US-CERT Cyber Security Bulletin

SB04-119 ***April 28, 2004***

Information previously published in CyberNotes will now be incorporated into US-CERT Cyber Security Bulletins, which are available from the US-CERT web site at http://www.us-cert.gov/cas/bulletins/index.html. You can also receive this information through e-mail by joining the Cyber Security Bulletin mailing list. Instructions are located at http://www.us-cert.gov/cas/signup.html#tb.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between April 6 and April 26, 2004. 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
Apache Software Foundation[1] ***Vendors issue advisories*** [2, 3]	**Unix**	**Gregory Trubetskoy mod_python 2.7-2.7.8, 3.0-3.0.3**	**A remote Denial of Service vulnerability exists when a malicious user submits a malformed query.**	**Upgrade available at: http://httpd.apache.org/modules/python-download.cgi** ***Conectiva:*** **ftp://atualizacoes.conectiva.com.br/** ***TurboLinux:*** **ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32**	**Apache mod_python Module Remote Denial of Service** **CVE Name: CAN-2003-0973**	**Low**	**Bug discussed in newsgroups and websites.**
Apache Software Foundation[4]	Windows 95/98/NT 4.0/2000, XP, Mac OS X 10.x, Unix	Apache 1.3.29 & prior	A buffer overflow vulnerability exists in the 'ebcdic2ascii()' function in 'src/ap/ap_ebcdi.c,' when a 64 byte value is copied into a variable that may not be properly sized on some older architectures, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Apache ebcdic2ascii() Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

[1] Secunia Advisory, SA10325, December 1, 2003.
[2] Turbolinux Security Advisory, TLSA-2004-13, April 7, 2004.
[3] Conectiva Linux Security Announcement, CLA-2004:837, April 12, 2004.
[4] Bugtraq, April 24, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Apache Software Foundation[5] *Vendors issue advisories* [6, 7] *HP issues advisory*[8, 9, 10, 11]	Mac OS X 10.x, Unix	Apache 2.0.35-2.0.48	A remote Denial of Service vulnerability exists due to a handling error within the SSL engine when receiving normal HTTP requests on the SSL port of a SSL-enabled server.	Patch available at: http://cvs.apache.org/viewcvs.cgi/httpd-2.0/modules/ssl/ssl_engine_io.c?r1=1.117&r2=1.118 *Netwosix:* http://www.netwosix.org/adv06.html *Trustix:* http://www.trustix.org/errata/misc/2004/TSL-2004-0017-apache.asc.txt *Conectiva:* http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000839 *Hewlett Packard:* http://www.software.hp.com/ *SuSE:* ftp://ftp.suse.com/pub/suse/i386/update/ *TurboLinux:* ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/Desktop/10/updates/	Apache Mod_SSL HTTP Request Remote Denial of Service CVE Name: CAN-2004-0113	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Apache Software Foundation[12] *Trustix issues advisory*[13] *More advisories issued*[14, 15, 16]	MacOS X 10.x, Unix	Apache 2.0 a9, 2.0, 2.0.28 Beta, 2.0.28, 2.0.32, 2.0.35-2.0.48	An input validation vulnerability exists because escape character sequences can be injected into apache log files, which could let a remote malicious user create arbitrary files or execute arbitrary code.	Upgrades available at: http://httpd.apache.org/download.cgi Netwosix http://download.netwosix.org/0006/nepote *Trustix:* http://www.trustix.org/errata/ *Hewlett Packard:* http://www.software.hp.com/ *SuSE:* ftp://ftp.suse.com/pub/suse/i386/update/ *TurboLinux:* ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/Desktop/10/updates/	Apache Error Log Escape Sequence Injection CVE Name: CAN-2003-0020	High	Bug discussed in newsgroups and websites. There is no exploit code required.

[5] Secunia Advisory, SA11092, March 10, 2004.
[6] Netwosix Linux Security Advisory, LNSA-#2004-0006, March 25, 2004.
[7] Trustix Secure Linux Security Advisory, TSLSA-2004-0017, March 30, 2004.
[8] Turbolinux Security Advisory, TLSA-2004-11, April 7, 2004.
[9] HP Security Bulletin, HPSBUX0102, April 26, 2004.
[10] SUSE Security Announcement, SuSE-SA:2004:009, April 14, 2004.
[11] Conectiva Security Advisory, CLSA-2004:839, April 14, 2004.
[12] SecurityFocus, March 20, 2004.
[13] Trustix Secure Linux Security Advisory, TSLSA-2004-0017, March 30, 2004.
[14] Turbolinux Security Advisory, TLSA-2004-11, April 7, 2004. .
[15] HP Security Bulletin, HPSBUX01022, April 26, 2004.
[16] SUSE Security Announcement, SuSE-SA:2004:009, April 14, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Apache Software Foundation[17, 18] ***Trustix issues advisory***[19] ***More advisories issued***[20, 21, 22]	**MacOS X 10.x, Unix**	**Apache 2.0 a9, 2.0, 2.0.28 Beta, 2.0.28, 2.0.32, 2.0.35-2.0.48**	**A remote Denial of Service vulnerability exists via a listening socket on a rarely accessed port.**	**Upgrades available at:** **http://httpd.apache.org/download.cgi** **Netwosix** **http://download.netwosix.org/0006/nepote** ***Trustix:*** **http://www.trustix.org/errata/** ***Hewlett Packard:*** **http://www.software.hp.com/** ***IBM:*** **http://www-1.ibm.com/support/docview.wss?rs=177&context=SSEQTJ&uid=swg24006719** ***SuSE:*** **ftp://ftp.suse.com/pub/suse/i386/update/**	**Apache Connection Blocking Denial of Service** **CVE Name: CAN-2004-0174**	**Low**	**Bug discussed in newsgroups and websites.**
artmedic webdesign [23]	Windows, Unix	Artmedic Hpmaker	A vulnerability exists in the 'index.php' script due to insufficient validation of the 'start.htm' file, which could let a remote malicious user execute arbitrary code and obtain sensitive information.	No workaround or patch available at time of publishing.	Artmedic Webdesign Hpmaker 'index.php' script	Medium/ **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 has been published.
BEA Systems, Inc.[24, 25]	Windows NT 4.0/2000, Unix	WebLogic Express & Server 7.0, SP1-SP4, 8.1, SP1&SP2, Win32 7.0, SP1-SP4, Win32 8.1, SP1&SP2	A vulnerability exists in the default authentication provider, which could let a remote malicious user obtain unauthorized administrative access.	Updates available at: http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04_52.00.jsp	WebLogic Server/Express Authentication Provider Privilege Inheritance	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.

[17] SecurityFocus, March 19, 2004.
[18] VU#132110, https://www.kb.cert.org/vuls/id/132110.
[19] Trustix Secure Linux Security Advisory, TSLSA-2004-0017, March 30, 2004.
[20] IBM Advisory, PQ85834, April 7, 2004.
[21] HP Security Bulletin, HPSBUX01022, April 26, 2004.
[22] SUSE Security Announcement, SuSE-SA:2004:009, April 14, 2004.
[23] SecurityFocus, April 24, 2004.
[24] BEA Security Advisory, BEA04-52.00, April 13, 2004.
[25] VU#470470, http://www.kb.cert.org/vuls/id/470470.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
BEA Systems, Inc.[26, 27]	Windows NT 4.0/2000, Unix	WebLogic Express & Server 7.0, SP1-SP4, 8.1, SP1&SP2, Win32 7.0, SP1-SP4, Win32 8.1, SP1&SP2	A vulnerability exists when SSL connections are established because a connection may be approved if the certificate chain is valid but the custom trust manager rejects the chain, which could let a remote malicious user impersonate a target user or a target server.	Updates available at: ftp://ftpna.beasys.com/pub/releases/security/CR129371_81sp2.jar	WebLogic Server/Express Certificate Chain User Impersonation	Medium	Bug discussed in newsgroups and websites.
BEA Systems, Inc.[28, 29]	Windows NT 4.0/2000, Unix	WebLogic Express & Server 7.0, SP1-SP4, 8.1, SP1, Win32 7.0, SP1-SP4, Win32 8.1, SP1	A vulnerability exists in web applications using the 'illegal' URL pattern '/dir*' instead of the valid syntax '/dir/*,' which could let a remote malicious user obtain sensitive information.	Upgrades available at: http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04_56.00.jsp	WebLogic Server & WebLogic Express Illegal URI Pattern Potential	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
BEA Systems, Inc.[30, 31]	Windows NT 4.0/2000, Unix	WebLogic Express & Server 6.1, SP1-SP6, 7.0, SP1-SP4, 8.1, SP1&SP2, Win32 6.1, SP1-SP6, Win32 7.0, SP1-SP4, Win32 8.1, SP1&SP2	A vulnerability exists in 'config.xml' due to clear text storage of credentials, which could let a malicious user obtain sensitive information.	Updates available at: http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04_53.00.jsp	WebLogic Server/Express Potential Password Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[26] BEA Security Advisory, BEA04-54.00, April 13, 2004.
[27] VU#566390, http://www.kb.cert.org/vuls/id/566390.
[28] BEA Systems Security Advisory, BEA04-56.00, April 20, 2004.
[29] VU#184558, http://www.kb.cert.org/vuls/id/184558.
[30] BEA Security Advisory, BEA04-53.00, April 13, 2004.
[31] VU#920238, http://www.kb.cert.org/vuls/id/920238.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
BEA Systems, Inc[32, 33]	Windows NT 4.0/2000, Unix	WebLogic Express & Server 7.0 .0.1, SP1-SP4, 7.0, SP1-SP4, 8.1, SP1&SP2, Win32 7.0.0.1, SP1&SP2, Win32 7.0, SP1-SP4, Win32 8.1, SP1&SP2	A vulnerability exists due to a design error that implements certain internal methods that can reveal the username and passwords that were used to boot the system, which could let a malicious user obtain administrative access.	Updates available at: http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04_55.00.jsp	WebLogic Server/Express Password Disclosure Vulnerability	**High**	Bug discussed in newsgroups and websites.
BEA Systems, Inc.[34, 35]	Windows NT 4.0/2000, Unix	WebLogic Express & Server 6.1, SP1-SP6, 7.0, SP1-SP4, 8.1, SP1&SP2, Win32 6.1, SP1-SP6, Win32 7.0, SP1-SP4, Win32 8.1, SP1&SP2	A vulnerability exists when an application invokes a 'remove()' method from EJB (Enterprise Java Bean) Objects, which could let a remote malicious user cause a Denial of Service.	Upgrades available at: http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04_57.00.jsp	WebLogic Server/Express EJB Object Removal Remote Denial of Service	Low	Bug discussed in newsgroups and websites.
BEA Systems, Inc.[36, 37]	Windows NT 4.0/2000, Unix	WebLogic Express & Server 8.1, SP1&SP2, Win32 8.1, SP1&SP2	A vulnerability exists in the 'config.sh' and 'config.cmd' scripts, which could let a malicious user obtain knowledge of administrative credentials.	Upgrades available at: http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04_58.00.jsp	WebLogic Server/Express 'config.sh' & 'config.cmd' Information Disclosure	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.

[32] BEA Security Advisory, BEA04-55.00, April 13, 2004.
[33] VU#352110, http://www.kb.cert.org/vuls/id/352110.
[34] BEA Systems Security Advisory, BEA04-57.00, April 20, 2004.
[35] VU#658878, http://www.kb.cert.org/vuls/id/658878.
[36] BEA Systems Security Advisory, BEA04-58.00, April 20, 2004.
[37] VU#574222, http://www.kb.cert.org/vuls/id/574222.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Black board[38]	Windows, NT 4.0/2000, Unix	Black board 5.0, 5.0.2, 5.5, 5.5.1, 6.0	Multiple Cross-Site Scripting vulnerabilities exist in the 'addressbook.pl,' 'tasks.pl,' and 'calendar.pl' scripts due to insufficient validation of user-supplied URI input, which could let a remote malicious user execute arbitrary HTML or script code.	No workaround or patch available at time of publishing.	Blackboard Learning System Multiple Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Exploits have been published.
bsd-games [39]	Unix	bsd-games 2.9, 2.12-2.14	A buffer overflow vulnerability exists due to insufficient bounds checking of file names, which could let a malicious user obtain elevated privileges.	No workaround or patch available at time of publishing.	BSD-Games File Name Buffer Overflow	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
cdp. Source forge.net [40] ***Exploit script published [41]***	**Unix**	**cdp 0.4, 0.33**	**A buffer overflow vulnerability exists in the 'printTOC()' function due to insufficient bounds checking, which could let a malicious user cause a Denial of Service and execute arbitrary code.**	**No workaround or patch available at time of publishing.**	**CDP PrintTOC Function Buffer Overflow**	**Low/High (High if arbitrary code can be executed)**	**Bug discussed in newsgroups and websites.** ***Exploit script has been published.***
Chi Kien Uong [42]	Windows, Unix	Advanced Guest-book 2.2	An input validation vulnerability exists when a specially crafted password value is supplied that contains no username value, which could let a remote malicious user obtain administrative access.	No workaround or patch available at time of publishing.	Advanced Guestbook Input Validation	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Cisco Systems[43, 44, 45]	Multiple	Cisco IOS 12.x, R12.x	A remote Denial of Service vulnerability exists due to an error within the processing of solicited SNMP requests.	Updates and workarounds available at: http://www.cisco.com/warp/public/707/cisco-sa-20040420-snmp.shtml	Cisco Internet Operating System SNMP Message Processing Remote Denial of Service	Low	Bug discussed in newsgroups and websites.

[38] Secunia Advisory, SA11355, April 14, 2004.
[39] SecurityFocus, April 17, 2004.
[40] SecurityTracker Alert, 1009606, April 1, 2004.
[41] SecurityFocus, April 14, 2004.
[42] SecurityTracker Alert , 1009928, April 23, 2004.
[43] Cisco Security Advisory, 50980, April 23, 2004.
[44] VU#162451, http://www.kb.cert.org/vuls/id/162451.
[45] TA04-111B, http://www.us-cert.gov/cas/techalerts/TA04-111B.html.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Cisco Systems[46]	Windows, Unix	Cisco VPN Client for Linux 3.5.1, 3.5.2 B, 3.5.2, 3.5.4, 3.6, 3.6.1, VPN Client for Windows 2.0, 3.0, 3.0.5, 3.1, 3.5.1 C, 3.5.1, 3.5.2 B, 3.5.2, 3.5.4, 3.6 (Rel), 3.6, 3.6.1, 4.0.2 C, 4.0.2 A	A vulnerability exists because Group Passwords are stored in memory in clear text, which could let a malicious user obtain sensitive information.	The vendor has advised that due to the documented risks associated with Group Password authentication schemes, organizations should evaluate their necessity and implement more secure authentication protocols where possible.	Cisco IPsec VPN Client Group Password Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published. Vulnerability has appeared in the press and other public media.
Citadel/ UX[47]	Unix	Citadel/ UX 5.90, 5.91	A vulnerability exists due to insecure default permissions on the 'data' directory and database files, which could let a malicious user obtain sensitive information.	Upgrades available at: http://my.citadel.org/download/citadel-ux-6.20p1.tar.gz	Citadel/UX Insecure Default Permissions	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
David Collier-Brown[48]	Unix	ssmtp 2.50.6	Two vulnerabilities exist due to format string errors within the 'die()' and 'log_event()' functions, which could let a remote malicious user cause a Denial of Service and potentially execute arbitrary code.	**Debian:** http://security.debian.org/pool/updates/main/s/ssmtp/	ssmtp Mail Transfer Format String Vulnerabilities	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
David Collier-Brown[49]	Unix	ssmtp 2.50.6	A vulnerability exists due to a design error that causes the application to fail to validate files before writing to them, which could let a remote malicious user corrupt arbitrary system files, obtain elevated privileges or cause a Denial of Service.	No workaround or patch available at time of publishing.	SSMTP Mail Transfer Agent Symbolic Link	Low/ Medium (Medium if files are corrupted or elevated privileges are obtained)	Bug discussed in newsgroups and websites. There is no exploit code required.

[46] Cisco Security Notice, 50600, April 15, 2004.
[47] Securiteam, April 18, 2004.
[48] Debian Security Advisory, DSA 485-1, April 14, 2004.
[49] Bugtraq, April 18, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
emil[50] ***SuSE issues advisory***[51]	**Unix**	**emil 2.0.4, 2.0.5, 2.1.0-beta9**	**Multiple vulnerabilities exist: a buffer overflow vulnerability exists due to boundary errors exist within the 'encode_mime(),' 'encode_uuencode(),' and 'decode_uuencode()' functions, which could let a local/remote malicious user execute arbitrary code; and format string errors exist in various functions when constructing error messages, which could let a local/remote malicious user execute arbitrary code.**	**Debian:** **http://security.debian.org/pool/updates/main/e/emil/** ***SuSE:*** **ftp://ftp.suse.com/pub/suse/i386/update/**	**Emil Multiple Buffer Overflow & Format String**	**High**	**Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.**
Emule-Project.net[52] ***Exploit script published***[53]	**Windows**	**Emule 0.42 d**	**A buffer overflow vulnerability exists due to a boundary error within the 'DecodeBase16()' function that is used in the web server and IRC client code for decoding hexadecimal strings, which could let a remote malicious user execute arbitrary code.**	**Upgrade available at:** **http://umn.dl.sourceforge.net/sourceforge/emule/eMule0.42e-Installer.exe**	**eMule Remote Buffer Overflow**	**High**	***Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.***
Epic Games[54]	Windows, MacOS, Unix	Unreal Engine 436, 433, Unreal Tourna-ment 451b, 2003 2225 win32, macOS, 2003 2199 win32, macOS	An input validation vulnerability exists in the UMOD 'manifest.ini' file, which could let a remote malicious user overwrite files on the target system.	No workaround or patch available at time of publishing.	Unreal Game Engine UMOD Input Validation	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
eSignal[55] ***Upgrade now available***[56]	**Windows**	**eSignal 7.5, 7.6**	**A buffer overflow vulnerability exists due to a due to a boundary error within 'Specs.dll' when parsing incoming data requests, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.**	***Upgrade available at:*** **http://www.esignal.com/executables/esignal_76.exe**	**ESignal Remote Buffer Overflow**	**Low/High** **(High if arbitrary code can be executed)**	**Bug discussed in newsgroups and websites. Exploit script has been published.**

[50] Debian Security Advisory, DSA 468-1, March 24, 2004.
[51] SuSE Security Announcement, SuSE-SA:2004:009, April 14, 2004.
[52] SecurityTracker Alert, 1009651, April 3, 2004
[53] SecurityFocus, April 13, 2004.
[54] SecurityFocus, April 22, 2004.
[55] Secunia Advisory, SA11222, March 26, 2004.
[56] Bugtraq, April 6, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Ethereal Group[57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69] ***Advisories issued and exploit script published***[70, 71, 72, 73] ***More advisories issued***[74, 75]	**Windows 95/98/ME/ NT 4.0, Unix**	**Ethereal 0.8.13, 0.8.14, 0.8.18, 0.8.19, 0.9-0.9.16, 0.10-0.10.2**	**Multiple vulnerabilities exist: Thirteen stack-based buffer overflow vulnerabilities exist in various protocol dissectors (BGP, EIGRP, IGAP, IRDA, NetFlow, PGM, UCP, NetFlow, IrDA, ISUP, and TCAP), which could let a remote malicious user execute arbitrary code; a remote Denial of Service exists when a malicious user submits a carefully-crafted RADIUS packet; a remote Denial of Service vulnerability exits due to a zero length Presentation protocol selector; and a remote Denial of Service vulnerability exist within the handling of malformed color filter files.**	**Upgrades available at:** **http://www.ethereal.com/download.html** ***Conectiva:*** **http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000835** ***Netwosix:*** **http://download.netwosix.org/0007/nepote** ***Mandrake:*** **http://www.mandrakesecure.net/en/advisories/** ***RedHat:*** **ftp://updates.redhat.com/9/en/os/** ***OpenPKG:*** **ftp://ftp.openpkg.org/release/** ***SGI:*** **ftp://patches.sgi.com/support/free/security/advisories/**	**Ethereal Multiple Vulnerabilities** **CVE Names: CAN-2004-0176, CAN-2004-0365, CAN-2004-0367**	**Low/High** **(High if arbitrary code can be executed)**	**Bug discussed in newsgroups and websites. Exploit script has been published.**
Fastream[76]	Windows	NetFILE FTP/Web Server 6.5.1 .980	A remote Denial of Service vulnerability exists due to an error within the login procedure of the FTP server.	Affected users should contact the vendor to obtain upgrades.	NetFile FTP/Web Server Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Vulnerability may be exploited with an FTP or telnet client.

[57] Ethereal Advisory, enpa-sa-00013, March 22, 2004.
[58] VU#119876, https://www.kb.cert.org/vuls/id/119876.
[59] VU#124454, https://www.kb.cert.org/vuls/id/124454.
[60] VU#125156, https://www.kb.cert.org/vuls/id/125156.
[61] VU#433596, https://www.kb.cert.org/vuls/id/433596.
[62] VU#591820, https://www.kb.cert.org/vuls/id/591820.
[63] VU#644886, https://www.kb.cert.org/vuls/id/644886.
[64] VU#659140, https://www.kb.cert.org/vuls/id/659140.
[65] VU#695486, https://www.kb.cert.org/vuls/id/695486.
[66] VU#740188, https://www.kb.cert.org/vuls/id/740188.
[67] VU#792286, https://www.kb.cert.org/vuls/id/792286.
[68] VU#864884, https://www.kb.cert.org/vuls/id/864884.
[69] VU#931588, https://www.kb.cert.org/vuls/id/931588.
[70] Netwosix Linux Security Advisory, LNSA-#2004-0007, March 29, 2004.
[71] Mandrakelinux Security Update Advisory, MDKSA-2004:024, March 31, 2004.
[72] Red Hat Security Advisories RHSA-2004:136-09 & RHSA-2004:137-01, March 30 & 31, 2004.
[73] Conectiva Linux Security Advisory, CLSA-2004:835, March 31, 2004.
[74] OpenPKG Security Advisory, OpenPKG-SA-2004.015, April 16, 2004.
[75] SGI Security Advisory, 20040404-01-U, April 21, 2004.
[76] Securiteam, April 21, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Francisco Burzi[77]	Windows, Unix	PHP-Nuke 6.0, 6.5, RC1-RC3, FINAL, BETA 1, 6.6, 6.7, 6.9, 7.0. FINAL, 7.1, 7.2	A Cross-Site Scripting vulnerability exists in the 'cookiedecode()' function in 'mainfile.php' due to insufficient sanitization, which could let a remote malicious user execute arbitrary HTML or script code.	No workaround or patch available at time of publishing.	PHP-Nuke 'cookie decode()' Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Francisco Burzi[78]	Windows, Unix	PHP-Nuke 6.0, 6.5, RC1-RC3, FINAL, BETA 1, 6.6, 6.7, 6.9, 7.0, FINAL, 7.1, 7.2	Multiple vulnerabilities exist: a vulnerability exists because input passed to the 'user' parameter is base64 decoded before it is used in SQL queries, which could let a remote malicious user bypass authentication procedures, obtain sensitive information, or execute arbitrary code; and a vulnerability exists in the 'admin' parameter, which could let a remote malicious user perform certain administrative functions.	No workaround or patch available at time of publishing.	PHP-Nuke Multiple SQL Injection Vulnerabilities	Medium/ **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 has been published.
Fusionphp [79]	Windows, Unix	Fusion News 3.6.1	A Cross-Site Scripting vulnerability exists because input passed to 'id' parameter in 'fullnews.php' isn't properly verified before it is returned to the user, which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	Fusion News Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
Gnome Development Team[80]	Unix	Eazel Nautilus 1.0.4, 2.2, 2.2.1	A Denial of Service vulnerability exists due to a buffer overflow when a user attempts to delete a malicious directory and that directory is later operated on in the 'Trash' folder.	No workaround or patch available at time of publishing.	Eazel Nautilus Trash Folder Handler Buffer Overflow	Low	Bug discussed in newsgroups and websites.

