



Department of Homeland Security

Information Analysis and Infrastructure Protection Directorate

CyberNotes

Issue #2003-24

December 1, 2003

CyberNotes is published every two weeks by the Department of Homeland Security/Information Analysis and Infrastructure Protection (IAIP) Directorate. Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the Department of Homeland Security Information Analysis Infrastructure Protection Directorate Web site at <http://www.nipc.gov>.

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

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between November 11 and November 26, 2003. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Alexander Konig ¹ <i>Another exploit published²</i>	Unix	TerminatorX 3.81	Multiple vulnerabilities exist: a vulnerability exists in the 'load_tt_part()' function, which could let a malicious user execute arbitrary code; a vulnerability exists in the 'get_rc_name()' function, which could let a malicious user execute arbitrary code; a vulnerability exists in the 'LADSPA_PATH' environment variable, which could let a malicious user execute arbitrary code; and a vulnerability exists in the 'tx_note()' function, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	TerminatorX Multiple Command-line Vulnerabilities	High	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Anthill ³	Multiple	Anthill 0.2.5	A vulnerability exists in the code that handles attachments, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://anthill.vmlinux.ca/download/anthill-0.2.6.tar.gz	Anthill Remote File Include	High	Bug discussed in newsgroups and websites. There is no exploit code required.
Apache Software Foundation ⁴ <i>Vendors issue advisories^{5, 6}</i> <i>More advisories issued^{7, 8}</i>	Unix, MacOS X 10.x	Apache 2.0, 2.0.28, 2.0.32, 2.0.35-2.0.47	A vulnerability exists in the 'mod_cgid' module when threaded MPM is used due to the way CGI redirect paths are handled, which could let a malicious user obtain sensitive information or unauthorized access.	Upgrade available at: http://apache.sunsite.ualberta.ca/httpd/httpd-2.0.48.tar.gz <i>Conectiva:</i> ftp://atualizacoes.conectiva.com.br/ <i>Mandrake:</i> http://www.mandrakesecurity.net/en/ftp.php <i>Hewlett Packard:</i> http://www.software.hp.com <i>Trustix:</i> http://http.trustix.org/pub/trustix/updates/ <i>OpenBSD:</i> http://www.openbsd.org/errata.html	Apache Web Server mod_cgid Module CGI Data Redirection CVE Name: CAN-2003-0789	Medium	Bug discussed in newsgroups and websites.

¹ Secunia Advisory, SA10118, November 11, 2003.

² SecurityFocus, November 17, 2003.

³ Secunia Advisory, SA10281, November 24, 2003.

⁴ SecurityFocus, October 29, 2003.

⁵ Mandrake Linux Security Update Advisory, MDKSA-2003:103, November 4, 2003.

⁶ Conectiva Linux Security Announcement, CLA-2003:775, November 5, 2003.

⁷ Hewlett-Packard Company Security Bulletin, HPSBUX0311-301, November 18, 2003.

⁸ Trustix Secure Linux Security Advisory, TSLSA-2003-0041, November 15, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
<p>Apache Software Foundation^{9,10}</p> <p><i>More advisories issued^{11, 12, 13, 14, 15}</i></p> <p><i>More advisories issued^{16, 17}</i></p>	Windows, NT 4.0/2000, Unix, BSD/OS 4.0, MacOS X 10.x	Apache 1.3, 1.3.1, 1.3.3, 1.3.4, 1.3.6, 1.3.9, 1.3.11, 1.3.12, 1.3.14, 1.3.17-1.3.20, 1.3.22-1.3.28, 2.0, 2.0.28, 2.0.32, 2.0.35-2.0.47	A buffer overflow vulnerability exists in the 'mod_alias' and 'mod_rewrite' modules due to insufficient bounds checking, which could let a malicious user execute arbitrary code.	<p><u>Apache:</u> http://apache.mirror.seconchapter.info/httpd/apache_1.3.29.tar.gz</p> <p><u>Immunix:</u> http://download.immunix.org/ImmunixOS/7+/Updates/</p> <p><u>OpenPKG:</u> Ftp://ftp.openpkg.org/release</p> <p><u>Conectiva:</u> ftp://atualizacoes.conectiva.com.br/</p> <p><u>Engarde:</u> http://infocenter.guardiandigital.com/advisories/</p> <p><u>Mandrake:</u> http://www.mandrakesecurity.net/en/ftp.php</p> <p><u>SCO:</u> ftp://ftp.sco.com/pub/updates/OpenServer/CSSA-2003-SCO.28</p> <p><u>Slackware:</u> ftp://ftp.slackware.com/pub/slackware/</p> <p><u>Hewlett Packard:</u> http://www.software.hp.com</p> <p><u>Trustix:</u> http://http.trustix.org/pub/trustix/updates/</p> <p><u>OpenBSD:</u> http://www.openbsd.org/errata.html</p>	Apache Web Server Buffer Overflow	High	Bug discussed in newsgroups and websites.
Apple ¹⁸	MacOS X 10.3	MacOS X 10.3, 10.3.1, MacOS X Server 10.3, 10.3.1	An access validation vulnerability exists in the finder function, which could let a malicious user in the 'admin' group obtain write access to arbitrary directories.	No workaround or patch available at time of publishing.	Mac OS X Finder Application Access Validation	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

⁹ OpenPKG Security Advisory, penPKG-SA-2003.046, October 28, 2003.
¹⁰ Immunix Secured OS Security Advisory, IMNX-2003-7+-025-01, October 29, 2003.
¹¹ Mandrake Linux Security Update Advisory, MDKSA-2003:103, November 4, 2003.
¹² Slackware Security Advisory, SSA:2003-308-01, November 5, 2003.
¹³ Conectiva Linux Security Announcement, CLA-2003:775, November 5, 2003.
¹⁴ Guardian Digital Security Advisory, ESA-20031105-030, November 5, 2003.
¹⁵ SCO Security Advisory, CSSA-2003-SCO.28, November 7, 2003.
¹⁶ Hewlett-Packard Company Security Bulletin, HPSBUX0311-301, November 18, 2003.
¹⁷ Trustix Secure Linux Security Advisory, TSLSA-2003-0041, November 15, 2003.
¹⁸ SecurityTracker Alert, 1008278, November 22, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Apple ¹⁹	MacOS X 10.x	MacOS X 10.0.2, 10.0.3, MacOS X Server 10.2-10.2.8, 10.3, 10.3.1	A vulnerability exists due to insecure default settings when handling DHCP traffic, which could let a malicious user obtain root access.	No workaround or patch available at time of publishing.	MacOS X DHCP Response Root Access	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Apple ²⁰	Multiple	Safari 1.0, 1.1	A vulnerability exists due to an error when handling URLs, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Safari Web Browser Null Character Cookie Stealing	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Apple ²¹	MacOS X 10.x	MacOS X 10.0, 10.2-10.2.8, 10.3, 10.3.1, MacOS X Server 10.2-10.2.8, 10.3, 10.3.1,	Apple has released security updates to address several known vulnerabilities in components included in Jaguar and Panther releases of MacOS X.	Updates available at: http://www.info.apple.com/support/downloads.html	Mac OS X Jaguar/Panther Multiple Vulnerabilities	Medium	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Apple ²²	MacOS X 10.2/10.3	MacOS X 10.2.3, 10.2.7, 10.3	A vulnerability exists in the 'sudo' command due to improper verification of password information, which could let a malicious user obtain unauthorized access.	No workaround or patch available at time of publishing.	MacOS X Terminal sudo command Unauthorized Access	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

¹⁹ MacOS X Security Advisory, November 26, 2003.

²⁰ Secunia Advisory, SA10252, November 25, 2003.

²¹ SecurityFocus, November 20, 2003.

²² SecurityFocus, November 19, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
BEA Systems, Inc. ²³	Windows NT 4.0/2000, Unix	WebLogic Express 6.1, SP1-SP 5, WebLogic Express 7.0.0.1, SP1&SP2, 7.0, SP1-SP3, 8.1, SP1, WebLogic Express for Win32 6.1, SP1-SP 5, 7.0.0.1, SP1&SP2, 7.0, SP1-SP3, Weblogic Server 6.1, SP1-SP 5, 7.0.0.1, SP1&SP2, 7.0, SP1-SP3, WebLogic Server for Win32 6.1 SP1-SP5, 7.0.0.1, SP1&SP2, 7.0, SP1-SP3,	Multiple vulnerabilities exist: a remote Denial of Service vulnerability exists in the proxy plug-in due to a failure to handle certain incorrectly formatted URLs; a vulnerability exists due to a failure to wrap T3 in SSL when the URI handler has been specified as T3S, which could let a remote malicious user obtain sensitive information; a vulnerability exists in the 'config.xml' file because passwords for foreign JMS providers are showed and stored in clear-text, which could let a remote malicious user obtain sensitive information; a remote Denial of Service vulnerability exists in the Node Manager due to a failure to handle invalid data such as data generated by port scanning tools; and an information disclosure vulnerability exists because a remote malicious user with Remote Method Invocation (RMI) access can access 'MbeanHome' by default.	Remedies available to prevent proxy plug-in Denial of Service available at: http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA03_39.00.jsp Patches for the T3 vulnerability available at: http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA03_40.00.jsp Patches for the password vulnerability available at: http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA03_41.00.jsp Patches for the Node Manager Denial of Service vulnerability available at: http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA03_42.00.jsp Workaround for the MbeanHome vulnerability available at: http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA03_43.00.jsp	Multiple WebLogic Server/Express Denial of Service & Information Disclosure Vulnerabilities	Low/Medium (Medium if sensitive information can be obtained)	Bug discussed in newsgroups and websites.
Digicraft Software ²⁴ <i>Upgrade now available</i> ²⁵	Windows	Yak! 2.0-2.0.2	A vulnerability exists when connecting to TCP port 3535 and logging into the FTP service using a standard username and password, which could let an unauthorized remote malicious user obtain access.	<i>Upgrade available at:</i> http://www.digicraft.com.au/yak/Yak210.exe	Yak! Chat Client FTP Server Default Credentials	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Digicraft Software ²⁶	Multiple	Yak! 2.1 .0	A vulnerability exists because the username is the same on all systems and passwords are generated systematically, which could let a malicious user easily guess the password.	No workaround or patch available at time of publishing.	Yak! Chat Client FTP Server Default Username	Medium	Bug discussed in newsgroups and websites.

²³ BEA Systems Security Advisories, BEA03-39.00, 40.00, 41.00, 42.00, 43.00, November 13, 2003.

²⁴ SecurityTracker Alert, 1007694, September 13, 2003.

²⁵ SecurityFocus, November 14, 2003.

²⁶ Bugtraq, November 19, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Effect Office ²⁷	Windows	Effect Office Server 2.6	A buffer overflow vulnerability exists due to a boundary error when handling data sent to the service on port 56004/tcp, which could let a malicious user cause a Denial of Service or execute arbitrary code.	No workaround or patch available at time of publishing.	EffectOffice Server Remote Service Buffer Overflow	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Epic Project ²⁸ <i>RedHat issues advisory & exploit script published</i> ²⁹	Unix	Epic4 pre2.003, pre2.002, 1.0.1, 1.1.3-1.1.7, 1.1.7.20020907, 1.1.10, 1.1.11	A buffer overflow vulnerability exists in 'ctcp.c' due to an error when handling CTCP requests from overly large nicknames, which could let a remote malicious user execute arbitrary code.	Patch available at: ftp://ftp.prbh.org/pub/epic/patches/alloca_underrun-patch-1 Debian: http://security.debian.org/pool/updates/main/e/epic4/ RedHat: http://rhn.redhat.com/errata/RHSA-2003-342.html	Epic4 CTCP Nickname Server Message Remote Buffer Overflow CVE Name: CAN-2003-0328	High	Bug discussed in newsgroups and websites. <i>Exploit script has been published.</i>
Ethereal Group ^{30, 31, 32} <i>More advisories issued</i> ^{33, 34}	Windows 95/98/ME/NT 4.0/2000, XP, Unix	Ethereal 0.9-0.9.15	Multiple vulnerabilities exist: a buffer overflow vulnerability exists in the 'GTP MSISDN' string, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code; a remote Denial of Service vulnerability exists when a malicious user submits a malformed 'ISAKMP' or 'MEGACO' packet; and a buffer overflow vulnerability exists in the 'SOCKS' dissector, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code.	Ethereal Group: http://www.ethereal.com/download.html Conectiva: ftp://atualizacoes.conectiva.com.br/ RedHat: ftp://updates.redhat.com/ SGI: ftp://patches.sgi.com/support/free/security/	Multiple Ethereal Protocol Dissector Vulnerabilities CVE Names: CAN-2003-0925, CAN-2003-0926, CAN-2003-0927	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites.
Free RADIUS Server Project ³⁵	Unix	Free RADIUS 0.4, 0.5, 0.8, 0.8.1, 0.9- 0.9.2	Two vulnerabilities exist: a remote Denial of Service vulnerability exists when a malicious user submits an 'Access-Request' packet that contains a 'Tunnel-Password' attribute; and a remote Denial of Service vulnerability exists due to the way tag field input is handled.	Upgrade available at: ftp://ftp.freeradius.org/pub/radius/freeradius-0.9.3.tar.gz	FreeRADIUS Remote Denial of Service	Low	Bug discussed in newsgroups and websites.

²⁷ Secunia Advisory, SA10272, November 21, 2003.

²⁸ Debian Security Advisory, DSA 399-1, November 10, 2003.

²⁹ RedHat Security Advisory, RHSA-2003:342-05, November 17, 2003.

³⁰ Ethereal Security Advisory, enpa-sa-00011, November 3, 2003.

³¹ Conectiva Linux Security Announcement, CLA-2003:780, November 7, 2003.

