges.	Upgrade available at: http://www.openssh.org/portable.html **OpenPKG:** ftp.openpkg.org **Slackware:** ftp://ftp.slackware.com/pub/slackware **TurboLinux:** ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/ **Sun Microsystems:** http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F56862	Multiple Portable OpenSSH PAM Vulnerabilities CVE Names: CAN-2003-0786, CAN-2003-0787	Medium/ **High** **(High if root access can be obtained)**	Bug discussed in newsgroups and websites.

[111] Secunia Advisory, SA9845, September 25, 2003.
[112] Securiteam, October 2, 2003.
[113] OpenPKG Security Advisory, OpenPKG-SA-2003.042, September 24, 2003.
[114] Slackware Security Advisory, SSA:2003-266-01, September 24, 2003.
[115] Turbolinux Security Advisory, TLSA-2003-53, September 24, 2003.
[116] Sun(sm) Alert Notification, 56862, September 24, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
PHP[117]	MacOS X 10.x, Unix	PHP 4.0, 4.0.1, pl1&pl2, 4.0.2-4.0.6, 4.0.7, rc1-rc3, 4.1.0-4.1.2, 4.2.0-4.2.3, 4.3-4.3.2	A vulnerability exists in the 'base64_encode()' function due to an unsigned integer value wrapping to a value of zero, which could let a malicious user corrupt sensitive information.	Upgrade available at: http://www.php.net/ **Conectiva:** ftp://atualizacoes.conectiva.com.br/	PHP4 Base64_ Encode() Integer Overflow	Medium	Bug discussed in newsgroups and websites.
phpBB Group[118] ***Fix now available*** [119]	**Windows, Unix**	**phpBB 2.0.6**	**A Cross-Site Scripting vulnerability exists in the '[url]' BBCode tag due to insufficient sanitization of user-supplied URL BBCode tags, which could let a remote malicious user execute arbitrary code.**	***Patch available at:*** **http://www.phpbb.com/phpBB/viewtopic.php?t=135116**	**PHPBB URL BBCode Cross-Site Scripting**	**High**	**Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.**
Pierre Chifflier [120]	Windows 2000, XP, Unix	wzdftpd 0.1 rc5	A remote Denial of Service vulnerability exists when a malicious user submits a single CRLF character during the login process.	Update available at: http://www.wzdftpd.net/design2/download.html	wzdftpd Login Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Plug and Play Software [121]	Windows NT 4.0/2000, XP	Web Server 1.0 002c	Multiple buffer overflow vulnerabilities exist when FTP commands arguments that are of excessive size are submitted, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code.	No workaround or patch available at time of publishing.	Multiple Web Server Remote Buffer Overflows	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
Postgre SQL[122]	Unix	Postgre SQL 7.2-7.2.4, 7.3-7.3.3	A buffer overflow vulnerability exists in the 'PostgreSQL to_ascii()' function, which could let a malicious user execute arbitrary code.	Upgrade available at: http://www.postgresql.org/	PostgreSQL To_Ascii() Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

[117] Conectiva Linux Security Announcement, CLA-2003:749, September 24, 2003.
[118] Bugtraq, September 8, 2003.
[119] SecurityFocus, September 18, 2003.
[120] Moozatech Advisory, September 23, 2003.
[121] Securiteam, September 21, 2003.
[122] SecurityFocus, October 1, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
ProFTPD Project[123, 124, 125, 126, 127, 128, 129,]	Unix	ProFTPD 1.2.7, rc1-rc3, 1.2.8, rc1&rc2, 1.2.9 rc1&rc2	A buffer overflow vulnerability exists due to the way incoming ACSII transfer files are handled, which could let a remote malicious user execute arbitrary code.	Upgrade available at: ftp://ftp.proftpd.org/ **Conectiva:** ftp://atualizacoes.conectiva.com.br/9/ **Mandrake:** http://www.mandrakesecure.net/en/advisories/ **OpenPKG:** ftp://ftp.openpkg.org/release **TurboLinux:** ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/ **Trustix:** http://www.trustix.net/pub/Trustix/updates/ **Slackware:** http://www.slackware.org/security/viewer.php?l=slackware-security&y=2003&m=slackware-security.392320	ProFTPD ASCII File Transfer Remote Buffer Overflow CVE Name: CAN-2003-0831	**High**	Bug discussed in newsgroups and websites.
Re-Boot Design[130]	Windows	ASP Forum 1.1	A vulnerability exists due to insufficient validation of user-supplied input, which could let a remote malicious user obtain unauthorized access.	No workaround or patch available at time of publishing.	ASP Forum SQL Injection	Medium	Bug discussed in newsgroups and websites.
Savant[131]	Windows	Savant Webserver 3.1	A Denial of Service vulnerability exists when a malicious user submits a specially crafted HTTP GET request.	No workaround or patch available at time of publishing.	Savant Web Server Denial of Service	Low	Bug discussed in newsgroups and websites. Vulnerability may be exploited via a web browser, however, a Proof of Concept exploit has been published.
Secure Comput-ing[132]	Unix	Gauntlet Firewall for Unix 6.0	A remote Denial of Service vulnerability exists in 'sql-gw' when a malicious user submits multiple requests that contain invalid data.	No workaround or patch available at time of publishing.	Gauntlet Firewall 'SQL-GW' Connection Remote Denial of Service	Low/**High** **(High if DDoS best practices not in place)**	Bug discussed in newsgroups and websites. Exploit has been published.

[123] Internet Security Systems Security Advisory, September 23, 2003.
[124] Slackware Security Advisory, SSA:2003-259-02, September 23, 2003.
[125] Conectiva Linux Security Announcement, CLA-2003:750, September 29, 2003.
[126] Mandrake Linux Security Update Advisory, MDKSA-2003:095, September 29, 2003.
[127] OpenPKG Security Advisory, OpenPKG-SA-2003.043, September 29, 2003.
[128] Trustix Secure Linux Security Advisory, TSLSA-2003-0037, September 29, 2003.
[129] Turbolinux Security Advisory, TLSA-2003-54, September 30, 2003.
[130] Bugtraq, September 24, 2003.
[131] Secunia Advisory, SA9852, September 26, 2003.
[132] SecurityTracker Alert, 1007799, September 24, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
SepCity[133]	Windows NT	Community Wizard 5.1	A vulnerability exists in the authentication process due to missing input validation in 'login.asp,' which could let a remote malicious user obtain sensitive information and administrative privileges.	Update available at: http://www.commwiz.com/fldesoft.asp?ID=24&CatID=3&SubCatID=0	Community Wizard 'login.asp' Authentication Bypass	**High**	Bug discussed in newsgroups and websites.
Silly Poker[134]	Unix	Silly Poker 0.25.5	A buffer overflow vulnerability exists in the HOME environment variable due to insufficient bounds checking, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Silly Poker HOME Environment Variable Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
SMC[135]	Multiple	SMC2404 WBR, SMC7004 VWBR 1.21a, SMC7004 VWBR 1.22, SMC7004 VWBR 1.23	A remote Denial of Service vulnerability exists when a malicious user submits UDP packets randomly to ports 0-65000.	No workaround or patch available at time of publishing.	SMC Router Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Software 602[136]	Windows 98/ME/NT 4.0/2000, XP	602Pro LAN SUITE 2003	Multiple vulnerabilities exist: a vulnerability exists because 'GetFile' requests are not properly validated, which could let a remote malicious user obtain sensitive information; and a vulnerability exists in the '/mail' folder because a remote malicious user can obtain sensitive information.	Patch available at: http://download3.software602.com/ls2003.exe	602Pro LAN SUITE 2003 Information Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required, however, a Proof of Concept exploits have been published.
Software 602[137]	Windows 98/ME/NT 4.0/2000, XP	602Pro LAN SUITE 2002, 2003	Several vulnerabilities exist which could let an unauthorized remote malicious user obtain elevated privileges and access.	No workaround or patch available at time of publishing.	602Pro LAN SUITE 2003 Multiple Remote Vulnerabilities	Medium	Bug discussed in newsgroups and websites.
Sun Micro-systems, Inc.[138]	Unix	StorEdge 3310 SCSI Array, StorEdge T3	A vulnerability exists due to the way specific types of network traffic are handled by Sun StorEdge T3 systems, which could let remote malicious user cause a Denial of Service.	Workaround available at: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F26464	Sun StorEdge T3 Security Scan Master Controller Failure	Low	Bug discussed in newsgroups and websites. Vulnerability may be exploited with free publicly available software.

[133] Securiteam, September 21, 2003.
[134] Bugtraq, September 30, 2003.
[135] SecurityFocus, September 30, 2003.
[136] Bugtraq, September 24, 2003.
[137] Bugtraq, September 25, 2003.
[138] Sun(sm) Alert Notification, 26464, September 24, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Sun Micro-systems, Inc.[139]	Unix	Solaris 8.0, 8.0_x86, 9.0, 9.0_x86	A Denial of Service vulnerability exists when handling excessive quantities of output data.	Patch available at: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F56820	Solaris Excessive Output Data Denial of Service	Low	Bug discussed in newsgroups and websites.
Sun Micro-systems, Inc.[140]	Unix	Java JRE 1.3.x, 1.4.x, SDK 1.3.x, SDK 1.4.x	A remote Denial of Service vulnerability exists because JAXP can't handle XML documents that contain deeply nested entity definitions.	Update available at: http://java.sun.com/j2se/1.4.2/download.html	Java XML Document Nested Entity Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Sun Micro-systems, Inc.[141]	Multiple	Perfor-mance Suite 4.0, Utilization Suite 4.0	A Denial of Service vulnerability exists in the SAM-FS file system implementation when applications create large files and subsequently truncate to a non-zero file.	Patches available at: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F56920	Sun SAM-FS File System Denial of Service	Low	Bug discussed in newsgroups and websites.
Sun Micro-systems, Inc.[142]	Unix	ONE Application Server 7.0 Standard Edition, 7.0 Platform Edition	A vulnerability exists when authenticating against LDAP, which could let a malicious user obtain unauthorized access.	Upgrades available at: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F55460	Sun One Application Server LDAP Unauthorized Access	Medium	Bug discussed in newsgroups and websites.
TCLHttpd[143]	Unix	TCLHttpd 3.4.2	Multiple vulnerabilities exist: a vulnerability exists in the 'dirlist.tcl' script due to insufficient validation of user-supplied paths when performing directory listings, which could let a remote malicious user obtain sensitive information; and multiple Cross-Site Scripting vulnerabilities exist in the 'Debug' module (enabled by default) and other modules (including the Status, Mail, and Admin modules) due to insufficient filtering of HTML code from user-supplied input, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	TCLHttpd Information Disclosure & Cross-Site Scripting	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required for the information disclosure vulnerability. Bug discussed in newsgroups and websites. Proof of Concept exploits have been published for the Cross-Site Scripting vulnerabilities.