[77] waraxe-2004-SA#016, April 12, 2004.
[78] waraxe-2004-SA#017, April 13, 2004.
[79] Secunia Advisory, SA11474, April 23, 2004.
[80] Bugtraq, April 12, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
GNU[81, 82, 83, 84] ***SGI issues another advisory***[85] ***SuSE issues advisory***[86]	**Unix**	**Mailman 1.0, 1.1, 2.0 beta3 - beta5, 2.0-2.0.13, 2.1, 2.3**	**A remote Denial of Service vulnerability exists in 'MailCommandHandler.py' when a malicious user submits a specially crafted e-mail message.**	**Upgrade available at:** **http://ftp.gnu.org/gnu/mailman/** **Debian:** **http://security.debian.org/pool/updates/main/m/mailman/** **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** **RedHat:** **http://rhn.redhat.com/errata/RHSA-2004-019.html** **SGI:** **ftp://patches.sgi.com/support/free/security/patches/ProPack/2.3/patch10050.tar.gz** ***SuSE:*** **ftp://ftp.suse.com/pub/suse/i386/update/**	**GNU Mailman Remote Denial of Service** **CVE Name: CAN-2003-0991**	**Low**	**Bug discussed in newsgroups and websites.**
Green Eggs, Inc.[87]	Windows	News TraXor Website Management Script 2.9 beta	A vulnerability exists in the default installation because the 'Dbase/nTrax.mdb' file stores usernames, passwords, and configuration data. in a publicly accessible directory, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	NewsTraXor Remote Database Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
IpSwitch[88]	Windows NT 4.0/2000, XP, 2003	IMail Express 8.0 3	A buffer overflow vulnerability exists in the Web Messaging component due to insufficient bounds checking of HTML messages, which could let a remote malicious user execute arbitrary code.	Upgrade available at: ftp://ftp.ipswitch.com/install/imailex.exe	IMail Express Web Messaging Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
isesam.com [89]	Windows, Unix	isesam Gemitel 3.50	A vulnerability exists in the 'html/affich.php' file due to insufficient validation of the 'sp-turn.php' file, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Gemitel 'html/affich.php' file Arbitrary Code Execution	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.

[81] Debian Security Advisories, DSA 436-1 & DSA 436-2, February 8 & 21, 2004.
[82] RedHat Security Advisory, RHSA-2004:019-04, February 9, 2004.
[83] SGI Security Advisory, 20040201-01-U, February 11, 2004.
[84] Mandrake Linux Security Update Advisory, MDKSA-2004:013, February 13, 2004.
[85] SGI Security Advisory, 20040202-01-U:, February 26, 2004.
[86] SUSE Security Announcement, SuSE-SA:2004:009, April 14, 2004.
[87] SecurityFocus, April 22, 2004.
[88] Secunia Advisory, SA11352, April 13, 2004.
[89] Securiteam, April 18, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Jon Middelton [90]	Unix	Psionic Logcheck 1.1.1	A vulnerability exists due to the insecure creation of temporary directories in the '/var/tmp' directory, which could let a malicious user obtain root privileges.	Upgrade available at: http://security.debian.org/pool/updates/main/l/logcheck/	Logcheck Unsafe Temporary Directory CVE Name: CAN-2004-0404	**High**	Bug discussed in newsgroups and websites.
Journal-ness Project [91]	Windows, Unix	Project Journal-ness 1.11-1.13, 2.1-2.1.4, 3.0.0-3.0.5. 3.0.7	An unspecified vulnerability has been reported in Journalness that may permit unauthorized users to create or modify journal posts.	Upgrade available at: https://sourceforge.net/project/showfiles.php?group_id=101583	Journalness Unspecified Post Access	Medium	Bug discussed in newsgroups and websites.
KAME Project [92]	Unix	Racoon	A Denial of Service vulnerability exits due to an error when allocating memory for ISAKMP messages.	Patch available at: http://www.securityfocus.com/data/vulnerabilities/patches/racoon_patch	Racoon Malformed ISAKMP Packet Denial of Service	Low	Bug discussed in newsgroups and websites.
KDE [93]	Unix	Kon-queror 3.2.1	A Denial of Service vulnerability exists when processing malformed bitmap files.	No workaround or patch available at time of publishing.	Konqueror Bitmap File Processing Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
Kine-sphere Corpora-tion [94]	Windows	eXchange POP3 4.0, 5.0	A buffer overflow vulnerability exists due to a boundary error when handling SMTP connections, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Exchange POP3 Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.

[90] Debian Security Advisory, DSA 488-1, April 16, 2004.
[91] Secunia Advisory, SA11431, April 21, 2004.
[92] Secunia Advisory, SA11410, April 19, 2004.
[93] SecurityFocus, April 13, 2004.
[94] Bugtraq, April 19, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
LBL[95, 96] ***More vendors issue advisories***[97, 98, 99, 100]	**Unix**	**tcpdump 3.4 a6, 3.4, 3.5 alpha, 3.5, 3.5.2, 3.6.2 3.6.3, 3.7-3.7.2, 3.8.1**	**Two vulnerabilities exist: a buffer overflow vulnerability exists in 'print-isakmp.c' due to insufficient validation of user-supplied input in ISAKMP packets, which could let a remote malicious user cause a Denial of Service and possibly allow the execution of arbitrary code; and a vulnerability exists when a remote malicious user submits an ISAKMP Identification payload with a specially crafted payload length value that is less than eight bytes.**	**Upgrades available at: http://www.tcpdump.org/release/tcpdump-3.8.3.tar.gz** **Trustix:** **ftp://ftp.trustix.org/pub/trustix/updates/** ***Debian:*** **http://security.debian.org/pool/updates/main/t/tcpdump** ***Mandrake:*** **Http://www.mandrakesecure.net/en/advisories/** ***OpenPKG:*** **ftp://ftp.openpkg.org/release/** ***Slackware:*** **ftp://ftp.slackware.com/pub/slackware/**	**TCPDump ISAKMP Buffer Overflow & ISAKMP Identification Payload Integer Underflow** **CVE Names: CAN-2004-0183, CAN-2004-0184**	**Low/High** **(High if arbitrary code can be executed)**	**Bug discussed in newsgroups and websites. An exploit script has been published for the ISAKMP Identification Payload vulnerability.**
LCDProc[101] ***Exploit script published***[102]	**Unix**	**LCDProc 0.3, 0.4, 0.4.1 -r1, 4.0, 4.1-4.4**	**Multiple vulnerabilities exist: a buffer overflow vulnerability exists, which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability exists in the 'parse_all_client_messages()' Function, which could let a remote malicious user execute arbitrary code; and a buffer overflow and format string vulnerability exists in the 'test_func_func()' function, which could let a remote malicious user execute arbitrary code.**	**Upgrade available at: http://lcdproc.omnipotent.net/download/lcdproc-0.4.5.tar.gz**	**LCDd Multiple Remote Vulnerabil-ities**	**High**	**Bug discussed in newsgroups and websites. *Proof of Concept exploit script has been published.***
Macro-media[103]	Windows NT 4.0/2000, XP, Unix	Cold Fusion MX 6.0, J2EE 5.0, J2EE 6.0	A remote Denial of Service vulnerability exists when the software attempts to write oversized error messages.	Upgrades available at: http://www.macromedia.com/software/coldfusion/productinfo/upgrade/	ColdFusion MX Oversized Error Message Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.

[95] Rapid7, Inc. Security Advisory, R7-0017, March 30, 2004.
[96] Trustix Secure Linux Security Advisory, TSLSA-2004-0015, March 30, 2004.
[97] Debian Security Advisory, DSA 478-1, April 6, 2004.
[98] OpenPKG Security Advisory, OpenPKG-SA-2004.010, April 7, 2004.
[99] Mandrakelinux Security Update Advisory, MDKSA-2004:030, April 15, 2004.
[100] Slackware Security Advisory, SSA:2004-108-01, April 17, 2004.
[101] Priv8 Security Research - #2004-001, April 8, 2004.
[102] PacketStorm, April 9, 2004.
[103] Securiteam, April 18, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Macro-media[104]	Windows NT 4.0/2000, XP, Unix	Cold Fusion MX 6.1, J2EE 6.1	A remote Denial of Service vulnerability exits when file uploads are started via an HTML form, but are interrupted before they complete.	Patches available at: http://download.macromedia.com/pub/security/mpsb04-06.zip	ColdFusion MX File Upload Remote Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required. Vulnerability has appeared in the press and other public media.
Mambo[105] ***Update available & exploit script published***[106]	**Unix**	**Mambo Open Source 4.5, 4.6**	**A vulnerability exists in the 'mosConfig_absolute_path' parameter due to insufficient verification, which could let a remote malicious user execute arbitrary code.**	**Update available at:** http://prdownloads.sourceforge.net/mambo/MamboV4.5-Stable.tar.gz?download	**Mambo Open Source mosConfig_ absolute_path**	**High**	**Bug discussed in newsgroups and websites. There is no exploit code required.** ***Exploit script has been published.***
Martin Prikryl[107]	Windows	WinSCP 3.5.6	A remote Denial of Service vulnerability exists when a malicious user submits a specially crafted 'sftp://' or 'scp://' URL.	No workaround or patch available at time of publishing.	WinSCP Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
McAfee[108]	Windows	ePolicy Orchestra-tor 2.5, SP1, 2.5.1, 3.0, SP2a	An unspecified vulnerability exists which could let a malicious user execute arbitrary commands.	Upgrades available at: http://download.nai.com/products/patches/	ePolicy Orchestrator Undisclosed Command Execution CVE Name: CAN-2004-0038	**High**	Bug discussed in newsgroups and websites.
Michael Bacarella[109]	Unix	ident2 .999 c, 1.3-1, 1.3, 1.4	A buffer overflow vulnerability exists in the 'common.c' in the child_service() function due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code.	**Debian:** http://security.debian.org/pool/updates/main/i/ident2	IDent2 Daemon Child_Service Remote Buffer Overflow CVE Name: CAN-2004-0408	**High**	Bug discussed in newsgroups and websites.

[104] Macromedia Security Bulletin, MPSB04-06, April 15, 2004.
[105] Bugtraq, January 18, 2004.
[106] SecurityFocus, April 16, 2004.
[107] Securiteam, April 15, 2004.
[108] Secunia Advisory, SA11471, April 23, 2004.
[109] Debian Security Advisory, DSA 494-1, April 21, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [110]	Windows 98/ME/NT 4.0/2000, XP	Office XP, SP1-SP3, Developer Edition, Visual Studio .NET Enterprise Architect Edition, Developer Edition, Profes-sional Edition, Trial Edition,	A vulnerability exists due to a configuration error that allows users outside of the Administrator and Debbugger groups to debug JavaScripts, which could let a malicious user execute arbitrary code.	Updates available at: http://www.microsoft.com/downloads/details.aspx?familyid=12A8CCDF-2643-477D-94D4-4677A02AAA7E&displaylang=en	Visual Studio .NET Debugger Privilege Enforcement Weakness	**High**	Bug discussed in newsgroups and websites.
Microsoft [111]	Windows 95/98/ME/ NT 4.0/2000, XP, 2003	Internet Explorer 5.5, preview, SP1&SP2, 6.0 SP1	A Denial of Service vulnerability exists when processing malformed bitmap files.	No workaround or patch available at time of publishing.	Internet Explorer Bitmap File Processing Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
Microsoft [112] ***Microsoft re-releases bulletin[113]*** ***Microsoft updates bulletin[114]***	**Windows NT 4.0/2000**	**Exchange Server 5.5, 5.5SP1-4, 2000 Advanced Server 0.0, 0.0SP1& 2, Data-center Server 0.0, 0.0SP1& 2, Profes-sional 0.0, 0.0SP1& 2, 2000 Server 0.0, 0.0SP1&2**	**A vulnerability exists in the way that the Windows 2000 SMTP service and Microsoft Exchange Server 5.5 interact with the NTLM authentication layer, which could let a malicious user obtain unauthorized user-level access to the SMTP service.** ***Updated bulletin issued states that the Windows 2000 patch for MS02-012 and MS02-011 are the same.*** ***Bulletin updated to advise of the availability of an update for Windows NT Server 4.0 and to advise Exchange Server 5.0 customers on how to better protect themselves.***	**Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-011.asp**	**Microsoft Windows SMTP Service Authenti-cation** **CVE Name: CAN-2002-0054**	**Medium**	**Bug discussed in newsgroups and websites.**

[110] SecurityFocus, April 16, 2004.
[111] SecurityFocus, April 14, 2004.
[112] Microsoft Security Bulletin, MS02-011, February 27, 2002.
[113] Microsoft Security Bulletin, MS02-011 (Version 2.0), March 12, 2002.
[114] Microsoft Security Bulletin, MS02-011 V3.0, April 13, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [115] *Avaya releases an advisory to announce Avaya System Products shipping on Microsoft platforms are also affected by this vulnera-bility*[116]	Windows 2000, XP	Windows 2000 Advanced Server, SP1-SP4, 2000 Data-center Server, SP1-SP4, 2000 Profes-sional, SP1-SP4, 2000 Server, SP1-SP4, XP Home, SP1, XP Media Center Edition, XP Profes-sional, SP1 *Avaya Definity One Media Servers, IP600 Media Servers, S3400 Modular Messag-ing, S8100 Media Servers*	A multi-threaded race condition vulnerability exists in the Windows RPC DCOM functionality with the MS03-039 patch installed when handling a large number of RPC requests, which could let a remote malicious user cause a Denial of Service. *Note: This vulnerability exists in the most current patch-levels of the Windows operating systems, including computers patched against the issues described in Microsoft Security Bulletin MS03-039.*	Due to the possibility of the existence of working exploit being distributed in the wild, users are advised to apply all available workarounds until the vendor can acknowledge and patch the issue. Workarounds available at: http://xforce .iss.net/xforce/alerts/id/155 *Avaya advise that customers follow the Microsoft recommendations for the resolution of this issue.*	Windows RPCSS Multi-thread Race Condition CVE Name: CAN-2003-0813	Low	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Microsoft [117] *Microsoft updates bulletin*[118]	Windows NT 4.0	Microsoft Exchange Server 5.5	A security vulnerability exists which could let a malicious user cause an Exchange server to fail. *Bulletin updated to advise of the availability of an update for Exchange Server 5.0.*	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq00-082.asp	Malformed MIME Header	Low	Bug discussed in newsgroups and websites. Exploit has been published.

[115] Internet Security Systems Security Advisory, October 14, 2003.
[116] SecurityFocus, April 21, 2004.
[117] Microsoft Security Bulletin, MS00-082, October 31, 2000.
[118] Microsoft Security Bulletin, MS00-082 V2.0, April 13, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133] *Avaya releases an advisory to announce Avaya System Products shipping on Microsoft platforms are also affected by this vulnerability*[134]	Windows 98/SE/ME, NT 4.0/2000, XP, 2003	Windows NT Workstation 4.0 SP6a, NT Server 4.0 SP6a, 4.0, Terminal Server Edition SP6, Windows 2000, SP2-SP4, XP, SP1, XP 64-Bit Edition, SP1, 64-Bit Edition Version 2003, Windows Server™ 2003, 2003 64-Bit Edition, NetMeeting, Windows 98, SE, ME; *Avaya Definity One Media Servers, IP600 Media Servers, S3400 Modular Messaging, S8100 Media Servers*	A vulnerability exists in LSASS, which could let a remote malicious user execute arbitrary code; a DoS vulnerability exists in LSASS when processing LDAP requests; a vulnerability exists in the PCT protocol, which could let a remote malicious user execute arbitrary code; a vulnerability exists in Winlogon, which could let a remote malicious user execute arbitrary code; a vulnerability exists when rendering Metafiles, which could let a remote malicious user execute arbitrary code; a vulnerability exists in the 'Help and Support Center' when handling HCP URLs, which could let a remote malicious user execute arbitrary code; a vulnerability exists in the Utility Manager, which could let a remote malicious user obtain SYSTEM privileges; a vulnerability exists in Windows task management, which could let a remote malicious user execute arbitrary code; a vulnerability exists when creating entries in the Local Descriptor Table, which could let a malicious user obtain elevated privileges; a vulnerability exists in the H.323 protocol, which could let a malicious user execute arbitrary code; a vulnerability exists in the Virtual DOS Machine subsystem, which could let a malicious user obtain elevated privileges; a DoS vulnerability exists in Negotiate Security Software Provider, which could also let a remote malicious user execute arbitrary code; a DoS vulnerability exists in the SSL library & ASN.1 Library, which could also 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/security/bulletin/MS04-011.mspx *Avaya advise that customers follow the Microsoft recommendations for the resolution of this issue.*	Microsoft Windows Multiple Vulnerabilities CVE Names: CAN-2003-0533, CAN-2003-0663, CAN-2003-0719, CAN-2003-0806, CAN-2003-0906, CAN-2003-0907, CAN-2003-0908, CAN-2003-0909, CAN-2003-0910, CAN-2003-0117, CAN-2003-0118, CAN-2003-0119, CAN-2004-0120, CAN-2004-0123	Low/ Medium/ High (Low if a DoS; Medium if elevated privileges obtained; and High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. *Exploit script has been published for the PCT protocol vulnerably.*

[119] Microsoft Security Bulletin, MS04-011, April 13, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [135] ***Exploit script has been published & bulletin updated*** [136, 137] ***Microsoft updates bulletin*** [138]	**Windows NT 4.0/2000**	**Exchange Server 5.5, SP1-SP4 Exchange 2000 Server, SP1-SP3**	**A buffer overflow vulnerability exists due to a failure to handle certain SMTP extended verbs correctly.** ***V1.1: Removed unnecessary information from "Deployment" in the "Exchange Server 5.5 Service Pack 4" section of "Security Patch information."*** ***V2.0: Bulletin updated to advise of the availability of an update for Exchange Server 5.0***	**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/MS03-046.asp**	**Exchange Server Buffer Overflow** **CVE Name: CAN-2003-0714**	**High**	**Bug discussed in newsgroups and websites.** ***Exploit script has been published.*** **Vulnerability has appeared in the press and other public media.**
Microsoft [139] ***Microsoft updates bulletin*** [140]	**Windows NT 4.0/2000**	**Exchange Server 5.5, 2000; SQL Server 7.0, 2000; Windows NT 4.0, 2000**	**A remote Denial of Service vulnerability exists in several of the RPC servers associated with system services because inputs are not adequately validated.** ***Bulletin updated to advise of the availability of an update for Exchange Server 5.0.***	**Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/ms01-041.asp**	**Windows Malformed RPC Request Denial of Service** **CVE Name: CAN-2001-0509**	**Low**	**Bug discussed in newsgroups and websites.**
Microsoft [141]	Windows	Outlook Express 6.0	A remote Denial of Service vulnerability exists when a malicious user submits a specially crafted EML file that has a 'Sender' value but no 'From' value.	No workaround or patch available at time of publishing.	Outlook Express Malformed EML File Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.

[120] VU#260588, http://www.kb.cert.org/vuls/id/260588.
[121] VU#150236, http://www.kb.cert.org/vuls/id/150236.
[122] VU#255924, http://www.kb.cert.org/vuls/id/255924.
[123] VU#638548, http://www.kb.cert.org/vuls/id/638548.
[124] VU#783748, http://www.kb.cert.org/vuls/id/783748.
[125] VU#353956, http://www.kb.cert.org/vuls/id/353956.
[126] VU#122076, http://www.kb.cert.org/vuls/id/122076.
[127] VU#206468, http://www.kb.cert.org/vuls/id/206468.
[128] VU#526084, http://www.kb.cert.org/vuls/id/526084.
[129] VU#547028, http://www.kb.cert.org/vuls/id/547028.
[130] VU#639428, http://www.kb.cert.org/vuls/id/639428.
[131] VU#471260, http://www.kb.cert.org/vuls/id/471260.
[132] VU#753212, http://www.kb.cert.org/vuls/id/753212.
[133] VU#586540, http://www.kb.cert.org/vuls/id/586540.
[134] SecurityFocus, April 21, 2004.
[135] Microsoft Security Bulletin, MS03-046, October 15, 2003.
[136] PacketStorm, October 29, 2003.
[137] Microsoft Security Bulletin, MS03-046 V 1.1, October 22, 2003.
[138] Microsoft Security Bulletin, MS03-046 V2.0, April 13, 2004
[139] Microsoft Security Bulletin, MS01-041, July 27, 2001.
[140] Microsoft Security Bulletin, MS01-041V2.0, April 13, 2004.
[141] SecurityTracker Alert, 1009743, April 13, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [142, 143] ***Avaya releases an advisory to announce Avaya System Products shipping on Microsoft platforms are also affected by this vulnera-bility***[144]	**Windows 98/SE/ME, NT 4.0/2000, XP, 2003**	**Windows NT Work-station 4.0 SP6a, NT Server 4.0 SP6a, 4.0, Terminal Server Edition SP6, Windows 2000, SP2-SP4, XP, SP1, XP 64-Bit Edition, SP1, 64-Bit Edition Version 2003, Windows Server™ 2003, 2003 64-Bit Edition, Windows 98, SE, ME** ***Avaya Definity One Media Servers, IP600 Media Servers, S3400 Modular Messag-ing, S8100 Media Servers***	**A buffer overflow vulnerability exists in the Jet Database Engine (Jet), which could let a remote malicious user execute arbitrary code.**	**Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/MS04-014.mspx** ***Avaya advise that customers follow the Microsoft recommendations for the resolution of this issue.***	**Jet Database Engine Buffer Overflow** **CVE Name: CAN-2004-0197**	**High**	**Bug discussed in newsgroups and websites.**

[142] Microsoft Security Bulletin, MS04-014, April 13, 2004.
[143] VU#740716, http://www.kb.cert.org/vuls/id/740716.
[144] SecurityFocus, April 21, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[145, 146, 147, 148] ***Avaya releases an advisory to announce Avaya System Products shipping on Microsoft platforms are also affected by this vulnerability***[149]	**Windows 98/SE/ME, NT 4.0/2000, XP, 2003**	**Windows NT Workstation 4.0 SP6a, NT Server 4.0 SP6a, 4.0, Terminal Server Edition SP6, Windows 2000, SP2-SP4, XP, SP1, XP 64-Bit Edition, SP1, 64-Bit Edition Version 2003, Windows Server™ 2003, 2003 64-Bit Edition, Windows 98, SE, ME** ***Avaya Definity One Media Servers, IP600 Media Servers, S3400 Modular Messaging, S8100 Media Servers***	**Multiple vulnerabilities exist: a race condition exists in the RPC Runtime Library, which could let a remote malicious user execute arbitrary code; a Denial of Service vulnerability exists in the RPCSS service when a malicious user submits a specially crafted message; a Denial of Service vulnerability exists in the CIS and in the RPC over HTTP Proxy components when a forwarded request to a backend system passes through them; and a an information disclosure vulnerability exists due to the way object identities are created, which could let a malicious user cause applications to listen on unexpected ports.**	**Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/MS04-012.mspx** ***Avaya advise that customers follow the Microsoft recommendations for the resolution of this issue.***	**Windows RPC/DCOM Multiple Vulnerabilities** **CVE Names: CAN-2003-0813, CAN-2003-0816, CAN-2003-0807, CAN-2004-0124, CAN-2004-0116**	**Low/High** **(High if arbitrary code can be executed)**	**Bug discussed in newsgroups and websites.**

[145] Microsoft Security Bulletin, MS04-012, April 13, 2004.
[146] VU#417052, http://www.kb.cert.org/vuls/id/417052.
[147] VU#212892, http://www.kb.cert.org/vuls/id/212892.
[148] VU#698564, http://www.kb.cert.org/vuls/id/471260.
[149] SecurityFocus, April 21, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [150, 151] ***Avaya releases an advisory to announce Avaya System Products shipping on Microsoft platforms are also affected by this vulnera-bility***[152]	**Windows 98/SE/ME, NT 4.0/2000, XP, 2003**	**Windows NT Work-station 4.0 SP6a, NT Server 4.0 SP6a, 4.0, Terminal Server Edition SP6, Windows 2000, SP2-SP4, XP, SP1, XP 64-Bit Edition, SP1, 64-Bit Edition Version 2003, Windows Server™ 2003, 2003 64-Bit Edition, Windows 98, SE, ME** ***Avaya Definity One Media Servers, IP600 Media Servers, S3400 Modular Messag-ing, S8100 Media Servers***	**A vulnerability exists when processing specially crafted MHTML URLs, which could let a remote malicious user execute arbitrary code.**	**Frequently asked questions regarding this vulnerability and the patch can be found at:** **http://www.microsoft.com/technet/security/bulletin/MS04-013.mspx** ***Avaya advise that customers follow the Microsoft recommendations for the resolution of this issue.***	**Outlook Express MHTML URL Processing Vulnerability** **CVE Name: CAN-2004-0380**	**High**	**Bug discussed in newsgroups and websites.** ***This vulnerability appears to be exploited by the Ibiza Trojan, W32/Bugbear. E, and various web sites that host malicious URLs and related malware.***

[150] Microsoft Security Bulletin, MS04-013, April 13, 2004.
[151] VU#323070, http://www.kb.cert.org/vuls/id/323070.
[152] SecurityFocus, April 21, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [153]	Windows 98/ME/NT 4.0/2000, XP, 2003	Windows 2000 Advanced Server, SP1-SP4, Data-center Server, SP1-SP4, Profes-sional, SP1-SP4, 2000 Server, SP1-SP4, Windows 98, SE, ME, NT Enterprise Server 4.0, SP1-SP6a, NT Server 4.0, SP1-SP6a, NT Terminal Server 4.0, SP1-SP6a, NT Work-station 4.0, SP1-SP6a, XP 64-bit Edition, SP1, XP 64-bit Edition Version 2003, SP1, XP Home, SP1, XP Media Center Edition, XP Profes-sional, SP1, XP Tablet PC Edition	A buffer overflow vulnerability exists when a client attempts to connect to an SMB share with an overly long name, which could let a remote malicious user execute arbitrary code or cause a Denial of Service.	No workaround or patch available at time of publishing.	Windows Long Share Name Buffer Overflow	Bug discussed in newsgrou ps and websites. Proof of Concept e	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[153] Bugtraq, April 25, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [154]	Windows 98/ME/NT 4.0/2000, XP, 2003	Outlook 2002, SP1, 2003, Outlook Express 6.0	A remote Denial of Service vulnerability exists when a NULL is encountered in the message body of an e-mail.	No workaround or patch available at time of publishing.	Outlook/ Outlook Express Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Microsoft [155]	Windows 98/ME/NT 4.0/2000, XP, 2003	Internet Explorer 6.0, SP1	A Denial of Service vulnerability exists when a malicious web page specifies an Object element with a data property that has a value of "?" or "#" in addition to specifying a type property that refers to an image type.	No workaround or patch available at time of publishing.	Internet Explorer Object Element Data Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Mister [156]	Windows, Unix	Protector System 1.15 b1	Multiple vulnerabilities exist: a vulnerability exists in the 'blocker_query.php' script when an invalid value is supplied to the 'portNum' parameter, which could let a remote malicious user obtain sensitive information; a vulnerability exists in the 'blocker_query.php' script due to insufficient verification of the 'target' and portNum' parameters, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability exists due to insufficient of input passed to 'GET' queries, which could let a remote malicious user execute arbitrary SQL code; and a vulnerability exists because it is possible to bypass the SQL injection filter system, which could let a remote malicious user bypass anti-sql-injection filters.	No workaround or patch available at time of publishing.	Multiple Protector System Multiple Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.