³² Red Hat Security Advisory, RHSA-2003:323-01, November 10, 2003.

³³ SGI Security Advisory, 20031101-01-U, November 19, 2003.

³⁴ RedHat Security Advisory, RHSA-2003:324-09, November 12, 2003.

³⁵ Bugtraq, November 20, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
GNOME ³⁶	Unix	gEdit 2.0.2, 2.2.0	A vulnerability exists due to the way certain files are handled, which could let a malicious user corrupt memory.	No workaround or patch available at time of publishing.	GEdit Large IOStream File Memory Corruption	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
Hewlett Packard Company ³⁷	Windows	ProCurve Switch 5304XL J4850A, 5308XL J4819A, 5348XL J4849A, 5372XL J4848A	A Denial of Service vulnerability exists due to an unspecified error when handling RPC traffic.	Upgrade available at: http://www.hp.com/md/software/switches.htm	HP ProCurve Switch Denial of Service	Low	Bug discussed in newsgroups and websites. Vulnerability can be exploited via RCP worms and exploits have been published.
Hewlett Packard Company ³⁸	Unix	HP-UX 11.0, 11.11	A remote Denial of Service vulnerability exists in the Distributed Computing Environment (DCE) when a malicious user submits certain network traffic.	Patches available at: http://itrc.hp.com	HP-UX DCE Remote Denial of Service	Low	Bug discussed in newsgroups and websites.
Hewlett Packard Company ³⁹	Unix	HP-UX 11.23	A vulnerability exists due to a validation error in Partition Manager (parmgr) when handling certificates from 'cimserver,' which could let a remote malicious user obtain sensitive information and potentially unauthorized access.	Patch available at: http://software.hp.com/portals/swdepot/displayProductInfo.do?productNumber=Parmgr	HP-UX Partition Manager	Medium	Bug discussed in newsgroups and websites.
Hewlett Packard Company ⁴⁰	Unix	HP-UX 11.0, 11.11, 11.22, 11.23	A vulnerability exists because the IPFilter does not provide protection for unsupported network interfaces, which could lead a network administrator into a false sense of security.	Patches available at: ftp://ftp.itrc.hp.com/export/patches/hp-ux_patch_matrix/	HP-UX IPFilter Unsupported Interface	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Hewlett Packard Company ⁴¹	Unix	HP-UX 11.0, 11.11, 11.22, 11.23	A buffer overflow vulnerability exists due to a boundary error in the 'dtmailpr' function, which could let a remote malicious user execute arbitrary code.	Patches available at: http://itrc.hp.com	HP-UX CDE 'dtmailpr' Display Environment Variable Buffer Overflow	High	Bug discussed in newsgroups and websites.

³⁶ SecurityFocus, November 22, 2003.

³⁷ Hewlett-Packard Company Security Bulletin, HPSBMI0311-006, November 24, 2003.

³⁸ Hewlett-Packard Company Security Bulletin, HPSBUX0311-299, November 17, 2003.

³⁹ Hewlett-Packard Company Security Bulletin, HPSBUX0311-296, November 13, 2003.

⁴⁰ Hewlett-Packard Company Security Bulletin, HPSBUX0311-298, November 16, 2003.

⁴¹ Hewlett-Packard Company Security Bulletin, HPSBUX0311-300, November 17, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Hylafax ⁴² 43,44 <i>Debian issues advisory</i> ⁴⁵	Unix	Hylafax 4.1-4.1.3, 4.1.5-4.1.7	A format string vulnerability exists in the 'hfaxd' daemon, which could let a remote malicious user execute arbitrary code.	Upgrade available at: ftp://ftp.hylafax.org/source/hylafax-4.1.8.tar.gz Conectiva: ftp://atualizacoes.conectiva.com.br/9/RPMS/hylafax-4.1.3-19097U90_1cli386.rpm Mandrake: http://www.mandrakesecure.net/en/mlist.php SuSE: ftp://ftp.suse.com/pub/suse Debian: http://security.debian.org/pool/updates/main/h/hylafax/	Hylafax HFaxD Remote Format String CVE Name: CAN-2003-0886	High	Bug discussed in newsgroups and websites.
IBM ⁴⁶	Unix	AIX 4.3.3, 5.1, 5.2	A buffer overflow vulnerability exists in the 'rpc' utility due to insufficient bounds checking when handling command-line or environment data, which could let a malicious user execute arbitrary code with root privileges.	Updates available at: https://techsupport.services.ibm.com/server/aix.fdc	AIX RCP Utility Buffer Overflow CVE Name: CAN-2003-0954	High	Bug discussed in newsgroups and websites.
Imatix ⁴⁷	Windows 95/98/NT 4.0/2000	Xitami 2.4d9, 2.4d4, 2.4d3, 2.4d10, 2.4c3, 2.4b1, 2.4b 2.4 a1, 2.4, 2.5 c0, 2.5 b4-b6, 2.5	A remote Denial of Service vulnerability exists when a malicious user submits an HTTP POST header line that does not contain a colon character	No workaround or patch available at time of publishing.	Xitami Post Request Header Remote Denial Of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
International Ispell ⁴⁸	Multiple	International Ispell 3.2.06. epa1-3.2.06. epa6	A vulnerability exists due to insecure temporary file creation in the 'munchlist' and 'findaffix' shell scripts, which could let a malicious user cause a Denial of Service, loss of data, or obtain elevated privileges.	Upgrades available at: http://membled.com/work/patches/ispell/ispell-3.2.06.epa7.tar.bz2	International Ispell Munchlist/ Findaffix Insecure Temporary File Creation	Low/ Medium (Medium if data is lost or elevated privileges can be obtained)	Bug discussed in newsgroups and websites. There is no exploit code required.

⁴² SUSE Security Announcement, SuSE-SA:2003:045, November 10, 2003.

⁴³ Mandrake Linux Security Update Advisory, MDKSA-2003:105, November 11, 2003.

⁴⁴ Conectiva Linux Security Announcement, CLA-2003:783, November 12, 2003.

⁴⁵ Debian Security Advisory, DSA 401-1, November 17, 2003.

⁴⁶ IBM Security Advisory, November 20, 2003.

⁴⁷ Bugtraq, November 21, 2003.

⁴⁸ SecurityFocus, November 19, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Internet Express Products ⁴⁹	Unix	CommerceSQL Shopping Cart 2.2	A Directory Traversal vulnerability exists in the 'index.cgi' script due to insufficient sanitization of user-supplied input, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Shopping Cart 'index.cgi' Directory Traversal	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Justin Hagstrom ⁵⁰	Unix	Auto Directory Index 1.2.3	A Cross-Site Scripting vulnerability exists in the 'dir' parameter due to insufficient sanitization of user-supplied data, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://sourceforge.net/project/showfiles.php?group_id=82718	Auto Directory Index Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
KDE ^{51, 52} 53, 54, 55 <i>More advisories issued</i> ^{56, 57} <i>More advisories issued</i> ^{58, 59}	Unix	KDE 1.1-1.1.2, 1.2, 2.0 BETA, 2.0- 2.2.2, 3.0- 3.0.5, 3.1- 3.1.3	Two vulnerabilities exist: a vulnerability exists in the KDE Display Manager (KDM) when used in combination with Pluggable Authentication Modules (PAM), which could let an unauthorized remote malicious user obtain root access; and a vulnerability exists due to a weak session cookie algorithm that does not fully use the available 128 bits of entropy, which could let a remote malicious user obtain system access.	Patches available at: ftp://ftp.kde.org/pub/kde/security_patches Conectiva: ftp://atualizacoes.conectiva.com.br/ Debian: http://security.debian.org/pool/updates/main/k/kdebase/ Mandrake: http://www.mandrakesecurity.net/en/advisories/ RedHat: ftp://updates.redhat.com/ SGI: http://www.sgi.com/support/security/ TurboLinux: ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/Server/8/updates/	KDM PAM Module PAM_SetCred Privilege Escalation CVE Names: CAN-2003-0690, CAN-2003-0692	High	Bug discussed in newsgroups and websites.
KDE ⁶⁰	Unix	KDE 3.1	A vulnerability exists in 'kdeglobals' and other configuration files due to insecure permissions, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	KDE Global Configuration Files Insecure Default Permissions	High	Bug discussed in newsgroups and websites. Exploit has been published.

⁴⁹ Securiteam, November 26, 2003.

⁵⁰ Securiteam, November 16, 2003.

⁵¹ KDE Security Advisory, September 16, 2003.

⁵² Red Hat Security Advisory, RHSA-2003:269-01, September 16, 2003.

⁵³ Mandrake Linux Security Update Advisory, MDKSA-2003:091, September 17, 2003.

⁵⁴ Conectiva Linux Security Announcement, CLA-2003:747, September 19, 2003.

⁵⁵ Debian Security Advisory, DSA 388-1, September 19, 2003.

⁵⁶ TurboLinux Security Advisory, TLSA-2003-59, October 20, 2003.

⁵⁷ SGI Security Advisory, 20031002-01-U, October 27, 2003.

⁵⁸ SGI Security Advisory, 20031101-01-U, November 19, 2003.

⁵⁹ Red Hat Security Advisory, RHSA-2003:286-01 & 287-01 November 25, 2003.

⁶⁰ SecurityFocus, November 14, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Kerio Technologies ⁶¹	Windows	WinRoute Firewall 5.10	A vulnerability exists if proxy authentication is used, which could let a remote malicious user obtain authentication credentials.	Upgrade available at: http://www.kerio.com/kwf_download.html	WinRoute Firewall Authentication Credentials Exposure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Koch Roland ⁶²	Windows, Unix	Rolis Guestbook 1.0	A vulnerability exists because the 'insert.inc.php' file does not validate user-supplied input in the \$path variable, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Rolis Guestbook \$path Remote File Include	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Lottasophie ⁶³	Windows, Unix	My_eGallery 3.1.1 f, 3.1.1	A vulnerability exists because parameters used in include statements are not properly verified, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://lottasophie.sourceforge.net/modules.php?op=modload&name=Downloads&file=index&req=getit&lid=22	My_eGallery Remote Include Command Injection	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Macro-media ⁶⁴	Windows, Unix	JRun 4.0 build 61650	A Cross-Site Scripting vulnerability exists in 'clusterframe.jsp' and 'webservice.jsp' due to a failure to filter HTML scripting code from user-supplied input, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	JRun Multiple Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Mark Brady ⁶⁵	Multiple	Php Friendly Admin 1.0, 1.1, 1.3, 1.4	A Cross-Site Scripting vulnerability exists due to insufficient sanitization of user-supplied data, which could let a remote malicious user execute arbitrary HTML or script code.	Upgrades available at: http://phpfriendly.sourceforge.net/download/index.php	PhpFriendly Admin Cross-Site Scripting	High	Bug discussed in newsgroups and websites. There is no exploit code required.
Media Wiki ⁶⁶	Multiple	Media Wiki-stable 20031107, 20030829	A vulnerability exists in 'UpdateClasses.php,' 'Title.php,' 'Setup.php,' 'GlobalFunctions.php,' and 'DatabaseFunctions.php' due to an input validation error, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://prdownloads.sourceforge.net/wikipedia/mediawiki-20031117.tar.gz?download	MediaWiki 'IP' Parameter Remote Arbitrary Code	High	Bug discussed in newsgroups and websites.

⁶¹ Securiteam, November 19, 2003.

⁶² RusH Security Team Advisory #13, November 16, 2003.

⁶³ Bugtraq, November 26, 2003.

⁶⁴ SecurityFocus, November 26, 2003.

⁶⁵ Secunia Advisory, SA10268, November 20, 2003.

⁶⁶ Secunia Advisory, SA10231, November 17, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft ⁶⁷ <i>Microsoft updates bulletin</i> ⁶⁸	Windows	Office 97, 2000, XP, Word 98 (J), Front Page 2000, 2002, Publisher 2000, 2002, Works Suite 2001, 2002, 2003	A buffer overflow vulnerability exists because the WordPerfect converter does not correctly validate certain parameters when it opens a WordPerfect document, which could let a remote malicious user execute arbitrary code. <i>V1.2: Added Microsoft Works Suite 2004 to affected products.</i>	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/MS03-036.asp	Microsoft Converter for WordPerfect Remote Buffer Overflow CVE Name: CAN-2003-0666	High	Bug discussed in newsgroups and websites.
Microsoft ⁶⁹ <i>Microsoft updates bulletin</i> ⁷⁰	Windows 2000, XP	Front Page Server Extensions 2000, 2002, SharePoint Team Services 2002, Windows 2000 Advanced Server SP2 & SP3, 2000 Data-center Server SP2 & SP3, 2000 Professional SP2 & SP3, 2000 Server SP2 & SP3, Windows XP 64-bit Edition SP1, XP Home SP1, XP Professional SP1	Two vulnerabilities exist: a buffer overflow vulnerability exists in FrontPage Server Extensions via the remote debugging functionality when a chunked-encoded HTTP POST request is submitted, which could let a remote malicious user execute arbitrary code; and a remote Denial of Service vulnerability exists in the SmartHTML interpreter component of FrontPage Server Extensions when malicious HTTP requests are submitted. <i>V1.2: Updated information on affected versions of Microsoft Office, updated information in the workarounds section.</i> <i>V1.3: Updated information on setup switches in the Security Update Information section and corrected text in Severity Rating section for SharePoint Team Services 2002.</i>	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/MS03-051.asp	FrontPage Server Extensions Remote Debug Buffer Overflow & SmartHTML Interpreter Remote Denial of Service CVE Names: CAN-2003-0822, CAN-2003-0824	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Exploit script has been published.

⁶⁷ Microsoft Security Bulletin, MS03-036 V1.1, September 4, 2003.

⁶⁸ Microsoft Security Bulletin, MS03-036 V1.2, November 24, 2003.