[139] Sun(sm) Alert Notification, 56820, September 26, 2003.
[140] Secunia Advisory, SA9797, September 22, 2003.
[141] SecurityFocus, September 25, 2003.
[142] Sun(sm) Alert Notification, 55460, September 25, 2003.
[143] Securiteam, October 1, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Univer-sity of Minne-sota[144] ***This software is no longer main-tained[145]*** ***Debian issues advisory[146]***	**Unix**	**gopherd 1.12, 2.0.3, 2.0.4, 2.3, 2.3.1, 3.0.0-3.0.5**	**Two vulnerabilities exist: a buffer overflow vulnerability exists in the 'GopherFile()' function, which could let a remote malicious user execute arbitrary code; and a buffer overflow vulnerability exists in the 'GSisText()' function, which could let a remote malicious user execute arbitrary code.**	***All users of gopherd are advised to immediately upgrade to PyGopherds as UMN gohperd has been removed from distribution and is no longer supported.*** **http://quux.org/devel/gopher/pygopherd** ***It is important to note that all versions of gopherd currently deployed now have known security holes.*** ***Debian:*** http://security.debian.org/pool/updates/main/g/gopher/	**GopherD Buffer Overflows** **CVE Name: CAN-2003-0805**	**High**	**Bug discussed in newsgroups and websites. Exploit scripts have been published.**
Valve Software[147]	Windows 95/98/SE/ NT 4.0	Half-Life 1.1.0.9, 1.1.0.8, 1.1.0.4 Windows, 1.1.1 .0	A format string vulnerability exists when an invalid command is issued to the server and an error response is returned, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Half-Life Format String	**High**	Bug discussed in newsgroups and websites.
Washing-ton University[148]	Unix	wu-ftpd 2.5.0, 2.6.0-2.6.2	A buffer overflow vulnerability exists in the 'SockPrintf()' function due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code.	**Slackware:** ftp://ftp.slackware.com/pub/slackware/	Wu-Ftpd SockPrintf() Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Webfs[149]	Unix	WebFS 1.1.7-1.1.9, 1.17	Several vulnerabilities exist: an information disclosure vulnerability exists due to insufficient sanitization of user-supplied hostnames when accessing virtual hosts, which could let a malicious user obtain sensitive information; and a buffer overflow vulnerability in 'ls.c' when processing very long file names, which could let a malicious user execute arbitrary code.	Patch available at: http://bytesex.org/misc/webfs_1.20.tar.gz **Debian:** http://security.debian.org/pool/updates/main/w/webfs/	Webfs Information Disclosure & Buffer Overflow CVE Names: CAN-2003-0832, CAN-2003-0833	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required for the information disclosure vulnerability.

[144] Bugtraq, July 12, 2003.
[145] Bugtraq, August 18, 2003.
[146] Debian Security Advisory DSA 387-1, September 18, 2003.
[147] SecurityFocus, September 29, 2003.
[148] Slackware Security Advisory, SSA:2003-259-03, September 23, 2003.
[149] Debian Security Advisory, DSA 392-1, September 29, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
WeOnly Do! Software [150]	Windows	WodFTP Server 1.1 .0.4	A buffer overflow vulnerability exists due to a boundary error when handling input supplied to various FTP commands, which could let a remote malicious user execute arbitrary code.	Update available at: http://www.weonlydo.com/index.asp?showform=FTPServer	WodFTPServer FTP Command Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
XFree86 [151]	Unix	XFree86 X11R6 4.3	A buffer overflow vulnerability exists in the 'XLOCALEDIR' environment variable due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	XFree86 'XLOCAL EDIR' Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
yMonda Limited[152]	Windows	Comment Board 1.0 u	Cross-Site Scripting vulnerabilities exist due to missing validation of input supplied to the 'Topic Title,' 'Name,' and 'Message' fields, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Comment Board Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
yMonda Limited[153]	Windows	Thread-IT Message Board 1.6	Cross-Site Scripting vulnerabilities exist due to missing validation of input supplied to the 'Topic Title,' 'Name,' and 'Message' fields, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Thread-IT Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
yMonda Limited[154]	Windows	Thread-ITSQL 2.0	Cross-Site Scripting vulnerabilities exist due to missing validation of input supplied to the 'Topic Title,' 'Name,' and 'Message' fields, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Thread-ITSQL Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Yong-guang Zhang[155]	Unix	Debian hztty 2.0-5.2	Two buffer overflow vulnerabilities exist in the hztty program that translates Chinese character encoding in a terminal session due to insufficient bounds checking, which could let a malicious user execute arbitrary code.	Upgrades available at: http://security.debian.org/pool/updates/main/h/hztty/	Debian hztty Multiple Buffer Overflow Vulnerabilities CVE Name: CAN-2003-0783	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.

[150] Secunia Advisory, SA9837, September 24, 2003.
[151] SecurityFocus, September 23, 2003.
[152] SecurityTracker Alert, 1007811, September 25, 2003.
[153] SecurityTracker Alert, 1007803, September 24, 2003.
[154] Secunia Advisory, SA9843, September 24, 2003.
[155] Debian Security Advisory, DSA 385-1, September 18, 2003.

*"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 September 21 and October 1, 2003, 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, 27 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
October 1, 2003	**c-sillyPoker.c**	**Proof of Concept exploit for the Silly Poker HOME Environment Variable Buffer Overflow vulnerability.**
October 1, 2003	**winshadow.txt**	**Exploit for the winShadow Remote Denial of Service & Buffer Overflow vulnerability.**
October 1, 2003	**winshadow.zip**	**Exploit for the winShadow Remote Denial of Service & Buffer Overflow vulnerability.**
September 30, 2003	MPlayer_POC.txt	Exploit for the MPlayer Remote Buffer Overflow vulnerability.
September 30, 2003	**zonealarm-udp-dos.pl**	**Perl script that exploits the SMC Router Remote Denial of Service vulnerability.**
September 29, 2003	cfengine.c	Script that exploits the CFServD Remote Buffer Overflow vulnerability.
September 29, 2003	cnex.c	Script that exploits the CFServD Remote Buffer Overflow vulnerability.
September 29, 2003	**mj-server-ex.c**	**Script that exploits the Mah-Jong Buffer Overflow vulnerability.**
September 29, 2003	nikto-1.31.tar.gz	A PERL, open source web server scanner that supports SSL.
September 29, 2003	packetp-0.4.1.tar.gz	A library that provides a portable API for intercepting, rewriting, and otherwise mangling flows of packets. It provides multiple mechanisms through the same interface for tweaking these packets, all without the local host's kernel being aware, or requiring any kernel modules.
September 29, 2003	shatterSEH3.txt	Version three of this paper discusses more shatter attacks that are possible using progress bars.
September 29, 2003	stegtunnel-0.4.tar.gz	A tool written to hide data within TCP/IP header fields that was designed to be undetectable, even by people familiar with the tool.

Date of Script (Reverse Chronological Order)	Script name	Script Description
September 26, 2003	c-marbles.c	Script that exploits the Marbles Local Home Environment Variable Buffer Overflow vulnerability.
September 26, 2003	DSR-cfengine.pl	Script that exploits the CFServD Remote Buffer Overflow vulnerability.
September 26, 2003	IBM-DB2-db2licm.c	Script that exploits the DB2 'db2licm' Buffer Overflow vulnerability.
September 26, 2003	**smc2404WBR.txt**	**Exploit for the SMC Router Remote Denial of Service vulnerability.**
September 25, 2003	**atphttp0x06.c**	**Script that exploits the Athttpd Remote Buffer Overflow vulnerability.**
September 23, 2003	wzdftpd_dos.pl	Perl script that exploits the Login Remote Denial of Service vulnerability.
September 23, 2003	**xmpg123.c**	**Script that exploits the MPG123 Remote Buffer Overflow vulnerability.**
September 22, 2003	lsh_exploit.c	Script that exploits the LSH Remote Buffer Overflow vulnerability.
September 22, 2003	**xitami-shtm-dos.pl**	**Perl script that exploits the Xitami Long Header Remote Denial of Service vulnerability.**
September 21, 2003	0x333hztty.c	Script that exploits the Debian hztty Multiple Buffer Overflow Vulnerabilities.
September 21, 2003	0x4553-silencer-public.tgz	Silencer holds three different functionalities. It will deploy a backdoor in a listening service that a malicious user must connect to, feed the magic word, and then portscan the machine to find the bindshell spawned, it has an Apache backdoor that allows a connection over HTTP to drop to a shell, and it also has a read sniffer built in that goes through the kernel read() process and then logs it to /tmp/.es.rox.
September 21, 2003	amap-4.3.tar.gz	A next-generation scanning tool that allows you to identify the applications that are running on a specific port. It does this by connecting to the port(s) and sending trigger packets.
September 21, 2003	ark_sink.c	Script that exploits the Arkeia Remote Buffer Overflow vulnerability.
September 21, 2003	netris-shash.c	Remote exploit for Netris version 0.5 on RedHat 8.0 that makes use of a buffer overflow vulnerability.
September 21, 2003	nmap-3.45.tgz	A utility for port scanning large networks, although it works fine for single hosts.
September 21, 2003	**ppftpdos.pl**	**Perl script that exploits the Plug & Play Web Server Remote Buffer Overflow vulnerability.**

Trends

- **The National Cyber Security Division (NCSD) of the Department of Homeland Security (DHS) / Information Analysis and Infrastructure Protection (IAIP) Directorate has issued an advisory in consultation with the Microsoft Corporation to heighten awareness of potential Internet disruptions resulting from the possible spread of malicious software exploiting the Microsoft Operating Systems' Remote Procedure Call Server Service (RPCSS) vulnerability. For more information, see "Bugs, Holes & Patches" Table and advisory located at: http://www.nipc.gov/warnings/advisories/2003/Advisory9102003.htm. The Microsoft advisory is located at: http://www.microsoft.com/security/security_bulletins/ms03-039.asp. Tools have been developed to exploit this vulnerability and there is an increased likelihood that new viruses will emerge soon.**