[154] NTBugtraq, April 14, 2004.
[155] SecurityFocus, April 17, 2004.
[156] Securiteam, April 25, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Mozilla.org[157]	Windows 95/98/ME/ NT 4.0/2000, Mac OS 9 9.x, Mac OS X 10.x, Unix	Mozilla Browser M16, M15, 0.8, 0.9.2 .1, 0.9.2-0.9.9, 0.9.35, 0.9.48, 1.0, RC1& RC2, 1.0.1, 1.0.2, 1.1, Alpha, Beta, 1.2, Alpha, Beta, 1.2.1, 1.3, 1.3.1, 1.4, a&b, 1.4.1, 1.4.2, 1.4.5	A remote Denial of Service vulnerability exists when a NULL is encountered in the message body of an e-mail.	No workaround or patch available at time of publishing.	Mozilla Messenger Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Multiple Vendors [158, 159, 160]	Multiple	Multiple (See advisory located at: http://www.uniras.gov.uk/vuls/2004/236929/index.htm for complete list)	A vulnerability exists that affects implementations of the Transmission Control Protocol (TCP) that comply with the Internet Engineering Task Force's (IETF's) Requests For Comments (RFCs) for TCP. The impact of this vulnerability varies by vendor and application but could let a remote malicious user cause a Denial of Service, or allow unauthorized malicious users to inject malicious data into TCP streams.	List of updates available at: http://www.uniras.gov.uk/vuls/2004/236929/index.htm	Multiple Vendor TCP Sequence Number Approximation CVE Name: CAN-2004-0230	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published. Vulnerability has appeared in the press and other public media.
Multiple Vendors [161]	Unix	Linux kernel 2.5.0-2.5.69, 2.6, 2.6 -test1-test11, 2.6.1, rc1&rc2, 2.6.2-2.6.5	A vulnerability exists in the 'cpufreq_userspace' proc handler, which could let a malicious user obtain sensitive information.	Update available at: http://www.kernel.org/pub/linux/kernel/ **Fedora:** http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/	Linux Kernel CPUFreq Proc Handler Information Disclosure CVE Name: CAN-2004-0228	Medium	Bug discussed in newsgroups and websites.

[157] SecurityFocus, April 15, 2004.
[158] NISCC Vulnerability Advisory, 236929, April 23, 2004.
[159] VU#415294, http://www.kb.cert.org/vuls/id/415294.
[160] TA04-111A, http://www.us-cert.gov/cas/techalerts/TA04-111A.html.
[161] Fedora Update Notification, FEDORA-2004-111, April 22, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [162] ***SuSE issues advisory*** [163]	**MacOS X 10.x, Unix**	**OpenSSH OpenSSH 3.0, p1, 3.0.1, p1, 3.0.2, p1, 3.1, p1, 3.2, 3.2.2 p1, 3.2.3 p1, 3.3, p1, 3.4, p1**	**A vulnerability exists in the OpenSSH 'scp' utility, which could let a malicious user corrupt files.**	**Conectiva:** **ftp://ul.conectiva.com.br/updates/1.0/RPMS.core/openssh-3.4p1-263.i586.rpm** ***SuSE:*** **ftp://ftp.suse.com/pub/suse/i386/update/**	**OpenSSH 'SCP' Client File Corruption**	**Medium**	**Bug discussed in newsgroups and websites.**
Multiple Vendors [164]	Unix	Linux kernel 2.4.22	An unspecified vulnerability exists in the i810 DRM driver, which could let a malicious user cause a Denial of Service or obtain elevated privileges.	**Fedora:** http://download.fedora.redhat.com/pub/fedora/linux/core/updates/	Linux kernel i810 DRM driver Unspecified Vulnerability	Low/ Medium (Medium if elevated privileges can be obtained)	Bug discussed in newsgroups and websites.
Multiple Vendors [165]	Unix	Linux kernel 2.4.22, 2.4.23, 2.4.23 -ow2, 2.4.23 -pre9, 2.4.24, 2.4.24 -ow1, 2.4.25, 2.6.1, rc1&4c2, 2.6.2, 2.6.3	An integer overflow vulnerability exists in the 'ip_setsockopt()' function when handling the 'MCAST_MSFILTER' socket option, which could let a malicious user cause a Denial or Service or execute arbitrary code.	Upgrades available at: http://www.kernel.org/pub/linux/kernel/v2.4/linux-2.4.26.tar.bz2 **RedHat:** http://rhn.redhat.com/errata/RHSA-2004-183.html	Linux Kernel MCAST_ MSFILTER Integer Overflow CVE Name: CAN-2004-0424	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proof of Concept Denial of Service exploit script has been published.
Multiple Vendors [166]	Unix	Linux kernel 2.4.0-test1-2.4.0-test12, 2.4, 2.4.1-2.4.25, 2.6, 2.6 -test1- 2.6 -test11, 2.6.1 -rc1&rc2, 2.6.2, 2.6.3	A remote Denial of Service vulnerability exists via the Kernel signal queue when a malicious user submits an excessive number of threads that are left in a zombie state.	No workaround or patch available at time of publishing.	Linux Kernel Sigqueue Blocking Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.

[162] Conectiva Security Advisory, CLSA-2004:831, March 26, 2004.
[163] SUSE Security Announcement, SuSE-SA:2004:009, April 14, 2004.
[164] Fedora Update Notification, FEDORA-2004-111, April 22, 2004.
[165] RedHat Security Advisory, RHSA-2004:183-03, April 22, 2004.
[166] Bugtraq April 12, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [167, 168] ***Trustix issues advisory*** [169] ***SuSE issues advisory*** [170]	**Unix**	**RedHat sysstat-4.0.7-3.i386.rpm; SGI ProPack 2.3, 2.4; Sysstat Sysstat 4.0.7, 4.1.1-4.1.7, 5.0.1**	**Two vulnerabilities exist: a vulnerability exists in the monitoring utility due to insecure creation of temporary files, which could let a malicious user corrupt system files, cause a loss of data, or a Denial of Service; and a vulnerability exists in the 'isag' utility because temporary files are created with predictable names, which could let a malicious user cause a Denial of Service or obtain elevated privileges.**	**RedHat:** ftp://updates.redhat.com/9/en/os/i386/sysstat-4.0.7-4.rhl9.1.i386.rpm **SGI:** ftp://patches.sgi.com/support/free/security/patches/ProPack/ **Sysstat:** http://perso.wanadoo.fr/sebastien.godard/download_en.html ***Trustix:*** http://www.trustix.org/errata/misc/2004/TSL-2004-0011-sysstat.asc.txt ***SuSE:*** ftp://ftp.suse.com/pub/suse/i386/update/	**Sysstat Insecure Temporary File Creation & Names** **CVE Names: CAN-2004-0107, CAN-2004-0108**	**Low/ Medium** **(Medium if data is corrupted or lost)**	**Bug discussed in newsgroups and websites. There is no exploit code required.**
Multiple Vendors [171, 172]	Unix	RedHat Advanced Work-station for the Itanium Processor 2.1, Enterprise Linux ES 2.1, AS 2.1; SGI ProPack 2.3, 2.4	An updated mailman package has been issued that closes a remote Denial of Service vulnerability that was introduced by RHSA-2004:019. The DoS exists if an e-mail destined for a list contains an empty subject field.	Update available at: http://rhn.redhat.com/errata/RHSA-2004-156.html **SGI:** ftp://patches.sgi.com/support/free/security/patches/	Red Hat Linux GNU Mailman Remote Denial of Service CVE Name: CAN-2004-0182	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Multiple Vendors [173, 174]	Unix	Linux kernel 2.4, 2.4 .0-test1-test12, 2.4.1-2.4.25, 2.6, test1-test11, 2.6.1 -rc1&rc2, 2.6.2-2.6.4	A vulnerability exists in the Linux kernel when writing to the XFS file system, which could let a malicious user obtain sensitive information.	Upgrade available at: http://www.kernel.org/pub/linux/kernel/v2.4/linux-2.4.26.tar.bz2 **Mandrake:** http://www.mandrakesecure.net/en/ftp.php **Trustix:** http://http.trustix.org/pub/trustix/updates/	Linux Kernel XFS File System Information Leakage CVE Name: CAN-2004-0133	Medium	Bug discussed in newsgroups and websites. Vulnerability may be exploited via a web browser.

[167] Red Hat Security Advisory, RHSA-2004:093-01, March 10, 2004.
[168] SGI Security Advisory, 20040302-01-U, March 12, 2004.
[169] Trustix Secure Linux Security Advisory, TSLSA-2004-0011, March 18, 2004.
[170] SUSE Security Announcement, SuSE-SA:2004:009, April 14, 2004.
[171] RedHat Security Advisory, RHSA-2004:156-07, April 14, 2004.
[172] SGI Security Advisory, 20040404-01-U, April 21, 2004.
[173] Mandrakelinux Security Update Advisory, MDKSA-2004:029, April 14, 2004.
[174] Trustix Secure Linux Security Advisory, TSLSA-2004-0020, April 15, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [175, 176, 177]	Unix	MySQL AB MySQL 3.20.32 a, 3.22.26-3.22.30, 3.22.32, 3.23.2-3.23.5, 3.23.8-3.23.10, 3.23.22-3.23.34, 3.23.36-3.23.56, 3.23.58, 4.0 .0-4.0.15, 4.0.18, 4.1.0-0, 4.1 .0-alpha	A vulnerability exists in the MySQL 'mysqld_multi' script due to insecure temporary file handling, which could let a malicious user obtain elevated privileges.	**Debian:** http://security.debian.org/pool/updates/main/m/mysql/ **Mandrake:** http://www.mandrakesecure.net/en/ftp.php **OpenPKG:** ftp://ftp.openpkg.org/release/2.0/UPD/mysql-4.0.18-2.0.1.src.rpm	MySQL 'mysqld_multi' Insecure Temporary File Handling CVE Name: CAN-2004-0388	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Multiple Vendors [178, 179, 180]	Unix	Linux kernel 2.4, 2.4 .0-test1-test12, 2.4.1-2.4.25, 2.6, test1-test11, 2.6.1 -rc1&rc2, 2.6.2-2.6.4	Multiple vulnerabilities exist: a vulnerability exists due to information leaks within the JFS file system code, which could let a malicious user obtain sensitive information; and a Denial of Service vulnerability exists in the Linux Sound Blaster driver.	Upgrade available at: http://www.kernel.org/pub/linux/kernel/v2.4/linux-2.4.26.tar.bz2 **Mandrake:** http://www.mandrakesecure.net/en/ftp.php **SuSE:** ftp://ftp.suse.com/pub/suse/i386/update/ **Trustix:** http://http.trustix.org/pub/trustix/updates/	Linux Kernel Multiple Vulnerabilities CVE Names: CAN-2004-0178, CAN-2004-0181	Low/ Medium (Medium if sensitive informa-tion can be obtained)	Bug discussed in newsgroups and websites.
Multiple Vendors [181, 182, 183]	Unix	Slackware Linux – current, 9.1; utempter utempter 0.5.2, 0.5.3	Multiple vulnerabilities exist: a vulnerability exists due to an input validation error that causes the application to exit improperly, which could let a malicious user obtain root privileges; and a vulnerability exists due to a failure to validate buffer boundaries, which could let a malicious user cause a Denial of Service.	**Fedora:** http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/ **Mandrake:** http://www.mandrakesecure.net/en/ftp.php **Slackware:** ftp://ftp.slackware.com/pub/slackware/slackware-current/slackware/l/utempter-1.1.1-i486-1.tgz	UTempter Multiple Local Vulnerabilities CVE Name: CAN-2004-0233	Low/**High** **(High if root access can be obtained)**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[175] Debian Security Advisory, DSA 483-1, April 14, 2004.
[176] OpenPKG Security Advisory, OpenPKG-SA-2004.014, April 14, 2004.
[177] Mandrakelinux Security Update Advisory, MDKSA-2004:034, April 20, 2004.
[178] Mandrakelinux Security Update Advisory, MDKSA-2004:029, April 14, 2004.
[179] SUSE Security Announcement, SuSE-SA:2004:009, April 14, 2004.
[180] Trustix Secure Linux Security Advisory, TSLSA-2004-0020, April 15, 2004.
[181] Slackware Security Advisory, SSA:2004-110-01, April 19, 2004.
[182] Fedora Update Notification, FEDORA-2004-108, April 21, 2004.
[183] Mandrakelinux Security Update Advisory, MDKSA-2004:031-1, April 21, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [184, 185, 186, 187188]	Unix	Linux kernel 2.4, 2.4 .0-test1-test12, 2.4.1-2.4.25	A buffer overflow vulnerability exists due to a boundary error within the ISO9660 ('isofs') file system component when handling symbolic links, which could let a malicious user execute arbitrary code.	Upgrade available at: http://www.kernel.org/pub/linux/kernel/v2.4/linux-2.4.26.tar.bz2 **Debian:** http://security.debian.org/pool/updates/main/k/ **Mandrake:** http://www.mandrakesecure.net/en/ftp.php **RedHat:** ftp://updates.redhat.com/9/en/os/ **SuSE:** ftp://ftp.suse.com/pub/suse/i386/update/ **Trustix:** http://http.trustix.org/pub/trustix/updates/	Linux Kernel ISO9660 File System Buffer Overflow CVE Name: CAN-2004-0109	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Multiple Vendors [189, 190, 191, 192, 193]	Unix	Linux kernel 2.4, 2.4 .0-test1-test12, 2.4.1-2.4.25, 2.6, test1-test11, 2.6.1 - rc1&rc2, 2.6.2-2.6.4	A vulnerability exists in the Linux kernel when writing to an ext3 file system due to a design error that causes some kernel information to be leaked, which could let a malicious user obtain sensitive information.	Upgrade available at: http://www.kernel.org/pub/linux/kernel/v2.4/linux-2.4.26.tar.bz2 **Conectiva:** ftp://ul.conectiva.com.br/updates/1.0/ **Debian:** http://security.debian.org/pool/updates/main/k/ **Mandrake:** http://www.mandrakesecure.net/en/ftp.php **RedHat:** ftp://updates.redhat.com **Trustix:** http://http.trustix.org/pub/trustix/updates/	Linux Kernel EXT3 File System Information Leakage CVE Name: CAN-2004-0177	Medium	Bug discussed in newsgroups and websites. Vulnerability may be exploited via a web browser.

[184] Debian Security Advisories, DSA 479-1, 479-2, DSA 482-1, & DSA 491-1, April 14 & 17, 2004.
[185] Mandrakelinux Security Update Advisory, MDKSA-2004:029, April 14, 2004.
[186] SUSE Security Announcement, SuSE-SA:2004:009, April 14, 2004.
[187] Trustix Secure Linux Security Advisory, TSLSA-2004-0020, April 15, 2004.
[188] Red Hat Security Advisory, RHSA-2004:166-01, April 21, 2004.
[189] Mandrakelinux Security Update Advisory, MDKSA-2004:029, April 14, 2004.
[190] Trustix Secure Linux Security Advisory, TSLSA-2004-0020, April 15, 2004.
[191] Debian Security Advisories, DSA 489-1 & 491-1, April 17, 2004.
[192] Conectiva Security Advisory, CLSA-2004:829, April 15, 2004.
[193] Red Hat Security Advisories, RHSA-2004:166-01 & 166-08, April 21, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [194][195], [196], [197], [198], [199], [200]	Unix	ArX Distrib-uted Revision Control System 1.0 pre10-pre 16, 1.0.17, 1.0.18; Cadaver WebDAV Client 0.20 .0-0.20.5, 0.21 .0, 0.22 .0; Neon Client Library 0.19.3, 0.23-0.23.8, 0.24-0.24.4; Netwosix Netwosix Linux 1.0, 1.1; RedHat Advanced Work-station for the Itanium Processor 2.1, Enterprise Linux WS 2.1, ES 2.1, AS 2.1	Multiple format string vulnerabilities exist when processing XML/207 response messages, which could let a remote malicious user execute arbitrary code.	**ArX Distributed:** http://superbeast.ucsd.edu/~landry/ArX/ArX-1.0.19.tar.gz **Cadaver:** http://www.webdav.org/cadaver/ **Debian:** http://security.debian.org/pool/updates/main/n/neon/ **Mandrake:** http://www.mandrakesecure.net/en/ftp.php **Neon Client:** http://www.webdav.org/neon/neon-0.24.5.tar.gz **Netwosix:** http://download.netwosix.org/0012/nepote **OpenPKG:** ftp.openpkg.org/release/2.0/UPD/neon-0.24.4-2.0.1.src.rpm **RedHat:** ftp://updates.redhat.com/9/en/os/ **SGI:** ftp://patches.sgi.com/support/free/security/advisories/ **SuSE:** ftp://ftp.suse.com/pub/suse/i386/update	WebDAV Client Library Format String Vulnerabilities CVE Name: CAN-2004-0179	High	Bug discussed in newsgroups and websites. Exploit has been published.

[194] Red Hat Security Advisories, RHSA-2004: 157-06, 158-01, & 159-01, April 14 & 15, 2004.
[195] Debian Security Advisory, DSA 487-1, April 16, 2004.
[196] SUSE Security Announcement, SuSE-SA:2004:009, April 14, 2004.
[197] OpenPKG Security Advisory, OpenPKG-SA-2004.016, April 16, 2004.
[198] Netwosix Linux Security Advisory #2004-0012, April 18, 2004.
[199] Mandrakelinux Security Update Advisory, MDKSA-2004:032, April 20, 2004.
[200] SGI Security Advisory, 20040404-01-U, April 21, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [201, 202, 203, 204, 205, 206, 207, 208, 209]	Unix	CVS 1.10.7, 1.10.8, 1.11, 1.11.1 p1, 1.11.1-1.11.6, 1.11.10, 1.11.11, 1.11.14, 1.12.1, 1.12.2, 1.12.5; FreeBSD FreeBSD 4.10-PRE-Release, 4.0.x, 4.0 – RELENG, alpha, 4.0, 4.1-4.1.1, 4.2-4.9; Netwosix Linux 1.0, 1.1; RedHat Advanced Workstation for the Itanium Processor 2.1 RedHat cvs-1.11.2-10.i386.rpm, Enterprise Linux WS 3, 2.1, ES 3, 2.1, AS 3, 2.1; Slackware Linux – current, 8.1, 9.0, 9.1	Several vulnerabilities exist: a vulnerability exists in the CVS client revision control system (RCS) diff files, which could let a remote malicious user create or modify arbitrary files; and an access validation vulnerability exists due to insufficient validation of piped checkouts, which could let a remote malicious user obtain sensitive information.	**CVS:** http://ccvs.cvshome.org/servlets/ProjectDownloadList?action=download&dlID=466 **Debian:** http://security.debian.org/pool/updates/main/c/cvs/ **FreeBSD:** ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-04:07/cvs.patch **Mandrake:** http://www.mandrakesecure.net/en/ftp.php **Netwosix:** http://www.netwosix.org/0011/nepote **OpenPKG:** ftp://ftp.openpkg.org/release/2.0/UPD/cvs-1.12.5-2.0.1.src.rpm **RedHat:** ftp://updates.redhat.com/9/en/os **SGI:** ftp://patches.sgi.com/support/free/security/advisories/ **Slackware:** ftp://ftp.slackware.com/pub/slackware/ **SuSE:** ftp://ftp.suse.com/pub/suse/	CVS Client RCS Diff File Corruption & Piped Checkout Access Validation CVE Names: CAN-2004-0180, CAN-2004-0405	Medium	Bug discussed in newsgroups and websites.