⁶⁹ Microsoft Security Bulletin, MS03-051 & V1.1, November 11 & 12, 2003.

⁷⁰ Microsoft Security Bulletin, MS03-051 V1.2 & V1.3. November 14 & 19, 2003

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft ⁷¹ <i>Microsoft updates bulletin</i> ⁷²	Windows 95/98/ME/NT 4.0/2000, XP	Word 2000, SR1a, SR1, SP2 & SP3, Word 2002, SP1 & SP2, Word 97, SR1 & SR2, Word 98, Japanese Version, Works Suite 2001, 2002, 2003	A vulnerability exists because Word does not properly check certain properties in a modified document and it is possible to craft a malicious document that will bypass the macro security model (even if macro security features are enabled), which could let a remote malicious execute arbitrary code. <i>V1.2: Added Microsoft Works Suite 2004 to affected products.</i>	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/MS03-035.asp	Microsoft Word Document Validation Error CVE Name: CAN-2003-0664	High	Bug discussed in newsgroups and websites.
Microsoft ⁷³ <i>Microsoft updates bulletin</i> ⁷⁴	Windows 95/98/ME/NT 4.0/2000, XP	Office 2000, SP2 & SP3, Office XP, SP1 & SP2, Project 2000, 2002, Visio Professional 2002, Visual Basic for Applications SDK 5.0, SDK 6.0, SDK 6.2, SDK 6.3	A buffer overflow vulnerability exists because VBA does not properly check certain document properties passed to it when a document is opened by the host application, which could let a remote malicious user execute arbitrary code. <i>V1.1: Added Microsoft Works Suite 2004 to affected products</i>	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/MS03-037.asp	Visual Basic for Applications (VBA) Remote Buffer Overflow CVE Name: CAN-2003-0347	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

⁷¹ Microsoft Security Bulletin, MS03-035, September 3, 2003.

⁷² Microsoft Security Bulletin, MS03-035 V1.2, November 24, 2003.

⁷³ Microsoft Security Bulletin, MS03-037, September 3, 2003.

⁷⁴ Microsoft Security Bulletin, MS03-037 V1.1, November 24, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft ⁷⁵ <i>Microsoft updates bulletin</i> ⁷⁶ <i>Exploits published</i> ⁷⁷ <i>Microsoft updates bulletin</i> ⁷⁸	Windows NT 4.0/2000, 2003, XP	Windows 2000 Advanced Server, SP1-SP4, Data center Server, SP1-SP4, Professional, SP1-SP4, 2000 Server, SP1-SP4, Windows ME, NT Enterprise Server 4.0, SP1-SP6a, NT Terminal Server 4.0, SP1-SP6a, NT Workstation 4.0, SP1-SP6a, 2003 Data center Edition, 64-bit, 2003 Enterprise Edition, 64-bit, 2003 Standard Edition, 2003 Web Edition, XP 64-bit Edition, SP1, XP Home, SP1, XP Professional, SP1	<p>A buffer overflow vulnerability exists because the length of messages is not verified, which could let a remote malicious user execute arbitrary code.</p> <p><i>V1.1: Updated the "Security Patch Information" section for Windows Server 2003, Windows XP, and Windows 2000.</i></p> <p><i>V2.0: A revised version of the security patch for Windows 2000, Windows XP, and Windows Server 2003 has been released to correct the issue documented by Knowledge Base Article 830846.</i></p> <p><i>V2.1: Bulletin updated to reflect correct file versions for Windows XP update.</i></p> <p><i>V2.2: Subsequent to the release of this bulletin, it was determined that the update for Windows XP did not properly place the updated file wkssvc.dll into the %systemroot%\system32\dllicache. Caveats section has been updated to include new information relevant to NT 4.0 clients.</i></p>	<p>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/MS03-043.asp</p> <p><i>Microsoft recommends that customers who have previously applied the security update reinstall the latest version to insure that their system remains protected in the event that the wkssvc.dll is ever deleted or becomes corrupt. More information on this is available in the FAQ section at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-043.asp</i></p>	<p>Messenger Service Buffer Overflow</p> <p>CVE Name: CAN-2003-0717</p>	High	<p>Bug discussed in newsgroups and websites. Exploit scripts have been published.</p> <p><i>Vulnerability has appeared in the press and other public media.</i></p>

⁷⁵ Microsoft Security Bulletin, MS03-043, October 15, 2003.

⁷⁶ Microsoft Security Bulletin, MS03-043 V1.1 & V2.0, October 22 & 29, 2003.

⁷⁷ SecurityFocus, October 30, 2003.

⁷⁸ Microsoft Security Bulletin, MS03-043 V2.1 & V2.2, November 13 & 14, 2003

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
<p>Microsoft⁷⁹</p> <p><i>Microsoft updates bulletin⁸⁰</i></p> <p><i>Exploits published⁸¹</i></p> <p><i>Microsoft updates bulletin⁸²</i></p>	Windows NT 4.0/2000, 2003, XP	Windows 2000 Advanced Server, SP1-SP4, Data center Server, SP1-SP4, Professional, SP1-SP4, 2000 Server, SP1-SP4, Windows ME, NT Enterprise Server 4.0, SP1-SP6a, NT Terminal Server 4.0, SP1-SP6a, NT Workstation 4.0, SP1-SP6a, 2003 Data center Edition, 64-bit, 2003 Enterprise Edition, 64-bit, 2003 Standard Edition, 2003 Web Edition, XP 64-bit Edition, SP1, XP Home, SP1, XP Professional, SP1	<p>A buffer overflow vulnerability exists because the 'ListBox' and 'ComboBox' controls due to insufficient validation of user-supplied parameters, which could let a remote malicious user execute arbitrary code.</p> <p><i>V1.1: Re-issued to advise of a language specific compatibility issue with some third-party software.</i></p> <p><i>V2.0 : Version changed to reflect the availability of updated patch for specific languages.</i></p> <p><i>V3.0: A revised version of the security patch for Windows XP has been released to correct the issue documented by Knowledge Base Article 830846.</i></p> <p><i>V3.3: Bulletin updated to reflect correct file versions for Windows NT 4.0 update.</i></p>	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/MS03-045.asp	Windows ListBox & ComboBox Control Buffer Overflow CVE Name: CAN-2003-0659	High	<p>Bug discussed in newsgroups and websites.</p> <p>Vulnerability has appeared in the press and other public media.</p> <p><i>Exploit scripts have been published.</i></p>

⁷⁹ Microsoft Security Bulletin MS03-045, October 15, 2003.

⁸⁰ Microsoft Security Bulletin MS03-045 V1.1, V2.0 & V3.0, October 17, 22, & 29, 2003.

⁸¹ SecurityFocus, November 13, 2003.

⁸² Microsoft Security Bulletin, MS03-045 V3.3, November 13, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft ⁸³ <i>Microsoft updates bulletin & another exploit published</i> ⁸⁴	Windows 2000, XP	Windows 2000 Advanced Server, SP1-SP4, 2000 Data center Server, SP1-SP4, 2000 Professional, SP1-SP4, 2000 Server, SP1-SP4, Windows XP 64-bit Edition, SP1, XP Home, SP1, XP Media Center Edition, XP Professional, SP1	A buffer overflow vulnerability exists in 'WKSSVC.DLL' due to the way requests are handled, which could let a remote malicious user execute arbitrary code. <i>V1.1: Updated the File Manifest and Restart Requirement sections for Windows 2000.</i> <i>V1.2: Updated Information Relating to the Windows XP Security Update.</i>	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/MS03-049.asp	Windows Workstation Service Remote Buffer Overflow CVE Name: CAN-2003-0812	High	Bug discussed in newsgroups and websites. Exploit scripts have been published. <i>Another exploit script has been published.</i>
Microsoft ⁸⁵ <i>Hotfix now available</i> ⁸⁶	Windows NT	ASP.NET 1.1	A Cross-Site Scripting vulnerability exists in the 'Request Validation' feature due to insufficient sanitization of user-supplied input, which could let a malicious user bypass the security mechanism and execute arbitrary code.	<i>Microsoft has addressed this issue in a Hotfix rollup package and is available by contacting the vendor. Further information can be obtained from the following link:</i> http://support.microsoft.com/default.aspx?scid=kb;EN-US;821349	ASP.NET Cross-Site Scripting	High	Bug discussed in newsgroups and websites. There is no exploit code required.
Microsoft ⁸⁷	Windows 95/98/ME/NT 4.0/2000, XP	MSN Messenger Service 1.0, 2.0, 2.2, 3.0, 3.6, 4.0, 4.5, 4.6, 6.0, 6.0.602	An information leakage vulnerability exists during file invitation requests, which could let a malicious user obtain sensitive information.	Users are advised to upgrade to MSN 6.1 that is not vulnerable to this issue.	MSN Messenger Information Leakage	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

⁸³ Microsoft Security Bulletin, MS03-049, November 11, 2003.

⁸⁴ Microsoft Security Bulletin, MS03-049 V1.1 & 1.2, November 11 & 19 2003.

⁸⁵ WebCohort Research Advisory, September 8, 2003.

⁸⁶ SecurityFocus, November 14, 2003.

⁸⁷ SecurityFocus, November 20, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft ⁸⁸	Windows 95/98/ME/NT 4.0/2000, 2003, XP	Internet Explorer 5.0, 5.0.1, SP1-SP3, 5.5, SP1&SP2, 6.0, SP1	Multiple vulnerabilities exist: a vulnerability exists when handling MHTML file and res URIs due to a failure to securely handle URIs that reference two files, which could let a remote malicious user bypass security checks and execute arbitrary code; a vulnerability exists in the download functionality when an invalid ContentType is specified in an HTTP response to the browser, which could let a remote malicious user obtain sensitive information; a vulnerability exists which could let a remote malicious user hijack a user's clicks and perform certain actions without the user's knowledge; a vulnerability exists in the 'MhtRedirParsesLocalFile,' which could let a remote malicious user execute arbitrary code; and a Cross-Site Scripting vulnerability exists which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Internet Explorer Multiple Vulnerabilities	Medium/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Proof of Concept exploits have been published and an exploit script has been published for the MHTML redirect vulnerability. Vulnerabilities have appeared in the press and other public media.
Mozilla ⁸⁹	Windows 95/98/ME/NT 4.0, MacOS X 9.x,10.x, Unix	Mozilla Browser 0.9.3, 0.9.4.1, 0.9.4, 0.9.35, 0.9.48, 1.4, 1.4 a & b, 1.5	Several vulnerabilities exist: a buffer overflow vulnerability exists in the Chatzilla IRC URI handler when handling URIs of excessive length, which could let a remote malicious user execute arbitrary code; and a buffer overflow vulnerability exists when processing the '/Nick' command, which could let a malicious user cause a Denial of Service.	No workaround or patch available at time of publishing.	Mozilla Remote Buffer Overflow & Denial of Service	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites.

⁸⁸ Secunia Advisory, SA10289, November 25, 2003.

⁸⁹ SecurityTracker Alert, 1008301, November 26, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors ⁹⁰ <i>More advisories issued^{91, 92, 93}</i>	Unix	GNU Zebra 0.91a, 0.92a, 0.93b, 0.93a; Quagga Routing Software Suite 0.96.2, 0.96.3	A remote Denial of Service vulnerability exists when a malicious user attempts to connect to the Zebra telnet management port while a password is enabled.	<u>Quagga:</u> http://www.quagga.net/download/quagga-0.96.4.tar.gz <u>RedHat:</u> ftp://updates.redhat.com/ <u>Conectiva:</u> ftp://atualizacoes.conectiva.com.br/9/ <u>OpenPKG:</u> ftp://ftp.openpkg.org/release/ <u>SGI:</u> http://support.sgi.com/	GNU Zebra / Quagga Remote Denial of Service CVE Name: CAN-2003-0795	Low	Bug discussed in newsgroups and websites.
Multiple Vendors ⁹⁴ <i>More vendors issue advisories^{95, 96, 97}</i>	Unix	GNU glibc 2.3.2, Zebra 0.91a, 0.92a, 0.93b, 0.93a; Quagga Routing Software Suite 0.96.2; RedHat Advanced Workstation for the Itanium Processor 2.1, Enterprise Linux WS 2.1 IA64, WS 2.1, ES 3, ES 2.1 IA64, ES 2.1, AS 3, AS 2.1 IA64, AS 2.1	A Denial of Service vulnerability exists in applications that implement the 'getifaddrs()' function because it is possible to spoof messages sent to the kernel netlink interface.	<u>RedHat:</u> ftp://updates.redhat.com/ <u>SGI:</u> ftp://patches.sgi.com/support/free/security/advisories <u>Conectiva:</u> ftp://atualizacoes.conectiva.com.br/9/ <u>OpenPKG:</u> ftp://ftp.openpkg.org/release	Spoofed Kernel Netlink Interface Message Denial of Service CVE Name: CAN-2003-0859	Low	Bug discussed in newsgroups and websites.

⁹⁰ Red Hat Security Advisory, RHSA-2003:305-12, 307-01, November 12 & 13, 2003.

⁹¹ SGI Security Advisory, 20031101-01-U, November 19, 2003.

⁹² Conectiva Linux Security Announcement, CLA-2003:786, November 20, 2003.

⁹³ OpenPKG Security Advisory, OpenPKG-SA-2003.049, November 25, 2003.

⁹⁴ Red Hat Security Advisory, RHSA-2003: 325-01, 315-08, 317-08, 305-12, & 307-01, November 12 & 13, 2003.

⁹⁵ SGI Security Advisory, 20031101-01-U, November 19, 2003.

⁹⁶ Conectiva Linux Security Announcement, CLA-2003:786, November 20, 2003.