- **The CERT/CC has noticed an increase in traffic directed at port 554/tcp. This port is used by the Real Time Streaming Protocol (RTSP). This activity may be related to a recently discovered vulnerability in Real Networks' Media Server. For more information see" Helix Universal Server Remote Buffer Overflow" entry in the "Bugs, Holes & Patches" Table. A new worm that exploits the same security weakness as the Blaster worm (also known as "lovsan" or "msblast") has been released on the Internet. This new worm, dubbed "nachi," "welchia," or "msblast.d" does not infect systems that have been updated to counter the Blaster worm in accordance with Microsoft's instructions http://www.microsoft.com/security/incident/blast.asp. This new worm will re-infect computers that are currently infected with Blaster or one of its variants. It deletes the original worm, patches the system by downloading the update from Microsoft, and replaces the original worm with itself. For more information see Department of Homeland Security advisory located at: http://www.nipc.gov/warnings/advisories/2003/Advisory8182003.htm**
- **The DHS/Information Analysis and Infrastructure Protection (IAIP) National Cyber Security Division (NCSD) has issued a second update to the security advisory on Microsoft's DCOM RPC Buffer Overflow vulnerability. Malicious code dubbed "MSBLAST," "LOVSAN," or "BLASTER" began circulating on the Internet on August 11th. This worm takes advantage of the vulnerability discussed in Microsoft's advisory located at: http://www.microsoft.com/technet/security/bulletin/MS03-026.asp and contains code that will target Microsoft's update servers on August 16th. This additional attack could cause significant Internet-wide disruptions. It is also possible that other worms based on this vulnerability will be released over the next few days as "copy cat" attacks. Also numerous exploits and Trojans have been reported in the wild that exploit this vulnerability. Please ensure that you have applied the Microsoft patch for this vulnerability.**
- **Online vandals are using a program to compromise Windows servers and remotely control them through Internet relay chat (IRC) networks. Several programs, including one that exploits a recent vulnerability in computers running Windows, have been cobbled together to create a remote attack tool. The tool takes commands from a malicious user through the IRC networks and can scan for and compromise computers vulnerable to the recently discovered flaw in Windows The CERT/CC has received reports of systems being compromised by two recently discovered vulnerabilities in the Microsoft Remote Procedure Call (RPC) service. Additionally, the CERT/CC has received reports of widespread scanning for systems with open Microsoft RPC ports (135, 139, 445). For more information, see "Exploitation of Microsoft RPC Vulnerabilities" located at: http://www.cert.org/current/.**
- **The Department of Homeland Security (DHS) / Information Analysis and Infrastructure Protection (IAIP) National Cyber Security Division (NCSD) has issued an advisory in consultation with the Microsoft Corporation to heighten awareness of potential Internet disruptions resulting from the possible spread of malicious software exploiting a vulnerability in popular Microsoft Windows operating systems. DHS expects that exploits are being developed for malicious use. For more information see, "Bugs, Holes & Patches" Table "Windows DCOM RPC Buffer Overflow" and DHS/IAIP Advisory located: http://www.nipc.gov/warnings/advisories/2003/Potential72403.htm. Additional information on the Microsoft vulnerability may also be found at: http://microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-026.asp.**

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.*

Antinny (Alias: W32.HLLW.Antinny) (Internet Worm): This worm will spread though the P2P network of the Japanese software, Winny P2P. The file length is 651264.

Kromber (Alias: IRC-Worm.Kromber, W32/Kromber, TrojanDropper.VBS.Inor) (Internet Worm): This worm spreads though the IRC network by sending a link to a web page that contains an exploit and runs a script. This script drops and runs a file called browsercheck.exe.

VBS.Biscuit.A@mm (Aliases: Worm.Win32.Registra, VBS/Bisquit) (Visual Basic Script Worm): This is a mass-mailing worm that sends itself as an attachment to the first 50 e-mail addresses in the Microsoft Outlook Address Book. The e-mail message will have the following characteristics:

- Subject: Adsl no problem!!!
- Attachments: Adsl_no_problem.pdf<184 spaces>.vbs

The worm attempts to copy itself to both the local host and reachable remote network shares. It will copy itself to the root of the network share as Netlog.vbs. It will also copy the original worm filename to the following folders if it is able to copy netlog.vbs to the root of the share:

- <network share root>\Windows\Menu Avvio\Programmi\Esecuzione automatica\
- <network share root>\Windows\startm~1\programs\startup\
- <network share root>\Windows\
- <network share root>\Windows\start menu\programs\startup\
- <network share root>\Win95\start menu\programs\startup\

On the 10th of every month, VBS.Biscuit.A@mm will display a pop-up message.

VBS.Mill.H (Visual Basic Script Worm): This worm uses Microsoft Outlook to send itself to all the contacts in the Outlook Address Book. It also attempts to spread itself through KaZaA, Pirch, and mIRC. The e-mail has the following characteristics:

- Subject: my picture
- Attachment: The attachment file name will vary.

VBS.Taber (Alias: Worm.P2P.Tabe.b) (Visual Basic Script Worm): This is a worm that attempts to spread through the KaZaA file-sharing network as "Britney_and_Madonna_fucking.mov.vbs." The worm attempts to delete C:\Windows\Explorer.exe and make some configuration changes to Internet Explorer by editing the registry keys. It will only execute on Windows 95/98/ME systems.

W32/Anvil.2044 (Win32 Virus): The W32/Anvil.2044 and W32/Anvil.2045 viruses are encrypted, non-memory resident PE file infectors. When an infected file is run, the virus infects EXE files and DLL libraries in the Windows and Windows System directories.

W32/Dumaru-B (Aliases: I-Worm.Dumaru.c, PE_DUMARU.B) (Win32 Worm): This is an e-mail worm with backdoor functions. The worm arrives in a message with the following characteristics:

- From: security@microsoft.com
- Subject line: Use this patch immediately !
- Attached file: patch.exe

The worm copies itself to the Windows folder as dllreg.exe, the Windows system folder as load32.exe and vxdmgr.exe, and the startup folder as rundllw.exe. It also creates the file guid32.dll in the Windows folder. Guid32.dll monitors running programs and keypresses and logs the information in the file vxdload.log in the Windows folder. The worm also logs information in the file winload.log in the Windows folder. The logs of system activity may be uploaded to a remote FTP server. W32/Dumaru-B creates the following entries in the registry in order to ensure that the worm is run each time Windows is started:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\load32 = load32.exe

It also creates another registry entry as a marker:

- HKLM\Software\SARS\kwmfound

The worm also adds the name of one of the copies of itself to the Run= line of win.ini and the shell= line of system.ini. W32/Dumaru-B drops and runs file <Windows>\windrive.exe. Windrv.exe is a backdoor Trojan. It also attempts to terminate various processes.

W32/Dumaru-E (Win32 Worm): This is an e-mail worm with backdoor functions. The worm arrives in a message with the following characteristics:

- From: security@microsoft.com
- Subject line: Use this patch immediately!
- Attached file: patch.exe

The worm copies itself to the Windows folder as dllreg.exe, the Windows system folder as load32.exe and vxdmgr.ex, and the startup folder as rundllw.exe. The worm also creates the file guid32.dll in the Windows folder. Guid32.dll monitors running programs and keypresses and logs the information in the file vxdload.log in the Windows folder. It also logs information in the file winload.log in the Windows folder. The logs of system activity may be uploaded to a remote FTP server. W32/Dumaru-E creates the following entries in the registry in order to ensure that the worm is run each time Windows is started:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\load32 = load32.exe
- HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\startup = load32.exe

The worm also adds the name of one of the copies of itself to the Run= line of win.ini and the shell= line of system.ini. W32/Dumaru-E searches for e-mail addresses to send itself to in the files with the extensions HTM, WAB, HTML, DBX, TBB and ABD. It may also terminates various processes. W32/Dumaru-E includes a backdoor component that uses port 2283 and an FTP server that uses port 10000.

W32.Dumaru.M@mm (Win32 Worm): This is a mass-mailing worm that drops an IRC Trojan onto an infected computer. The worm gathers e-mail addresses from certain file types and uses its own SMTP engine to e-mail itself. The e-mail has the following characteristics:

- From: "Microsoft" security@microsoft.com
- Subject: Use this patch immediately !
- Attachment: Patch.exe

W32.Dumaru.M@mm will also infect the .exe files on NTFS partitions. It will listen on ports:

- TCP 10000
- TCP 1001
- TCP 2283

The worm logs the keystrokes and sends the data to a specified e-mail address.

W32.Galil.C@mm (Win32 Worm): This is a mass-mailing worm that sends itself to the e-mail addresses it finds in the files that have the .htm, .html, .eml, and .txt file extensions. The e-mail will have a variable subject line and attachment name. This worm sends itself to all the contacts in the Microsoft Outlook Address Book and MSN messenger contact list, and it attempts to spread itself through the KaZaA file-sharing network. It is written in the Microsoft Visual Basic programming language and is compressed with UPX.

W32.HLLW.Donk.B (Aliases: W32/Sdbot.worm, Backdoor.SdBot.gen) (Win32 Worm): This is a network-aware worm that attempts to connect to a predetermined IRC server to receive instructions from its author. It is written in Microsoft Visual C++ and is encrypted with PE-Shield and WinKript.

W32.HLLW.Fatee.B (Alias: W2.HLLW.Fatee) (Win32 Worm): This is a worm that spreads through file-sharing networks. It also tries to spread through the network shares.

W32.HLLW.Gaobot.AG (Alias: Backdoor.Agobot.3.h) (Win32 Worm): This is a minor variant of W32.HLLW.Gaobot.AE. It attempts to spread to network shares that have weak passwords and allows malicious users to access an infected computer through an IRC channel. The worm uses multiple vulnerabilities, including:

- The DCOM RPC vulnerability (described in Microsoft Security Bulletin MS03-026) using TCP port 135. Using this exploit, the worm specifically targets Windows XP computers.
- The RPC locator vulnerability (described in Microsoft Security Bulletin MS03-001) using TCP port 445.

It is compressed with UPX.

W32/HLL.cmp.406528 (Win32 Worm): This is a companion virus. When an infected file is executed, it renames the original file by adding a blank character at the end of the filename and copies itself to the original filename. For example a file names "Calc.exe" becomes "Calc .exe" and now the file "Calc.exe" is a copy of the virus. The virus is only able to spread on computers having the short date format configured as "yyyy-MM-dd." If not, only an error message is displayed.

W32.HLLW.Gaobot.AN (Alias: W32.HLLW.Gaobot.AF) (Win32 Worm): W32.HLLW.Gaobot.AN is a minor variant of W32.HLLW.Gaobot.AF. It attempts to spread to network shares that have weak passwords and allows malicious users to access an infected computer through an IRC channel. The worm takes advantage of multiple vulnerabilities including:

- The DCOM RPC vulnerability (described in Microsoft Security Bulletin MS03-026) using TCP port 135. Using this exploit, the worm specifically targets Windows XP computers.
- The RPC locator vulnerability (described in Microsoft Security Bulletin MS03-001) using TCP port 445.

It is compressed with UPX.

W32.HLLW.Gaobot.AO (Win32 Worm): This is a minor variant of W32.HLLW.Gaobot.AF. It attempts to spread to network shares that have weak passwords and allows malicious users to access an infected computer through IRC. It uses multiple vulnerabilities to spread, including:

- The DCOM RPC vulnerability (described in Microsoft Security Bulletin MS03-026) using TCP port 135.
- The RPC locator vulnerability (described in Microsoft Security Bulletin MS03-001) using TCP port 445. The WebDav vulnerability (described in Microsoft Security Bulletin MS03-007) using TCP port 80.

It is compressed with UPX.

W32.HLLW.LyndEgg (Win32 Worm): This is a worm that spreads itself through file-sharing networks. It also attempts to erase hard drives.