[201] Mandrakelinux Security Update Advisory, MDKSA-2004:028, April 14, 2004.
[202] SUSE Security Announcement, SuSE-SA:2004:008, April 14, 2004.
[203] OpenPKG Security Advisory, OpenPKG-SA-2004.013, April 14, 2004.
[204] Red Hat Security Advisories, RHSA-2004:154-01, 154-07, 153-09 April 14 & 17, 2004.
[205] FreeBSD Security Advisory, FreeBSD-SA-04:07, April 15, 2004.
[206] Debian Security Advisory, DSA 486-1, April 16, 2004.
[207] Netwosix Linux Security Advisory #2004-0011, April 18, 2004.
[208] Slackware Security Advisory, SSA:2004-108-02, April 18, 2004.
[209] SGI Security Advisory, 20040404-01-U, April 21, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
NcFTP Software [210]	Unix	NcFTP 3.0 .0-3.0.4, 3.1.0-3.1.7	A vulnerability exists because arguments that are passed to the client software are not correctly obfuscated, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	NcFTP Information Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Netegrity [211]	Windows NT 4.0/2000, 2003, Unix	Side Minder Affiliate Agent 4.0	A buffer overflow vulnerability exists in the processing of the 'SMPROFILE' cookie, which could let a remote malicious user execute arbitrary code.	Upgrade available at: Https://support.netegrity.com	SiteMinder Affiliate Agent 'SMPROFILE' Cookie Remote Buffer Overflow CVE Name: CAN-2004-0425	**High**	Bug discussed in newsgroups and websites.
NetWin [212]	Windows NT 4.0/2000, XP, 2003, Unix	Surge LDAP 1.0g, 1.0e, 1.0 d	A Directory Traversal vulnerability exists in the 'user.cgi' script due to insufficient validation of user-supplied input in the 'page' parameter, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	SurgeLDAP User.CGI Directory Traversal	Medium	Bug discussed in newsgroups and websites. Vulnerability may be exploited via a web browser.
Novell [213]	Multiple	Nsure Identity Manager 2.0	A vulnerability exists when Novell Identity Manager Password Policies have been installed and the universal password option has been enabled because the user "password hint" is stored in clear text, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Nsure Identity Manager Password Hint Plaintext Storage	Medium	Bug discussed in newsgroups and websites.
Nuked-Klan [214]	Windows, Unix	Nuked-Klan 1.2, 1.2 beta, 1.3 , 1.3 beta, 1.4, 1.5, SP2	Multiple vulnerabilities exist: a vulnerability exists in the '$language' variable, which could let a malicious user obtain sensitive information; a vulnerability exists when a specially crafted URL is submitted that redefines global variables, which could let a remote malicious user execute arbitrary code; and a Denial of Service vulnerability exists in the 'update.php' function.	Patch available at: http://nk.gamez.solexine.fr/index.php?file=Download&op=description&dl_id=194	Nuked-Klan Multiple Vulnerabilities	Low/ Medium/ **High** **(Low if a DoS; Medium is sensitive informa-tion can be obtained; and High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[210] Secunia Advisory, SA11438, April 22, 2004.
[211] @stake, Inc. Security Advisory, a042204-1, April 23, 2004.
[212] SecurityTracker Alert, 1009732, April 12, 2003.
[213] Novell Technical Information Document, TID10092410, April 12, 2004.
[214] Security Corporation Security Advisory, SCSA-028, April 17, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Peter Zelezny [215, 216]	Unix	X-Chat 1.8-1.8.2, 1.8.6-1.8.9, 2.0.1, 2.0.5-2.0.8	A buffer overflow vulnerability exists in the SOCKS 5 proxy code, which could let a remote malicious user execute arbitrary code.	Patch available at: http://www.xchat.org/files/source/2.0/patches/xc208-fixsocks5.diff **Debian:** http://security.debian.org/pool/updates/main/x/xchat/ **Mandrake:** http://www.mandrakesecure.net/en/ftp.php	XChat SOCKS 5 Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Phorum[217]	Windows, Unix	Phorum 3.4.7, 3.4.8	A vulnerability exists in the 'include/userlogin.php' script due to insufficient verification of the 'phorum_uriauth' parameter, which could let a remote malicious user execute arbitrary code.	Upgrades available at: http://phorum.org/downloads/phorum-3.4.8a.tar.gz	Phorum_URIAuth SQL Injection	**High**	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit script has been published.
phpBB Group[218]	Windows, Unix	phpBB 2.0 .0-2.0.8	A vulnerability exists in 'common.php' script due to an input validation error in the handling of remote IP addresses, which could let a remote malicious user hide their identity and bypass IP restrictions.	No workaround or patch available at time of publishing.	PHPBB Common.php IP Address Spoofing	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
phpBB Group[219]	Windows, Unix	phpBB 2.0 .0, 2.0 RC1-RC4, 2.0.1-2.0.8	A vulnerability exists in the 'album_portal_php' file, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	PHPBB album_portal.php Remote File Include	**High**	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.

[215] Debian Security Advisory, DSA 493-1, April 21, 2004.
[216] Mandrakelinux Security Update Advisory, MDKSA-2004:036, April 22, 2004.
[217] waraxe-2004-SA#019, April 18, 2004.
[218] Bugtraq, April 19, 2004.
[219] Securiteam, April 21, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
phpbt. Source forge.net [220]	Windows, Unix	PhpBug Tracker Incident Manag-ement System 0.9 .0rc1, 0.9 .0, 0.9.1	Multiple input validation vulnerabilities exist: a vulnerability exists in the 'user.php,' 'bug.php,' and 'query.php' scripts, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability exists due to insufficient filtering of HTML code from user-supplied input in some scripts, which could let a remote malicious user execute arbitrary code; and a vulnerability exists due to insufficient verification of bug report entries, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	PHPBug Tracker Multiple Input Validation Vulnerabilities	**High**	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proofs of Concept exploits have been published.
phpro. nabirov. net [221]	Windows, Unix	PhProfes-sion 2.5	Multiple vulnerabilities exist: A vulnerability exists in the 'jcode' parameter due to insufficient verification, which could let a remote malicious user execute arbitrary HTML or script code; a vulnerability exists in the 'offset' parameter due to insufficient verification, which could let a remote malicious user execute arbitrary code; and a vulnerability exists in the 'upload.php' script if error messages hasn't been turned off in PHP, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	PHProfession Multiple Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.
pisg. Source forge.net [222]	Windows, Unix	pisg 0.54	A Cross-Site Scripting vulnerability exists in the 'nick' field when parsing log files, which could let a remote malicious user execute arbitrary HTML or script code.	No workaround or patch available at time of publishing.	PISG IRC Nick Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[220] Bugtraq, April 15, 2004.
[221] waraxe-2004-SA#021, April 21, 2004.
[222] SecurityTracker Alert, 1009907, April 26, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
PostNuke Development Team[223]	Windows, Unix	PostNuke Phoenix 0.726	Several vulnerabilities exist: a vulnerability exists in 'modules/NS-Comments/index.php' due to insufficient verification of user-supplied input in the 'sid' variable, which could let a remote malicious user execute arbitrary SQL code; and a vulnerability exists in 'module/NS-Your_Account/user/modules/changeinfo.php' due to insufficient verification of user-supplied input to the 'timezoneoffset' variable, which could let a remote malicious user execute arbitrary SQL code.	Patch available at: http://download.hostnuke.com/sf/postnuke/PNSA2004-2.tar.gz Upgrade available at: http://download.hostnuke.com/sf/postnuke/PostNuke-0.726-2.tar.gz	PostNuke Phoenix Multiple Module SQL Injection	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
PostNuke Development Team[224]	Windows, Unix	PostNuke Phoenix 0.726	Multiple vulnerabilities exist: Cross-Site Scripting vulnerabilities exist in the Downloads and Web_Links modules and the 'openwindow.php' script, which could let a remote malicious user execute arbitrary HTML or script code; and several path disclosure vulnerabilities exist when a user directly requests scripts in the '/includes/blocks/' and 'pnadodb' directories, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	PostNuke Phoenix Cross-Site Scripting & Path Disclosure	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.
Productive Computer Insight[225]	Windows	Net Support School 7.0, 7.0 1, 7.5	A password encryption vulnerability exists due to a failure of the application to protect passwords with a sufficiently affective encryption scheme, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	NetSupport School Weak Password Encoding	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.

[223] PostNuke Security Advisory, PNSA 2004-2, April 21, 2004.
[224] waraxe-2004-SA#022, April 21, 2004.
[225] SecurityTracker Alert, 1009556, March 26, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
PW New Media Network [226]	Windows	Modular Site Manage-ment System 0.2.1	A vulnerability exists in the 'ver.asp' file, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Modular Site Management System 'Ver.asp' Information Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
Qual-comm [227]	Windows, MacOS X, Unix	Eudora 6.0.3	A remote Denial of Service vulnerability exists when handling e-mail that contains excessive MIME nesting.	No workaround or patch available at time of publishing.	Eudora Nested MIME Content Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Rajesh Kumar Mada-manchi [228] ***Exploit has been published*** [229]	**Unix**	**RSniff 1.0**	**A remote Denial of Service vulnerability exists when a client repeatedly connects to the RSniff daemon and does not issue the 'AUTHENTICATE' command to log in or simply closes the connection.**	**No workaround or patch available at time of publishing.**	**RSniff Remote Denial of Service**	**Low**	**Bug discussed in newsgroups and websites. There is no exploit code required.** ***Exploit script has been published.***
Real Networks [230]	Windows NT 4.0/2000, Unix	Helix Universal Server 9.01, 9.0.2.881, 9.0.2.802, Real Networks Helix Universal Server 9.0.2 .794	A remote Denial of Service vulnerability exists due to a failure to handle malformed RTSP (Real-Time Streaming Protocol) requests.	No workaround or patch available at time of publishing.	Helix Universal Server Remote Denial of Service CVE Name: CAN-2004-0389	Low	Bug discussed in newsgroups and websites. There is no exploit code required; however a Proof of Concept has been published.
Rhino Software [231]	Windows	Zaep AntiSpam 2.0, 2.0.0.1	A Cross-Site Scripting vulnerability exists due to insufficient sanitization of user-supplied URI input, which could let a remote malicious user execute arbitrary HTML or script code.	Patch available at: http://www.zaep.com/	Zaep AntiSpam Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.

[226] SecurityTracker Alert , 1009929, April 23, 2004.
[227] Secunia Advisory, SA11360, April 13, 2004.
[228] Secunia Advisory, SA11339, April 10, 2004.
[229] PacketStorm, April 9, 2004.
[230] iDEFENSE Security Advisory, April 15, 2004.
[231] Securiteam, April 14, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
RhinoSoft [232]	Windows	Serv-U 3.0, 3.1, 4.0 .0.4, 4.1 .0.11, 4.1, 4.2, 5.0 .0.4	A buffer overflow vulnerability exits due to an out-of-bounds read error within a routine used for handling input passed to the 'LIST' command's '-l' parameter, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.	Upgrade available at: http://www.serv-u.com/customer/record.asp?prod=su	Serv-U FTP Server LIST '-l:' Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
Shaun@shat.net [233]	Unix	Network Query Tool 1.0, 1.6	Several vulnerabilities exist: a Cross-Site Scripting vulnerability exists in the 'portNum' variable due to insufficient validation, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability exists in the 'portNum' variable when an invalid value is supplied, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Network Query Tool Cross-Site Scripting & Information Disclosure	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required.
Softwin [234]	Windows	Bit Defender	Several vulnerabilities exist: a vulnerability exists in the 'AvxScanOnline' file due to a design error, which could let a remote malicious user execute arbitrary code; and an information disclosure vulnerability exists in the 'AvxScanOnlineCtrl' COM object, which could let a remote malicious user obtain sensitive information.	Update available at: http://www.bitdefender.com/scan/license.php	BitDefender Remote File Upload & Execution & Information Disclosure	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[232] Securiteam, April 19, 2004.
[233] waraxe-2004-SA#024, April 24, 2004.
[234] SecurityTracker Alert, 1009862, April 19, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Squid Guard[235] ***Vendors issue advisories***[236, 237, 238, 239, 240,241, 242, 243]	**Unix**	**Squid Guard 1.0.0, 1.1.0-1.1.5, 1.2.0**	**A vulnerability exists due to a failure to filter out invalid URIs, which could let a remote malicious user obtain unauthorized access.**	***Conectiva:*** **ftp://atualizacoes.conectiva.com.br/** ***Debian:*** **http://security.debian.org/pool/updates/main/s/squid/** ***Fedora:*** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/** ***Mandrake:*** **http://www.mandrakesecure.net/en/ftp.php** ***OpenPKG:*** **ftp://ftp.openpkg.org/release/** ***RedHat:*** **ftp://updates.redhat.com/** ***SGI:*** **ftp://patches.sgi.com/support/free/security/advisories** ***Squid:*** **http://www.squid-cache.org/Versions/v2/2.5/** ***Trustix:*** **http://www.trustix.org/errata/trustix-2.0/**	**SquidGaurd NULL URL Character Unauthorized Access** **CVE Name: CAN-2004-0189**	**Medium**	**Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.**
Squirrel Mail [244]	Imox	Squirrel Mail change_ passwd 3.1 -1.2.8	A buffer overflow vulnerability exists in the 'change_passwd' plug-in utility due to a boundary error, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	SquirrelMail Change_ Passwd Plug-in Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit scripts have has been published.
STC Corpora-tion[245]	Windows 2000	Campus Pipeline 1.0, 2.0, 2.1, 2.2, 3.0, 3.1, 3.2	A Cross-Site Script vulnerability exists in the e-mail interface due to insufficient filtering of certain scripting handles such as onload(), onmouseover(), and onclick(), which could let a remote malicious user execute arbitrary HTML and script code.	The vendor has acknowledged this issue and provided resolution information via customer support services. This issue has been assigned answer ID 923 by the vendor. Users should contact the vendor for more information.	Campus Pipeline Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.

[235] SecurityFocus, March 19, 2004.
[236] Red Hat Security Advisories, RHSA-2004:133-12 & RHSA-2004:134-01, March 29, & April 14, 2004.
[237] Mandrakelinux Security Update Advisory, MDKSA-2004:025, March 30, 2004.
[238] OpenPKG Security Advisory, OpenPKG-SA-2004.008, April 1, 2004.
[239] Debian Security Advisory, DSA 474-1, April 4, 2004.
[240] Conectiva Linux Security Announcement, CLA-2004:838, April 12, 2004.
[241] Fedora Update Notification, FEDORA-2004-104, April 15, 2004.
[242] Trustix Secure Linux Bugfix Advisory, TSL-2004-0019, April 16, 2004.
[243] SGI Security Advisory, 20040404-01-U, April 21, 2004.
[244] Bugtraq, April 17, 2004.
[245] SecurityTracker Alert, 1009816, April 15, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Sun Micro-systems, Inc. [246]	Unix	Netra 1280 Sun Fire 3800, 4800, 4810, 6800, V1280	A remote Denial of Service vulnerability exists due to a failure to handle IP packets that have the Type of Service (TOS) field set.	Patches available at: http://sunsolve.sun.com/pub-cgi/	Sun Fire/Netra Remote Denial of Service	Low	Bug discussed in newsgroups and websites.
Sun Micro-systems, Inc.[247]	Unix	Solaris 8.0, 8.0_x86, 9.0, 9.0_x86	A Denial of Service vulnerability exists in the 'sendfilev(3EXT)' function.	Patches available at: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F57470	Solaris SendFileV Denial of Service	Low	Bug discussed in newsgroups and websites.
Sun Micro-systems, Inc.[248] ***Exploit script published*** [249]	**Unix**	**Solaris 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86, 9.0, 9.0_x86**	**A vulnerability exists in the 'vfs_getvfssw()' function due to insufficient sanitization, which could let a malicious user obtain root access.**	**Patches available at: http://sunsolve.sun.com/pub-cgi/**	**Solaris 'vfs_getvfssw' function Root Access**	**High**	**Bug discussed in newsgroups and websites.** ***Exploit has been published.***
Symantec [250]	Windows	Client Firewall 5.0 1, 5.1.1, Client Security 1.0, 1.1, Norton Internet Security 2003, Profes-sional Edition, 2004, Profes-sional Edition, Norton Personal Firewall 2003, 2004	A remote Denial of Service vulnerability exists in 'SYMNDIS.SYS' when a malicious user submits a malicious TCP packet.	Customers are advised to run LiveUpdate to address this issue.	Symantec Client Firewall SYMNDIS. SYS TCP Remote Denial of Service CVE Name: CAN-2004-0375	Low	Bug discussed in newsgroups and websites.

[246] Sun(sm) Alert Notification, 57544, April 19, 2004.
[247] Sun(sm) Alert Notification, 57470, April 22, 2004.
[248] SecurityFocus, March 23, 2004.
[249] PacketStorm, April 7, 2004.
[250] Symantec Security Response, SYM04-007, April 20, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
TikiWiki Project[251]	Windows, Unix	TikiWiki 1.8, 1.8.1	Multiple vulnerabilities exist: a vulnerability exists when invalid input is submitted or certain scripts are requested directly, which could let a remote malicious user obtain sensitive information; a Cross-Site Scripting vulnerability exits in multiple scripts due to insufficient verification of input, which could let a remote malicious user execute arbitrary HTML or script code; a vulnerability exists in multiple scripts due to insufficient sanitization of input before it is used in SQL queries, which could let a remote malicious user execute arbitrary code; a vulnerability exists because various functionality parameters allow URLs and scripts to be inserted, which could let a remote malicious user execute arbitrary code; a Directory Traversal vulnerability exists, which could let a remote malicious user obtain sensitive information; and a vulnerability exists in the '/imp/wike_up/' folder, which could let a remote malicious user execute arbitrary code.	Upgrades available at: http://prdownloads.sourceforge.net/tikiwiki/tikiwiki-1.8.2.tar.gz?download	TikiWiki Project Multiple Input Validation Vulnerabilities	Medium/ **High** **(Medium is sensitive informa-tion can be obtained; and High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.
Torsten Schoenitz & Joerg Wunsch[252]	Unix	xonix 1.4	A vulnerability exists due to a failure to drop privileges before launching an external program, which could let a malicious user obtain elevated privileges.	**Debian:** http://security.debian.org/pool/updates/main/x/xonix/	Xonix X11 Game Elevated Privileges CVE Name: CAN-2004-0157	Medium	Bug discussed in newsgroups and websites.

[251] GulfTech Security Research Team Advisory, April 11, 2004.
[252] Debian Security Advisory, DSA 484-1, April 14, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Tutos[253]	Unix	Tutos 1.1 .20031017	Multiple vulnerabilities exist: a vulnerability exists in the 'company_new.php,' 'app_new.php,' and 'task_new.php' scripts due to insufficient sanitization, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability exist in the 'note_overview.php' script due to insufficient verification of the 'id' parameter, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://download.sourceforge.net/tutos/tutos-php-1.1.20040412.tar.bz2	TUTOS Multiple Input Validation Vulnerabilities	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Wirlab [254]	Unix	KPhone 2.0, 2.1, 2.11, 3.0, 3.1, 3.11-3.14, 4.0.1	A remote Denial of Service vulnerability exists when a malicious user submits a specially crafted SIP (Session Initiation Protocol) STUN message.	Upgrades available at: http://www.wirlab.net/kphone/kphone-4.0.2.tar.gz	KPhone Malformed STUN Packet Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
xine[255, 256]	Unix	xine-lib 1-rc3c, 1-rc3b, 1-rc3a, 1-rc2, xine-ui 0.9.21-0.9.23	A vulnerability exists due to a design error because playlists can alter options in the configuration file, which could let a remote malicious user construct playlists that can overwrite arbitrary files with the privileges of the current user.	**Slackware:** ftp://ftp.slackware.com/pub/slackware/ **Xine:** http://www.xinehq.de/index.php/security/XSA-2004-1	Xine & Xine-Lib Multiple Remote File Overwrite	High	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
xinehq.de [257] ***Vendors issue advisories*** [258, 259]	**Unix**	**xine 1-rc3b, 1-rc3a, 1-rc1-rc3, 1-rc0a, 1-beta1-beta12, 0.9.13**	**A vulnerability exists because the 'xine-bugreport' and 'xine-check' scripts create temporary files in an insecure manner, which could let a malicious user obtain elevated privileges.**	***Debian:*** **http://security.debian.org/pool/updates/main/x/xine-ui/** ***Mandrake:*** **http://www.mandrakesecure.net/en/ftp.php**	**Xine Bug Reporting Script Insecure Temporary File Creation**	**Medium**	**Bug discussed in newsgroups and websites. There is no exploit code required.**
X-Micro[260]	Multiple	WLAN 11b Broad-band Router Firmware 1.2.2 .4, 1.2.2 .3, 1.2.2, 1.6.0.1, 1.6 .0	A vulnerability exists because the device contains a built-in username and password, which could let a remote malicious user obtain administrative access.	Updates available at: http://www.x-micro.com/temp/XWL-11bRRGVer-1.601.exe	WLAN 11b Broadband Router Built-in Backdoor Administrator Account	High	Bug discussed in newsgroups and websites. There is no exploit code required; however an exploit has been published.

[253] Kereval Security Advisory, KSA-005, April 14, 2004.
[254] Securiteam, April 15, 2004.
[255] Xine Security Advisories, XSA-2004-1 & XSA-2004-2, April 22, 2004.
[256] Slackware Security Advisory, SSA:2004-111-01, April 22, 2004.
[257] Bugtraq, March 20, 2004.
[258] Debian Security Advisory, DSA 477-1, April 6, 2004.
[259] Mandrakelinux Security Update Advisory, MDKSA-2004:033, April 20, 2004.
[260] Bugtraq April 10, 2004..

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Yahoo![261]	Windows	Yahoo! Mes-senger	A vulnerability exists which could let a remote malicious user bypass the e-mail filter to execute arbitrary scripting code and hijack a target user's account.	The vendor has issued a server-based fix. Affected users do not need to apply a fix.	Yahoo! Mail Scripting Filter Bypass	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Yahoo![262]	Windows	Yahoo! Mes-senger 5.6.0.1358 5.6.0.1356 5.6.0.1355 5.6.0.1351 5.6.0.1347 5.6	A buffer overflow vulnerability exists in the 'YInstHelper.YInstStarter.1' and 'YInstHelper.YsearchSetting2' COM objects, which could let a remote malicious user cause a Denial of Service.	No workaround or patch available at time of publishing.	Yahoo! Messenger YInsthelper. DLL Multiple Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Zone Labs[263]	Windows 95/98/ME/ NT 4.0/2000	Zone Alarm Plus 4.0, 4.5.538. 001, Zone Alarm Pro 2.4, 2.6, 3.0, 3.1, 4.0, 4.5 .538.001, 4.5	A vulnerability exists due to a failure to properly quarantine a file that contain an attachment with certain characters in the filename, which could let a remote malicious user bypass security filter restrictions.	No workaround or patch available at time of publishing.	ZoneAlarm Pro/Plus MailSafe Filter Bypass	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

*"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.

[261] SecurityTracker Alert, 1009872, April 20, 2004.
[262] SecurityTracker Alert, 1009914, April 22, 2004.
[263] Bugtraq, April 14, 2004.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between April 7 and April 28, 2004, 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 68 scripts, programs, and net-news messages containing holes or exploits were identified by US-CERT. *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
April 28, 2004	disconn.py	Proof of Concept exploit for the Multiple Vendor TCP Sequence Number Approximation vulnerability.
April 28, 2004	hydra-4.0-src.tar.gz	THC-Hydra is a high quality parallelized login hacker for Samba, Smbnt, Cisco AAA, FTP, POP3, IMAP, Telnet, HTTP Auth, LDAP, NNTP, MySQL, VNC, ICQ, Socks5, PCNFS, Cisco and more. Includes SSL support, parallel scans, and is part of Nessus.
April 28, 2004	Rkhunter-1.0.7.tar.gz	Rootkit Hunter scans files and systems for known and unknown rootkits, backdoors, and sniffers.
April 28, 2004	Tcp_reset.c	Proof of Concept exploit for the Multiple Vendor TCP Sequence Number Approximation vulnerability.
April 25, 2004	Kreset.pl	Proof of Concept exploit for the Multiple Vendor TCP Sequence Number Approximation vulnerability.
April 24, 2004	bgp-dosv2.pl	BGP proof of concept denial of service utility that sends out a RST flood to BGP connection providing the malicious user has already gained knowledge of the source port and sequence number.
April 24, 2004	reset-tcp.c	Proof of concept exploit for the Multiple Vendor TCP Sequence Number Approximation vulnerability.
April 24, 2004	reset-tcp_rfc31337-compliant.c	Proof of concept exploit for the Multiple Vendor TCP Sequence Number Approximation vulnerability.
April 24, 2004	SlippingInTheWindow_v1.0.doc	A whitepaper titled 'Slipping in the Window: TCP Reset Attacks' that explains TCP exploits.
April 24, 2004	SlippingInTheWindow_v1.0.ppt	A PowerPoint briefing titled 'Slipping in the Window: TCP Reset Attacks' that explains TCP exploits.
April 23, 2004	**YahooMPOCs.txt**	**Exploit for the Yahoo! Messenger YInsthelper. DLL Multiple Buffer Overflow vulnerabilities.**
April 22, 2004	reset.zip	This program will reset a TCP connection by guessing a valid sequence number.
April 22, 2004	setsockopt_poc.c	Proof of Concept Denial of Service for the Linux Kernel Setsockopt MCAST_MSFILTER Integer Overflow vulnerability.
April 22, 2004	thc_ssh_crack.c	THC SSH Cracker is a simple utility that attempts to crack SSH private keys via brute force.
April 22, 2004	THCIISSLame.c	Exploit for the THCIISSLame IIS 5 SSL remote root vulnerability.
April 22, 2004	**TournamentFileWritePOC.c**	**Proof of Concept exploit for the Unreal Game Engine UMOD Input Validation vulnerability.**
April 22, 2004	**umodpoc.zip**	**Proof of concept exploit for the Unreal Game Engine UMOD Input Validation vulnerability.**
April 20, 2004	04222004.reset.dpr.php	Exploit for the Multiple Vendor TCP Sequence Number Approximation vulnerability.