⁹⁷ OpenPKG Security Advisory, OpenPKG-SA-2003.049, November 25, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors ⁹⁸	Unix	Double Precision Incorporated Courier MTA 0.37.3, 0.38.1, 0.40, 0.40.1; Inter7 SqWeb Mail 3.4.1, 3.5.0-3.5.3, 3.6.0, 3.6.1	A vulnerability exists because a remote malicious user can obtain a target user's session ID and hijack the target user's session.	No workaround or patch available at time of publishing.	SqWebMail Session Hijacking	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Multiple Vendors ^{99, 100} <i>Exploit script published & more advisories issued^{101, 102, 103, 104}</i> <i>More advisories issued^{105, 106}</i>	Unix	GNU fileutils 4.0, 4.0.36, 4.1, 4.1.6, 4.17; Washington University wu-ftpd 2.4.1, 2.4.2 academ BETA1-15, BETA-18, 2.4.2 VR10 -VR17, 2.5.0, 2.6.0-2.6.2	An integer overflow vulnerability exists in /bin/lS, which could let a remote malicious user cause a Denial of Service.	Patches available at: http://mail.gnu.org/archive/html/bug-coreutils/2003-10/msg00070.html Conectiva: ftp://atualizacoes.conectiva.com.br/ Immunix: http://download.immunix.org/ImmunixOS/7+/Updates/RPMS/fileutils-4.0x-3_imnx_3.i386.rpm Mandrake: http://www.mandrakesecurity.net/en/ftp.php RedHat: ftp://updates.redhat.com/ SGL: ftp://patches.sgi.com/support/free/security/advisories Trustix: http://http.trustix.org/pub/trustix/updates/	Coreutils LS Width Argument Remote Denial of Service CVE Name: CAN-2003-0853	Low	Bug discussed in newsgroups and websites. There is no exploit code required; however, an exploit script has been published.

⁹⁸ PUCCIOLAB.ORG Advisories, November 18, 2003.

⁹⁹ Georgi Guninski Security Advisory #62, October 22, 2003

¹⁰⁰ Conectiva Linux Security Announcement, CLA-2003:768 & CLA-2003:771, October 22 & 24, 2003.

¹⁰¹ Immunix Secured OS Security Advisory, IMNX-2003-7+-026-01, October 31, 2003.

¹⁰² Red Hat Security Advisories, RHSA-2003:309-01 & RHSA-2003:310-10, November 3 & 12, 2003.

¹⁰³ SecurityFocus, November 13, 2003.

¹⁰⁴ Mandrake Linux Security Update Advisory, MDKSA-2003:106, November 13, 2003.

¹⁰⁵ SGI Security Advisory, 20031101-01-U, November 19, 2003.

¹⁰⁶ Trustix Secure Linux Security Advisory, TSLSA-2003-0042, November 17, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors 107, 108, 109 <i>BlueCoat security advisory issued¹¹⁰</i>	Windows, Unix	OpenSSL 0.9.x	A remote Denial of Service vulnerability exists due to an error when parsing certain ASN.1 tags.	OpenSSL: ftp://ftp.openssl.org/source/ Cisco: http://www.cisco.com/warp/public/707/cisco-sa-20030930-ssl.shtml Engarde: http://www.linuxsecurity.com/advisories/engarde_advisory-3757.html BlueCoat: http://www.bluecoat.com/support/knowledge/advisory_ASN1_parsing_0.9.6.html	OpenSSL ASN.1 Large Recursion Remote Denial of Service CVE Name: CAN-2003-0851	Low	Bug discussed in newsgroups and websites.
Multiple Vendors 111, 112, 113, 114, 115, 116	MacOS X, 10.x, Unix	FreeBSD 4.4-5.0; ISC BIND 8.2.3-8.2.7, 8.3.0-8.3.6, 8.4, 8.4.1; Sun Solaris 7.0, 7.0_x86, 8.0, 8.0_x86, 9.0, 9.0_x86	A Denial of Service vulnerability exists because negative answers may be cached from the wrong source.	Engarde: http://infocenter.guardiandigital.com/advisories/ FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/ Immunix: http://download.immunix.org/ImmunixOS/7+/Updates/ ISC: ftp://ftp.isc.org/isc/bind/src/ Sun: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F57434 SuSE: ftp://ftp.suse.com/pub/suse/ Trustix: ftp://ftp.trustix.org/pub/trustix/updates/	ISC BIND Negative Cache Poison Denial of Service CVE Name: CAN-2003-0914	Low	Bug discussed in newsgroups and websites.

¹⁰⁷ OpenSSL Security Advisory, November 4, 2003.

¹⁰⁸ Guardian Digital Security Advisory, ESA-20031104-029, November 4, 2003.

¹⁰⁹ Cisco Security Advisory, 45643 Rev. 2.1, November 7, 2003.

¹¹⁰ BlueCoat Security Advisory, November 14, 2003.

¹¹¹ Guardian Digital Security Advisory, ESA-20031126-031, November 26, 2003.

¹¹² Immunix Secured OS Security Advisory, IMNX-2003-7+-024-01, November 26, 2003.

¹¹³ Sun(sm) Alert Notification, 57434, November 26, 2003.

¹¹⁴ FreeBSD Advisory, FreeBSD-SA-03:19, November 28, 2003.

¹¹⁵ SUSE Security Announcement, SuSE-SA:2003:047, November 28, 2003.

¹¹⁶ Trustix Secure Linux Security Advisory, TSLSA-2003-0044, November 28, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors 117, 118 <i>Hewlett Packard issues advisory</i> 119	Unix	SCO Open UNIX 8.0, Unixware 7.1.1, 7.1.3; Sun Solaris 7.0, 7.0_x86, 8.0, 8.0_x86, 9.0, 9.0_x86	A buffer overflow vulnerability exists in CDE 'libDTHelp' when handling the 'DTHELPUSERSEARCH PATH' environment variable, which could let a malicious user execute arbitrary code.	<u>SCO:</u> ftp://ftp.sco.com/pub/updates/UnixWare/CSSA-2003-SCO.31 <u>Sun:</u> http://sunsolve.sun.com <u>Hewlett Packard:</u> http://itrc.hp.com	CDE LibDTHelp Buffer Overflow CVE Name: CAN-2003-0834	High	Bug discussed in newsgroups and websites.
myServer 120 <i>Exploit script published</i> 121	Windows	myServer 0.4.1	A Directory Traversal vulnerability exists which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	MyServer HTTP Server Directory Traversal	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

¹¹⁷ SCO Security Advisory, CSSA-2003-SCO.31, November 4, 2003.

¹¹⁸ Sun(sm) Alert Notification, 57414, November 7, 2003.

¹¹⁹ Hewlett-Packard Company Security Bulletin, HPSBUX0311-297, November 16, 2003.

¹²⁰ Secunia Security Advisory, June 16, 2003.

¹²¹ SecurityFocus, November 13, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
<p>MySQL AB^{122, 123, 124}</p> <p><i>More advisories issued^{125, 126, 127, 128}</i></p> <p><i>More advisories issued^{129, 130, 131}</i></p> <p><i>SGI issues advisory¹³²</i></p> <p><i>Sun issues update¹³³</i></p>	Unix	MySQL 3.23.x, 3.23.2-3.23.5, 3.23.8-3.23.10, 3.23.22-3.23.34, 3.23.36-3.23.56, 4.0.0-4.0.14, 4.1.0-alpha, 4.1.0-0	A buffer overflow vulnerability exists when handling user passwords of excessive size due to insufficient bounds checking, which could let a malicious user execute arbitrary code.	<p>Patch available at: http://www.mysql.com/downloads/mysql-4.0.html</p> <p>Debian: http://security.debian.org/pool/updates/main/m/mysql/</p> <p>OpenPKG: Ftp://ftp.openpkg.org/release/</p> <p>Trustix: http://www.trustix.net/pub/Trustix/updates/</p> <p>Conectiva: ftp://atualizacoes.conectiva.com.br/</p> <p>Engarde: http://www.linuxsecurity.com/advisories/engarde_advisory-3650.html</p> <p>Mandrake: http://www.mandrakesecure.net/en/ftp.php</p> <p>SuSE: ftp://ftp.suse.com/pub/suse</p> <p>RedHat: Ftp://updates.redhat.com/</p> <p>TurboLinux: ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/</p> <p>SGI: http://www.sgi.com/support/security/</p> <p>Sun: http://sunsolve.sun.com/pub-cgi/show.pl?target=cobalt/raq550.eng&nav=patchpage</p> <p>http://sunsolve.sun.com/pub-cgi/show.pl?target=cobalt/qube3.eng&nav=patchpage</p>	MySQL Password Handler Buffer Overflow	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published. An exploit script has also been published.

¹²² Debian Security Advisory, DSA 381-1, September 14, 2003.

¹²³ OpenPKG Security Advisory, OpenPKG-SA-2003.038, September 15, 2003.

¹²⁴ Trustix Secure Linux Security Advisory, TSLSA-2003-09-17, September 17, 2003.

¹²⁵ Conectiva Linux Security Announcement, CLA-2003:743, September 18, 2003.

¹²⁶ Guardian Digital Security Advisory, ESA-20030918-025, September 18, 2003.

¹²⁷ Mandrake Linux Security Update Advisory, MDKSA-2003:094, September 18, 2003.

¹²⁸ SuSE Security Announcement, SuSE-SA:2003:042, October 1, 2003

¹²⁹ TurboLinux Security Advisory, TLSA-2003-56, October 7, 2003.

¹³⁰ Red Hat Security Advisory, RHSA-2003:281-01, October 9, 2003.

¹³¹ Conectiva Linux Security Announcement, CLSA-2003:764, October 16, 2003.

¹³² SGI Security Advisory, 0031002-01-U, October 27, 2003.

¹³³ SecurityFocus, November 24, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Net-X Solutions ¹³⁴	Windows	NetServe Web Server 1.0.7	Several vulnerabilities exist: a Directory Traversal vulnerability exists due to insufficient sanitization, which could let a remote malicious user obtain sensitive information; and a vulnerability exists because the software stores the administrator's username and password in the 'config.dat' file, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	NetServe Web Server Directory Traversal & Password Storage	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
nfs ^{135, 136, 137, 138, 139, 140, 141, 142} <i>More upgrades issued^{143, 144}</i> <i>SCO issues advisory¹⁴⁵</i>	Unix	nfs-utils 0.2, 0.2.1, 0.3.1, 0.3.3, 1.0, 1.0.1, 1.0.3	A buffer overflow vulnerability exists due to a boundary error (off-by-one) in the 'xlog()' function when adding missing trailing newlines to a logged string, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code.	Upgrade available at: http://sourceforge.net/project/showfiles.php?group_id=14&release_id=171379 Conectiva: ftp://atualizacoes.conectiva.com.br/ Debian: http://security.debian.org/pool/updates/main/n/nfs-utils/ Immunix: http://download.immunix.org/ImmunixOS/7+/Updates/RPMS/nfs-utils-0.3.1-7_imnx_3.i386.rpm Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: ftp://updates.redhat.com/ Slackware: ftp://ftp.slackware.com/pub/slackware/ SuSE: ftp://ftp.suse.com/pub/suse/ Trustix: ftp://ftp.trustix.net/pub/Trustix/updates/ Sun: http://sunsolve.sun.com/pub/cgi/retrieve.pl?doc=fsalert%2F55882 YellowDog: ftp://ftp.yellowdoglinux.com/pub/yellowdog/updates/yellowdog-3.0/ SCO: Ftp://ftp.sco.com/pub/updates/OpenLinux/3.1.1/	NFS-Utills Xlog Remote Buffer Overflow CVE Name: CAN-2003-0252	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites.

¹³⁴ Bugtraq, November 17, 2003.

¹³⁵ Debian Security Advisory, DSA 349-1, July 14, 2003.

¹³⁶ Red Hat Security Advisory, RHSA-2003:206-01, July 14, 2003.

¹³⁷ Slackware Security Advisory, SSA:2003-195-01, July 15, 2003.

¹³⁸ Immunix Secured OS Security Advisory, IMNX-2003-7+-018-01, July 15, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Ondrej Jombik ¹⁴⁶	Windows, Unix	PhpWeb File Manager 2.0	A Directory Traversal vulnerability exists due to a validation error when handling input for the '\$f' variable, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	PhpWebFile Manager Directory Traversal	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
OpenBSD ¹⁴⁷	Unix	OpenBSD 2.0-2.9, 3.0-3.4	A buffer overflow vulnerability exists due to a boundary error in 'compat_ibcs2' in the kernel when handling malformed COFF executables, which could let a remote malicious user execute arbitrary code.	Patches available at: ftp://ftp.openbsd.org/pub/OpenBSD/patches/	OpenBSD IBCS2 Binary Length Parameter Kernel-Based Buffer Overflow CVE Name: CAN-2003-0955	High	Bug discussed in newsgroups and websites. Exploit script has been published.
OpenBSD ¹⁴⁸	Unix	OpenBSD 3.3, 3.4	A buffer overflow vulnerability exists in the 'semctl()' and 'semop()' functions due to improper bounds checking in 'sysv_sem.c,' which could let a malicious user cause a Denial of Service.	Patches available at: ftp://ftp.openbsd.org/pub/OpenBSD/patches/	OpenBSD semctl/semop Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
OpenSSH ¹⁴⁹	MacOS X 10.0x, 10.1x Unix	OpenSSH 3.0 p1, 3.0.1 p1, 3.0.2 p1, 3.1 p1, 3.2.2 p1, 3.2.3 p1, 3.3 p1, 3.4 p1, 3.5 p1, 3.6.1 p2, 3.6.1 p1, 3.7 p1, 3.7.1 p1, 3.7.1 p2	A vulnerability exists because aborted conversations with PAM modules are not handled correctly, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	OpenSSH PAM Conversation Memory Scrubbing Weakness	Medium	Bug discussed in newsgroups and websites.