W32.HLLP.Spreda.B (Aliases: W32.HLLP.Savno, W32/HLLP.Savno!p2p, Win32.HLLP.Sav) (Win32 Virus): This is a high-level language virus that spreads through KaZaA networks by infecting files in the KaZaA download folder. Under some conditions, W32.HLLP.Spreda.B inserts a password stealer onto the system.

W32.Israz.B@mm (Win32 Worm): This is a mass-mailing worm that uses its own SMTP engine to send itself to all the contacts in the Windows Address Book and Outlook Address Book. The e-mail has the following characteristics:

- Subject: Your file is attached to message.
- Attachment: game.exe

or:

- From: windows@microsoft.com
- Subject: Something new for you
- Attachment: tips.exe

The worm also attempts to spread itself through some file-sharing networks, such as KaZaA, Morpheus, eMule, eDonkey2000, BearShare, and iMesh. It is written in the Microsoft Visual Basic programming language.

W32/Lehs@MM (Alias: W32.HLLW.Lehs@mm) (Win32 Worm): This virus is written in Visual Basic. It is intended to mail itself to recipients in the Outlook address book. Outgoing messages are constructed as follows:

- From: Microsoft Support
- Subject: DCOM RPC Vulnerability Patch

W32.Logitall.A@mm (Win32 Worm): This is a mass-mailing worm that sends itself to the addresses found on the system. The worm also uploads user information to an FTP server that the worm's author specifies.

W32/Lovgate-R (Aliases: I-Worm.Lovgate.n, W32.HLLW.Lovgate@mm, Win32.HLLM.Lovgate, Lovgate.N, WORM_LOVGATE.O) (Win32 Worm): This is a worm and backdoor Trojan similar to W32/Lovgate-D. It spreads across the local network by copying itself into shared folders using various filenames. W32/Lovgate-R also attempts to spread via e-mail by sending itself to e-mail addresses collected from *.ht* files. E-mails sent to these addresses will have various characteristics. It copies itself into the Windows system folder as rpcsrv.exe, syshelp.exe, WinGate.exe, winrpc.exe, and WinRpcsrv.exe. The worm sets the following registry entries:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\syshelp = "<Windows system folder>\syshelp.exe"
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\WinGate initialize = "<Windows system folder>\WinGate.exe -remoteshell"
- HKLM\Software\CLASSES\txtfile\shell\open\command = "winrpc.exe %1"

W32/Lovgate-R is also a backdoor Trojan that provides a malicious user with unauthorized access to the user's computer and can send a notification e-mail message to the malicious user.

W32/Panoil.d@MM (Win32 Worm): This virus has the ability of spreading via E-mail, KaZaA file sharing networks, and MIRC. When executed, this worm installs itself onto the victim machine as:

- C:\Hacker_Hunter.exe.exe
- %Windir%\Hunter.exe

The following registry key is set to hook system startup:

- HKEY_LOCAL_MACHINE\Software\Microsft\Windows\CurrentVersion\Run\ "SecurityFix" = %WinDir%\Hunter.exe

The worm will modify the Internet Explorer start page setting in the registry to point to a website for a university in Turkey:

- HKEY_LOCAL_MACHINE\Software\Microsft\Windows\CurrentVersion\Run\"Start Page" = http :// www. ankara.edu.tr

This worm uses Microsoft Outlook to send itself to all the e-mail addresses found the Outlook Address Book. The worm copies itself to the KaZaA download directory as:

- Hunter.exe
- Hotmailhack.exe
- ICQ hack.exe
- Kernel hack.exe
- Linux Password Hack.exe
- Mail Hack.exe
- Matrix.exe

If MIRC is installed, script.ini is overwritten. The IRC client is used to send the virus to all users who join channels that the infected user is on.

W32/Randex-G (Aliases: Worm.Randex.g, W95/Randex.J, W32/Sdbot.worm.gen.b, Win32/Randex.G, W32.Randex.C, WORM_RANDEX.F) (Win32 Worm): This worm has been reported in the wild. It is a network worm with backdoor capabilities that allows a remote intruder to access and control a computer via IRC channels. W32/Randex-G spreads over a network by copying itself to the Windows system32 folder of C$ and Admin$ shares with weak passwords. Each time the worm is run, it tries to connect to a remote IRC server and join a specific channel. The worm then runs in the background as a server process, listening for commands to execute. When first run, it copies itself to Windows system folder as ntd32.exe and creates the following registry entries so that the worm is run when Windows starts up:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Microsoft Network Daemon for Win32 = ntd32.exe
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\Microsoft Network Daemon for Win32 = ntd32.exe

W32/Randex-G obtains and sends out the CD key for the following games:

- Battlefield 1942
- Battlefield 1942 The Road to Rome
- Half-Life
- Unreal Tournament 2003

W32.Randex.P (Win32 Worm): This is a network-aware worm that will attempt to connect to a predetermined IRC server to receive instructions from its author. When W32.Randex.P is executed, it copies itself as %System%\Cnqmax.exe and calculates a random IP address. It attempts to connect to the randomly generated IP addresses. The worm copies itself to \\<authenticated IP>\c$\winnt\system32\Amqj.exe on computers that have weak administrator passwords and schedules a Network Job to run the worm. W32.Randex.P adds the value, "Mspatch89"="%System%\cnqmax.exe," to the registry keys:

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

so that the worm runs when you start Windows. It connects to a specific IRC channel on a specific IRC server to receive remote instructions. The W32.Randex.P dropper will drop and run the worm file as Gfac.exe, as well as the Kp.exe file.

W32/Vybab@MM (Alias: PE_VYBAB.A) (Win32 Virus): This is a prepending virus that drops a Visual Basic Script file to mail itself to recipients listed in the Outlook address book. The VBS script that is dropped in order to mail the virus is VBS/Generic@MM. It prepends .EXE files on the victim machine (in the Program Files directory, and on D:, E:, F:, and G:). Infected files will increase in size by 141,824 bytes. The virus drops a VBS script into the user temporary folder in order to mail itself to recipients in the Outlook Address Book. Outgoing messages are constructed as follows:

- Subject: Microsoft Pack2, ;0)
- Attachment: (name of originally executed file)

The virus drops the file 123.TXT into %WinDir%. This file contains the following string, “babyv ; made of Ran.” It also drops a copy of the originally executed file as C:\SEEYOU.RAR . Other randomly named files are created with the following extensions:

- EXE
- BAT
- HTM
- RAR
- DOC
- XLS

The files merely contain a single string - their own filepath.

W32/Zezer.worm.gen (Win32 Worm): This worm attempts to harvest e-mail addresses from your MSN Messenger contact list. It may arrive in an e-mail message as follows:

- To: (The worm targets hotmail user accounts)
- Subject: Windows Update (MSN Messenger Update 6 MSN Messenger vulnerability)
- Attachment: Msn_inst.exe

When the attachment is run, the worm displays a fake error message. It copies itself to several locations on the local system:

- %StartUp folder%\msnexec.exe
- %WinDir%\Mscsgs.exe
- %WinDir%\Msn_inst.exe
- %WinDir%\Msn_updt.exe
- %SysDir%\Mscsgs32.exe

A registry run key is created to load the worm at startup:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "Mscsgs" = C:\WINDOWS\Mscsgs.exe

An additional registry key is created:

- HKEY_CURRENT_USER\Software\Zed\Dozer "Dozer" = W32/Dozer by Zed

A sub key named MSNContact may be created under this Dozer key.

W97M.Autch (Aliases: Macro.Word97.Tchau, W97M/Generic) (Word 97 Macro Virus): This is a macro virus that infects Microsoft Word documents and templates.

W97M/Kolop (Alias: WM97/Oragon-A) (Word 97 Macro Virus): W97M/Kolop will remove Tools/Macro menu bar. If it is the first day of the month, the virus will change Word application Caption name to the Username. It may also display the office assistant

WORM_SMIBAG.A (Alias: W32.Smibag.Worm) (Internet Worm): This multicomponent worm spreads through MSN Messenger by sending copies of itself to all MSN users found in the target user's contact list. It usually arrives as the file SMB.EXE, an SFX executable archive package. Upon execution, it drops the following files:

- C:\admagic.exe
- C:\SMB.EXE
- C:\TEST.TXT
- %System%\RAW32X.EXE
- %System%\SM.DLL
- %System%\UZ.EXE

The worm has a payload of showing popup advertisements from various adult sites. This MSN worm runs on Windows 95, 98, ME, NT, 2000 and XP. It is written and compiled in Visual C++.

XF97/Wisab-A (Aliases: Macro.Excel97.Wisab, XM.VNN, XF_SIC.A, XF/Sic.gen, X97M_WISAB.A) (Excel 97 Formula Virus): XF97/Wisab-A spreads using a Formula Sheet called XL4Test5. The virus creates a file in the XLSTART directory called BOOK1.

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table includes Trojans discussed in the last six months, with new items 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 #
A97M/AcceV	N/A	CyberNotes-2003-18
AdwareDropper-A	A	CyberNotes-2003-04
Adware-SubSearch.dr	dr	CyberNotes-2003-14
Afcore.q	**N/A**	**Current Issue**
AIM-Canbot	N/A	CyberNotes-2003-07
AprilNice	N/A	CyberNotes-2003-08
Backdoor.Acidoor	N/A	CyberNotes-2003-05
Backdoor.Amitis	N/A	CyberNotes-2003-01
Backdoor.Amitis.B	B	CyberNotes-2003-11
Backdoor.AntiLam.20.K	K	CyberNotes-2003-10
Backdoor.AntiLam.20.Q	20.Q	CyberNotes-2003-18
Backdoor.Apdoor	N/A	CyberNotes-2003-12