Date of Script (Reverse Chronological Order)	Script name	Script Description
April 20, 2004	**0x3142-sq-chpasswd.c**	**Script that exploits the SquirrelMail Change_ Passwd Plug-in Buffer Overflow vulnerability.**
April 20, 2004	bgp-dosv2.pl	Exploit for the Multiple Vendor TCP Sequence Number Approximation vulnerability.
April 20, 2004	**eudora61.pl**	**Perl script that exploits the Eudora Nested MIME Content Remote Denial of Service vulnerability.**
April 20, 2004	**eXchangePOP3_exp.pl**	**Proof of Concept exploit for the Exchange POP3 Remote Buffer Overflow vulnerability.**
April 20, 2004	p_xfree.c	Script that exploits the CopyISOLatin1Lowered() function buffer overflow vulnerability.
April 20, 2004	rhinoSoftServULISTovflwExpl.pl	Proof of Concept exploit for the Serv-U FTP Server LIST '-l:' Buffer Overflow vulnerability.
April 20, 2004	SlippingInTheWindow.tgz	Exploit for the Multiple Vendor TCP Sequence Number Approximation vulnerability.
April 20, 2004	THCbindinfo.c	Quick and dirty hack to grab the versions from ISC bind 8 and 9 nameservers.
April 19, 2004	**chpasswd-exploit.c**	**Script that exploits the SquirrelMail Change_ Passwd Plug-in Buffer Overflow vulnerability.**
April 19, 2004	**eudora_mime.pl**	**Perl script that exploits the Eudora MIME Message Nesting Denial of Service vulnerability.**
April 19, 2004	Exch.pl	Perl script that exploits the Kinesphere Corporation Exchange POP3 buffer overflow vulnerability.
April 19, 2004	knock-0.2.tar.gz	A server/client set of tools that implements the idea known as port-knocking. Port-knocking is a method of accessing a backdoor to your firewall through a special sequence of port hits.
April 19, 2004	kphone.stun.txt	Exploit for the KPhone Malformed STUN Packet Remote Denial of Service vulnerability.
April 19, 2004	**moron.pl**	**Script that exploits the SquirrelMail Change_ Passwd Plug-in Buffer Overflow vulnerability.**
April 19, 2004	**nestedMIMEEudora603expl.pl**	**Perl script that exploits the Eudora MIME Message Nesting Denial of Service vulnerability.**
April 19, 2004	reverse_backdoored_binaries.txt	A whitepaper about reverse engineering backdoored binaries.
April 19, 2004	**setegg.c**	**Script that exploits the SquirrelMail Change_ Passwd Plug-in Buffer Overflow vulnerability.**
April 19, 2004	**SPK-chpasswd.c**	**Script that exploits the SquirrelMail Change_ Passwd Plug-in Buffer Overflow vulnerability.**
April 18, 2004	gvexpl.tgz	Remote root Proof of Concept exploit for gv versions 3.5.8 and below vulnerability.
April 18, 2004	Phorum347SQL.pl	Perl script that exploits the Phorum_URIAuth SQL Injection vulnerability.
April 18, 2004	**SPK-chpasswd.tgz**	**Exploit for the SquirrelMail Change_ Passwd Plug-in Buffer Overflow vulnerability.**
April 17, 2004	billybastard.c	Script that exploits the Windows LSASS vulnerability.
April 17, 2004	ettercap-NG-0.7.0_pre1.tar.gz	A network sniffer/interceptor/logger for switched LANs that uses ARP poisoning and the man-in-the-middle technique to sniff all the connections between two hosts.
April 17, 2004	**gemitelv3.txt**	**Exploit for the Gemitel 'html/affich. php' file Arbitrary Code Execution vulnerability.**
April 17, 2004	**mille.c**	**Script that exploits the BSD-Games Mille Local Save Game File Name Buffer Overflow vulnerability.**
April 16, 2004	mamboConfigurationInfoDiscExpl. php	Exploit for the Mambo Open Source mosConfig_absolute_path vulnerability.
April 16, 2004	proxyscanner.zip	Proxy Scanner for Windows that tells you whether or not a proxy server can bounce your connection.

Date of Script (Reverse Chronological Order)	Script name	Script Description
April 16, 2004	XMicro.backdoor2.txt	Exploit for the WLAN 11b Broadband Router Built-in Backdoor Administrator Account vulnerability.
April 15, 2004	kphone-dos.pl	Perl script that exploits the KPhone Malformed STUN Packet Denial of Service vulnerability.
April 15, 2004	sslbomb.c	Remote denial of service exploit for Windows IIS SSL vulnerability.
April 15, 2004	**winscp_dos.txt**	**Proof of Concept exploit for the WinSCP Remote Denial of Service vulnerability.**
April 15, 2004	wz_ex.c	Proof of concept exploit for the UUDeview MIME Archive Buffer Overflow vulnerability.
April 14, 2004	**cdpexpl.tgz**	**Exploit for the CDP PrintTOC Function Buffer Overflow vulnerability.**
April 14, 2004	gdbvuln.txt	Brief tutorial on using gdb for developing exploits.
April 14, 2004	tutorial.txt	A tutorial discussing common types of exploitation methods that cites examples and points to other papers that can provide more information.
April 13, 2004	eMuleBufferOverflowExp10039.pl	Proof of Concept exploit for the eMule Remote Buffer Overflow vulnerability.
April 13, 2004	knock-0.1.tar.gz	a server/client set of tools that implements the idea known as port-knocking. Port-knocking is a method of accessing a backdoor to your firewall through a special sequence of port hits.
April 13, 2004	rkhunter-1.0.6.tar.gz	Rootkit Hunter scans files and systems for known and unknown rootkits, backdoors, and sniffers.
April 13, 2004	**tinybmp.htm**	**Proof of Concept exploit for the Konqueror Bitmap File Processing Denial of Service vulnerability.**
April 12, 2004	305monit.c	Script that exploits the Monit Buffer Overflow vulnerability.
April 12, 2004	**sigqueue-dos.c**	**Script that exploits the Linux Kernel Sigqueue Blocking Denial of Service vulnerability.**
April 12, 2004	**tinybmp.htm**	**Proof of Concept exploit for the Internet Explorer Bitmap File Processing Denial of Service vulnerability.**
April 12, 2004	**whosendthis.zip**	**Proof of Concept exploit for the Outlook Express Malformed EML File Denial of Service vulnerability.**
April 11, 2004	emule4x.pl	Perl script that exploits the eMule Remote Buffer Overflow vulnerability.
April 11, 2004	tikiwiki181.txt	Exploit for the TikiWiki Project Multiple Input Validation Vulnerabilities.
April 10, 2004	Xmicro.backdoor.txt	Exploit for the WLAN 11b Broadband Router Built-in Backdoor Administrator Account vulnerability.
April 9, 2004	cobain-monit.pl	Script that exploits the Monit Denial of Service vulnerability.
April 9, 2004	**Emptyconn.zip**	**Exploit for the RSniff Remote Denial of Service vulnerability.**
April 9, 2004	priv8lcd44.pl	Perl script that exploits the LCDd Multiple Remote Vulnerabilities.
April 7, 2004	rootme.tar	Exploit for the Solaris 'vfs_getvfssw' function Root Access vulnerability.

Trends

- **US-CERT is aware of network activity that is consistent with scanning and/or exploit attempts against the buffer overflow vulnerability in the Microsoft Private Communication Technology (PCT) protocol, which was remedied by the patches described in Microsoft Security Bulletin MS04-011. Reports indicate increased network traffic to ports 443/tcp and 31337/tcp. For more information, see US-CERT Activity located at: http://www.us-cert.gov/current/#pct.**
- **US-CERT is aware of exploitation of a cross-domain scripting vulnerability in the Outlook Express MIME Encapsulation of Aggregate HTML Documents (MHTML) protocol handler, which was remedied by the patches described in Microsoft Security Bulletin MS04-013. This vulnerability appears to be exploited by the Ibiza Trojan, W32/Bugbear.E, and various web sites that host malicious URLs and related malware. For more information, see US-CERT Activity located at: http://www.us-cert.gov/current/#pct.**
- **US-CERT is aware of exploitation of a cross-domain scripting vulnerability in the InfoTech Storage (ITS) protocol handlers used by Microsoft Internet Explorer (IE). By convincing a victim to view an HTML document (web page, HTML e-mail), an attacker could execute arbitrary code with the privileges of the user running IE and read or modify content in another web site. For more information see US-CERT Current Activity located at: http://www.us-cert.gov/current/current_activity.html.**
- **US-CERT is aware of a new mass-mailing malicious code known as "Sober.F." Sober.F arrives as an e-mail message written in German or English and containing a 42,496-byte e-mail attachment. For more information see US-CERT Current Activity located at: http://www.us-cert.gov/current/current_activity.html.**
- **Exploit code has been publicly released that takes advantage of multiple vulnerabilities in various Cisco products. For more information see US-CERT Current Activity located at: http://www.us-cert.gov/current/current_activity.html.**

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.

The Virus and Trojan sections are derived from compiling information from the following anti-virus vendors and security related web sites: Sophos, Trend Micro, Symantec, McAfee, Network Associates, Central Command, F-Secure, Kaspersky Labs, MessageLabs, and The WildList Organization International.

VBS_GEDZA.A (Aliases: W32/Cazdeg-C, VBS.Gaggle.D, I-Worm.Gedza, VBS/Gedza.A) (Visual Basic Script Worm): This malicious Visual Basic script file displays a picture of the popular Canadian singer, Avril Lavigne, when it is executed. It has payloads of dropping a file, displaying messages and opening the Avril Lavigne Web site, depending on the value of the current system day. It propagates via peer-to-peer file sharing networks by dropping copies of itself in a peer-to-peer shared folders, using interesting file names to entice users to download the files. It runs on Windows 98, ME, NT, 2000 and XP.

VBS/Yarr-A (Aliases: HTML_MOBA.A, VBS/Inor Trojan) (Visual Basic Script Worm): This worm overwrites notepad.exe with the W32/Mimail-V worm.

W32.Gaobot.ADX (Win32 Worm): This is a worm that spreads through open network shares, several Windows vulnerabilities, and backdoors that the Beagle and Mydoom families of worms install. It can act as a backdoor server program and attack other systems and attempts to kill the process of many antivirus and security applications.

W32/Agobot-EV (Aliases: W32/Gaobot.worm.gen.g virus, Win32/Agobot.IH Trojan, W32.HLLW.Gaobot.gen) (Win32 Worm): This is an IRC backdoor Trojan and peer-to-peer (P2P) worm which opens TCP ports to listen for and process commands received from a remote intruder. This worm will move itself into the Windows System32 folder under the filename regsvc32.exe and create the following registry entries so that it can execute automatically on system restart:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Generic Service Process = regsvc32.exe
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\Generic Service Process = regsvc32.exe

W32/Agobot-EV will attempt to terminate anti-virus and software firewall processes, in addition to other viruses, worms or Trojans. It will search for shared folders on the Internet with weak passwords and copy itself into them. W32/Agobot-EV can sniff HTTP, VULN, FTP, and IRC network traffic and steal data from them. This worm can also exploit the DCOM vulnerability on unpatched systems and manipulate registry keys. It will attempt to test the available bandwidth by posting data to various sites. W32/Agobot-EV can also be used to initiate Denial of Service and synflood/httpflood/udpflood attacks against remote systems. This worm can redirect TCP and GRE data and steal the Windows Product ID and keys from several computer games. W32/Agobot-EV maps several anti-virus and security-related websites to localhost within the windows hosts file so that they appear unreachable when a user tries to access them.

W32/Agobot-FV (Alias: W32.HLLW.Gaobot.gen) (Win32 Worm): This is an IRC backdoor Trojan and network worm. W32/Agobot-FV is capable of spreading to computers on the local network protected by weak passwords. When first run ,W32/Agobot-FV copies itself to the Windows system folder as regsvc32.exe and creates the following registry entries to run itself on startup:

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Generic Service Process = regsvc32.exe
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\Generic Service Process = regsvc32.exe

Each time W32/Agobot-FV is run it attempts to connect to a remote IRC server and join a specific channel. It then runs continuously in the background, allowing a remote malicious user to access and control the computer via IRC channels. W32/Agobot-FV attempts to terminate and disable various anti-virus and security-related programs.

W32/Agobot-FZ (Aliases: Backdoor.Agobot.kt, W32/Gaobot.worm.gen.j) (Win32 Worm): This worm has been reported in the wild. It is an IRC backdoor Trojan and network worm. W32/Agobot-FZ is capable of spreading to computers on the local network protected by weak passwords. When first run, W32/Agobot-FZ copies itself to the Windows system folder as msdtc32.exe and creates the following registry entries to run itself on startup:

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Video Device Loader = msdtc32.exe
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\Video Device Loader = msdtcc32.exe

Each time W32/Agobot-FZ is run, it attempts to connect to a remote IRC server and join a specific channel. It then runs continuously in the background, allowing a remote malicious user to access and control the computer via IRC channels. W32/Agobot-FZ attempts to terminate and disable various anti-virus and security-related programs.

W32/Agobot-GA (Aliases: Backdoor.Agobot.li, W32/Gaobot.worm.gen.g, W32.Gaobot.WX, WORM_AGOBOT.WN) (Win32 Worm): This is a backdoor Trojan and worm which spreads to computers protected by weak passwords. When first run, W32/Agobot-GA moves itself to the Windows system folder as windns32.exe and creates the following registry entries to run itself on startup:

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

Each time W32/Agobot-GA is run it attempts to connect to a remote IRC server and join a specific channel. It then runs continuously in the background, allowing a remote malicious user to access and control the computer via IRC channels. W32/Agobot-GA attempts to terminate and disable various anti-virus and security related programs and modifies the HOSTS file located at %Windows%\System32\Drivers\etc\HOSTS. Selected anti-virus websites are mapped to the loopback address 127.0.0.1 in an attempt to prevent access to these sites.

W32/Agobot-GG (Aliases: Backdoor.Agobot.gen, W32/Gaobot.wor m.gen.e, Win32/Agobot.3.NZ, W32.HLLW.Gaobot.gen, WORM_AGOBOT.SB) (Win32 Worm): This is an IRC backdoor Trojan and network worm. W32/Agobot-GG is capable of spreading to computers on the local network protected by weak passwords. When first run, W32/Agobot-GG moves itself to the Windows system folder as systems.exe. The worm may also add its pathname to the following registry entries to run itself on startup:

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

Each time W32/Agobot-GG is run, it attempts to connect to a remote IRC server and join a specific channel. W32/Agobot-GG then runs continuously in the background, allowing a remote malicious user to access and control the computer via IRC channels. W32/Agobot-GG attempts to terminate selected anti-virus and security-related programs.

W32/Agobot-GP (Aliases: W32.HLLW.Gaobot.gen, W32/Gaobot.worm.gen.j) (Win32 Worm): This is an IRC backdoor Trojan and network worm. W32/Agobot-GP is capable of spreading to computers on the local network protected by weak passwords. When first run, W32/Agobot-GP copies itself to the Windows system folder as csrss32.exe and creates the following registry entries to run itself on startup:

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Updater Service Process = csrss32.exe
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\Updater Service Process = csrss32.exe

Each time W32/Agobot-GP is run, it attempts to connect to a remote IRC server and join a specific channel. W32/Agobot-GP then runs continuously in the background, allowing a remote malicious user to access and control the computer via IRC channels. W32/Agobot-GP attempts to terminate and disable various anti-virus and security related programs. W32/Agobot-GP modifies the hosts file on the infected computer in an attempt to resolve a number of security related websites to the localhost address.

W32/Agobot-MN (Alias: Backdoor.Agobot.mn) (Win32 Worm): This is an IRC backdoor Trojan and network worm. It is capable of spreading to computers on the local network protected by weak passwords. When first run, W32/Agobot-MN copies itself to the Windows system folder as runtime.exe and creates the following registry entries to run itself on startup:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\smrtdrv = runtime.exe
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\smrtdrv = runtime.exe

On NT based versions of Windows, the worm creates a new service named "Smart Drive" with a display name of "smrtdrv" and a startup property of automatic, so that the service starts automatically each time Windows is started. The Trojan runs continuously in the background providing backdoor access to the computer. The Trojan attempts to terminate and disable various anti-virus and security related programs and modifies the HOSTS file located at %WINDOWS%\System32\Drivers\etc\HOSTS, mapping selected anti-virus websites to the loopback address 127.0.0.1 in an attempt to prevent access to these sites.

W32/Agobot-QF (Aliases: W32/Gaobot.worm.gen.e virus, W32.HLLW.Gaobot.gen, WORM_AGOBOT.QF) (Win32 Worm): This worm has been reported in the wild. It is an IRC backdoor Trojan and network worm which establishes an IRC channel to a remote server in order to grant an intruder access to the compromised machine. This worm will move itself into the Windows System32 folder under the filename EXPLORED.EXE and may create the following registry entries so that it can execute automatically on system restart:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Windows Login = explored.exe
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\Windows Login = explored.exe

This worm will also attempt to glean e-mail addresses from the Windows Address Book and send itself to these e-mail addresses using its own SMTP engine with itself included as an executable attachment. W32/Agobot-QF will attempt to terminate anti-virus and software firewall processes, in addition to other viruses, worms or Trojans. It will search for shared folders on the Internet with weak passwords and copy itself into them. A text file named HOSTS may also be dropped into C:\<Windows System32>\drivers\etc which may contain a list of anti-virus and other security related websites each bound to the IP loopback address of 127.0.0.1 which would effectively prevent access to these sites. W32/Agobot-QF can sniff HTTP, ICMP, FTP, VULN, and IRC network traffic and steal data from them. The following vulnerabilities can also be exploited to aid propagation on unpatched systems and manipulate registry keys:

- Remote Procedure Call (RPC) vulnerability
- Distributed Component Object Model (DCOM) vulnerability
- RPC Locator vulnerability
- IIS5/WEBDAV Buffer Overflow vulnerability

It can also polymorph on installation in order to evade detection and share/delete the admin$, ipc$, etc. drives. It can also test the available bandwidth by attempting to GET or POST data to various websites. W32/Agobot-QF can also be used to initiate Denial of Service and Distributed Denial of Service synflood/httpflood/fraggle/smurf etc attacks against remote systems. This worm can steal the Windows Product ID and keys from several computer applications or games. W32/Agobot-QF will delete all files named 'sound*.*' and the resident process will be very difficult to terminate.

W32/Agobot-ZY (Aliases: Backdoor.Agobot.ml, W32/Gaobot.worm.gen.k, Win32/Agobot.ML, WORM_AGOBOT.ZM) (Win32 Worm): This worm has been reported in the wild. It is a network worm which also allows unauthorized remote access to the computer via IRC channels. When executed, W32/Agobot-ZY moves itself to the Windows system folder with the filename smssv.exe and sets the registry entries:

- HKLM\SOFTWARE\Microsoft\RFC1156Agent\CurrentVersion\Parameters "TrapPollTimeMilliSecs"=dword:<value>
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices "Audoi Device Loader"="smssv.exe"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "Audoi Device Loader"="smssv.exe"

W32/Blaster-G (Aliases: Worm.Win32.Lovesan.f, W32/Blaster.worm.k, WORM_MSBLAST.I, W32.Blaster.T.Worm) (Win32 Worm): This worm has been reported in the wild. It uses the internet to exploit the DCOM vulnerability in the RPC (Remote Procedure Call). W32/Blaster-G copies itself to the Windows system folder as eschlp.exe. The worm also creates a backdoor Trojan component in the Windows system folder using the name svchosthlp.exe. The following registry entries are created to ensure both components are run at system logon:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Helper = <SYSTEM>\eschlp.exe /fstart MSUpdate = <SYSTEM>\svchosthlp.exe SPUpdate = <SYSTEM>\svchosthlp.exe

The following registry entry is modified to change the default Microsoft Internet Explorer start page to point to the following:

- HKCU\Software\Microsoft\Internet Explorer\Main\Start Page = http://www.getgood.biz

W32.Bugbear.E@mm (Win32 Worm): This is a mass-mailing worm that installs a keylogger to steal personal information. The worm is similar to W32.Bugbear.C@mm.

W32.Gaobot.AAY (Win32 Worm): This is a minor variant of W32.Gaobot.SY. This worm attempts to spread through network shares with weak passwords. It also allows malicious users to access an infected computer using a predetermined IRC channel. The worm uses multiple vulnerabilities to spread, including:

- The DCOM RPC vulnerability (described in Microsoft Security Bulletin MS03-026) using TCP port 135.
- The WebDav vulnerability (described in Microsoft Security Bulletin MS03-007) using TCP port 80.
- The Workstation service buffer overrun vulnerability (described in Microsoft Security Bulletin MS03-049) using TCP port 445. Windows XP users are protected against this vulnerability if Microsoft Security Bulletin MS03-043 has been applied. Windows 2000 users must apply MS03-049.
- The Microsoft Messenger Service Buffer Overrun Vulnerability (described in Microsoft Security Bulletin MS03-043).
- The Locator service vulnerability (described in Microsoft Security Bulletin MS03-001) using TCP port 445. The worm specifically targets Windows 2000 machines using this exploit.
- The UPnP vulnerability (described in Microsoft Security Bulletin MS01-059).
- The vulnerabilities in the Microsoft SQL Server 2000 or MSDE 2000 audit (described in Microsoft Security Bulletin MS02-061), using UDP port 1434.
- Sending itself to the backdoor ports that the Beagle and Mydoom families of worms open.

W32.Gaobot.AND (Win32 Worm): This is a minor variant of W32.Gaobot.SY. This worm attempts to spread through network shares that have weak passwords and allows malicious users to access an infected computer using a predetermined IRC channel. The worm uses multiple vulnerabilities to spread, including:

- The DCOM RPC vulnerability (described in Microsoft Security Bulletin MS03-026) using TCP port 135.
- The WebDav vulnerability (described in Microsoft Security Bulletin MS03-007) using TCP port 80.
- The Workstation service buffer overrun vulnerability (described in Microsoft Security Bulletin MS03-049) using TCP port 445. Windows XP users are protected against this vulnerability if Microsoft Security Bulletin MS03-043 has been applied. Windows 2000 users must apply MS03-049.
- The Microsoft Messenger Service Buffer Overrun Vulnerability (described in Microsoft Security Bulletin MS03-043)
- The Locator service vulnerability (described in Microsoft Security Bulletin MS03-001) using TCP port 445. The worm specifically targets Windows 2000 computers with this exploit.
- The UPnP vulnerability (described in Microsoft Security Bulletin MS01-059).
- The vulnerabilities in Microsoft SQL Server 2000 or MSDE 2000 audit (described in Microsoft Security Bulletin MS02-061) using UDP port 1434.
- Sending itself to the backdoor port that the Beagle family of worms opens.
- Sending itself to the backdoor port that the Mydoom family of worms opens.

This threat may be compressed with BJFNT.

W32.Gaobot.ADV (Win32 Worm): This is a minor variant of W32.Gaobot.SY. This worm attempts to spread through network shares that have weak passwords and allows malicious users to access an infected computer using a predetermined IRC channel. The worm uses multiple vulnerabilities to spread, including:

- The DCOM RPC vulnerability (described in Microsoft Security Bulletin MS03-026) using TCP port 135.
- The WebDav vulnerability (described in Microsoft Security Bulletin MS03-007) using TCP port 80.
- The Workstation service buffer overrun vulnerability (described in Microsoft Security Bulletin MS03-049) using TCP port 445. Windows XP users are protected against this vulnerability if Microsoft Security Bulletin MS03-043 has been applied. Windows 2000 users must apply MS03-049.
- The Microsoft Messenger Service Buffer Overrun Vulnerability (described in Microsoft Security Bulletin MS03-043)
- The Locator service vulnerability (described in Microsoft Security Bulletin MS03-001) using TCP port 445. The worm specifically targets Windows 2000 computers with this exploit.
- The UPnP vulnerability (described in Microsoft Security Bulletin MS01-059).
- The vulnerabilities in Microsoft SQL Server 2000 or MSDE 2000 audit (described in Microsoft Security Bulletin MS02-061) using UDP port 1434.
- Sending itself to the backdoor ports that the Beagle and Mydoom families of worms open.

It may be compressed with UPX and Yoda.