¹³⁹ Trustix Secure Linux Security Advisory, TSLSA-2003-0027, July 18, 2003.

¹⁴⁰ SuSE Security Announcement, SuSE-SA:2003:031, July 16, 2003.

¹⁴¹ Mandrake Linux Security Update Advisory, MDKSA-2003:076, July 21, 2003.

¹⁴² Conectiva Linux Security Announcement, CLA-2003:700, July 22, 2003.

¹⁴³ Yellow Dog Linux Security Announcement, YDU-20030718-1, July 18, 2003.

¹⁴⁴ Sun(sm) Alert Notification, 55882, July 23, 2003.

¹⁴⁵ SCO Security Advisory, CSSA-2003-037.0, November 17, 2003.

¹⁴⁶ RusH Security Team Advisory #12, November 16, 2003.

¹⁴⁷ Georgi Guninski Security Advisory #64, November 18, 2003.

¹⁴⁸ Bugtraq, November 21, 2003.

¹⁴⁹ Bugtraq, November 13, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
OpenBSD ¹⁵⁰	Unix	OpenBSD 3.3, 3.4	A Denial of Service vulnerability exists when handling malformed calls to sysctl..	Patches available at: ftp://ftp.OpenBSD.org/pub/OpenBSD/patches/	OpenBSD sysctl Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Opera Software ¹⁵¹	Windows, Unix	Opera Web Browser 7.22	Two vulnerabilities exist: a buffer overflow vulnerability exists due to the way zipped skin files are handled, which could let a remote malicious execute arbitrary code; and a Directory Traversal vulnerability exists when handling skin files, which could let a remote malicious user obtain sensitive information.	Update available at: http://www.opera.com/download/	Opera Skin Zip File Buffer Overflow & Directory Traversal	Medium/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
pan.rebelbase.com ¹⁵²	Unix	Pan 0.9.7, 0.11.4, 0.14.2	A remote Denial of Service exists when parsing an article header containing a very long author e-mail address.	Upgrade available at: ftp://updates.redhat.com/	Pan Long Author Address Remote Denial of Service CVE Name: CAN-2003-0855	Low	Bug discussed in newsgroups and websites.
People Soft ¹⁵³	Windows NT 4.0/2000, Unix	People Tools 8.4, 8.10-8.20, 8.40-8.43	A path disclosure vulnerability exists in the Gateway Administration servlet due to insufficient input validation, which could let a remote malicious user obtain sensitive information.	Patches available at: http://www.peoplesoft.com/corp/en/patch_fix/search.jsp	PeopleTools Gateway Administration Servlet Path Disclosure CVE Name: CAN-2003-0628	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
People Soft ¹⁵⁴	Windows NT 4.0/2000, Unix	People Tools 8.4, 8.10-8.20, 8.40-8.43	A Cross-Site Scripting vulnerability exists in the iClient servlet when a malformed URL is used in an HTTP request, which could let a remote malicious user execute arbitrary HTML and script code.	Patches available at: http://www.peoplesoft.com/corp/en/patch_fix/search.jsp	PeopleSoft IScript Remote Cross-Site Scripting CVE Name: CAN-2003-0629	High	Bug discussed in newsgroups and websites. There is no exploit code required.

¹⁵⁰ SecurityTracker Alert, 1008270, November 21, 2003.

¹⁵¹ Bugtraq, November 22, 2003.

¹⁵² Red Hat Security Advisory, RHSA-2003:311-01, November 24, 2003.

¹⁵³ Corsaire Security Advisory, November 13, 2003.

¹⁵⁴ Corsaire Security Advisory, November 13, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
People Soft ¹⁵⁵	Windows NT 4.0/2000, Unix	People Tools 8.4, 8.10-8.20, 8.40-8.43	A Directory Traversal vulnerability exists in the PeopleBooks component due to insufficient sanitization of the 'headername' and 'footername' arguments, which could let a remote malicious user obtain sensitive information.	Patches available at: http://www.peoplesoft.com/corp/en/patch_fix/search.jsp	PeopleBooks psdoccgi.exe Directory Traversal CVE Name: CAN-2003-0626	Medium	Bug discussed in newsgroups and websites.
People Soft ¹⁵⁶	Windows NT 4.0/2000, Unix	People Tools 8.4, 8.10-8.20, 8.40-8.43	A remote Denial of Service vulnerability exists in the 'psdoccgi.exe' script due to improper sanitization of user-supplied data.	Patches available at: http://www.peoplesoft.com/corp/en/patch_fix/search.jsp	PeopleBooks 'psdoccgi.exe' Remote Denial of Service CVE Name: CAN-2003-0627	Low	Bug discussed in newsgroups and websites.
People Soft ¹⁵⁷	Windows NT 4.0/2000, Unix	People Tools 8.4, 8.10-8.20, 8.40-8.43	A vulnerability exists in the IClient servlet due to the weak methods used when generating random directory names, which could let a remote malicious user execute arbitrary code.	Patches available at: http://www.peoplesoft.com/corp/en/patch_fix/search.jsp	PeopleTools IClient Servlet Arbitrary Code Execution	High	Bug discussed in newsgroups and websites.
phpPortals ¹⁵⁸	Windows, Unix	vbPortal 2.0 alpha 8.1	Two vulnerabilities exist: a vulnerability exists in the 'yname' and 'ymail' parameters, which could let a remote malicious user manipulate the content of the e-mails generated by 'SendStory' and 'SendSite;' and a vulnerability exists in the 'SendStory' and 'SendSite' functions due to insufficient user verification, which could let a remote malicious user send e-mails without being authenticated.	vbPortal 2.0 alpha 8.1 is no longer supported.	vbPortal Friend.PHP Remote E-Mail Relaying	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.

¹⁵⁵ Corsaire Security Advisory, November 13, 2003.

¹⁵⁶ Corsaire Security Advisory, November 13, 2003.

¹⁵⁷ Internet Security Systems Security Advisory, November 12, 2003.

¹⁵⁸ Security Corporation Security Advisory, SCSA-021, November 22, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
PostgreSQL ¹⁵⁹ <i>Vendors issue advisories</i> ^{160, 161} <i>More advisories issued</i> ^{162, 163, 164, 165, 166} <i>More advisories issued</i> ^{167, 168}	Unix	PostgreSQL 7.2-7.2.4, 7.3-7.3.3	A buffer overflow vulnerability exists in the 'PostgreSQL to_ascii()' function, which could let a malicious user execute arbitrary code.	Upgrade available at: http://www.postgresql.org/Conectiva: http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000772 OpenPKG: ftp://ftp.openpkg.org/release/1.2/UPD/ Debian: http://security.debian.org/pool/updates/main/p/postgresql/ Mandrake: http://www.mandrakesecurity.net/en/advisories/ OpenPKG: ftp://ftp.openpkg.org/release/1.2/UPD/ RedHat: ftp://updates.redhat.com/ SGI: ftp://patches.sgi.com/support/free/security/advisories Trustix: http://http.trustix.org/pub/trustix/updates/	PostgreSQL To_Ascii() Buffer Overflow CVE Name: CAN-2003-0901	High	Bug discussed in newsgroups and websites.
Qualcomm ¹⁶⁹	Windows	Eudora 6.0.1	A vulnerability exists in the 'LaunchProtect' implementation, which could let a malicious user trick users into performing dangerous actions.	No workaround or patch available at time of publishing.	Eudora Attachment LaunchProtect	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.

¹⁵⁹ SecurityFocus, October 1, 2003.

¹⁶⁰ Conectiva Linux Announcement, CLSA-2003:772, October 24, 2003.

¹⁶¹ OpenPKG Security Advisory, OpenPKG-SA-2003.047, October 30, 2003.

¹⁶² Mandrake Linux Security Update Advisory, MDKSA-2003:102, November 4, 2003.

¹⁶³ Debian Security Advisory, DSA 397-1, November 7, 2003.

¹⁶⁴ OpenPKG Security Advisory, OpenPKG-SA-2003.048, November 11, 2003.

¹⁶⁵ Conectiva Linux Security Announcement, CLA-2003:784, November 13, 2003.

¹⁶⁶ Red Hat Security Advisories, RHSA-2003:314-08 & 313-00, November 12 & 13, 2003.

¹⁶⁷ Trustix Secure Linux Security Advisory, TSLSA-2003-0040, November 17, 2003.

¹⁶⁸ SGI Security Advisory, 20031101-01-U, November 19, 2003.

¹⁶⁹ Securiteam, November 26, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
RedHat ¹⁷⁰ <i>Conectiva issues advisory</i> ¹⁷¹ <i>More vendors issue advisories</i> ^{172, 173, 174}	Unix	Enterprise Linux WS 2.1 IA64, 2.1, ES 2.1 IA64, 2.1, AS 2.1 IA64, 2.1	A buffer overflow vulnerability exists in the 'getgrouplist' function if the size of the group list is too small to hold all the user's groups, which could let a malicious user cause a Denial of Service.	Patches available at: http://rhn.redhat.com/errata/RHSA-2003-249.html <i>Conectiva:</i> ftp://atualizacoes.conectiva.com.br/ <i>Mandrake:</i> http://www.mandrakesecurity.net/en/advisories/ <i>RedHat:</i> ftp://updates.redhat.com/ <i>Trustix:</i> http://www.trustix.org/errata/misc/2003/TSL-2003-0039-glibc.asc.txt	Glibc Getgrouplist Function Buffer Overflow CVE Name: CAN-2003-0689	Low	Bug discussed in newsgroups and websites.
RedHat ¹⁷⁵	Unix	Linux 7.1 pseries, iseries, 7.1 i386, 7.2 ia64, i386, 7.3 i386, 8.0 i386, 9.0 i386	A Denial of Service vulnerability exists in 'iproute' because spoofed messages that are sent on the kernel netlink interface are accepted.	Upgrade available at: ftp://updates.redhat.com/	Linux IPRoute Spoofed Kernel Messages Denial of Service	Low	Bug discussed in newsgroups and websites.
Rob Kaper, ¹⁷⁶	Unix	monopd 0.8.2	A remote Denial of Service vulnerability exists when a malicious user submits a specially crafted message during certain game status conditions.	Upgrade available at: http://prdownloads.sourceforge.net/monopd/monopd-0.8.3.tar.gz	monopd Remote Denial of Service	Low	Bug discussed in newsgroups and websites.

¹⁷⁰ RedHat Security Advisory, RHSA-2003:249-11, August 22, 2003.

¹⁷¹ Conectiva Linux Security Announcement, CLA-2003:762, October 14, 2003.

¹⁷² Red Hat Security Advisory, RHSA-2003:325-01, November 13, 2003.

¹⁷³ Mandrake Linux Security Update Advisory, MDKSA-2003:107, November 19, 2003.

¹⁷⁴ Trustix Secure Linux Security Advisory, TSLSA-2003-0039, November 17, 2003.

¹⁷⁵ Red Hat Security Advisory, RHSA-2003:316-01, November 24, 2003.

¹⁷⁶ SecurityTracker Alert, 1008192, November 15, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
SANE ¹⁷⁷ <i>More advisories issued^{178, 179}</i> <i>More advisories issues^{180 181}</i> <i>SuSE issues advisory¹⁸²</i>	Unix	SANE 1.0.0-1.0.9, sane-backend 1.0.10	Multiple vulnerabilities exist: a vulnerability exists because the identity (IP address) of the remote host is not checked during the SANE_NET_INIT RPC call, which could let a remote malicious user obtain unauthorized access; a vulnerability exists because connection drops are not handled properly, which could let a remote malicious user obtain sensitive information and cause a Denial of Service; a vulnerability exists when a connection is dropped before the size value of malloc is set, which could let a remote malicious user cause a Denial of Service; a vulnerability exists because the validity of RPC numbers it gets before getting the parameters; a vulnerability exists when debug messages are enabled dropped connections are not properly handled, which could let a remote malicious user cause a Denial of Service; and a vulnerability exists because memory is not properly allocated in some cases, which could let a remote malicious user cause a Denial of Service.	<u>Debian:</u> http://security.debian.org/pool/updates/main/s/sane-backends/ <u>Mandrake:</u> http://www.mandrakesecurity.net/en/ftp.php <u>RedHat:</u> ftp://updates.redhat.com/ <u>Conectiva:</u> ftp://atualizacoes.conectiva.com.br/ <u>SGI:</u> http://www.sgi.com/support/security/ <u>SuSE:</u> ftp://ftp.suse.com/pub/suse/	Multiple Sane Package Remote Vulnerabilities CVE Names: CAN-2003-0773, CAN-2003-0774, CAN-2003-0775, CAN-2003-0776, CAN-2003-0777, CAN-2003-0778	Low/Medium (Medium if unauthorized access or sensitive information can be obtained)	Bug discussed in newsgroups and websites.
SAP ¹⁸³	Windows NT 4.0/2000, XP, Unix	DB 7.3.29, 7.3.00, 7.4, 7.4.3.7 Beta, 7.4.3	Multiple vulnerabilities exist: a vulnerability exists because the 'NETAPI32.DLL' file is loaded insecurely with '"LoadLibrary(),' which could let a malicious user obtain elevated privileges; and a buffer overflow vulnerability exists in 'niserver' (on Unix-based systems) and 'serv.exe' (on Windows), which could let a remote malicious user execute arbitrary code.	Update available at: http://www.sapdb.org/7.4/sap_db_software.htm	SAP DB Privilege Escalation & Buffer Overflow CVE Names: CAN-2003-0938, CAN-2003-0939	Medium/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites.

¹⁷⁷ Debian Security Advisory DSA 379-1, September 11, 2003.