Trojan	Version	CyberNotes Issue #
Backdoor.Assasin.D	D	CyberNotes-2003-01
Backdoor.Assasin.E	E	CyberNotes-2003-04
Backdoor.Assasin.F	F	CyberNotes-2003-09
Backdoor.Badcodor	N/A	CyberNotes-2003-12
Backdoor.Beasty	N/A	CyberNotes-2003-02
Backdoor.Beasty.B	B	CyberNotes-2003-03
Backdoor.Beasty.C	C	CyberNotes-2003-05
Backdoor.Beasty.Cli	Cli	CyberNotes-2003-10
Backdoor.Beasty.D	D	CyberNotes-2003-06
Backdoor.Beasty.dr	dr	CyberNotes-2003-16
Backdoor.Beasty.E	E	CyberNotes-2003-06
Backdoor.Beasty.G	G	CyberNotes-2003-16
Backdoor.Beasty.Kit	N/A	CyberNotes-2003-18
Backdoor.Bigfoot	N/A	CyberNotes-2003-09
Backdoor.Bmbot	N/A	CyberNotes-2003-04
Backdoor.Bridco	N/A	CyberNotes-2003-06
Backdoor.CamKing	N/A	CyberNotes-2003-10
Backdoor.CHCP	N/A	CyberNotes-2003-03
Backdoor.Cmjspy	N/A	CyberNotes-2003-10
Backdoor.Cmjspy.B	B	CyberNotes-2003-14
Backdoor.CNK.A	A	CyberNotes-2003-10
Backdoor.CNK.A.Cli	Cli	CyberNotes-2003-10
Backdoor.Colfuser	N/A	CyberNotes-2003-01
Backdoor.Coreflood.dr	Dr	CyberNotes-2003-19
Backdoor.Cow	N/A	CyberNotes-2003-01
Backdoor.CrashCool	N/A	CyberNotes-2003-19
Backdoor.Cybspy	N/A	CyberNotes-2003-01
Backdoor.Dani	N/A	CyberNotes-2003-04
Backdoor.Darmenu	N/A	CyberNotes-2003-05
Backdoor.Death.Cli	Cli	CyberNotes-2003-10
Backdoor.Deftcode	N/A	CyberNotes-2003-01
Backdoor.Delf.Cli	Cli	CyberNotes-2003-10
Backdoor.Delf.F	F	CyberNotes-2003-07
Backdoor.Drator	N/A	CyberNotes-2003-01
Backdoor.Dsklite	N/A	CyberNotes-2003-14
Backdoor.Dsklite.cli	cli	CyberNotes-2003-14
Backdoor.Dvldr	N/A	CyberNotes-2003-06
Backdoor.EggDrop	N/A	CyberNotes-2003-08
Backdoor.Evilbot.B	B	CyberNotes-2003-19
Backdoor.EZBot	N/A	CyberNotes-2003-18
Backdoor.Fatroj	N/A	CyberNotes-2003-10
Backdoor.Fatroj.Cli	Cli	CyberNotes-2003-10
Backdoor.Fluxay	N/A	CyberNotes-2003-07
Backdoor.FTP.Casus	N/A	CyberNotes-2003-02
Backdoor.FTP_Ana.C	C	CyberNotes-2003-07
Backdoor.FTP_Ana.D	D	CyberNotes-2003-08
Backdoor.Fxdoor	N/A	CyberNotes-2003-10
Backdoor.Fxdoor.Cli	Cli	CyberNotes-2003-10
Backdoor.Fxsvc	N/A	CyberNotes-2003-16

Trojan	Version	CyberNotes Issue #
Backdoor.Graybird	N/A	CyberNotes-2003-07
Backdoor.Graybird.B	B	CyberNotes-2003-08
Backdoor.Graybird.C	C	CyberNotes-2003-08
Backdoor.Graybird.D	D	CyberNotes-2003-14
Backdoor.Graybird.G	G	CyberNotes-2003-19
Backdoor.Grobodor	N/A	CyberNotes-2003-12
Backdoor.Guzu.B	B	CyberNotes-2003-14
Backdoor.HackDefender	N/A	CyberNotes-2003-06
Backdoor.Hale	N/A	CyberNotes-2003-16
Backdoor.Hazzer	**N/A**	**Current Issue**
Backdoor.Hethat	N/A	CyberNotes-2003-01
Backdoor.Hipo	N/A	CyberNotes-2003-04
Backdoor.Hitcap	N/A	CyberNotes-2003-04
Backdoor.Hornet	N/A	CyberNotes-2003-01
Backdoor.IRC.Aladinz	N/A	CyberNotes-2003-02
Backdoor.IRC.Aladinz.C	C	CyberNotes-2003-14
Backdoor.IRC.Bobbins	N/A	CyberNotes-2003-18
Backdoor.IRC.Cloner	N/A	CyberNotes-2003-04
Backdoor.IRC.Comiz	N/A	CyberNotes-2003-11
Backdoor.IRC.Flood.F	F	CyberNotes-2003-16
Backdoor.IRC.Hatter	N/A	CyberNotes-2003-18
Backdoor.IRC.Jemput	N/A	CyberNotes-2003-19
Backdoor.IRC.Lampsy	N/A	CyberNotes-2003-10
Backdoor.IRC.PSK	PSK	CyberNotes-2003-16
Backdoor.IRC.Ratsou	N/A	CyberNotes-2003-10
Backdoor.IRC.Ratsou.B	B	CyberNotes-2003-11
Backdoor.IRC.Ratsou.C	C	CyberNotes-2003-11
Backdoor.IRC.RPCBot.B:	B	CyberNotes-2003-18
Backdoor.IRC.RPCBot.C	C	CyberNotes-2003-18
Backdoor.IRC.RPCBot.D	D	CyberNotes-2003-18
Backdoor.IRC.RPCBot.F	F	CyberNotes-2003-19
Backdoor.IRC.Tastyred	**N/A**	**Current Issue**
Backdoor.IRC.Yoink	N/A	CyberNotes-2003-05
Backdoor.IRC.Zcrew	N/A	CyberNotes-2003-04
Backdoor.IRC.Zcrew.B	B	CyberNotes-2003-19
Backdoor.Kaitex.D	D	CyberNotes-2003-09
Backdoor.Kalasbot	N/A	CyberNotes-2003-09
Backdoor.Khaos	N/A	CyberNotes-2003-04
Backdoor.Kilo	N/A	CyberNotes-2003-04
Backdoor.Kodalo	N/A	CyberNotes-2003-14
Backdoor.Kol	N/A	CyberNotes-2003-06
Backdoor.Krei	N/A	CyberNotes-2003-03
Backdoor.Lala	N/A	CyberNotes-2003-01
Backdoor.Lala.B	B	CyberNotes-2003-16
Backdoor.Lala.C	C	CyberNotes-2003-16
Backdoor.Lanfilt.B	B	CyberNotes-2003-14
Backdoor.Lastras	N/A	CyberNotes-2003-17
Backdoor.LeGuardien.B	B	CyberNotes-2003-10
Backdoor.Litmus.203.c	c	CyberNotes-2003-09

Trojan	Version	CyberNotes Issue #
Backdoor.LittleWitch.C	C	CyberNotes-2003-06
Backdoor.Longnu	N/A	CyberNotes-2003-06
Backdoor.Lorac	N/A	CyberNotes-2003-17
Backdoor.Marotob	N/A	CyberNotes-2003-06
Backdoor.Massaker	N/A	CyberNotes-2003-02
Backdoor.MindControl	N/A	CyberNotes-2003-14
Backdoor.Monator	N/A	CyberNotes-2003-08
Backdoor.Mots	N/A	CyberNotes-2003-11
Backdoor.Mprox	**N/A**	**Current Issue**
Backdoor.MSNCorrupt	N/A	CyberNotes-2003-06
Backdoor.Netdevil.15	15	CyberNotes-2003-15
Backdoor.NetDevil.B	B	CyberNotes-2003-01
Backdoor.NetTrojan	N/A	CyberNotes-2003-01
Backdoor.Nibu	N/A	CyberNotes-2003-16
Backdoor.Nickser	N?A	CyberNotes-2003-14
Backdoor.Ohpass	N/A	CyberNotes-2003-01
Backdoor.OICQSer.165	N/A	CyberNotes-2003-01
Backdoor.OICQSer.17	17	CyberNotes-2003-01
Backdoor.Omygo	N/A	CyberNotes-2003-19
Backdoor.Optix.04.d	04.d	CyberNotes-2003-04
Backdoor.OptixDDoS	N/A	CyberNotes-2003-07
Backdoor.OptixPro.10.c	10.c	CyberNotes-2003-01
Backdoor.OptixPro.12.b	12.b	CyberNotes-2003-07
Backdoor.OptixPro.13	13	CyberNotes-2003-09
Backdoor.Peeper	**N/A**	**Current Issue**
Backdoor.Peers	N/A	CyberNotes-2003-10
Backdoor.Plux	N/A	CyberNotes-2003-05
Backdoor.Pointex	N/A	CyberNotes-2003-09
Backdoor.Pointex.B	B	CyberNotes-2003-09
Backdoor.Private	N/A	CyberNotes-2003-11
Backdoor.Prorat	N/A	CyberNotes-2003-13
Backdoor.PSpider.310	310	CyberNotes-2003-05
Backdoor.Pspider.310.b	310.b	CyberNotes-2003-18
Backdoor.Queen	N/A	CyberNotes-2003-06
Backdoor.Rado	N/A	CyberNotes-2003-18
Backdoor.Ranck	N/A	CyberNotes-2003-18
Backdoor.Ratega	N/A	CyberNotes-2003-09
Backdoor.Recerv	N/A	CyberNotes-2003-09
Backdoor.Redkod	N/A	CyberNotes-2003-05
Backdoor.Remohak.16	16	CyberNotes-2003-01
Backdoor.RemoteSOB	N/A	CyberNotes-2003-01
Backdoor.Rephlex	N/A	CyberNotes-2003-01
Backdoor.Roxy	N/A	CyberNotes-2003-16
Backdoor.Roxy.B	**B**	**Current Issue**
Backdoor.RPCBot.E	E	CyberNotes-2003-19
Backdoor.Rsbot	N/A	CyberNotes-2003-07
Backdoor.SchoolBus.B	B	CyberNotes-2003-04
Backdoor.Sdbot.C	C	CyberNotes-2003-02

Trojan	Version	CyberNotes Issue #
Backdoor.Sdbot.D	D	CyberNotes-2003-03
Backdoor.Sdbot.E	E	CyberNotes-2003-06
Backdoor.Sdbot.F	F	CyberNotes-2003-07
Backdoor.Sdbot.G	G	CyberNotes-2003-08
Backdoor.Sdbot.H	H	CyberNotes-2003-09
Backdoor.Sdbot.L	L	CyberNotes-2003-11
Backdoor.Sdbot.M	M	CyberNotes-2003-13
Backdoor.Sdbot.P	P	CyberNotes-2003-17
Backdoor.Semes	**N/A**	**Current Issue**
Backdoor.Serpa	N/A	CyberNotes-2003-03
Backdoor.Servsax	N/A	CyberNotes-2003-01
Backdoor.Sheldor	N/A	CyberNotes-2003-18
Backdoor.SilverFTP	N/A	CyberNotes-2003-04
Backdoor.Simali	N/A	CyberNotes-2003-09
Backdoor.Sixca	N/A	CyberNotes-2003-01
Backdoor.Slao	N/A	CyberNotes-2003-11
Backdoor.Smother	**N/A**	**Current Issue**
Backdoor.Snami	N/A	CyberNotes-2003-10
Backdoor.Snowdoor	N/A	CyberNotes-2003-04
Backdoor.Socksbot	N/A	CyberNotes-2003-06
Backdoor.Softshell	N/A	CyberNotes-2003-10
Backdoor.Sokacaps	N/A	CyberNotes-2003-18
Backdoor.Stealer	N/A	CyberNotes-2003-14
Backdoor.SubSari.15	15	CyberNotes-2003-05
Backdoor.SubSeven.2.15	2.15	CyberNotes-2003-05
Backdoor.Sumtax	N/A	CyberNotes-2003-16
Backdoor.Surdux	**N/A**	**Current Issue**
Backdoor.Syskbot	N/A	CyberNotes-2003-08
Backdoor.SysXXX	N/A	CyberNotes-2003-06
Backdoor.Talex	N/A	CyberNotes-2003-02
Backdoor.Tankedoor	N/A	CyberNotes-2003-07
Backdoor.Translat	**N/A**	**Current Issue**
Backdoor.Trynoma	N/A	CyberNotes-2003-08
Backdoor.Turkojan	N/A	CyberNotes-2003-07
Backdoor.Udps.10	1	CyberNotes-2003-03
Backdoor.UKS	N/A	CyberNotes-2003-11
Backdoor.Unifida	N/A	CyberNotes-2003-05
Backdoor.Upfudoor	N/A	CyberNotes-2003-01
Backdoor.Urat.b	b	CyberNotes-2003-18
Backdoor.Uzbet	N/A	CyberNotes-2003-15
Backdoor.VagrNocker	N/A	CyberNotes-2003-01
Backdoor.Vmz	N/A	CyberNotes-2003-01
Backdoor.Winet	N/A	CyberNotes-2003-11
Backdoor.WinJank	N/A	CyberNotes-2003-15
Backdoor.Winker	N/A	CyberNotes-2003-15
Backdoor.WinShell.50	N/A	CyberNotes-2003-16
Backdoor.Wollf.16	16	CyberNotes-2003-18
Backdoor.Xenozbot	N/A	CyberNotes-2003-01
Backdoor.Xeory	N/A	CyberNotes-2003-03