W32.Gaobot.ADW (Win32 Worm): This is a worm that attempts to spread through network shares that have weak passwords and allows malicious users to access an infected computer using a predetermined IRC channel. The worm uses multiple vulnerabilities to spread, including:

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

W32.Gaobot.WO (Aliases: Backdoor.Agobot.lh, W32/Gaobot.worm.gen.g) (Win32 Worm): This is a variant of W32.Gaobot.gen. It attempts to spread through network shares that have weak passwords. It also allows malicious users to access an infected computer through a predetermined IRC channel. The worm 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.
- The Workstation service buffer overrun vulnerability (described in Microsoft Security Bulletin MS03-049) using TCP port 445.

W32.Gaobot.WO is packed with FSG.

W32.Gaobot.YC (Alias:W23.HLLW.Gaobot.gen) (Win32 Worm): This is a variant of W32.HLLW.Gaobot.gen that attempts to spread to network shares and allows access to an infected computer through an IRC channel. The worm 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

W32.Gaobot.YC is packed with UPX and IHMOWrap3.

W32.Gaobot.YN (Win32 Worm): This is a variant of W32.HLLW.Gaobot.gen that attempts to spread to network shares and allows access to an infected computer through an IRC channel. The worm 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

W32.Gaobot.YN is packed with UPX and IHMOWrap3.

W32.Gaobot.ZW (Win32 Worm): This is a minor variant of W32.Gaobot.SY. This worm attempts to spread through network shares with weak passwords. It also allows malicious users to access an infected computer using a predetermined IRC channel. The worm uses multiple vulnerabilities to spread, including:

- The DCOM RPC vulnerability (described in Microsoft Security Bulletin MS03-026) using TCP port 135.
- The WebDav vulnerability (described in Microsoft Security Bulletin MS03-007) using TCP port 80.
- The Workstation service buffer overrun vulnerability (described in Microsoft Security Bulletin MS03-049) using TCP port 445. Windows XP users are protected against this vulnerability if Microsoft Security Bulletin MS03-043 has been applied. Windows 2000 users must apply MS03-049.
- The Microsoft Messenger Service Buffer Overrun Vulnerability (described in Microsoft Security Bulletin MS03-043).
- The Locator service vulnerability (described in Microsoft Security Bulletin MS03-001) using TCP port 445. The worm specifically targets Windows 2000 machines using this exploit.
- The UPnP vulnerability (described in Microsoft Security Bulletin MS01-059).
- The vulnerabilities in the Microsoft SQL Server 2000 or MSDE 2000 audit (described in Microsoft Security Bulletin MS02-061), using UDP port 1434.
- Sending itself to the backdoor ports that the Beagle and Mydoom families of worms open.

W32.Gaobot.ZX (Win32 Worm): This is a minor variant of W32.Gaobot.SY. This worm attempts to spread through network shares with weak passwords, and it also allows malicious users to access an infected computer using a predetermined IRC channel. The worm uses multiple vulnerabilities to spread, including:

- The DCOM RPC vulnerability (described in Microsoft Security Bulletin MS03-026) using TCP port 135.
- The WebDav vulnerability (described in Microsoft Security Bulletin MS03-007) using TCP port 80.
- The Workstation service buffer overrun vulnerability (described in Microsoft Security Bulletin MS03-049) using TCP port 445. Windows XP users are protected against this vulnerability if Microsoft Security Bulletin MS03-043 has been applied. Windows 2000 users must apply MS03-049.
- The Microsoft Messenger Service Buffer Overrun Vulnerability (described in Microsoft Security Bulletin MS03-043).

- The Locator service vulnerability (described in Microsoft Security Bulletin MS03-001) using TCP port 445. The worm specifically targets Windows 2000 machines using this exploit.
- The UPnP vulnerability (described in Microsoft Security Bulletin MS01-059).
- The vulnerabilities in the Microsoft SQL Server 2000 or MSDE 2000 audit (described in Microsoft Security Bulletin MS02-061), using UDP port 1434.
- Sending itself to the backdoor ports that the Beagle and Mydoom families of worms open.

This variant is often compressed with Yoda's Cryptor, PE_Patch, and UPX.

W32/Gbot.worm (Win32 Worm): This is an Internet worm that spreads both via network shares and by taking advantage of the Mydoom backdoor and installs a backdoor on the victim system. When run, it copies itself to the WINDOWS SYSTEM (%sysDir%) directory using a randomly created name and creates a registry run key to load the worm at system startup:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "random name" = [random file name].exe

It also creates copies of itself in C:\My Documents\. The BackDoor component listen on port tcp 113 for incoming connection and connects to an IRC channel at xxx.xxx.108.243 port 6659. The worm scans random IPs trying to access the netbios-ssn and microsoft-ds services. Once a system is found, the worm tries to connect to the 'C$' share on that machine. Although it could not directly observed it is believed the worm creates a number of files on the victim system named !ReadMe.exe in the root of all available local and network drivers and in C:\Documents and Settings\All Users\Start Menu\Programs\Startup\. It can also infect systems already infected by the BackDoor MyDoom.

W32.HLLW.Donk.M (Win32 Worm): This is a network-aware worm. It attempts to connect to a predetermined IRC server to get instructions from the malicious user. This variant may be compressed with PeX.

W32.HLLW.Donk.O (Win32 Worm): This is a worm that spreads through open network shares and attempts to exploit the Microsoft DCOM RPC vulnerability (as described in Microsoft Security Bulletin MS03-026). The worm can also open a backdoor on an infected computer.

W32.HLLW.Gearbug@mm (Win32 Worm): This is a simple mass-mailing worm that sends itself to all the addresses in the Microsoft Outlook Address Book. The e-mail has the following characteristics:

- Subject: Security Update
- Attachment: ElimB.exe

When W32.HLLW.Gearbug@mm runs, it copies itself as:

- C:\Windows\System32\ElimB.exe
- C:\Windows\System\ElimB.exe

These paths are hard-coded and do not depend on system variables.

W32.HLLP.Shodi.B (Win32 Virus): W32.HLLP.Shodi.B is a virus that prepends itself to the files that have a .exe extension.

W32.Kotira (Win32 Virus): This is a virus that overwrites executable files. When W32.Kotira is executed, it copies itself as the following:

- %System%\Arita.exe
- %Windir%\Arita.exe
- C:\Program Files\Atira.exe

The worm adds the value, "System"="C:\Progra~1\Atira.exe," to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CurrentVersion\Run

And attempts to create the following key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\CurrentVersion\arita by Lasiaf

W32/Lovgate-V (Aliases: I-Worm.LovGate.w, W32.Lovgate.Gen@mm, WORM_LOVGATE.V) (Win32 Worm): This worm has been reported in the wild. It is a variant of the W32/Lovgate family of worms that spread via e-mail, network shares and file sharing networks. W32/Lovgate-V copies itself to the Windows system folder as the files WinHelp.exe, iexplore.exe, kernel66.dll and ravmond.exe and to the Windows folder as

systra.exe. It also drops the files msjdbc11.dll, mssign30.dll, and odbc16.dll which provide unauthorized remote access to the computer over a network. The worm drops ZIP files containing a copy of the worm onto accessible drives. The ZIP file may also carry a RAR extension. The name of the contained unpacked file is either PassWord, e-mail, or book, with a file extension of EXE, SCR, PIF, or COM. In order to run automatically when Windows starts up W32/Lovgate-V creates the following registry entries:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Hardware Profile = <SYSTEM>\hxdef.exe Microsoft NetMeeting Associates, Inc. = NetMeeting.exe Protected Storage = RUNDLL32.EXE MSSIGN30.DLL ondll_reg VFW Encoder/Decoder Settings = RUNDLL32.EXE MSSIGN30.DLL ondll_reg WinHelp = <SYSTEM>\WinHelp.exe Program In Windows = <SYSTEM>\IEXPLORE.EXE
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\SystemTra = <WINDOWS>\SysTra.EXE
- HKU\Software\Microsoft\Windows NT\CurrentVersion\Windows\run = RAVM OND.exe

In addition W32/Lovgate-V copies itself to the file command.exe in the root folder and creates the file autorun.inf there containing an entry to run the dropped file upon system startup. W32/Lovgate-V spreads by e-mail. E-mail addresses are harvested from WAB, TXT, HTM, SHT, PHP, ASP, DBX, TBB, ADB, and PL files found on the system. The e-mail has various subject lines, message text, and attachments. W32/Lovgate-V also enables sharing of the Windows media folder and copies itself there using various filenames. The worm also attempts to reply to e-mails found in the user's inbox using the various filenames as attachments. The worm attempts to spread by copying itself to mounted shares using various filenames. It also attempts to spread via weakly protected remote shares by connecting using a password from an internal dictionary and copying itself as the file NetManager.exe to the system folder on the admin$ share. After successfully copying the file, W32/Lovgate-V attempts to start it as the service "Windows Management Network Service Extensions" on the remote computer. W32/Lovgate-V starts a logging thread that listens on port 6000, sends a notification e-mail to an external address and logs received data to the file C:\Netlog.txt. W32/Lovgate-V also overwrites EXE files on the system with copies of itself. The original files are saved with a ZMX extension.

W32.Maddis.B (Win32 Worm): This is a network-share worm that injects itself into various windows System processes. The worm will open several ports on an infected host. It also operates as a proxy and possibly a spam relay. This threat is written in x86 Assembly and is packed with ASPack 2.12.

W32/Mimail-V (Aliases: I-Worm.Mimail.r, VBS/Inor, Win32/Moba.A, W32.Opasa@mm, HTML_MOBA.A) (Win32 Worm): This is a Windows worm that spreads via e-mail and file sharing networks. W32/Mimail-V also has a backdoor component that allows a malicious user remote access to an infected computer. In order to run automatically when Windows starts up W32/Mimail-V copies itself to the Windows system folder using a random filename and creates registry entries pointing to this file under the following keys:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnceEx
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run

W32/Mimail-V also creates the log file xxxx.txt in the folder from which it was run. The worm attempts to copy itself to the various folders of popular P2P applications. When copying itself, the worm uses various filenames. W32/Mimail-V also spreads via e-mail. The subject lines and message texts are constructed randomly. The attachment is either an HTML file containing the embedded worm binary or a ZIP file containing the HTML page. In the latter case, the HTML file has the FOLDER extension which results in it being displayed by explorer or WinZip as a subfolder. When the user clicks on the icon to enter the folder, the worm is dropped and executed. The worm collects e-mail addresses by scanning files on the system. W32/Mimail-V attempts to terminate running processes of anti-virus and monitoring programs as well as of other worms such as W32/Bagle. W32/Mimail-V has functionality to hide its process id and therefore will not appear in the process list. When run, it attempts to connect to a remote IRC server and join a channel via which a malicious user can control a compromised computer. W32/Mimail-V also listens on port 6667 and waits for a URL string pointing to a file which the worm then downloads and executes.

W32.Mydoom.I@mm (Win32 Worm): This is a mass-mailing worm that arrives as an attachment. The worm is similar in functionality to W32.Mydoom.A@mm.

W32.Mydoom.J@mm (Aliases: WORM_MYDOOM.J, Win32.Mydoom.J, W32/Mydoom.j@MM) (Win32 Worm): This is an encrypted, mass-mailing worm that arrives as an attachment with either a .pif, .scr, .exe, .cmd, .bat, or .zip extension. The worm also contains keylogging capabilities. Unlike previous Mydoom variants, W32.Mydoom.J@mm does not appear to act as a backdoor, and it is similar in functionality to W32.Mydoom.A@mm. This threat is written in C++ and is packed with UPX.

W32/Nackbot-D (Aliases: Backdoor.Agobot.jy, W32.Randex.gen) (Win32 Worm): This is a peer-to-peer (P2P) worm which spreads via shared folders and has IRC backdoor functionality. When run, the worm copies itself to the Windows System (or System32) folder as the file MSCLOCK.EXE. To ensure that the worm is run each time Windows is started W32/Nackbot-D creates the registry entries:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Microsoft Digital Clock = msclock.exe
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\Microsoft Digital Clock = msclock.exe

W32/Nackbot-D attempts to spread to randomly chosen IP addresses. The worm attempts to access the C$, D$, E$, and Admin$ shares of the target computer using a list of passwords contained within the worm. The worm then copies itself to the Windows System (or System32) folder on the target computer as MSCLOCK.EXE. W32/Nackbot-D contains backdoor components which can be controlled by a remote malicious user via IRC. The backdoor functions include the ability to launch a Distributed Denial of Service. W32/Nackbot-D searches for the various virus, anti-virus and security-related processes and terminates them if they are running. W32/Nackbot-D can also be used to steal the Windows Product ID and the CD keys from several computer games.

W32/Netsky-U (Alias: I-Worm.NetSky.v) (Win32 Worm): This is a mass mailing worm with a backdoor component which is functionally identical to W32/Netsky-S. Please refer to W32/Netsky-S for further details.

W32/Netsky-V (Aliases: I-Worm.NetSky.w, W32/Netsky.v@MM, W32.Netsky.V@mm, HTML/Debeski) (Win32 Worm): This is a worm which uses a combination of e-mail, HTTP, and FTP to spread. The worm itself is a Windows program (EXE) file. W32/Netsky-V searches your hard disk for e-mail addresses and sends e-mail directly to them. Note that these e-mails do not contain an attached copy of W32/Netsky-V. Instead, they contain HTML instructions to fetch a copy of the worm. The e-mails use a subject and message are randomly selected. W32/Netsky-V opens up two TCP ports on your computer. An HTTP service listens on port 5557 and an FTP service listens on port 5556. These ports are used to "serve up" the virus to downstream victims to whom you have sent copies of the e-mail mentioned above. Downstream victims can become infected simply by reading an e-mail sent by the virus. Note, however, that this e-mail relies on a bug in Microsoft Outlook for which a patch has already been published. If you have downloaded and applied up-to-date patches from Microsoft, then the exploit used by this e-mail will not work and the e-mail is harmless. If your computer has an unpatched copy of Outlook, the W32/Netsky-V e-mail makes an HTTP (web) connection back to port 5557 on the computer which sent you the e-mail. This web connection is used to download a second HTML script. This script in turn exploits a second bug in Outlook to make an FTP connection back to port 5556. The FTP connection is used to download, install and run the W32/Netsky-V worm. W32/Netsky-V is installed into your Windows folder with the name KasperskyAVEng.exe. The worm adds the registry value, 'KasperskyAVEng,' to the registry key:

- HLKM\Software\Microsoft\Windows\CurrentVersion\Run

so that it runs automatically every time you logon to your computer. Between 22 April 2004 and 28 April 2004, W32/Netsky-V mounts a denial of service attack against the following sites:

- www.keygen.us
- www.freemule.net
- www.kazaa.com
- www.emule.de
- www.cracks.am

The Denial of Service consists of four redundant HTML requests to each of these sites every second.

W32/Netsky-W (Aliases: W32.Netsky.W@mm, Win32/Netsky.N@mm, I-Worm.NetSky.o, I-Worm.Win32.Netsky.24064.B, WORM_NETSKY.W) (Win32 Worm): This mass-mailing worm drops copies of itself in the Windows folder. It spreads via e-mail using its own Simple Mail Transfer Protocol (SMTP) engine. This malware obtains its target recipients from files with specific extension names. This malware has backdoor capabilities, and opens random TCP ports, where it awaits commands from a remote malicious user. It also has the capability to delete other malware autostart registry entries and other registry keys. It runs on Windows 95, 98, ME, NT, 2000 ,and XP.

W32/Netsky-X (Alias: W32/Netsky.y@mm) (Win32 Worm): This worm has been reported in the wild. It is an e-mail worm with backdoor functionality similar to W32/Netsky-Y The worm copies itself to the Windows folder using the name FirewallSvr.exe, creates a file called fuck_you_bagle.txt (a base64 encoded form of the worm) and sets the following registry entry to autostart on user login:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\FirewallSvr= C:\<WindowsFolder>\FirewallSvr.exe

The worm arrives in an e-mail with the following characteristics:

- Subject: Delivery failure notice (ID-<8_digit_random_hex_number>)
- Attachment: www.recipient_domain_name.recipient_username.session --<8_digit_random_hex_number_as_in_subject>.com

W32/Netsky-X has a backdoor component listening for connections on TCP port 82 allowing an unauthorized program to download and execute arbitrary code on the infected computer. The worm harvests e-mail addresses from files on the local drives with the following extensions: adb, asp, cfg, cgi, dbx, dhtm, doc, eml, htm, html, jsp, mbx, mdx, mht, mmf, msg, nch, oft, php, pl, ppt, rtf, shtm, tbb, txt, uin, vbs, wab, wsh, xls, or xml. W32/Netsky-X sends DNS queries for various servers. Between 27th and 31st April 2004 the worm will continuously request web pages from the following sites:

- www.nibis.de
- www.medinfo.ufl.edu
- www.educa.ch

W32/Netsky-Y (Aliases: I-Worm.NetSky.y, Win32.HLLM.Netsky.based, W32/Netsky.gen@MM) (Win32 Worm): This worm has been reported in the wild. It is a mass mailing worm with a backdoor component. The worm copies itself to the Windows folder using the name FirewallSvr.exe, creates a file called fuck_you_bagle.txt (a base64 encoded form of the worm) and sets the following registry entry to autostart on user login:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\FirewallSvr= C:\<WindowsFolder>\FirewallSvr.exe

W32/Netsky-Y has a backdoor component listening for connections on TCP port 1549 allowing an unauthorized program to download and execute arbitrary code on the infected computer. The worm harvests e-mail addresses from files on the local drives with the following extensions: adb, asp, cfg, cgi, dbx, dhtm, doc, eml, htm, html, jsp, mbx, mdx, mht, mmf, msg, nch, oft, php, pl, ppt, rtf, shtm, tbb, txt, uin, vbs, wab, wsh, xls, or xml. W32/Netsky-Y sends DNS queries for various servers. Between 27th and 31st April 2004 the worm will continuously request web pages from the following sites:

- www.nibis.de
- www.medinfo.ufl.edu
- www.educa.ch

W32/Netsky-Z (Win32 Worm): This worm has been reported in the wild. It is an Internet worm which spreads by e-mailing itself to addresses found within files on the local computer. When first run, W32/Netsky-Z copies itself to the Windows folder as Jammer2nd.exe and creates the following registry entry so that Jammer2nd.exe is run automatically each time Windows is started:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Jammer2nd = <WINDOWS>\Jammer2nd.exe

Copies of the worm in Base64 encoded and ZIP form are created in the Windows folder with names matching pk_zip?.log where '?' is a number. The e-mails use a subject and message randomly selected. W32/Netsky-Z also opens a listening port on TCP 665. The worm will launch a Denial of Service attack on the following sites between the 2nd and the 5th May 2004:

- www.educa.ch
- www.medinfo.ufl.edu
- www.nibis.de

W32.Opasa@mm (Win32 Worm): This is a mass-mailing worm that:

- Sends itself to the e-mail addresses that it finds on an infected computer
- Terminates processes and services, including various security programs
- Attempts to connect to various IRC servers to wait for additional commands from a malicious user.

The e-mail contains a .zip attachment, and the Subject line varies.

W32.Randex.AAS (Win32 Worm): This is a network-aware worm, which copies itself to, as the following, to the computers that have weak administrator passwords:

- \Admin$\system32\GT.exe
- \c$\winnt\system32\GT.exe

The worm receives instructions from an IRC channel on a predetermined IRC server. One such command will trigger the spreading across the previously mentioned network. The worm is written in Microsoft Visual C++ and is packed with UPX.

W32.Randex.UG (Aliases: Backdoor.IRC.Bot.gen, Backdoor.IRC/SdBot, W32/Sdbot.worm.gen) (Win32 Worm): This is a worm that may be remotely controlled via IRC. The worm includes Distributed Denial of Service (DDoS) capabilities and also tries to steal the CD keys of a number of games.

W32.Randex.YR (Win32 Worm): This is a worm that can be remotely controlled via IRC. The worm includes Distributed Denial of Service (DDoS) capabilities and also tries to steal CD keys for a number of video games. It is packed using the Exe32Pack utility.

W32/SdBot-CM (Aliases: W32/Sdbot.worm.gen, W32.Randex.gen, WORM_RBOT.C) (Win32 Worm): This is a network worm and a backdoor Trojan which runs in the background as a service process and allows unauthorized remote access to the computer via IRC channels. When executed W32/SdBot-CM copies itself to the Windows system folder with the filename msgfix.exe and sets the following registry entries with the path to the copy:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Configuration Loader
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\Configuration Loader
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Configuration Loader

W32/SdBot-CM attempts to copy itself to remote network shares with weak passwords. As a backdoor, W32/SdBot-CM can be used to install and execute programs on your computer, retrieve system information, and flood other computers with network packets. The information the worm retrieves includes computer name, user name, operating system, memory size, and CD-keys for various games.

W32/Sdbot-CP (Aliases: Backdoor.IRCBot.gen, W32/Spybot.worm.gen.a, Win32/IRCBot.DG, W32.Randex.gen, WORM_RBOT.G) (Win32 Worm): This is an IRC backdoor Trojan and network worm. W32/Sdbot-CP spreads to other computers on the local network protected by weak passwords. When first run, W32/Sdbot-CP copies itself to the Windows System folder as csrs32.exe and creates the following registry entries, so that csrs32.exe is run automatically each time Windows is started:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\System32-Driver = csrs32.exe
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\System32-Driver = csrs32.exe
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run\System32-Driver = csrs32.exe

The Trojan sets the following registry entry, in order to disable the use of certain system programs such as Regedit.exe:

- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableRegistryTools = 1

Each time the Trojan runs, it attempts to connect to a remote IRC server and join a specific channel. The Trojan then runs continuously in the background listening on the channel for commands to execute. It attempts to terminate selected anti-virus and security-related programs.

W32/Sdbot-HB (Aliases: Backdoor.IRCBot.gen, Win32/IRCBot.CL) (Win32 Worm): This is a worm which attempts to spread to remote network shares. It also contains backdoor Trojan functionality, allowing unauthorized remote access to the infected computer via IRC channels while running in the background as a service process. W32/Sdbot-HB spreads to network shares with weak passwords as a result of the backdoor Trojan element receiving the appropriate command from a remote user. W32/Sdbot-HB copies itself to the Windows system folder as MPTCLOAXS.EXE and creates an entry in the registry at the following location to run itself on system startup:

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

W32/Sdbot-HB attempts to terminate a number of process relating to anti-virus and security products, as well as some relating to W32/Blaster-A and its variants.

W32/Sdbot-HL (Aliases: Backdoor.IRCBot.gen, W32/Spybot.worm.gen.a, W32.Randex.gen, BKDR_IRCBOT.L) (Win32 Worm): This is a worm which attempts to spread to remote network shares. It also contains backdoor Trojan functionality, allowing unauthorized remote access to the infected computer via IRC channels while running in the background as a service process. W32/Sdbot-HL spreads to network shares with weak passwords as a result of the backdoor Trojan element receiving the appropriate command from a remote user, copying itself to the file CSNT.EXE on the local machine at the same time. W32/Sdbot-HL copies itself to the Windows system folder as CSRS.EXE and creates entries in the registry at the following locations to run itself on system startup:

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

W32/Sdbot-HL tries to delete the following registry entries to prevent the associated programs from running on system startup:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\pccclient.exe
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\pccguide.exe
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\pop3trap.exe

W32/Sdbot-HL sets the following registry entry in an attempt to disable the use of registry tools:

- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableRegistryTools = "1"

W32.Tunk.A (Aliases: W32/Shoder.a@MM, W32/Shodi.c@MM) (Win32 Virus): This is a file-prepending virus. From May 2004 onward, infected systems may fail to restart.

W32/Zafi-A (Aliases: I-Worm.Zafi, W32/Zafi@MM, Win32/Zafi.A, W32.Erkez.A@mm) (Win32 Worm): This worm has been reported in the wild. It is a worm that will copy itself to the Windows System or System32 folder as a randomly named DLL and randomly named EXE file and sets the following registry entry to ensure that it will be run on system restart:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\<random string> = C:\<Windows System32>\<filename.exe>

The following registry entry will also be created:

- HKLM\Software\Microsoft\Hazafi\

This registry entry will have a value name beginning with an uppercase 'R' followed by a number. Other information stored in the registry at this location includes the name of the infected system and the default e-mail address of the user. This worm will test for the presence of an Internet connection by attempting to connect to Google.com. It will also record the URL of every website visited by the user in keys within the following registry branch:

- HKCU\Software\Microsoft\Internet Explorer\TypedURLs\

W32/Zafi-A will also create other randomly named DLL files in the Windows System or System32 folder. This worm will glean e-mail addresses from files which have the following extensions and save them into the randomly named DLL files: HTM, WAB, TXT, DBX, TBB, ASP, PHP, SHT, ADB, MBX, EML, and PMR. W32/Zafi-A attempts to include itself as an attachment in e-mail messages sent to addresses in Hungary. The sender is either the user's default e-mail address or kepeslapok@meglep.hu. This worm will try to terminate several anti-virus and security related applications. This worm will only work during April 2004. W32/Zafi-A will display Hungarian text in a message box on screen if executed on the 1st May 2004.