¹⁷⁸ Red Hat Security Advisories, RHSA-2003:278-01 & RHSA-2003:285-03, October 7, 2003.

¹⁷⁹ Mandrake Linux Security Update Advisory, MDKSA-2003:099, October 10, 2003.

¹⁸⁰ Conectiva Linux Security Announcement, CLA-2003:769, October 22, 2003.

¹⁸¹ SGI Security Advisory, 20031002-01-U, October 27, 2003.

¹⁸² SUSE Security Announcement, SuSE-SA:2003:046, November 18, 2003.

¹⁸³ @stake, Inc. Security Advisory, a111703-1, November 17, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
SAP ¹⁸⁴	Windows NT 4.0/2000, XP, Unix	DB 7.3.29, 7.3.00, 7.4, 7.4.3.7 Beta, 7.4.3	Multiple vulnerabilities exist: a Directory Traversal vulnerability exists in the web-tools component due to an input validation error, which could let a remote malicious user obtain sensitive information; a vulnerability exists because by default any user with access to web-tools can access Web Agent Administration pages directly without prior authentication, which could let a remote malicious user obtain sensitive information; a buffer overflow vulnerability exists in the Web Agent Administration service, which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability exists in the Web Agent / WAECHO default installation, which could let a remote malicious user execute arbitrary code; and a vulnerability exists because the Web Database Manager generates predictable session Ids and Includes them in URL, which could let a remote malicious user obtain sensitive information.	Update available at: http://www.sapdb.org/7.4/sap_db_software.htm	DB web-tools Multiple Vulnerabilities CVE Names: CAN-2003-0940, CAN-2003-0941, CAN-2003-0942, CAN-2003-0943, CAN-2003-0944, CAN-2003-0945	Medium/ High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites.
SGI ¹⁸⁵	Unix	IRIX 6.5-6.5.22, 6.5.17 m- 6.5.21 m, 6.5.17 f- 6.5.21 f	Multiple vulnerabilities exist: a vulnerability exists because a remote malicious user may be able to mount a file system via an unprivileged port even if rpc.mountd is started with the '-n' option; a remote Denial of Service vulnerability exists in 'rpc.mountd' which would make NFS services unavailable; and a vulnerability exists because the 'rpc.mountd' service returns various replies depending on whether a requested file exists or not, which could let a malicious user obtain sensitive information.	Patches available at: ftp://patches.sgi.com/support/free/security/patches	SGI rpc.mountd Multiple Vulnerabilities CVE Name: CAN-2003-0796, CAN-2003-0797	Low/ Medium (Medium if sensitive information can be obtained)	Bug discussed in newsgroups and websites.
Sircd.org ¹⁸⁶	Unix	sircd 0.5.2, 0.5.3	A vulnerability exists in 's_client.c,' which could let a remote malicious user obtain elevated privileges.	No workaround or patch available at time of publishing.	SIRCD Server Operator Privilege Escalation	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

¹⁸⁴ @stake, Inc. Security Advisory, a111703-2, November 17, 2003.

¹⁸⁵ SGI Security Advisory, 20031102-01-P, November 21, 2003.

¹⁸⁶ Bugtraq, November 20, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
SNAP Innovation GmbH ¹⁸⁷	Unix	PrimeBase SQL Database Server 4.2	A vulnerability exists because the password is stored in plain text in the 'password.adm' file and the software is configured with a default Administrator account that requires no password, which could let a malicious user obtain unauthorized Administrative access.	No workaround or patch available at time of publishing.	PrimeBase SQL Database Server Password Storage	High	Bug discussed in newsgroups and websites. There is no exploit code required.
Sun Microsystems, Inc. ¹⁸⁸	Unix	Cobalt RaQ 550	An access validation vulnerability exists due to an unspecified error in the user interface, which could let a malicious user obtain sensitive information.	Upgrade available at: http://ftp.cobalt.sun.com/pub/packages/raq550/all/RaQ550-All-Security-0.0.1-16346.pkg	Cobalt RaQ550 Information Disclosure	Medium	Bug discussed in newsgroups and websites.
Sun Microsystems, Inc. ¹⁸⁹	Unix	Solaris 2.5.1, 2.6, 7.0, 8.0, 9.0	A vulnerability exists in the libraries associated with the PGX32 Frame Buffer, which could let a malicious user obtain unauthorized root privileges.	Patches available at: http://sunsolve.sun.com	Solaris PGX32 Libraries Root Privileges	High	Bug discussed in newsgroups and websites.
Sybase ¹⁹⁰	Windows NT 4.0, Unix	Adaptive Server Enterprise 12.5 Win, 12.5 Linux	A remote Denial of Service vulnerability exists when a malicious user submits invalid password.	Update available at: www.sybase.com/products/databaseservers/ase	Adaptive Server Remote Denial of Service CVE Name: CAN-2003-0327	Low	Bug discussed in newsgroups and websites.
Symantec ¹⁹¹	Windows	Pc Anywhere 10.0, 10.5 11.0	A vulnerability exists when pcAnywhere runs in 'service-mode,' which could let a local/remote malicious user obtain SYSTEM privileges.	This issue has been rectified and fixes are available via LiveUpdate.	PCAnywhere SYSTEM Privileges CVE Name: CAN-2003-0936	High	Bug discussed in newsgroups and websites. There is no exploit code required.
Symantec ¹⁹²	Windows 95/98/NT 4.0	Pc-Anywhere 9.0.1 9.2	A vulnerability exists because both local and remote users can interact with a chat session window running on the host spawned under the 'AWHOST32' process when Symantec pcAnywhere runs in 'service mode,' which could let a local/remote malicious user obtain elevated privileges.	This issue has been rectified and fixes are available via LiveUpdate.	PCAnywhere Chat Client Elevated Privileges	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

¹⁸⁷ SecurityTracker Alert, 1008280, November 22, 2003.

¹⁸⁸ SecurityFocus, November 18, 2003.

¹⁸⁹ Sun(sm) Alert Notification , 57360, November 19, 2003.

¹⁹⁰ Rapid7, Inc. Security Advisory, R7-0016, November 20, 2003.

¹⁹¹ Secure Network Operations, Inc. Security Advisory, SRT2003-11-13-0218, November 13, 2003.

¹⁹² Secunia Advisory, SA10238, November 17, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Thomson ¹⁹³	Multiple	TCM 305 Cable Modem, 315 Cable Modem	A remote Denial of Service vulnerability exists when a malicious user submits an overly long HTTP request (about 100 bytes) to the HTTP interface.	No workaround or patch available at time of publishing.	Thomson Cable Modem Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Thomson ¹⁹⁴	Multiple	Speed Touch 510 ADSL Router	A Denial of Service vulnerability exists when routing certain types of traffic.	No workaround or patch available at time of publishing.	SpeedTouch DSL Router Denial of Service	Low	Bug discussed in newsgroups and websites. Vulnerability may be exploited with a number of free, publicly available network auditing packages.
TildeSlash ¹⁹⁵	Unix	Monit 1.4, 1.4.1, 2.0, 2.1, 2.1.1, 2.2, 2.2.1, 2.3, 2.4, 2.4.1-2.4.3, 3.0, 3.1, 3.2, 4.0, 4.1	Multiple vulnerabilities exist: a remote Denial of Service vulnerability exists when a malicious user submits a negative value in a Content-Length header field; and a buffer overflow vulnerability exists due to insufficient bounds checking when handling overly long HTTP requests, which could let a remote malicious user execute arbitrary code with root privileges.	Upgrade available at: http://www.tildeslash.com/monit/dist/monit-4.1.1.tar.gz	Monit Remote Denial of Service & Buffer Overflow	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites.
Tincan LTD. ¹⁹⁶	Multiple	PHPList 2.6.2	An access validation vulnerability exists due to insufficient validation of certain input, which could let a remote malicious user execute arbitrary code.	Update available at: http://tincan.co.uk/phplist	PHPList Remote Code Execution	High	Bug discussed in newsgroups and websites.
True North Software ¹⁹⁷ <i>Another exploit published</i> ¹⁹⁸	Windows	IA WebMail Server 3.0, 3.1	A buffer overflow vulnerability exists due to insufficient bounds checking when handling GET requests, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	IA WebMail Server Remote Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit script has been published.

¹⁹³ Shell Security Advisory, November 23, 2003.

¹⁹⁴ Bugtraq, November 25, 2003.

¹⁹⁵ S-Quadra Advisory #2003-11-24, November 24, 2003.

¹⁹⁶ Bugtraq, November 14, 2003.

¹⁹⁷ SecurityTracker Alert, 1008075, November 3, 2003.

¹⁹⁸ SecurityFocus, November 19, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Valve Software ¹⁹⁹	Windows, Unix	Half-Life Dedicated Server 3.1.0.4-3.1.0.9 Linux, 3.1, 3.1.1.1d Linux, 3.1.1.1c1 Linux, 3.1.1.0 Linux, 3.1.3, 4.1.0.6 - 4.1.0.9 Win32, 4.1.0.4 Win32, 4.1.1.1c1 Win32, 4.1.1.0 Win32	An information disclosure vulnerability exists due to a flaw in the download functionality, which could let a malicious user cause a Denial of Service or obtain sensitive information.	No workaround or patch available at time of publishing.	Half-Life Dedicated Server Information Disclosure & Denial of Service	Low/ Medium (Medium is sensitive information can be obtained)	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Vladimir Litovka ²⁰⁰	Unix	Minimalist 2.2	A vulnerability exists due to an input validation error in the 'getAuth()' function, which could let a remote malicious user execute arbitrary commands.	Update available at: http://security.debian.org/pool/updates/main/m/minimalist/	Minimalist Unspecified mote Command Execution CVE Name: CAN-2003-0902	High	Bug discussed in newsgroups and websites.
Web Wiz Guide ²⁰¹	Windows	Web Wiz Forums 7.01	A Cross-Site Scripting vulnerability exists in the 'location,' 'signature,' and 'password' parameters due to insufficient verification in 'register_new_user.asp' and 'register.asp,' which could let a remote malicious user execute arbitrary HTML and script code.	Upgrade available at:	Web Wiz Forums Cross-Site Scripting	High	Bug discussed in newsgroups and websites. There is no exploit code required.

¹⁹⁹ Bugtraq, November 19, 2003.

²⁰⁰ Debian Security Advisory, DSA 402-1, November 17, 2003.

²⁰¹ Bugtraq, November 13, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Webfs ²⁰² <i>Exploit scripts published</i> ²⁰³	Unix	WebFS 1.1.7-1.1.9, 1.17	Several vulnerabilities exist: an information disclosure vulnerability exists due to insufficient sanitization of user-supplied hostnames when accessing virtual hosts, which could let a malicious user obtain sensitive information; and a buffer overflow vulnerability in 'ls.c' when processing very long file names, which could let a malicious user execute arbitrary code.	Patch available at: http://bytesex.org/misc/webfs_1.20.tar.gz Debian: http://security.debian.org/pool/updates/main/w/webfs/	Webfs Information Disclosure & Buffer Overflow CVE Names: CAN-2003-0832, CAN-2003-0833	Medium/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. There is no exploit code required for the information disclosure vulnerability. <i>Exploit scripts have been published.</i>
Web-washer AG ²⁰⁴	Windows	Web washer Classic 2.2.1, 3.3 build 44	A Cross-Site Scripting vulnerability exists because requests sent to WebWasher on the local host interface are returned unfiltered in an error message, which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	WebWasher Classic Error Message Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Winace ²⁰⁵ <i>Another exploit script published</i> ²⁰⁶	Unix	UnAce 2.2	A buffer overflow vulnerability exists due to a failure to handle ace filenames that are of excessive length, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	UnAce Buffer Overflow	High	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
Wireless Tools For Linux ²⁰⁷ <i>Exploit script has been published</i> ²⁰⁸ <i>More exploits published</i> ²⁰⁹	Unix	Wireless Tools Versions 19-26	A buffer overflow vulnerability exists in the 'iwconfig' program when handling strings on the commandline, which could let a malicious user obtain elevated privileges.	No workaround or patch available at time of publishing.	IWConfig Command Line Buffer Overflow	Medium	Bug discussed in newsgroups and websites. Exploit script has been published. <i>More exploit scripts have been published.</i>

²⁰² Debian Security Advisory, DSA 392-1, September 29, 2003.

²⁰³ SecurityFocus, November 22, 2003.

²⁰⁴ Bugtraq, November 13, 2003.

²⁰⁵ Bugtraq, November 9, 2003.

²⁰⁶ SecurityFocus, November 15, 2003.

²⁰⁷ Securiteam, October 26, 2003.

²⁰⁸ SecurityFocus, November 13, 2003.

²⁰⁹ SecurityFocus, November 13, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Wop poware Pty Ltd. ²¹⁰	Windows	PostMaster 3.16.1, 3.17.1	A Cross-Site Scripting vulnerability exists due to insufficient sanitization performed by the proxy service on user-supplied input, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	PostMaster Proxy Service Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

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

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

Medium – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between November 13 and November 26, 2003, listed by date of script, script names, script description, and comments. Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing. During this period, 44 scripts, programs, and net-news messages containing holes or exploits were identified. *Note: At times, scripts/techniques may contain names or content that may be considered offensive.*

Date of Script (Reverse Chronological Order)	Script name	Script Description
November 26, 2003	BackToFramedJpu.txt	Demonstration exploit for the Internet Explorer Cross-Site Scripting vulnerability.
November 26, 2003	epic4-exp.c	Exploit for the Epic4 CTCP Nickname Server Message Remote Buffer Overflow vulnerability.
November 26, 2003	eudora-launchprotex.pl	Perl script that exploits the Eudora Attachment LaunchProtect vulnerability.
November 26, 2003	hijack2.txt	Demonstration exploit for the Internet Explorer Hijack Click vulnerability.
November 26, 2003	IEcache.txt	Demonstration exploit for the Internet Explorer download function vulnerability.
November 26, 2003	IEcache2.txt	Exploit technique for the Microsoft Internet Explorer cache file disclosure vulnerability. .
November 26, 2003	mhtmlredir.txt	Demonstration exploit for the Internet Explorer MHTML redirection vulnerability.