Trojan	Version	CyberNotes Issue #
Backdoor.XTS	N/A	CyberNotes-2003-08
Backdoor.Zdemon	N/A	CyberNotes-2003-02
Backdoor.Zdemon.126	126	CyberNotes-2003-10
Backdoor.Zdown	N/A	CyberNotes-2003-05
Backdoor.Zix	N/A	CyberNotes-2003-02
Backdoor.Zombam	N/A	CyberNotes-2003-08
Backdoor.Zombam.B	**B**	**Current Issue**
Backdoor.Zvrop	N/A	CyberNotes-2003-03
Backdoor-AFC	N/A	CyberNotes-2003-05
Backdoor-AOK	N/A	CyberNotes-2003-01
BackDoor-AQL	N/A	CyberNotes-2003-05
BackDoor-AQT	N/A	CyberNotes-2003-05
BackDoor-ARR	ARR	CyberNotes-2003-06
Backdoor-ARU	ARU	CyberNotes-2003-06
BackDoor-ARX	ARX	CyberNotes-2003-06
BackDoor-ARY	ARY	CyberNotes-2003-06
BackDoor-ASD	ASD	CyberNotes-2003-07
BackDoor-ASL	ASL	CyberNotes-2003-07
BackDoor-ASW	ASW	CyberNotes-2003-08
BackDoor-ATG	ATG	CyberNotes-2003-09
BackDoor-AUP	N/A	CyberNotes-2003-11
BackDoor-AVF	AVF	CyberNotes-2003-12
BackDoor-AVH	AVH	CyberNotes-2003-12
BackDoor-AVO	AVO	CyberNotes-2003-12
BackDoor-AXC	AXC	CyberNotes-2003-14
BackDoor-AXQ	AXQ	CyberNotes-2003-15
Backdoor-AXR	AXR	CyberNotes-2003-16
Backdoor-AZF	**AZF**	**Current Issue**
BDS/AntiPC	N/A	CyberNotes-2003-02
BDS/Backstab	N/A	CyberNotes-2003-02
BDS/CheckESP	N/A	CyberNotes-2003-12
BDS/Ciadoor.10	10	CyberNotes-2003-07
BDS/Evilbot.A	A	CyberNotes-2003-09
BDS/Evolut	N/A	CyberNotes-2003-03
BDS/GrayBird.G	G	CyberNotes-2003-17
BDS/PowerSpider.A	A	CyberNotes-2003-11
BKDR_LITH.103.A	A	CyberNotes-2003-17
Cardown	N/A	CyberNotes-2003-19
CoolFool	N/A	CyberNotes-2003-17
Daysun	N/A	CyberNotes-2003-06
DDoS-Stinkbot	N/A	CyberNotes-2003-08
Delude	N/A	CyberNotes-2003-19
Desex	**N/A**	**Current Issue**
DoS-iFrameNet	N/A	CyberNotes-2003-04
Download.Aduent.Trojan	N/A	CyberNotes-2003-18
Download.Trojan.B	B	CyberNotes-2003-13
Downloader.BO.B	B	CyberNotes-2003-10
Downloader.BO.B.dr	B.dr	CyberNotes-2003-10

Trojan	Version	CyberNotes Issue #
Downloader.Dluca	N/A	CyberNotes-2003-17
Downloader.Dluca.B	B	CyberNotes-2003-19
Downloader.Dluca.C	**C**	**Current Issue**
Downloader.Mimail	N/A	CyberNotes-2003-16
Downloader-BN.b	BN.b	CyberNotes-2003-13
Downloader-BO.dr.b	N/A	CyberNotes-2003-02
Downloader-BS	N/A	CyberNotes-2003-02
Downloader-BW	N/A	CyberNotes-2003-05
Downloader-BW.b	BW.b	CyberNotes-2003-06
Downloader-BW.c	BW.c	CyberNotes-2003-07
Downloader-CY	CY	CyberNotes-2003-16
Downloader-DM	DM	CyberNotes-2003-16
Downloader-DN.b	DN.b	CyberNotes-2003-17
Downloader-EB	EB	CyberNotes-2003-18
DownLoader-EG	**EG**	**Current Issue**
ELF_TYPOT.A	A	CyberNotes-2003-13
ELF_TYPOT.B	B	CyberNotes-2003-13
Exploit-IISInjector	N/A	CyberNotes-2003-03
Gpix	N/A	CyberNotes-2003-08
Hacktool.Keysteal	N/A	CyberNotes-2003-19
Hacktool.PWS.QQPass	N/A	CyberNotes-2003-06
ICQPager-J	N/A	CyberNotes-2003-05
IRC/Backdoor.e	E	CyberNotes-2003-01
IRC/Backdoor.f	f	CyberNotes-2003-02
IRC/Backdoor.g	g	CyberNotes-2003-03
IRC/Flood.ap	N/A	CyberNotes-2003-05
IRC/Flood.bi	N/A	CyberNotes-2003-03
IRC/Flood.br	br	CyberNotes-2003-06
IRC/Flood.bu	bu	CyberNotes-2003-08
IRC/Flood.cd	cd	CyberNotes-2003-11
IRC/Flood.cm	cm	CyberNotes-2003-13
IRC/Fyle	N/A	CyberNotes-2003-16
IRC-BBot	N/A	CyberNotes-2003-16
IRC-Emoz	N/A	CyberNotes-2003-03
IRC-OhShootBot	N/A	CyberNotes-2003-01
IRC-Vup	N/A	CyberNotes-2003-09
JS.Fortnight.B	B	CyberNotes-2003-06
JS.Seeker.J	J	CyberNotes-2003-01
JS.Seeker.K	**K**	**Current Issue**
JS/Fortnight.c@M	c	CyberNotes-2003-11
JS/Seeker-C	C	CyberNotes-2003-04
JS/StartPage.dr	dr	CyberNotes-2003-11
JS_WEBLOG.A	A	CyberNotes-2003-05
Keylogger.Cone.Trojan	N/A	CyberNotes-2003-14
KeyLog-Kerlib	N/A	CyberNotes-2003-05
Keylog-Keylf	N/A	CyberNotes-2003-17
Keylog-Kjie	N/A	CyberNotes-2003-12
Keylog-Mico	**N/A**	**Current Issue**
Keylog-Perfect.dr	dr	CyberNotes-2003-09

Trojan	Version	CyberNotes Issue #
Keylog-Razytimer	N/A	CyberNotes-2003-03
KeyLog-TweakPan	N/A	CyberNotes-2003-02
Keylog-Yeehah	N/A	CyberNotes-2003-12
Linux/DDoS-Ferlect	N/A	CyberNotes-2003-17
Linux/Exploit-SendMail	N/A	CyberNotes-2003-05
Lockme	N/A	CyberNotes-2003-15
MultiDropper-FD	N/A	CyberNotes-2003-01
OF97/ExeDrop-B	N/A	CyberNotes-2003-19
Pac	N/A	CyberNotes-2003-04
Petala	**N/A**	**Current Issue**
ProcKill-AE	N/A	CyberNotes-2003-05
ProcKill-AF	N/A	CyberNotes-2003-05
ProcKill-AH	AH	CyberNotes-2003-08
ProcKill-AJ	AJ	CyberNotes-2003-13
ProcKill-Z	N/A	CyberNotes-2003-03
Proxy-Guzu	N/A	CyberNotes-2003-08
Proxy-Migmaf	N/A	CyberNotes-2003-14
PWS-Aileen	N/A	CyberNotes-2003-04
PWS-Moneykeeper	N/A	CyberNotes-2003-18
PWS-Sincom.dr	dr	CyberNotes-2003-17
PWSteal.ABCHlp	N/A	CyberNotes-2003-12
PWSteal.AlLight	N/A	CyberNotes-2003-01
PWSteal.Bancos	N/A	CyberNotes-2003-15
PWSteal.Bancos.B	B	CyberNotes-2003-16
PWSteal.Hukle	N/A	CyberNotes-2003-08
PWSteal.Kipper	N/A	CyberNotes-2003-10
PWSteal.Lemir.105	105	CyberNotes-2003-10
PWSteal.Lemir.C	C	CyberNotes-2003-17
PWSteal.Lemir.D	D	CyberNotes-2003-18
PWSteal.Lemir.E	**E**	**Current Issue**
PWSteal.Lemir.F	**F**	**Current Issue**
PWSteal.Rimd	N/A	CyberNotes-2003-01
PWSteal.Rimd.B	B	CyberNotes-2003-10
PWSteal.Senhas	N/A	CyberNotes-2003-03
PWSteal.Snatch	N/A	CyberNotes-2003-10
PWSteal.Sysrater	N/A	CyberNotes-2003-12
PWS-Tenbot	N/A	CyberNotes-2003-01
PWS-Train	N/A	CyberNotes-2003-17
PWS-Truebf	N/A	CyberNotes-2003-13
PWS-Watsn	N/A	CyberNotes-2003-10
PWS-Wexd	N/A	CyberNotes-2003-14
PWS-WMPatch	N/A	CyberNotes-2003-07
PWS-Yipper	N/A	CyberNotes-2003-10
QDel359	359	CyberNotes-2003-01
QDel373	373	CyberNotes-2003-06
Qdel374	374	CyberNotes-2003-06
Qdel375	375	CyberNotes-2003-06
Qdel376	376	CyberNotes-2003-07
QDel378	378	CyberNotes-2003-08