W97M.Adren (Alias: Macro.Word97.Adrine) (Word 97 Macro Virus): This is a Microsoft Word Basic Macro virus that spreads using Normal.dot and other templates in the Office\Startup folder. This virus contains two modules, ANDRENALINE and DEFTONES.

WORM_AGOBOT.DN (Win32 Worm): This memory-resident worm exploits certain vulnerabilities to propagate across networks. Like the earlier AGOBOT variants, it takes advantage of the following Windows vulnerabilities:

- Remote Procedure Call (RPC) Distributed Comp onent Object Model (DCOM) vulnerability
- IIS5/WEBDAV Buffer Overflow vulnerability
- RPC Locator vulnerability

It attempts to log on to systems using a predefined list of user names and passwords. It also has backdoor capabilities and may execute malicious commands on the host machine. It terminates antivirus-related processes and steals the Windows product ID and the CD keys of certain game applications. It disables access to certain antivirus Web sites by modifying the Windows HOSTS file and uses the affected machine to launch denial of service attacks against certain sites. This worm runs on Windows NT, 2000, and XP.

WORM_AGOBOT.IE (Win32 Worm): This memory-resident malware has both worm and backdoor capabilities. Like the earlier AGOBOT variants, it takes advantage of the following Windows vulnerabilities to propagate across networks:

- Remote Procedure Call (RPC) Distributed Component Object Model (DCOM) Vulnerability
- RPC Locator Vulnerability
- IIS5/WEBDAV Buffer Overflow Vulnerability

It drops itself as the file SMSSV.EXE in the Windows system folder and attempts to log into systems using a list of user names and passwords. It opens a random port and connects to an Internet Relay Chat (IRC) server. It then joins an IRC channel to receive malicious commands to be processed on a system. It also terminates antivirus-related programs and steals CD keys of certain game applications. It modifies the HOSTS file so that any access to specific antivirus Web sites is redirected to the IP address 127.0.0.1. It also deletes all files that contain the string sound in their file names. This malware runs on Windows 2000 and XP.

WORM_AGOBOT.LB (Aliases: W32/Gaobot.worm.gen.f, Backdoor.Agobot.lo) (Win32 Worm): This memory-resident worm exploits takes advantage of the following Windows vulnerabilities to propagate across networks:

- Remote Procedure Call (RPC) Distributed Component Object Model (DCOM) Vulnerability
- RPC Locator Vulnerability
- IIS5/WEBDAV Buffer Overflow Vulnerability

It attempts to log on to systems using a list of user names and passwords. It drops a copy of itself into accessible machines. It also has backdoor capabilities. It executes commands sent in via Internet Relay Chat (IRC) and can be used to launch as Denial of Service (DoS) attack against target sites. It terminates certain processes and files dropped by other malware. It steals CD keys of popular game applications. This malware is compressed using Morphine and UPX. It runs on Windows 2000 and XP.

WORM_AGOBOT.MB (Win32 Worm): This worm exploits certain vulnerabilities to propagate across networks. It takes advantage of the following Windows vulnerabilities:

- Remote Procedure Call (RPC) Distributed Component Object Model (DCOM) vulnerability
- IIS5/WEBDAV Buffer Overflow vulnerability
- RPC Locator Vulnerability

It attempts to log into systems using a list of user names and passwords. This worm then drops a copy of itself in accessed machines. It also terminates antivirus-related processes and dropped files by other malware. This worm steals CD keys of certain game applications, then sends gathered data to a remote user via mIRC, a chat application. It also has backdoor capabilities and may execute remote commands in the host machine. It runs on Windows NT, 2000, and XP.

WORM_AGOBOT.MJ (Win32 Worm): This memory-resident worm exploits certain vulnerabilities to propagate across networks. Like the earlier AGOBOT variants, it takes advantage of the following Windows vulnerabilities:

- Remote Procedure Call (RPC) Distributed Component Object Model (DCOM) vulnerability
- IIS5/WEBDAV Buffer Overflow vulnerability
- RPC Locator vulnerability

It attempts to log on to systems using a predefined list of user names and passwords. It also has backdoor capabilities and may execute malicious commands on the host machine. It terminates processes related to antivirus products and processes associated with other malware. It also steals CD keys of certain game applications.

WORM_AGOBOT.MQ (Win32 Worm): This memory-resident malware has both worm and backdoor capabilities. Like the earlier AGOBOT variants, it takes advantage of the following Windows vulnerabilities to propagate across networks:

- Remote Procedure Call (RPC) Distributed Component Object Model (DCOM) Vulnerability
- RPC Locator Vulnerability
- IIS5/WEBDAV Buffer Overflow Vulnerability
- Microsoft Workstation Service Buffer Overrun Vulnerability

It drops itself as SMSSS.EXE or EXPLORED.EXE in the Windows system folder and attempts to log into systems using a list of user names and passwords. It connects to an Internet Relay Chat (IRC) server and joins an IRC channel to receive malicious commands to be processed on a system. It also terminates antivirus-related programs and steals CD keys of certain game applications. It modifies the HOSTS file to prevent a user from visiting Web sites of several antivirus and security companies. It also attempts to launch a Distributed Denial of Service (DDoS) attack against specific Web sites by continuously feeding some HTTP requests. This malware runs on Windows NT, 2000, 2003, and XP.

WORM_AGOBOT.NM (Win32 Worm): This memory-resident malware has both worm and backdoor capabilities. Like the earlier AGOBOT variants, it takes advantage of the following Windows vulnerabilities to propagate across networks:

- Remote Procedure Call (RPC) Distributed Component Object Model (DCOM) Vulnerability
- RPC Locator Vulnerability
- IIS5/WEBDAV Buffer Overflow Vulnerability

It drops itself as SVCMNGMT.EXE in the Windows system folder and attempts to log on to systems using a list of user names and passwords. It opens a random port and connects to an Internet Relay Chat (IRC) server. It then joins an IRC channel to receive malicious commands to be processed on a system. It also terminates antivirus-related programs and steals CD keys of certain game applications. It modifies the HOSTS file to redirect any access to specific antivirus Web sites to 127.0.0.1. This UPX-compressed runs on Windows 2000 and XP.

WORM_AGOBOT.NQ (Win32 Worm): This memory-resident worm exploits certain vulnerabilities to propagate across networks. Like the earlier AGOBOT variants, it takes advantage of the following Windows vulnerabilities:

- Remote Procedure Call (RPC) Distributed Component Object Model (DCOM) vulnerability
- IIS5/WEBDAV Buffer Overflow vulnerability
- RPC Locator vulnerability

It attempts to log on to systems using a predefined list of user names and passwords. It also has backdoor capabilities and may execute malicious commands on the host machine. It terminates antivirus-related processes and steals the Windows product ID and the CD keys of certain game applications. It also disables access to certain antivirus Web sites by modifying the Windows HOSTS file. This worm runs on Windows NT, 2000, and XP.

WORM_AGOBOT.RD (Aliases: Worm/Agobot.IK.2, Backdoor.Agobot.ll, W32/Gaobot.worm.gen.d, W32.HLLW.Gaobot.gen) (Win32 Worm): This memory-resident worm exploits certain vulnerabilities to propagate across networks. Like the earlier AGOBOT variants, it takes advantage of the following Windows vulnerabilities:

- Remote Procedure Call (RPC) Distributed Component Object Model (DCOM) vulnerability
- IIS5/WEBDAV Buffer Overflow vulnerability
- RPC Locator vulnerability

It attempts to log on to systems using a predefined list of user names and passwords. It also has backdoor capabilities and may execute malicious commands on the host machine. It terminates antivirus-related processes and steals the Windows product ID and the CD keys of certain game applications. It also disables access to certain antivirus Web sites by modifying the Windows HOSTS file. This worm runs on Windows 2000 and XP.

WORM_AGOBOT.ST (Internet Worm): This memory-resident malware has both worm and backdoor capabilities. Like the earlier AGOBOT variants, it takes advantage of the following Windows vulnerabilities to propagate across networks:

- Remote Procedure Call (RPC) Distributed Component Object Model (DCOM) Vulnerability
- RPC Locator Vulnerability
- IIS5/WEBDAV Buffer Overflow Vulnerability

It drops itself as SERVICE32.EXE in the Windows system folder and attempts to log on to systems using a list of user names and passwords. It opens a random port and connects to an Internet Relay Chat (IRC) server. It then joins an IRC channel to receive malicious commands to be processed on a system. It terminates antivirus-related programs and steals CD keys of certain game applications. It also modifies the HOSTS file so that any access to specific antivirus Web sites is redirected to 127.0.0.1. It deletes all files that contain the string sound in their file names. This Petite-compressed malware runs on Windows 2000 and XP.

WORM_ANIG.B (Internet Worm): This memory-resident worm propagates by dropping copies of itself in shared network drives. It steals and saves logon information in a file, which can be retrieved by a remote user. It has a keylogger component that substitutes the standard Microsoft Graphical Identification and Authentication .DLL (MSGINA.DLL) to carry out its information-stealing routine. It has backdoor capabilities and listens to TCP port 5190 for remote commands. This malware is written using Borland Delphi, a high-level programming language, and runs on Windows NT, 2000, and XP.

WORM_BAGLE.X (Aliases: W32/Bagle.z@MM, w32.beagle.w@mm, W32/Bagle-W, Bagle.y) (Internet Worm): This worm has been reported in the wild. Several infection reports indicate that it is spreading in Europe, Latin America, and the US. This memory-resident worm propagates via e-mail and network shares. Upon execution, it drops the following files in the Windows system folder:

- Drvsys.exe
- Drvsys.exeopen
- Drvsys.exeopenopen

It may also create more copies of itself with the string open appended in its file name. The e-mail it sends out has varying subjects, message bodies, and attachment file names. It uses specific user names followed by the domain of the recipient's e-mail address to spoof the From field. It sends two attachments. One of them is a picture of a girl in .JPEG format. The other attachment is a copy of this malware with any of the following extension names: COM, CPL, EXE, HTA, SCR, VBS, or ZIP. It also searches for target e-mail addresses in files having certain extensions. However, it skips those addresses that contain particular strings. This malware drops copies of itself using specific file names in folders that contain the string shar in their folder names. It terminates several antivirus and security programs. It also creates a separate thread and listens to port 2535 for its backdoor capability. It then tries to connect to several Web sites. It deletes several registry keys that WORM_NETSKY variants and other normal applications use to automatically run. After January 25, 2005, it also deletes a certain registry key and entry. This UPX-compressed malware runs on Windows 95, 98, ME, NT, 2000, and XP.

WORM_MSBLAST.I (Aliases: Worm.W32.Lovsan.f, W32.Blaster.worm) (Internet Worm): To propagate, this worm exploits the RPC DCOM BUFFER OVERFLOW, a vulnerability in a Windows Distributed Component Object Model (DCOM) Remote Procedure Call (RPC) interface allows a malicious user to gain full access and execute any code on a target machine, leaving it compromised. This worm connects to a particular site and downloads an updated copy of itself. It also modifies the Internet Explorer home page, redirecting it to a certain Web site.

WORM_MYDOOM.I (Aliases: I-Worm.Mydoom.h, W32/Mydoom.i@MM, W32.Mydoom.I@mm) (Internet Worm): This variant spreads by sending itself via e-mail to target addresses it gathers from the Windows Address Book (WAB) and from certain files in the affected system. It also constructs additional e-mail addresses as target recipients. The e-mail it sends out has varying subjects, message bodies, and attachment file names. This worm launches a distributed denial of service (DDoS) attack against a certain site by continuously requesting for the main page of the said site. It bears the text file icon.

WORM_MYDOOM.J (Internet Worm): This mass-mailing worm obtains target e-mail addresses from files in the Temporary Internet Files folders. It also constructs possible targets based on obtained addresses. It uses its built-in Simple Mail Transfer Protocol engine to send e-mail and does not require other e-mail clients to propagate. It sends e-mail with varying content. This worm has backdoor capabilities. It opens a random port from 1000 and above to allow remote users to access infected systems. It also drops a malicious file detected as WORM_BUGBEAR.A to log user keystrokes. It terminates a list of security-related processes, including antivirus, firewall, and monitoring applications. When executed, this worm drops a text file named Message, which contains garbage data, in the Windows temporary folder. It then opens the file using Notepad. This worm runs on Windows 95, 98, ME, NT, 2000, and XP.

WORM_RBOT.SN (Alias: W32.Gaobot.SN) (Internet Worm): This worm spreads via network shares. It scans the network for systems with weak passwords and attempts to drop a copy of itself on target machines. It forces its way into a system using a list of user names and passwords as hardcoded in its body. It also has backdoor functionalities. It connects to the Internet Relay Chat (IRC) server spazattack.hax0r3d.net and then automatically joins the IRC channel #g0dl1k3 to wait for commands from a malicious user. This worm steals the CD keys of popular game applications. It runs on Windows NT, 2000, and XP.

WORM_SPYBOT.RB (Alias: Worm/Spyboter.d) (Internet Worm): This worm drops a copy of itself as WINUSER32.EXE in the Windows system folder. It modifies the Windows registry so that it runs at every system startup. To propagate, this worm searches for specific network shares and attempts to copy itself to accessed systems as WINUSER32.EXE. However if the found shared folders have restricted access rights, this worms uses a list of commonly-used user names and passwords to gain entry to the target system. This malware has backdoor capabilities. It has a built-in IRC (Internet Chat Relay) client engine, which enables it to connect to an IRC channel. It opens a random port and awaits commands from a remote user. This worm steals the Windows Product ID as well as the CD keys of several games. It terminates certain antivirus-related processes. It is also able to launch flood attacks against a target Web site. It runs on Windows 98, ME, NT, 2000 and XP.

WORM_SDBOT.JS (Win32 Worm): This worm exploits certain vulnerabilities to propagate across networks. It takes advantage of the following Windows vulnerabilities:

- Remote Procedure Call (RPC) Distributed Component Object Model (DCOM) vulnerability
- IIS5/WEBDAV Buffer Overflow vulnerability
- RPC Locator Vulnerability

It attempts to log on to systems using a list of user names and passwords. This worm then drops a copy of itself in accessed machines. This worm steals CD keys of certain game applications, then sends gathered data to a remote user via mIRC, a chat application. It also has backdoor capabilities and may execute remote commands in the host machine. This worm is written using Visual C++ and runs on Windows NT, 2000 and XP.

WORM_SDBOT.RG (Alias: Backdoor.Win32.SdBot.14672) (Win32 Worm): To spread, this worm attempts to establish a connection with specific shares on a randomly-generated IP address. It also attempts to access target systems using a list of common user names and passwords. This malware has backdoor capabilities. It has a built in IRC (Internet Relay Chat) client engine, which enables it to connect to an IRC channel and await commands from a remote user. It steals the CD keys of several software, and performs different kinds of denial of service (DoS) attacks against target systems. It runs on Windows 95, 98, ME, NT, 2000 and XP.

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.*

The Virus and Trojan sections are derived from compiling information from the following anti-virus vendors and security related web sites: Sophos, Trend Micro, Symantec, McAfee, Network Associates, Central Command, F-Secure, Kaspersky Labs, MessageLabs and The WildList Organization International.

Trojan	Version	CyberNotes Issue #
Backdoor.Anyserv.B	**B**	**Current Issue**
Backdoor.Aphexdoor	N/A	CyberNotes-2004-03
Backdoor.Berbew.B	**B**	**Current Issue**
Backdoor.Berbew.D	**D**	**Current Issue**
Backdoor.Carufax.A	**A**	**Current Issue**
Backdoor.Cazno	N/A	SB04-091
Backdoor.Cazno.Kit	N/A	SB04-091
Backdoor.Danton	N/A	SB04-091
Backdoor.Domwis	N/A	CyberNotes-2004-04
Backdoor.Evivinc	**N/A**	**Current Issue**
Backdoor.Gaster	N/A	CyberNotes-2004-01
Backdoor.Graybird.H	H	CyberNotes-2004-01
Backdoor.Graybird.I	**I**	**Current Issue**
Backdoor.IRC.Aimwin	N/A	SB04-105
Backdoor.IRC.Aladinz.F	F	CyberNotes-2004-01
Backdoor.IRC.Aladinz.G	G	CyberNotes-2004-02
Backdoor.IRC.Aladinz.H	H	CyberNotes-2004-02
Backdoor.IRC.Aladinz.J	J	CyberNotes-2004-04
Backdoor.IRC.Aladinz.L	L	CyberNotes-2004-05
Backdoor.IRC.Aladinz.M	M	CyberNotes-2004-05
Backdoor.IRC.Aladinz.N	N	SB04-105
Backdoor.IRC.Aladinz.O	O	SB04-105
Backdoor.IRC.Aladinz.P	**P**	**Current Issue**
Backdoor.IRC.Loonbot	N/A	CyberNotes-2004-05
Backdoor.IRC.Mutebot	N/A	SB04-105
Backdoor.IRC.MyPoo	N/A	SB04-091
Backdoor.IRC.MyPoo.Kit	N/A	SB04-091
Backdoor.IRC.Spybuzz	N/A	SB04-091
Backdoor.IRC.Zcrew.C	**C**	**Current Issue**
Backdoor.Kaitex.E	E	CyberNotes-2004-05
Backdoor.Medias	N/A	SB04-105
Backdoor.NetCrack.B	**B**	**Current Issue**
Backdoor.Nibu.D	**D**	**Current Issue**
Backdoor.OptixPro.13.C	13.C	CyberNotes-2004-04
Backdoor.OptixPro.13b	13b	CyberNotes-2004-02

Trojan	Version	CyberNotes Issue #
Backdoor.Portless	N/A	CyberNotes-2004-01
Backdoor.R3C.B	B	SB04-091
Backdoor.Ranky.E	E	SB04-091
Backdoor.Ranky.F	F	SB04-105
Backdoor.Sdbot.S	S	CyberNotes-2004-01
Backdoor.Sdbot.T	**T**	**Current Issue**
Backdoor.Sdbot.Y	**Y**	**Current Issue**
Backdoor.Threadsys	N/A	CyberNotes-2004-02
Backdoor.Trodal	N/A	CyberNotes-2004-01
Backdoor.Tumag	N/A	SB04-091
Backdoor.Tuxder	N/A	CyberNotes-2004-02
BackDoor-AWQ.b	B	CyberNotes-2004-01
BackDoor-CBH	N/A	CyberNotes-2004-01
BackDoor-CCT	**CCT**	**Current Issue**
BDS/Purisca	N/A	CyberNotes-2004-01
BKDR_UPROOTKIT.A	A	CyberNotes-2004-01
Dial/ExDial-A	A	CyberNotes-2004-01
DOS_MASSMSG.A	A	CyberNotes-2004-01
Download.Berbew.dam	N/A	CyberNotes-2004-01
Download.Chamber	N/A	SB04-091
Download.Chamber.Kit	N/A	SB04-091
Download.SmallWeb	N/A	SB04-091
Download.SmallWeb.Kit	N/A	SB04-091
Download.Tagdoor	N/A	SB04-105
Downloader.Botten	N/A	CyberNotes-2004-05
Downloader.Mimail.B	B	CyberNotes-2004-02
Downloader.Psyme	N/A	SB04-105
Downloader-GD	GD	CyberNotes-2004-01
Downloader-GH	GH	CyberNotes-2004-02
Downloader-GN	GN	CyberNotes-2004-02
Downloader-IU	IU	SB04-105
Dyfuca	N/A	CyberNotes-2004-01
Exploit-URLSpoof	N/A	CyberNotes-2004-01
Hacktool.Sagic	N/A	CyberNotes-2004-01
IRC-Bun	N/A	CyberNotes-2004-01
Java.StartPage	N/A	CyberNotes-2004-05
JS/AdClicker-AB	AB	CyberNotes-2004-01
Keylogger.Stawin	N/A	CyberNotes-2004-03
Keylog-Ramb	**N/A**	**Current Issue**
MAC_MP3CONCEPT.A	**A**	**Current Issue**
MultiDropper-GP.dr	GP.dr	CyberNotes-2004-04
MultiDropper-JW	JW	SB04-091
Needy.C	C	CyberNotes-2004-03
Needy.D	D	SB04-105
Needy.E	E	SB04-105
Needy.F	F	SB04-105
Needy.G	G	SB04-105
Needy.H	H	SB04-105
Needy.I	I	SB04-105
Ouch	N/A	CyberNotes-2004-02
Perl/Exploit-Sqlinject	N/A	CyberNotes-2004-01
Phish-Potpor	N/A	CyberNotes-2004-04
Proxy-Agent	N/A	CyberNotes-2004-03
Proxy-Cidra	N/A	CyberNotes-2004-01
PWS-Datei	N/A	CyberNotes-2004-01
PWSteal.Bancos.D	D	CyberNotes-2004-01
PWSteal.Bancos.E	E	CyberNotes-2004-05
PWSteal.Bancos.F	F	SB04-091

Trojan	Version	CyberNotes Issue #
PWSteal.Bancos.G	G	SB04-091
PWSteal.Bancos.H	**H**	**Current Issue**
PWSteal.Banpaes.C	C	CyberNotes-2004-05
PWSteal.Freemega	N/A	CyberNotes-2004-02
PWSteal.Goldpay	N/A	SB04-105
PWSteal.Irftp	N/A	CyberNotes-2004-05
PWSteal.Lemir.G	G	SB04-105
PWSteal.Leox	N/A	CyberNotes-2004-02
PWSteal.Olbaid	N/A	CyberNotes-2004-03
PWSteal.Sagic	N/A	CyberNotes-2004-01
PWSteal.Souljet	N/A	SB04-105
PWSteal.Tarno.B	B	CyberNotes-2004-05
PWSteal.Tarno.C	C	SB04-091
PWSteal.Tarno.E	**E**	**Current Issue**
QReg-9	9	CyberNotes-2004-04
Spy-Peep	N/A	SB04-091
Startpage-AI	AI	CyberNotes-2004-01
StartPage-AU	AU	CyberNotes-2004-02
StartPage-AX	AX	CyberNotes-2004-02
TR/DL906e	N/A	CyberNotes-2004-01
TR/Psyme.B	B	CyberNotes-2004-01
Troj/AdClick-Y	Y	CyberNotes-2004-03
Troj/Adtoda-A	A	SB04-105
Troj/Agent-C	C	CyberNotes-2004-01
Troj/Antikl-Dam	N/A	CyberNotes-2004-01
Troj/Apher-L	L	CyberNotes-2004-02
Troj/Badparty-A	A	SB04-091
Troj/Banker-S	**S**	**Current Issue**
Troj/Bdoor-CCK	CCK	CyberNotes-2004-05
Troj/BeastDo-M	M	CyberNotes-2004-01
Troj/BeastDo-N	N	CyberNotes-2004-01
Troj/ByteVeri-E	E	CyberNotes-2004-03
Troj/Chapter-A	A	CyberNotes-2004-03
Troj/Cidra-A	A	CyberNotes-2004-01
Troj/Cidra-D	D	CyberNotes-2004-05
Troj/Control-E	E	CyberNotes-2004-03
Troj/CoreFloo-D	D	CyberNotes-2004-01
Troj/Daemoni-B	B	CyberNotes-2004-03
Troj/Daemoni-C	C	CyberNotes-2004-03
Troj/Darium-A	A	CyberNotes-2004-01
Troj/DDosSmal-B	**B**	**Current Issue**
Troj/DDosSmal-B	B	CyberNotes-2004-04
Troj/Delf-JV	JV	CyberNotes-2004-02
Troj/Delf-NJ	NJ	CyberNotes-2004-01
Troj/DelShare-G	G	CyberNotes-2004-01
Troj/Digits-B	B	CyberNotes-2004-03
Troj/Divix-A	A	CyberNotes-2004-02
Troj/Dloader-K	K	CyberNotes-2004-01
Troj/Domwis-A	A	CyberNotes-2004-05
Troj/Eyeveg-C	C	CyberNotes-2004-05
Troj/Femad-B	B	CyberNotes-2004-03
Troj/Femad-D	D	CyberNotes-2004-01
Troj/Flator-A	A	CyberNotes-2004-01
Troj/Flood-CR	CR	CyberNotes-2004-02
Troj/Flood-DZ	DZ	CyberNotes-2004-03
Troj/Getdial-A	A	CyberNotes-2004-01
Troj/HacDef-100	100	CyberNotes-2004-05
Troj/Hackarmy-A	A	CyberNotes-2004-02