²¹⁰ Global Security Solution IT, November 14, 2003.

Date of Script (Reverse Chronological Order)	Script name	Script Description
November 26, 2003	MhtRedirLaunchInetExe-Demo.zip	Demonstration exploit for the Internet Explorer MHTML Redirect vulnerability.
November 24, 2003	ike-scan-1.5.1.tar.gz	A utility that discovers IKE hosts and can also fingerprint them using the retransmission backoff pattern.
November 24, 2003	istumbler-83.tgz	A Mac OS/X utility for finding 802.11b & 802.11g wireless networks and services which combines a compact Aqua user interface with advanced wireless scanning and reporting.
November 24, 2003	kill-Taidu.c	Script that exploits the Webfs Buffer Overflow vulnerability.
November 24, 2003	mimedefang-2.39.tar.gz	A flexible MIME e-mail scanner designed to protect Windows clients from viruses.
November 24, 2003	pkcs12bf.tar.gz	A patch for OpenSSL 0.9.7c that adds a PKCS#12 brute-forcing option which takes in a wordlist.
November 24, 2003	stunnel-3.26.tar.gz	A program that allows you to encrypt arbitrary TCP connections inside SSL (Secure Sockets Layer) available on both Unix and Windows.
November 24, 2003	stunnel-4.04.tar.gz	A program that allows you to encrypt arbitrary TCP connections inside SSL (Secure Sockets Layer) available on both Unix and Windows.
November 24, 2003	teptrack-1.0.0.tar.gz	A packet sniffer that passively watches for connections on a specified network interface, tracking their states and listing them in a manner similar to the top command. It displays source and destination addresses and ports, connection state, idle time, and bandwidth usage.
November 23, 2003	thomson-dos.c	Script that exploits the Thomson Cable Modem Remote Denial of Service vulnerability.
November 22, 2003	buffer.c	Script that exploits the GEdit Large IOStream File Memory Corruption vulnerability.
November 22, 2003	vbportal-spam.php	Exploit for the vbPortal Friend.PHP Remote E-Mail Relaying vulnerability.
November 22, 2003	webfs-lnamexp.c	Script that exploits the Webfs Buffer Overflow vulnerability.
November 21, 2003	OBSD-semop-crash.c	Exploit for the OpenBSD semctl/semop Denial of Service vulnerability.
November 21, 2003	tunnelshell_2.3.tgz	A client/server program written in C for Linux users that tunnels a shell using various methods that can bypass firewalls, such as fragmented packets, tcp ACK packets, UDP, ICMP, and raw IP packets (ipsec).
November 20, 2003	85mod_gzip.c	Remote exploit for Mod_gzip Debug vulnerability.
November 20, 2003	amap-4.5.tar.gz	A next-generation scanning tool that allows you to identify the applications that are running on a specific port.
November 20, 2003	WifiScanner-0.9.3.tar.gz	An analyzer and detector of 802.11b stations and access points that can listen alternatively on all the 14 channels, write packet information in real time, search access points and associated client stations, and can generate a graphic of the architecture using GraphViz.
November 19, 2003	djohn-0.9.8.1.tgz	With Distributed John (DJohn) you can crack passwords using several machines to get passwords sooner than using a single machine.
November 19, 2003	iawebmail.pl	Script that exploits the IA WebMail Server Remote Buffer Overflow vulnerability.
November 19, 2003	msuxobsd2.c	Script that exploits the OpenBSD IBCS2 Binary Length Parameter Kernel-Based Buffer Overflow vulnerability.
November 18, 2003	bb.c	A tool that assists in building buffer overflow strings for local and remote exploits.
November 18, 2003	openbsd_exp.c	Script that exploits the OpenBSD IBCS2 Binary Length Parameter Kernel-Based Buffer Overflow vulnerability.
November 15, 2003	FBHterminator.c	Script that exploits the TerminatorX LADSPA_PATH environment variable vulnerability.

Date of Script (Reverse Chronological Order)	Script name	Script Description
November 15, 2003	gEEk-0verkill.c	Proof of Concept exploit for the Overkill HomeVariable Buffer Overflow vulnerability.
November 15, 2003	unace-exp.c	Proof of Concept exploit script for the UnAce Buffer Overflow vulnerability.
November 15, 2003	xor-analyze-0.5.tar.gz	A program for cryptanalysis that is one of the most easily breakable and commonly used ciphers.
November 14, 2003	11.14.MS03-049-II.c	Script that exploits the Windows Workstation Service Remote Buffer Overflow vulnerability.
November 14, 2003	execdror5-Demo.zip	Six step cache attack for Internet Explorer 6 SP1 (up to date on 10/30/2003) that combines several older unpatched and recently discovered vulnerabilities to execute code remotely by viewing a web page or HTML e-mail.
November 14, 2003	gEEk-terminatorX.c	Script that exploits the TerminatorX vulnerability.
November 14, 2003	sp-myserver0.5-dos.c	Script that exploits the MyServer HTTP Server Directory Traversal vulnerability.
November 13, 2003	iwconfig.c	Script that exploits the IWConfig Command Line Buffer Overflow vulnerability.
November 13, 2003	PST_iwconfig.c	Script that exploits the IWConfig Command Line Buffer Overflow vulnerability.

Trends

- The CERT/CC has received reports of several new variants of the 'Mimail' worm. The most recent variant of the worm (W32/Mimail.J) arrives as an email message alleging to be from the Paypal financial service. For more information, see Virus Section below.
- The CERT/CC received a number of reports indicating that malicious user are actively exploiting the Microsoft Internet Explorer vulnerabilities described in the "Bugs, Holes & Patches" Table.
- The SANS Twenty Most Critical Internet Security Vulnerabilities list has been published. This updated SANS Top Twenty is actually two Top Ten lists: the ten most commonly exploited vulnerable services in Windows and the ten most commonly exploited vulnerable services in UNIX and Linux. For more information see the list located at: <http://www.sans.org/top20/>.
- **The National Cyber Security Division (NCS) of the Department of Homeland Security (DHS) / Information Analysis and Infrastructure Protection (IAIP) Directorate has issued an advisory in consultation with the Microsoft Corporation to heighten awareness of potential Internet disruptions resulting from the possible spread of malicious software exploiting the Microsoft Operating Systems' Remote Procedure Call Server Service (RPCSS) vulnerability. For more information, see "Bugs, Holes & Patches" Table and advisory located at: <http://www.nipc.gov/warnings/advisories/2003/Advisory9102003.htm>. The Microsoft advisory is located at: http://www.microsoft.com/security/security_bulletins/ms03-039.asp. Tools have been developed to exploit this vulnerability and there is an increased likelihood that new viruses will emerge soon.**

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.*

JS/Flea-B (Aliases: JS.Flea.b, JS/Flea.B, JS.Fortnight.D, JS/Fortnight.gen@M) (JavaScript Worm):

This worm has been reported in the wild. It propagates via HTML e-mail. The worm arrives as the signature to an HTML e-mail. When the HTML e-mail is rendered, a webpage is loaded and a JavaScript component is run. The JavaScript then attempts to run a Java class file from the same site.

W32.Azha.Worm (Win32 Worm): This is a worm that spreads through file-sharing programs. Upon execution, W32.Azha.Worm copies itself to the %System% as Azah.exe.

W32.Bolgi.Worm (Win32 Worm): This is a worm that exploits the DCOM RPC vulnerability (described in Microsoft Security Bulletin MS03-026) using TCP port 445. It attempts to download the file to the %WinDir%\system32 directory, and then execute it. The worm only targets Windows 2000 and Windows XP machines. While Windows NT and Windows 2003 Server machines are vulnerable to the aforementioned exploit (if not properly patched), the worm is not coded to replicate to those systems.

W32.Francette.Worm (Aliases: Worm.Win32.Francette.a, W32/Tumbi.worm) (Win32 Worm): This is a worm that exploits the DCOM RPC vulnerability (described in Microsoft Security Bulletin MS03-026) using TCP port 135, as well as the Microsoft IIS Web Server Folder Traversal vulnerability (described in Microsoft Security Bulletin MS00-078). The existence of the file syshost.exe is an indication of a possible infection. This worm is written in Borland Delphi and is packed with ASPack.

W32/Gogo.cmp (Companion Virus): This is a companion virus. When an infected file is executed, it renames all *.EXE files to *.EX1. For example the file "Calc.exe" becomes "Calc .ex1" and now the file "Calc.exe" is a copy of the virus. The virus will search for EXE files on the following drives: C:, D:, E:, F:, G:, H:, I:, J:, L:, and M:. Files in the %Windir%, and %Sysdir% folder are not infected. Also, the file IEXPLORE.EXE, is not infected.

W32.HLLW.Anarch@mm (Win32 Worm): This is a worm that attempts to spread through file-sharing networks and mIRC. It uses Microsoft Outlook to send itself to all the contacts in the Outlook Address Book. The e-mail has the following characteristics:

- Subject: New Media Player!!
- Attachment: M_Player_v1.0.exe

It is written in the Microsoft Visual Basic programming language.

W32.HLLW.Bandie (Win32 Worm): This is a worm that attempts to spread itself through the KaZaA and ICQ file-sharing networks. It is written in the Microsoft Visual Basic programming language.

W32.HLLW.Bereb (Win32 Worm): This is a worm that spreads using the WinMx file-sharing program. It is written in Borland Delphi and is packed with UPX.

W32/Mimail-J (Aliases: I-Worm.Mimail.j, W32/Mimail.j@MM virus, W32.Mimail.J@mm, WORM_MIMAIL.J, Win32.Mimail.J) (Win32 Worm): This worm has been reported in the wild. It is very similar to W32/Mimail-I. This variant tries to get you to give up your credit card details, just like W32/Mimail-I, but also asks you for additional personal information such as your Social Security Number and your mother's maiden name. W32/Mimail-J drops itself to your Windows folder using the names SvcHost32.exe and ee98af.tmp. The worm also creates fake PayPal web pages in your root directory using the names, pp.hta and index2.hta. These web pages include scripts that ask you for the personal information described above.

W32/Mimail-K (Win32 Worm): This worm has been reported in the wild. It is a worm that spreads via e-mail using addresses harvested from the hard drive of the infected computer. All e-mail addresses found on the computer are saved in a file named eml.tmp in the Windows folder. In order to run itself automatically when Windows starts up, the worm copies itself to the file sysload32.exe in the Windows folder and adds the following registry entry:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\SystemLoad32

The e-mails sent by the worm may have the following characteristics:

- Subject line : don't be late!<30 spaces><random characters>
- Attached file : readnow.zip

W32/Mimail-K spoofs 'From' field of the sent e-mails using the e-mail address john@<your domain>.

Readnow.zip is a compressed file that contains an executable file named readnow.doc.scr. It also creates a copy of itself named exe.tmp and a copy of readnow.zip named zip.tmp, both in the Windows folder. While searching for e-mail addresses in files on the local hard drive, W32/Mimail-K attempts to exclude files that have various extensions from the search. W32/Mimail-K also attempts denial of service attacks targeting:

- darkprofits.cc
- www.darkprofits.cc
- darkprofits.ws
- www.darkprofits.ws

W32.NGVCK.4920 (Win32 Virus): This is a virus that is based on the W32.NGVCK virus creation kit. It will infect executable files when they are run. When W32.NGVCK.4920 is executed, it attempts to import several Windows functions from various .dll files. These functions will be used later to find and infect files and creates the file, UnBlaster.exe, in the %System% folder. This file is a copy of the virus. The virus installs a Windows hook so that it can infect Windows PE executable files when they are executed and checks the system time to determine whether it should display a message box. The message, if displayed, is written in an Asian language.

W32.Notime (Win32 Virus): This is a polymorphic Windows virus that appends itself to executable files. When W32.Notime is executed, it checks if the current month/day equals a stored value. If the current month and day does not equal the value, the worm will search the following folders for files that have the extensions .exe, .scr, and .cpi to infect:

- Current folder
- %Windir%
- %System%

The virus appends itself to the end of the infected files, changing the original entry point to point to itself, so that it will be executed before the original file and attempts to display a series of dialog boxes that tell a story. It enters an endless loop whereby it continuously opens and closes the CD drive and passes control back to the original host program.

W32/Opaserv-V (Win32 Worm): This is a worm that spreads by copying itself to network shares. The worm drops copies of itself to the Windows folder as Banda!, Podre!! and speedy.pif, then adds an entry to the registry at:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Spees3

to run itself on system restart. The worm attempts to copy itself to the Windows folder on networked computers with open shared drives. It then modifies the win.ini on the remote machine to ensure it will be run on system restart. W32/Opaserv-V also attempts to update itself periodically from a pre-configured website.

W32.Randex.AR (Win32 Worm): This is a network-aware worm that attempts to connect to a predetermined IRC server to receive instructions from its author. It is written in Microsoft Visual C++ and is packed with Exe32Pack and ASPack.

W32.Randex.AT (Win32 Worm): This is a network-aware worm that attempts to connect to a predetermined IRC server to receive instructions from its author. It is written in Microsoft Visual C++ and is packed with UPX.

W32.Randex.AW (Win32 Worm): This is a network-aware worm that spreads through shared network drives and opens random ports. The worm can receive instructions from a channel on a predetermined IRC server.