Trojan	Version	CyberNotes Issue #
QDel379	369	CyberNotes-2003-09
QDel390	390	CyberNotes-2003-13
QDel391	391	CyberNotes-2003-13
QDel392	392	CyberNotes-2003-13
QDial11	1	CyberNotes-2003-14
QDial6	6	CyberNotes-2003-11
Renamer.c	N/A	CyberNotes-2003-03
Reom.Trojan	N/A	CyberNotes-2003-08
StartPage-G	G	CyberNotes-2003-06
Startpage-N	N	CyberNotes-2003-13
StartPage-U	**U**	**Current Issue**
Stealther	N/A	CyberNotes-2003-16
Stoplete	N/A	CyberNotes-2003-06
Swizzor	N/A	CyberNotes-2003-07
Tellafriend.Trojan	N/A	CyberNotes-2003-04
Tr/Decept.21	21	CyberNotes-2003-07
Tr/Delf.r	r	CyberNotes-2003-16
Tr/DelWinbootdir	N/A	CyberNotes-2003-07
TR/Fake.YaHoMe.1	N/A	CyberNotes-2003-02
TR/Gaslide.C	C	CyberNotes-2003-17
Tr/SpBit.A	A	CyberNotes-2003-04
Tr/VB.t	T	CyberNotes-2003-11
TR/WinMx	N/A	CyberNotes-2003-02
Troj/Apdoor-A	A	CyberNotes-2003-19
Troj/Ataka-E	E	CyberNotes-2003-15
Troj/Autoroot-A	A	CyberNotes-2003-16
Troj/Backsm-A	A	CyberNotes-2003-19
Troj/Bdoor-RQ	RQ	CyberNotes-2003-17
Troj/Dloader-BO	BO	CyberNotes-2003-02
Troj/DownLdr-DI	DI	CyberNotes-2003-15
Troj/Eyeveg-A	A	CyberNotes-2003-19
Troj/Golon-A	A	CyberNotes-2003-15
Troj/Hackarmy-A	**A**	**Current Issue**
Troj/Hacline-B	B	CyberNotes-2003-13
Troj/IRCBot-C	C	CyberNotes-2003-11
Troj/Manifest-A	N/A	CyberNotes-2003-03
Troj/Migmaf-A	A	CyberNotes-2003-15
Troj/Mystri-A	A	CyberNotes-2003-13
Troj/PcGhost-A	A	CyberNotes-2003-13
Troj/Peido-B	B	CyberNotes-2003-10
Troj/Qhosts-1	**N/A**	**Current Issue**
Troj/QQPass-A	A	CyberNotes-2003-16
Troj/Qzap-248	N/A	CyberNotes-2003-01
Troj/SadHound-A	N/A	CyberNotes-2003-03
Troj/Sandesa-A	A	CyberNotes-2003-14
Troj/Slacker-A	A	CyberNotes-2003-05
Troj/Slanret-A	N/A	CyberNotes-2003-03
Troj/TKBot-A	A	CyberNotes-2003-04

Trojan	Version	CyberNotes Issue #
Troj/Webber-A	A	CyberNotes-2003-15
TROJ_JBELLZ.A	A	CyberNotes-2003-02
TROJ_KILLBOOT.B	B	CyberNotes-2003-01
TROJ_RACKUM.A	A	CyberNotes-2003-05
Trojan.Abaxo	**N/A**	**Current Issue**
Trojan.Ailati	N/A	CyberNotes-2003-15
Trojan.Analogx	N/A	CyberNotes-2003-17
Trojan.AprilFool	N/A	CyberNotes-2003-08
Trojan.Barjac	N/A	CyberNotes-2003-05
Trojan.Boxer	N/A	CyberNotes-2003-19
Trojan.Dasmin	N/A	CyberNotes-2003-01
Trojan.Dasmin.B	B	CyberNotes-2003-03
Trojan.Downloader.Aphe	N/A	CyberNotes-2003-06
Trojan.Downloader.Inor	N/A	CyberNotes-2003-02
Trojan.Fwin	N/A	CyberNotes-2003-18
Trojan.Gaslide.Intd	**N/A**	**Current Issue**
Trojan.Grepage	N/A	CyberNotes-2003-05
Trojan.Guapeton	N/A	CyberNotes-2003-08
Trojan.Idly	N/A	CyberNotes-2003-04
Trojan.Ivanet	N/A	CyberNotes-2003-02
Trojan.Kaht	N/A	CyberNotes-2003-10
Trojan.KillAV.B	B	CyberNotes-2003-19
Trojan.KKiller	N/A	CyberNotes-2003-01
Trojan.Lear	N/A	CyberNotes-2003-10
Trojan.Mumuboy	N/A	CyberNotes-2003-13
Trojan.Mumuboy.B	**B**	**Current Issue**
Trojan.Myet	N/A	CyberNotes-2003-12
Trojan.Norio	N/A	CyberNotes-2003-19
Trojan.OptixKiller	N/A	CyberNotes-2003-16
Trojan.Poetas	N/A	CyberNotes-2003-14
Trojan.Poldo.B	B	CyberNotes-2003-02
Trojan.Poot	N/A	CyberNotes-2003-05
Trojan.PopSpy	N/A	CyberNotes-2003-11
Trojan.Progent	N/A	CyberNotes-2003-16
Trojan.ProteBoy	N/A	CyberNotes-2003-04
Trojan.PSW.Gip	N/A	CyberNotes-2003-06
Trojan.PSW.Platan.5.A	N/A	CyberNotes-2003-01
Trojan.PWS.QQPass.D	N/A	CyberNotes-2003-02
Trojan.PWS.QQPass.E	**E**	**Current Issue**
Trojan.Qforager	N/A	CyberNotes-2003-02
Trojan.Qforager.Dr	N/A	CyberNotes-2003-02
Trojan.Qwe	N/A	CyberNotes-2003-02
Trojan.Sarka	N/A	CyberNotes-2003-14
Trojan.Sidea	N/A	CyberNotes-2003-12
Trojan.Snag	N/A	CyberNotes-2003-02
Trojan.Unblockee	N/A	CyberNotes-2003-01
Trojan.Vardo	**N/A**	**Current Issue**
Trojan.Visages	N/A	CyberNotes-2003-15

Trojan	Version	CyberNotes Issue #
Trojan.Windelete	N/A	CyberNotes-2003-14
TrojanGaslid	N/A	CyberNotes-2003-18
Uploader-D	D	CyberNotes-2003-06
Uploader-D.b	D.b	CyberNotes-2003-07
VBS.ExitWin	N/A	CyberNotes-2003-12
VBS.Flipe	N/A	CyberNotes-2003-17
VBS.Kasnar	N/A	CyberNotes-2003-06
VBS.Moon.B	B	CyberNotes-2003-02
VBS.StartPage	N/A	CyberNotes-2003-02
VBS.Trojan.Lovcx	N/A	CyberNotes-2003-05
VBS.Zizarn	N/A	CyberNotes-2003-09
VBS/Fourcourse	N/A	CyberNotes-2003-06
W32.Adclicker.C.Trojan	C	CyberNotes-2003-09
W32.Bambo	N/A	CyberNotes-2003-14
W32.Benpao.Trojan	N/A	CyberNotes-2003-04
W32.CVIH.Trojan	N/A	CyberNotes-2003-06
W32.Laorenshen.Trojan	N/A	CyberNotes-2003-14
W32.Noops.Trojan	N/A	CyberNotes-2003-09
W32.Socay.Worm	N/A	CyberNotes-2003-02
W32.Spybot.dr	dr	CyberNotes-2003-15
W32.Systentry.Trojan	N/A	CyberNotes-2003-03
W32.Trabajo	N/A	CyberNotes-2003-14
W32.Xilon.Trojan	N/A	CyberNotes-2003-01
W32.Yinker.Trojan	N/A	CyberNotes-2003-04
W32/Igloo-15	N/A	CyberNotes-2003-04
W97M.Tabi.Trojan	**N/A**	**Current Issue**
Woodcot	N/A	CyberNotes-2003-16
Xin	N/A	CyberNotes-2003-03

Afcore.q (Aliases: TrojanDropper.Win32.Emaner, Backdoor.Afcore.q): This backdoor and its dropper incorporate the novel feature of using a particular mode of storing data, provided by the NTFS file system. The backdoor itself allows remote usage of the infected machine.

Backdoor-AZF: The Trojan runs as a DLL within svchost.exe. Currently, the Trojan needs to be manually installed and connected in order to achieve remote access to the victim's machine. The following registry value is created upon execution:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Svchost\netsvcs "Strings" = abc.dll@dancewithdolphin

Within the registry, the Trojan also replaces two Windows DLL, rasauto.dll and qmgr.dll with itself, depending on what mode the backdoor is running under:

- HKEY_LOCAL_MACHINE\System\ControlSet001\Services\RasAuto\Parameters "ServiceDLL" = "C:\bits.dll"
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RasAuto\Parameters "ServiceDLL" = "C:\bits.dll"
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\BITS\Parameters "ServiceDLL" = "C:\bits.dll"
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet Services\BITS\Parameters "ServiceDLL" = "C:\bits.dll"

Backdoor.Hazzer (Aliases: TROJ_RSLOCAL, Trojan.Win32.Rslocal.b): This is a Trojan Horse that downloads pornographic pictures from hard-coded URLs. It is written in Microsoft Visual C++ and is packed with UPX. When Backdoor.Hazzer is executed, it adds the value, "svchost"=<path to Trojan> or, "winlogon"=<path to Trojan> to the registry key:

- HKEY_CURRRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that the Trojan runs when you start Windows. This Trojan may copy itself to %Windir% as:

- Svchost.exe
- Explore.exe
- Exp20re.exe
- L2logon.exe
- Winlogon.exe

It also tries to delete C:\Msdos.exe and download pornographic pictures from these hard-coded URLs:

- www.xxxposition.net
- thesuperhzpcsite.com

and saves them to %Windir%.

Backdoor.IRC.Tastyred (Alias: Backdoor.IRCBot.gen): This is a Backdoor Trojan Horse that installs an mIRC client that has backdoor capabilities, which gives the Trojan's creator unlimited access to your computer. When Backdoor.IRC.Tastyred is executed, it attempts to delete %System%\Netstat.exe and drops a copy of itself to %System%\Metalrock.exe. The Trojan Horse adds the value, "Windows MeTaLRoCk service" = "metalrock.exe," to the registry key:

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

so that the Trojan runs when you start Windows. Next it attempts to connect to an IRC server to notify the author of the infection and awaits further instructions.

Backdoor.Mprox: This is a Backdoor Trojan Horse that opens a proxy server on TCP port 57123. When Backdoor.Mprox is executed, it adds the value, "Mspatch69"="<path to the Trojan>," to the registry key:

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

so that the Trojan starts when you start Windows.

Backdoor.Peeper: This is a Trojan Horse that allows its creator to control an infected computer. By default, it listens on TCP port 5180. When Backdoor.Peeper is executed, it copies itself to %System%\Internt.exe and %System%\Progmon.exe. It adds the values:

- "Internet = %System%\Internt.exe..."
- "Program File = %System%\Progmon.exe..."

to the registry key:

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

Backdoor.Peeper waits for commands from a remote user.