Trojan	Version	CyberNotes Issue #
Troj/Hidemirc-A	A	CyberNotes-2004-03
Troj/Hosts-A	A	CyberNotes-2004-01
Troj/Hosts-B	B	CyberNotes-2004-02
Troj/IEStart-G	G	CyberNotes-2004-02
Troj/Inor-B	B	CyberNotes-2004-02
Troj/Ipons-A	A	CyberNotes-2004-01
Troj/Ircbot-S	S	CyberNotes-2004-02
Troj/IRCBot-U	U	CyberNotes-2004-03
Troj/Ircfloo-A	A	CyberNotes-2004-03
Troj/JDownL-A	A	SB04-105
Troj/Ketch-A	A	CyberNotes-2004-01
Troj/Kuzey-A	A	CyberNotes-2004-02
Troj/Lalus-A	A	CyberNotes-2004-01
Troj/Ldpinch-C	C	CyberNotes-2004-02
Troj/LDPinch-G	G	CyberNotes-2004-05
Troj/LDPinch-H	H	CyberNotes-2004-05
Troj/LdPinch-L	**L**	**Current Issue**
Troj/Legmir-E	E	CyberNotes-2004-01
Troj/Legmir-K	**K**	**Current Issue**
Troj/Lindoor-A	A	CyberNotes-2004-02
Troj/Linploit-A	A	CyberNotes-2004-02
Troj/Loony-E	**E**	**Current Issue**
Troj/Mahru-A	A	CyberNotes-2004-03
Troj/Mircsend-A	A	CyberNotes-2004-02
Troj/Mmdload-A	A	CyberNotes-2004-02
Troj/MsnCrash-B	B	CyberNotes-2004-01
Troj/Mssvc-A	A	CyberNotes-2004-01
Troj/Myss-C	C	CyberNotes-2004-04
Troj/Narhem-A	A	CyberNotes-2004-05
Troj/NoCheat-B	B	CyberNotes-2004-03
Troj/Noshare-K	K	CyberNotes-2004-02
Troj/Pinbol-A	A	CyberNotes-2004-04
Troj/Prorat-D	D	SB04-091
Troj/Proxin-A	A	CyberNotes-2004-02
Troj/Ranckbot-A	A	SB04-091
Troj/Ranck-K	K	CyberNotes-2004-05
Troj/Rybot-A	A	SB04-105
Troj/Saye-A	A	CyberNotes-2004-02
Troj/Sdbot-AP	AP	CyberNotes-2004-03
Troj/SdBot-BB	BB	CyberNotes-2004-02
Troj/Sdbot-CY	CY	CyberNotes-2004-01
Troj/Sdbot-EF	EF	CyberNotes-2004-01
Troj/SdBot-EG	EG	CyberNotes-2004-01
Troj/SdBot-EI	EI	CyberNotes-2004-01
Troj/Sdbot-EJ	EJ	CyberNotes-2004-02
Troj/Sdbot-EK	EK	CyberNotes-2004-02
Troj/Sdbot-EL	EL	CyberNotes-2004-02
Troj/Sdbot-FM	FM	CyberNotes-2004-04
Troj/Search-A	A	CyberNotes-2004-02
Troj/Sect-A	A	CyberNotes-2004-02
Troj/Seeker-F	F	CyberNotes-2004-01
Troj/Small-AG	**AG**	**Current Issue**
Troj/Small-AW	AW	CyberNotes-2004-03
Troj/Spooner-C	C	CyberNotes-2004-02
Troj/SpyBot-AA	AA	CyberNotes-2004-01
Troj/Spybot-AM	AM	CyberNotes-2004-01
Troj/Spybot-C	C	CyberNotes-2004-01
Troj/StartPa-AE	**AE**	**Current Issue**

Trojan	Version	CyberNotes Issue #
Troj/StartPag-C	C	CyberNotes-2004-01
Troj/StartPag-E	E	CyberNotes-2004-02
Troj/StartPg-AU	AU	CyberNotes-2004-01
Troj/StartPg-AY	AY	CyberNotes-2004-01
Troj/StartPg-BG	BG	CyberNotes-2004-01
Troj/StartPg-U	U	CyberNotes-2004-01
Troj/Stawin-A	A	CyberNotes-2004-03
Troj/TCXMedi-E	E	CyberNotes-2004-01
Troj/Tofger-F	F	CyberNotes-2004-01
Troj/Tofger-L	L	CyberNotes-2004-01
Troj/Troll-A	A	CyberNotes-2004-02
Troj/Uproot-A	A	CyberNotes-2004-01
Troj/Volver-A	A	CyberNotes-2004-03
Troj/Weasyw-A	A	CyberNotes-2004-02
Troj/Webber-D	D	CyberNotes-2004-01
Troj/Webber-H	**H**	**Current Issue**
Troj/Winpup-C	C	CyberNotes-2004-03
Trojan.Anymail	N/A	CyberNotes-2004-01
Trojan.AphexLace.Kit	N/A	SB04-105
Trojan.Bansap	N/A	CyberNotes-2004-04
Trojan.Bookmarker	N/A	CyberNotes-2004-01
Trojan.Bookmarker.B	B	CyberNotes-2004-02
Trojan.Bookmarker.C	C	CyberNotes-2004-02
Trojan.Bookmarker.D	C	CyberNotes-2004-03
Trojan.Bookmarker.E	E	CyberNotes-2004-03
Trojan.Bookmarker.F	F	CyberNotes-2004-05
Trojan.Bookmarker.G	G	SB04-091
Trojan.Brutecode	N/A	SB04-105
Trojan.Cookrar	N/A	SB04-105
Trojan.Download.Revir	N/A	CyberNotes-2004-01
Trojan.Dustbunny	N/A	SB04-091
Trojan.Etsur	N/A	CyberNotes-2004-05
Trojan.Gema	N/A	CyberNotes-2004-01
Trojan.Gipma	N/A	CyberNotes-2004-05
Trojan.Gutta	N/A	CyberNotes-2004-04
Trojan.Httpdos	N/A	CyberNotes-2004-02
Trojan.KillAV.D	D	SB04-091
Trojan.Linst	N/A	SB04-091
Trojan.Lyndkrew	N/A	SB04-105
Trojan.Mercurycas.A	**A**	**Current Issue**
Trojan.Mitglieder.C	C	CyberNotes-2004-02
Trojan.Mitglieder.D	D	CyberNotes-2004-05
Trojan.Mitglieder.E	E	CyberNotes-2004-05
Trojan.Mitglieder.F	F	SB04-105
Trojan.Mitglieder.H	**H**	**Current Issue**
Trojan.Mitglieder.I	**I**	**Current Issue**
Trojan.Noupdate	N/A	CyberNotes-2004-05
Trojan.Noupdate.B	B	SB04-091
Trojan.Popdis	**N/A**	**Current Issue**
Trojan.PWS.Qphook	N/A	CyberNotes-2004-01
Trojan.PWS.QQPass.F	F	CyberNotes-2004-04
Trojan.Regsys	N/A	SB04-091
Trojan.Simcss.B	B	CyberNotes-2004-05
Trojan.Tilser	N/A	CyberNotes-2004-05
Trojan.Trunlow	N/A	SB04-105
Unix/Exploit-SSHIDEN	N/A	CyberNotes-2004-02
UrlSpoof.E	E	CyberNotes-2004-03
VBS.Bootconf.B	B	CyberNotes-2004-04

Trojan	Version	CyberNotes Issue #
VBS.Shania	N/A	CyberNotes-2004-03
VBS/Inor-C	C	CyberNotes-2004-03
VBS/Suzer-B	B	CyberNotes-2004-01
VBS/Wisis-A	A	CyberNotes-2004-02
W32.Bizten	N/A	CyberNotes-2004-01
W32.Dumaru.AI	**AI**	**Current Issue**
W32.Hostidel.Trojan.B	B	CyberNotes-2004-03
W32.Kifer	N/A	CyberNotes-2004-04
W32.Kifer.B	B	CyberNotes-2004-04
W32.Tuoba.Trojan	N/A	SB04-091
Xombe	N/A	CyberNotes-2004-01

Backdoor.Anyserv.B: This is a Trojan horse that gives a malicious user remote access to an infected computer. This threat is written in C++ and is packed with ASPack. When Backdoor.Anyserv.B is executed, it injects the Rasaccs.dll file into Svchost.exe, so that it can run unnoticed and may copy several .dll and executable files to the %Windir% folder. It may also attempt to hijack the "Routing and Remote Access" service by setting the value, "ServiceDLL" = "%Windir%\rasaccs.dll," in the registry key:

- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RemoteAccess\Parameters

The Trojan monitors keystrokes and logs them to a file in the %Temp% folder and registers a temporary Internet address with tzo.com and notifies the malicious user of the infection. It listens on port 1129 for connections.

Backdoor.Berbew.B: This is a Backdoor Trojan horse that allows a compromised computer to be used as a Web proxy. This Trojan also attempts to steal cached passwords from an infected computer.

Backdoor.Berbew.D (Alias: Backdoor.Padodor.e): This is a Backdoor Trojan horse that attempts to steal cached passwords.

Backdoor.Carufax.A: This is a backdoor Trojan horse program that allows unauthorized remote access to a compromised system. It is written in C++ and is packed with PECompact.

BackDoor-CCT: This Trojan bears strong similarities to the W32/Dumaru family. It opens a backdoor on the victim machine, and also steals data from the machine. The Trojan targets applications with specific strings in the window title in an attempt to log keystrokes related to online financial transactions. Windows with titles containing various strings are targeted. The Trojan also harvests data from the temporary Internet files on the victim machine. Data is sent to the malicious user via HTTP (a completed HTML form is written to %WinDir%\TEMP\feff35a0.htm, and IEXPLORE.EXE is launched to initiate its posting). Users should block HTTP access to the following domain:

- http://govno.ws

Stolen data may also be sent to the malicious user via e-mail - the Trojan contains its own SMTP engine to construct outgoing messages. The backdoor functionality includes an FTP server, screen captures, webcam control and file execution.

Backdoor.Evivinc: This is a Backdoor Trojan horse that installs WinVNC without a user's knowledge. It also allows unauthorized, remote access to an infected computer.

Backdoor.Graybird.I (Alias: Backdoor.GrayBird.m): This is a Trojan horse and a variant of Backdoor.Graybird. It gives a malicious user access to your computer. The existence of the file, Graypigeon.dll, is an indication of a possible infection. This threat is written in Borland Delphi.

Backdoor.IRC.Aladinz.P: This is a backdoor Trojan horse that uses malicious mIRC scripts. This Trojan allows a malicious user to access your computer. By default the Trojan listens on TCP port 2688.

Backdoor.IRC.Zcrew.C: This is a backdoor Trojan horse that may allow for the remote control of an infected system through IRC and FTP.

Backdoor.NetCrack.B: This is a Backdoor Trojan horse that gives a malicious user unauthorized access to an infected computer. It can be programmed to perform different actions. Depending on how it was programmed, the Trojan may use different .dll files. This Trojan horse is created using the NetCrack Trojan creator.

Backdoor.Nibu.D (Aliases: Bloodhound.Exploit.6, W32/Dumaru.w.gen, Exploit-MhtRedir): This is a Trojan horse that attempts to steal passwords and bank account information.

Backdoor.Sdbot.T: This is a backdoor Trojan horse that is similar to Backdoor.Sdbot.S. It allows a malicious user to control an infected computer. When Backdoor.Sdbot.T runs, it copies itself as %System%\kgzgjkpcw.exe and %System%\zonealarm.exe. It attempts to end the following processes:

- Netstat.exe
- Msconfig.exe
- Regedit.exe

And adds the value, "Winsock2 driver"="kgzgjkpcw.exe," to the registry keys:

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

It also adds the value, "Winsock2 driver"="ZONEALARM.EXE," to the registry keys:

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

The Trojan uses its own IRC client to connect to a specified IRC channel and wait for the commands to perform various actions.

Backdoor.Sdbot.Y (Aliases: Backdoor.Sdbot.U, W32/Sdbot.worm.gen.e): This is a Backdoor Trojan horse that allows unauthorized remote access to an infected computer. When Backdoor.Sdbot.Y is executed, it copies itself as %System%\IEXPLORE.EXE and creates a service for the Trojan named "Internet Explorer." To do this, the Trojan creates the registry key:

- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\iexplore

The Trojan connects to an IRC server and waits for commands.

Keylog-Ramb: This is a keylogging Trojan, designed to steal data from the victim machine. The threat consists of two components:

- an EXE which installs itself on the victim machine, hooking system startup.
- a DLL, dropped by the above EXE. This DLL is injected into the EXPLORER.EXE process on the victim machine. This technique is often used as a means of bypassing personal firewall protection (EXPLORER.EXE is often granted permissions 'foreign' processes are not).

The Trojan contains its own SMTP engine to construct outgoing messages containing the stolen data. The following files are dropped into the Windows system directory on the victim machine:

- %SysDir%\SVCROOT.EXE (8,704 bytes)
- %SysDir%\SVCROOT.DLL (5,120 bytes)

The following Registry key is added to hook system startup:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "explorer" = %SysDir%\SVCROOT.EXE

Logged keystrokes (together with the application they are associated with) are written to the following file in the Windows system directory:

- %SysDir%\GDISYS32.DLL

The Trojan also logs details specific to Internet Explorer (IEXPLORE.EXE) sessions. The window title (typically the title from within the HTML) is logged together with the filename of the page being viewed, and keystrokes entered within that session. This data is logged to the following file:

- %SysDir%\MSNSYS32.DLL

The Trojan uses its own SMTP engine to construct an e-mail message containing the harvested data.

MAC_MP3CONCEPT.A (Aliases: MP3Concept, MP3Virus.Gen, MAC.Amphimix, MacOS/Amphimix, MP3Virus.gen): This is a Proof of Concept Trojan that only affects the Macintosh platform. It does not have any destructive payload or viral routine to infect or damage the target system. It also has no spreading capability. The Trojan's only exploit is in its icon, which appears to be a valid MP3 file but is actually a Macintosh executable with an MP3 file inside. Upon execution, it plays an MP3 file depicting the sound of a laughing man. Simultaneously, it also displays a message box with any of the following text:

"Yep, this is an application (So what is your iTunes playing right now?)"

"(But you can add it to your iTunes library too.)"

PWSteal.Bancos.H: This is a Trojan horse that mimics the online interfaces of certain Brazilian banks to try to steal account information. It is a minor variant of PWSteal.Bancos.F. This threat is packed using ASPack and may be contained in a self-extracting RAR file. See the "Technical Details" section for the login screens that may be displayed.

PWSteal.Tarno.E: This is a Trojan horse that tries to steal information that you enter into certain Web forms.

Troj/Banker-S: This is a password stealing Trojan that attempts to capture keylogs associated with web browsing. Troj/Banker-S creates the following files which are all detected by this identity:

- <Windows>\dllreg.exe
- <Windows>\sock64.dll
- <StartUp>\rundllw.exe
- <Windows System>\load32.exe
- <Windows System>\vxdmgr32.exe

In order to run on system restart, Troj/Banker-S creates the following registry entry:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\load32

Troj/Banker-S adds the name of one of the copies of itself to the Run= line of win.ini and the shell= line of system.ini. Troj/Banker-S uses its own SMTP engine to send results of the keylogger to a Russian e-mail address.

Troj/DDosSmal-B: This is a Trojan that attempts a Denial of Service attack on a website. It repeatedly sends random TCP/IP packets to diana23.dyndns.org port 80 (HTTP). It does this for 10 minutes, then sets a timeout for 1 minute. After the timeout elapses, it goes back to the start (repeating the 10 minute flood). In order to run automatically when Windows starts up, the Trojan copies itself to the file winsys.exe in the Windows folder and adds the following registry entry:

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

Troj/LdPinch-L (Aliases: Trojan.PSW.LdPinch.ce, PWS-LDPinch, TROJ_LDPINCH.E): This is a password stealing Trojan. Upon execution it collects passwords from the computer and e-mails them to a remote address. The Trojan moves itself to the Windows folder and sets the following registry entry to auto start:

- HKCU\Software\Microsoft\Windows\CurrentVersion\Run\SVCHOST = <windows folder>\<Trojan name>

On Windows 2000, the Trojan will attempt to connect to a web page. The Trojan also attempts to drop and load a helper DLL (ihook.dll) into the Windows folder which is detected as Troj/Klog-A.

Troj/Legmir-K (Aliases: PSW.QQpass.ak, Lemir-Gen, Legmir-AH): This is a password-stealing Trojan. In order to run automatically when Windows starts up, the Trojan copies itself to the file intrenat.exe in the Windows folder and adds the following registry entries:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Internet = C:\WINDOWS\intrenat.exe
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\Intrenat = :\WINDOWS\intrenat.exe

Troj/LegMir-K also creates the file exp1orer.dll in the Windows folder. This file is already detected as Troj/LegMir-E. To avoid detection, Troj/LegMir-K attempts to terminate the following processes:

- EGHOST.EXE
- MAILMON.EXE
- KAVPFW.EXE

- RAVTIMER.EXE
- RAVMON.EXE
- CCENTER.EXE
- NAVAPW32.EXE

Troj/LegMir-K stores stolen passwords in the HKCR section of the registry and sends them to the author via e-mail. The destination e-mail address and the exact location in the registry can both be configured by the author.

Troj/Loony-E (Alias: Backdoor.SdBot.iw): This is a backdoor Trojan that allows unauthorized access and control of the infected computer from a remote location via IRC channels. Troj/Loony-E copies itself to the Windows system folder as SVSHOST.EXE and creates the following registry entry in order to run itself on system startup:

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

Troj/Small-AG (Aliases: TrojanDownloader.Win32.Small.fv, Win32/TrojanDownloader.Esepor.G): Troj/Small-AG will download and install a Trojan when executed. The installed Trojan will drop the hidden files TMKSRVU.EXE and XPLUGIN.DLL into the Windows System folder and a small text file, HOSTS, into the Windows folder upon execution. The following registry entry will be created:

- HKLM\Software\TMKSoft\XPlugin\

This Trojan will attempt to connect to the various sites and may also try to display adverts from these websites:

- http://www.xxxod.net
- http://connect.online-dialer.com
- http://download.online-dialer.com
- http://www.adultfriendfinder.com
- http://www.freepassbucks.com

Troj/Webber-H (Aliases: TrojanDownloader.Win32.Small.hg, Trojan.Download.Berbew, Downloader-DI Trojan, Downloader-DI!zip): This Trojan has been reported in the wild. It is a two component backdoor Trojan. The downloader component of the Trojan appears to have been mass mailed out. When run, the Trojan downloads a remote file to C:\windows\usermade.exe and executes it. The downloaded component is a password stealing Trojan that attempts to extract sensitive information from several locations on the system and sends it to a remote computer. The downloaded component copies itself as a file with a random name into the Windows system folder and drops and executes a DLL file, also with a random name, that runs the copy of the Trojan. In order to be started automatically the Trojan creates the following registry entries:

- HKLM\Software\CLASSES\CLSID\{79FB9088-19CE-715D-D900-216290C5B738} \InProcServer32
- HKLM\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad\Web Event Logger

Troj/Webber-H also sets the following Microsoft Internet Explorer related registry entries to prompt the user into entering passwords:

- HCU\Software\Microsoft\Internet Explorer\Main\FormSuggest Passwords
- HCU\Software\Microsoft\Internet Explorer\Main\FormSuggest PW Ask
- HCU\Software\Microsoft\Internet Explorer\Main\Use FormSuggest

Trojan.Mercurycas.A: This is a Trojan horse that allows an infected computer to be used as an e-mail relay. The Trojan is written in C++ and is packed with UPX.

Trojan.Mitglieder.H (Alias: W32/Bagle.x!proxy): This is a minor variant of Trojan.Mitglieder. This Trojan horse opens a proxy on your system that allows it to relay e-mail. It can update or uninstall itself. Unlike its previous variants, Trojan.Mitglieder.H does not try to stop security software.

Trojan.Mitglieder.I: This is a minor variant of Trojan.Mitglieder. This Trojan horse opens a proxy on your system that allows it to relay e-mail.

Trojan.Popdis: This is a Trojan horse that modifies the registry keys and overwrites the Hosts file. The file, Addcls.exe (detected as Downloader.Trojan), downloads Trojan.Popdis. The Trojan.Popdis executable usually uses the file name Dp.dll, but other file names are possible.

Troj/StartPa-AE (Alias: Trojan.WinREG.StartPage): This Trojan changes browser settings for Microsoft Internet Explorer each time Windows is started. Troj/StartPa-AE is simply a text file (typically named sysdll.reg) which can be used as an input to Regedit to set the following registry entries:

- HKCU\Software\Microsoft\Internet Explorer\Main\Start Page
- HKCU\Software\Microsoft\Internet Explorer\Main\HOMEOldSP
- HKCU\Software\Microsoft\Internet Explorer\Main\Search Bar
- HKCU\Software\Microsoft\Internet Explorer\Main\Search Page
- HKCU\Software\Microsoft\Internet Explorer\Search\SearchAssistant
- HKLM\Software\Microsoft\Internet Explorer\Main\Start Page
- HKLM\Software\Microsoft\Internet Explorer\Main\HOMEOldSP
- HKLM\Software\Microsoft\Internet Explorer\Main\Search Bar
- HKLM\Software\Microsoft\Internet Explorer\Main\Search Page
- HKLM\Software\Microsoft\Internet Explorer\Search\SearchAssistant
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\sys = "regedit -s sysdll.reg"

The last of these registry entries causes the registry to be updated using Troj/StartPa-AE each time Windows is started. Troj/StartPa-AE may be installed on the computer by Troj/AdClick-AE.

W32.Dumaru.AI: This is a Trojan horse that attempts to steal information from an infected computer. When W32.Dumaru.AI is executed, it creates the mutex, "WMMMutext," to allow only one instance of the Trojan to execute and copies itself as:

- %System%\Load32.exe
- %System%\Vxdmgr32.exe
- %Windir%\Dllreg.exe
- %Startup%\Rundllw.exe

It may create the following files:

- %Windir%\sock32.dll: This is the keylogger module and is detected as W32.Dumaru.AI.
- %Windir%\vxdload.log: This is a log file, which is not malicious and can be manually deleted.
- %Windir%\rundllx.sys: This is a log file, which is not malicious and can be manually deleted.
- %Windir%\rundlln.sys: This is a log file, which is not malicious and can be manually deleted.

And modifies the [boot] section of the System.ini file (Windows 95/98/Me only) as follows:

```
[boot]
shell=explorer.exe %System%\vxdmgr32.exe
```

The Trojan also modifies the value, Shell, in the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon

From, "explorer.exe" to "explorer.exe %System%\vxdmgr32.exe" so that the Trojan runs when you start Windows NT/2000/XP. It modifies the [windows] section of the Win.ini file (Windows 95/98/ME only) as follows:

```
[windows]
run=%Windir%\dllreg.exe
```

and adds the value, "run"="%Windir%\dllreg.exe," in the registry key:

- HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows

so that the Trojan runs when you start Windows NT/2000/XP. It also adds the value, "load32"="%System%\load32.exe," to the registry key:

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

so that the Trojan runs when you start Windows. W32.Dumaru.AI monitors the clipboard and stores the data pasted to the clipboard in the file, %Windir%\Rundllx.sys and adds the value, kwmfound, to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\SARS

It also captures the keystrokes entered into windows, which have the title, "WEBMONEY Keeper Shell." It stores the data in the file, %Windir%\Vxdload.log and periodically e-mails the contents of Vxdload.log, rundlln.sys, and Rundllx.sys to an e-mail address that is hard-coded in the Trojan.