Backdoor.Roxy.B (Alias: TrojanProxy.Win32.Small.a): This is a proxy HTTP server that listens on TCP ports 3800, 3801, and 3802. When Backdoor.Roxy.B runs, it tries to create a mutex named Mssysviewer32 and exits if it already exists. This stops multiple instances of the backdoor from running at the same time. The Trojan adds the value, "System Initialization"= "<path to backdoor>," to the registry key:

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

so that the Backdoor runs when you start Windows. A notification is sent on UDP port 48992 to a hard-coded IP address, indicating that it is running.

Backdoor.Semes: This is a Trojan Horse that installs itself in memory and attempts to send confidential information to the Trojan's creator. It also sets the start page of Internet Explorer to a hard-coded URL. Backdoor.Semes is written in Microsoft Visual C++ and is UPX-packed.

Backdoor.Smother: Backdoor.Smother gives its creator complete access to your computer. By default, the Trojan connects on port 3264 to a server whose address is hard coded in the Trojan. When Backdoor.Smother is executed, it adds the value, "Internal"="<trojan filename>," to the registry key:

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

so that the Trojan runs when you start Windows. This Trojan connects to a specific IRC server and joins a specific channel to listen for commands. By default, it connects to port 3264 on the server.

Backdoor.Surdux: This is a Backdoor Trojan Horse that allows its creator to control your computer using Internet Relay Chat (IRC). When Backdoor.Surdux runs, it copies itself as %System%\rundlll.exe and adds the value, "PowerManagement"="Rundlll.exe," to the registry key:

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

so that the Trojan runs when you start Windows. This Trojan uses its own IRC client to connect to an IRC channel that was programmed into the Trojan.

Backdoor.Translat (Alias: Backdoor.Translat.b): This is a Backdoor Trojan Horse that gives a remote malicious user complete control over a compromised system. When Backdoor.Translat is activated, it adds the value, "Internal"="<path to trojan>," to the registry key:

- HKey_Local_Machine\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

The Trojan Horse creates the registry key:

- HKey_Current_User\Software\Microsoft\Windows\CurrentVersion\Time

and adds the value, "time"="<a number representing a date/time stamp>." It also connects to an IRC server and logs in to a predetermined channel.

Backdoor.Zombam.B (Alias: Backdoor.Zombam.i): This is a Backdoor Trojan that allows its creator to use a Web browser to access your computer. The Trojan attempts to terminate various antivirus and firewall processes. The Trojan is created using Hacktool.HTTPRat. It opens port 80, by default.

Desex (Alias: DDoS.Win32.Desex.a): This is a DDoS (Distributed Denial of Service) Trojan. It can perform a DoS attack on certain servers on Internet. The Trojan can be hiddenly dropped to users' computers and then used to perform a DoS attack. It is written in Visual C++ and its file is packed with UPX file compressor. The packed executable size is 6656 bytes, the unpacked length is 9216 bytes. Desex Trojan attacks the following 3 servers:

- 212.7.144.70
- 193.219.15.17
- 212.7.128.165

To attack these servers the Trojan uses certain functions from WS2_32.DLL library: WSAStartup, htons, inet_addr, socket, sendto, and WSACleanup. The Trojan contains the following text strings:

- sex
- de

Downloader.Dluca.C (Alias: TrojanDownloader.Win32.Dluca.a): This is a variant of the Downloader.Dluca Trojan Horse that sends information about your computer to a specific web site and downloads files onto your computer.

DownLoader-EG: Upon execution, this Trojan tries to download Trojan.exe from a web site and execute it. At the time of this description the file Trojan.exe, which purpose is currently unknown, is unavailable from the above website. It is known to have been distributed from this website using an Internet explorer vulnerability. A vulnerable browser would download and run the Trojan just by visiting the web site.

JS.Seeker.K (Alias: Trojan.JS.Seeker): This is a Trojan Horse that uses the Windows Scripting Host (WSH) to run. It modifies some Internet Explorer settings and adds a shortcut to the Favorites folder.

Keylog-Mico: This is a keylogging Trojan designed to log information on the victim machine, and post it to a remote server. Information logged includes:

- Keystrokes
- window titles
- clipboard data

Logged data is sent to a remote server (the IP of which is hardcoded in the Trojan)

Petala (Alias: Backdoor.Petala): The backdoor provides a limited access to an infected system for remote malicious users. The backdoor originate from Brazil. It is written in Visual Basic. Its file is 331 kilobytes long and has VB P-Code instead of normal Assembly instructions.

PWSteal.Lemir.E: This is a Trojan Horse that attempts to steal the password to the "Legend of Mir 2" online game and send it to the creator of the Trojan. When PWSteal.Lemir.E is executed, it copies itself as \WINNT\Intrenat.exe and %System%\WinSocks.dll and adds the value, "Intrenat"="C:\WINNT\Intrenat.exe" to the registry keys:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices

PWSteal.Lemire.E registers itself as a service process and attempts to terminate the Zone Alarm firewall program. It captures and sends the "Legend of Mir 2" password back to the Trojan's author.

PWSteal.Lemir.F (Alias: Trojan.PSW>Legendmir.aa): This is a Trojan Horse that attempts to steal the password to the "Legend of Mir 2" online game and send it to the creator of the Trojan. It is written in Delphi and is packed with UPX. When PWSteal.Lemir.D is executed, it drops a copy of itself to %System%\Wintask.exe and adds the value. "wintask"="%system%\wintask.exe," to the registry key:

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

StartPage-U (Aliases: W32/Linkadd.A, Win32.Startpage.K): This Trojan is packed with ASPack. When executed, this Trojan modifies the Internet Explorer search and start page settings to: http://www.serchv.com/1/. These changes are made through the registry:

- Hkey_Current_User\Software\Microsoft\Internet Explorer\Main\
- Hkey_Current_User\Software\Microsoft\Internet ExplorerSearch\

Various shortcuts are added to the Favorites list.

Troj/Hack, -A (Alias: Backdoor.Hackarmy, W32/Rawbot.worm, BackDoor-AZV): This is an IRC backdoor Trojan that copies itself into the Windows system folder as win32server.scr and sets the following registry entry:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Winsock32driver = win32server.scr.

The Trojan then logs on to a predefined IRC server and waits for backdoor commands.

Troj/Qhosts-1(Aliases: Qhosts-1, Delude, Qhost, TROJ_QHOSTS.A, QHOSTS-1.DR): This is a Trojan that changes the Windows primary DNS server setting so that all infected machines use the same host for the DNS queries. If the number of infected computers is high, it may effectively launch a Denial of Service attack on the DNS server. It also "hijacks" Internet Explorer browser usage so those web requests are redirected to the server chosen by the Trojan writer. The Trojan is installed and run if a user visits a web page that exploits a vulnerability in Internet Explorer. A VB script embedded in the web page is run automatically when the page is viewed using Internet Explorer. The VB script drops and runs file aolfix.exe to the user's temporary folder. Aolfix.exe is a Windows batch file that is converted to the Windows binary executable using the demo version of the Batch file Compiler V5.1 utility. Aolfix.exe creates a hidden folder bdtmp\tmp, extracts a batch file with a random name and runs the batch file. The batch file creates several files in the Windows folder. The file Hosts is responsible for Internet Explorer "hijack." Troj/Qhosts-1 copies the file HOSTS into the folder <Windows>\Help and appends the original HOST file to it. The Trojan changes the registry values:

- HKLM\System\ControlSet001\Services\Tcpip\ Parameters\DataBasePath
- HKLM\System\ControlSet002\Services\Tcpip\ Parameters\DataBasePath

so that the Trojan copy of the HOSTS files is used by the system. There are few known variants of the Trojan. Depending on the variant the Trojan may set some other registry values, such as:

- HKLM\System\CurrentControlSet\Services\VxD\MSTCP
  EnableDNS = 1
  NameServer = 216.127.92.38 or 69.57.146.14, 69.57.147.175
  Hostname = "host"
  Domain= "mydomain.com"
- HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings
  ProxyEnable= 00000000
  MigrateProxy=00000000
- HKCU\Software\Microsoft\Internet Explorer\Main
  Use Search Asst=no
  Search Page= http://www.google.com
  Search Bar=http://www.google.com/ie
- HKCU\Software\Microsoft\Internet Explorer\SearchURL
  ""="http://www.google.com/keyword/provider=gogl
- HKLM\SOFTWARE\Microsoft\Internet Explorer\Search
  SearchAssistant=http://www.google.com/ie
- HKLM\SYSTEM\ControlSet001\Services \Tcpip\Parameters\interfaces\windows r0x=your s0x
- HKLM\SYSTEM\ControlSet002\Services \Tcpip\Parameters\interfaces\windowsr0x=your s0x

Some of the variants drop and run VB script o.vbs into the Windows folder. The script attempts to use Windows Management Instrumentation to change the primary DNS server setting for the network interface.

Trojan.Abaxo: This is a Trojan Horse that sends banking details to a remote sever for the Trojan's author to collect. The Trojan arrives as a form that looks like a Bingo application from Banco Itaú.

Trojan.Gaslide.Intd: This is a variant of Trojan.Gaslide that attempts to modify how executable files are run and to changes the Home page in Microsoft Internet Explorer. Note: Due to flaws in the program, the Trojan does not behave as intended.

Trojan.Mumuboy.B (Alias: PWS-SinCom): This is a Trojan Horse that steals information from an infected computer and e-mails this information to the person who created the Trojan. It is a minor variant of Trojan.Mumuboy. When Trojan.Mumuboy.B is executed, it copies itself as %Windows%\Yz.exe and creates a .dll file with a random name in the %System% folder. The Trojan Horse steals information from an infected computer and e-mails it to the Trojan's creator. It starts an infinite loop to set the value to, "yz.exe"="<path to yz.exe>," in the registry key:

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

It attempts to terminate the following processes:

- Eghost.exe
- PasswordGuard.exe

Trojan.PWS.QQPass.E: This is another variant of the Trojan.PWS.QQPass family. It is a password stealing Trojan Horse that steals passwords and user information. The Trojan is a Visual Basic application that requires the presence of Microsoft Visual Basic run-time libraries for it to run.

Trojan.Vardo: This is a Trojan Horse program that attempts to close any windows that belong to the processes using the name Ravmon.exe. This is a file that belongs to the Reliable AntiVirus program (RAV). When Trojan.Vardo runs, it copies itself to the %System% folder and adds the value, “yyyyyyyy"="<path to trojan>,” to the registry key:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

W97M.Tabi.Trojan: This is a downloader Trojan Horse that downloads a program from a Web site, and then executes it. It is written as a Microsoft Word macro. When W97M.Tabi.Trojan runs, it connects to Taranti.homelinux.org and negotiates with it using port 23 and downloads the file, Ww.exe to C:\. This virus also executes Ww.exe.