W32.Randex.AX (Win32 Worm): This is a network-aware worm that spreads through shared network drives and opens random ports. The worm can receive instructions from a channel on a predetermined IRC server.

W32.Spex.B.Worm (Alias: Worm.P2P.Specx) (Win32 Worm): This is a worm that spreads through the KaZaA and iMesh file-sharing networks. It can also terminate security programs and system administration tools, steal CD keys of computer games, and perform Denial of Service attacks. The worm is packed with ExeStealth and ASPack.

W32.Taplak (Win32 Worm): This is a worm that attempts to spread through the KaZaA file-sharing network. It is written in Visual Basic, and current submissions have been packed with ASPack. Upon execution, W32.Taplak drops the following files:

- %System%\SetupIE.com
- %System%\config.com
- %System%\backup.com

The Worm adds the values:

- "AolCon"="%System%\config.com"
- "MemConfig"="%System%\SetupIE.com"

to the registry key:

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

And creates the registry key:

- HKEY_CURRENT_USER\Software\VB and VBA Program Settings\paltalk

The worm checks whether KaZaA is installed, and, if found, will locate KaZaA's My Shared Folder and drop copies of itself with various names.

W32.Widare (Win32 Virus): This is an encrypted, file-appending virus that attempts to infect the .exe, .cpl, and .scr files.

WORM_ADURK.A (Alias: W32.Adurk.A@mm) (Win32 Worm): This worm propagates into network shares and via e-mail. It drops a copy of itself into network shares as the file I_LOVE_YOU.EXE. To propagate via e-mail, it sends out e-mail messages with the following details using Simple Mail Transfer Protocol (SMTP):

- From: <spoofed sender address>
- Subject: CARTOON <random number>
- Attachment: CARTOON_<random number>.exe

It runs on Windows 95, 98, ME, 2000, and XP.

Worm/Agobot.64512 (Internet Worm): This is a memory resident Internet worm that spreads through open or weakly protected network shares. It also exploits some well-known Microsoft vulnerabilities in order to propagate itself. If executed, the worm adds the following file to the \windows%\system% directory, "syst19b.exe." So that it gets run each time a user restart their computer the following registry keys get added:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
"System Loaderav"="syst19b.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
"System Loaderav"="syst19b.exe"

The follow registry key is also created:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WM_Control
"ImagePath"=hex(2):22,00,43,00,3a,00,5c,00,57,00,49,00,4e,00,44,00,4f,00,57,00,\53,00,5c,00,53,00,79,00,73,00,74,00,65,00,6d,00,33,00,32,00,5c,00,77,00,69,\00,6e,00,6d,00,75,00,72,00,33,00,32,00,2e,00,65,00,78,00,65,00,22,00,20,00,\2d,00,73,00,65,00,72,00,76,00,69,00,63,00,65,00,00,00

Worm/Agobot.78336 (Internet Worm): This is a memory resident Internet worm that spreads through open or weakly protected network shares. It also exploits some well-known Microsoft vulnerabilities in order to propagate itself. If executed, the worm adds the following file to the \windows%\system% directory, "syst18b.exe." So that it gets run each time a user restart their computer the following registry keys get added:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
"System Loaderav"="syst18b.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
"System Loaderav"="syst18b.exe"

The follow registry key is also created:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WM_Control
"ImagePath"=hex(2):22,00,43,00,3a,00,5c,00,57,00,49,00,4e,00,44,00,4f,00,57,00,\53,00,5c,00,53,00,79,00,73,00,74,00,65,00,6d,00,33,00,32,00,5c,00,77,00,69,\00,6e,00,6d,00,75,00,72,00,33,00,32,00,2e,00,65,00,78,00,65,00,22,00,20,00,\2d,00,73,00,65,00,72,00,76,00,69,00,63,00,65,00,00,00

WORM_AGOBOT.AQ (Alias: Worm/Agobot.AQ) (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

For more information about these Windows vulnerabilities, please refer to the following Microsoft bulletins:

- Microsoft Security Bulletin MS03-026
- Microsoft Security Bulletin MS03-001
- Microsoft Security Bulletin MS03-007

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 antiviral-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.AR (Alias: Worm/Agobot.ARE) (Win32 Worm): This worm is similar to another AGOBOT variant, WORM_AGOBOT.AQ, because it 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

For more information about these Windows vulnerabilities, please refer to the following Microsoft bulletins:

- Microsoft Security Bulletin MS03-026
- Microsoft Security Bulletin MS03-001
- Microsoft Security Bulletin MS03-007

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 antiviral-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.AS (Aliases: W32/Gaobot.worm.gen, W32/Agobot-AS) (Win32 Worm): This is an IRC backdoor Trojan and network worm. W32/Agobot-AS copies itself to network shares with weak passwords and attempts to spread to computers using the DCOM RPC and the RPC locator vulnerabilities. These vulnerabilities allow the worm to execute its code on target computers with System level privileges. For further information on these vulnerabilities and for details on how to patch the computer against such attacks please see Microsoft security bulletins MS03-026 and MS03-001. When first run, W32/Agobot-AS copies itself to the Windows system folder with the filename syst18b.exe and creates the following registry entries so that the worm is run when Windows starts up:

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\System Loaderav = syst18b.exe
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\System Loaderav = syst18b.exe

W32/Agobot-AS also registers itself as a service that will be activated when Windows starts up. The name of the service is System Loaderav. It connects to a remote IRC server and joins a specific channel. A malicious user using the IRC network can then access the backdoor functionality of the worm. The worm also attempts to terminate and disable various security related programs.

WORM_AGOBOT.AV (Aliases: W32.HLLW.Gaobot.gen, Win32.HLLW.Agobot, Worm/Agobot) (Internet Worm): This memory-resident malware has both worm and backdoor capabilities. Like earlier AGOBOT variants, this worm also exploits the following Windows vulnerabilities to propagate across the network:

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

Additional information regarding these vulnerabilities are available at the following Microsoft pages:

- Microsoft Security Bulletin MS03-026
- Microsoft Security Bulletin MS03-001
- Microsoft Security Bulletin MS03-007

It also performs the following malicious tasks:

- Connect to an Internet Relay Chat (IRC) channel and wait for commands from a remote user
- Terminate several antiviral and security programs, and system files
- Steal the Windows Product ID and CD Keys of many popular games
- Terminate the processes of other malware

This UPX-compressed worm runs on Windows 2000 and XP.

WORM_AGOBOT.AX (Alias: W32.HLLW.Gaobot.BC) (Internet Worm): This 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

For more information about these Windows vulnerabilities, please refer to the following Microsoft Web pages:

- Microsoft Security Bulletin MS03-026
- Microsoft Security Bulletin MS03-001
- Microsoft Security Bulletin MS03-007

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 antiviral-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/LazyMin.31 (Alias: Win32/LazyMin.31) (File Infector Worm): This is memory resident file infector with various backdoor functionalities. If executed, the worm drops the files:

- C:\WINDOWS\SYSTEM\EELGFA32.DLL (this DLL will have random filenames)
- C:\WINDOWS\TEMP\ALIYPQHT.VCU.

Additionally, the following registry key gets added:

- HKEY_CLASSES_ROOT\CLSID\{52F7FFDF-D0CF-5CC3-5F4F-C6D8F7D65F0D}\InProcServer32 @="C:\WINDOWS\SYSTEM\Eelgfa32.dll"

WORM_SDBOT.AY (Alias: Backdoor/Spyboter.68096) (Internet Worm): This malware is both a backdoor and a worm. It copies itself into the Admin folder of network machines that it is able to access using a long list of logon names and passwords. The malware opens port 113 of an infected system and listens for commands coming from a remote user. It allows remote users to do the following:

- Disable network shares
- Update this malware
- Download and execute a file
- Flood other targets using ICMP or UDP flood
- List processes
- Terminate processes
- Terminate this malware

It runs on Windows 95, 98, ME, NT, 2000, and XP.

WORM_SDBOT.D (Aliases: Backdoor.SDBot.Gen, Backdoor/SdBot.Server, IRC/BackDoor.SdBot.VW) (Win32 Worm): This memory-resident worm propagates into network shares on random IP addresses. It forces itself into inaccessible shares using a predefined list of user names and passwords. The worm drops itself into network shares as the file SERVICE.EXE. Worm_Sdbot.D also has backdoor capabilities. It can run as an Internet Relay Chat (IRC) client and connect to an IRC channel, where it can receive commands from a remote malicious user. The worm can process a variety of commands, including instructions to flood certain targets. This worm, which runs on Windows NT, 2000, and XP, can download files and update itself.

Worm/SpyBot.55199 (Internet Worm): This is a memory resident Internet worm that spreads through the use of the popular file-sharing program KaZaA. It copies itself in the \windows%\system% directory under the filename "fucker.exe" and in the C:\windows\system\kazaabackupfiles directory under the filename "download_me.exe." So that it gets run each time a user restart their computer the following registry keys get added:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Runonce
"spolerv.exe"="FUCKER.EXE"
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
"spolerv.exe"="FUCKER.EXE"

To make itself available through the KaZaA file sharing program, the following registry key is modified:

- HKEY_CURRENT_USER\Software\Kazaa\LocalContent
"Dir0"="012345:C:\\WINDOWS\\SYSTEM\\kazaabackupfiles\\"

WORM_WOZER.A (Alias: W32/Wozer.worm@MM, W32.Wozer.Worm, I-Worm.Poffer.b, W32/Wozer.worm) (Win32 Worm): This memory-resident worm propagates via e-mail, network shares, and mIRC. It mass-mails copies of itself to e-mail addresses found in certain files on the target system. To facilitate its propagation via mIRC, this worm drops the malicious script, IRC_WOZER.A, on the infected system. This dropped file sends a copy of the worm to all users who are in the same mIRC channel as the infected user. This worm also attempts to terminate processes associated with certain antiviral programs. 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.

Trojan	Version	CyberNotes Issue #
A97M/AcceV	N/A	CyberNotes-2003-18
AdwareDropper-A	A	CyberNotes-2003-04
Adware-SubSearch.dr	dr	CyberNotes-2003-14
Afcore.q	N/A	CyberNotes-2003-20
AIM-Canbot	N/A	CyberNotes-2003-07
AprilNice	N/A	CyberNotes-2003-08
Backdoor.Acidoor	N/A	CyberNotes-2003-05
Backdoor.Amitis	N/A	CyberNotes-2003-01
Backdoor.Amitis.B	B	CyberNotes-2003-11
Backdoor.AntiLam.20.K	K	CyberNotes-2003-10
Backdoor.AntiLam.20.Q	20.Q	CyberNotes-2003-18
Backdoor.Apdoor	N/A	CyberNotes-2003-12
Backdoor.Asoxy	N/A	Current Issue
Backdoor.Assasin.D	D	CyberNotes-2003-01
Backdoor.Assasin.E	E	CyberNotes-2003-04
Backdoor.Assasin.F	F	CyberNotes-2003-09
Backdoor.Augudor	N/A	CyberNotes-2003-23
Backdoor.Badcodor	N/A	CyberNotes-2003-12
Backdoor.Beasty	N/A	CyberNotes-2003-02
Backdoor.Beasty.B	B	CyberNotes-2003-03
Backdoor.Beasty.C	C	CyberNotes-2003-05
Backdoor.Beasty.Cli	Cli	CyberNotes-2003-10
Backdoor.Beasty.D	D	CyberNotes-2003-06
Backdoor.Beasty.dr	dr	CyberNotes-2003-16
Backdoor.Beasty.E	E	CyberNotes-2003-06
Backdoor.Beasty.G	G	CyberNotes-2003-16
Backdoor.Beasty.Kit	N/A	CyberNotes-2003-18
Backdoor.Bigfoot	N/A	CyberNotes-2003-09
Backdoor.Bionet.404	404	CyberNotes-2003-23
Backdoor.Bmbot	N/A	CyberNotes-2003-04
Backdoor.Bridco	N/A	CyberNotes-2003-06
Backdoor.CamKing	N/A	CyberNotes-2003-10
Backdoor.CHCP	N/A	CyberNotes-2003-03
Backdoor.Ciador.B	B	Current Issue
Backdoor.Cmjspy	N/A	CyberNotes-2003-10
Backdoor.Cmjspy.B	B	CyberNotes-2003-14
Backdoor.CNK.A	A	CyberNotes-2003-10
Backdoor.CNK.A.Cli	Cli	CyberNotes-2003-10

Trojan	Version	CyberNotes Issue #
Backdoor.Colfuser	N/A	CyberNotes-2003-01
Backdoor.Coreflood.dr	Dr	CyberNotes-2003-19
Backdoor.Cow	N/A	CyberNotes-2003-01
Backdoor.CrashCool	N/A	CyberNotes-2003-19
Backdoor.Cyberspy	N/A	CyberNotes-2003-01
Backdoor.Daemonize	N/A	CyberNotes-2003-21
Backdoor.Dani	N/A	CyberNotes-2003-04
Backdoor.Darmenu	N/A	CyberNotes-2003-05
Backdoor.Death.Cli	Cli	CyberNotes-2003-10
Backdoor.Deftcode	N/A	CyberNotes-2003-01
Backdoor.Delf.Cli	Cli	CyberNotes-2003-10
Backdoor.Delf.F	F	CyberNotes-2003-07
Backdoor.Dister	N/A	CyberNotes-2003-23
Backdoor.DMSpammer	N/A	CyberNotes-2003-22
Backdoor.Drator	N/A	CyberNotes-2003-01
Backdoor.Dsklite	N/A	CyberNotes-2003-14
Backdoor.Dsklite.cli	cli	CyberNotes-2003-14
Backdoor.Dvldr	N/A	CyberNotes-2003-06
Backdoor.EggDrop	N/A	CyberNotes-2003-08
Backdoor.Evilbot.B	B	CyberNotes-2003-19
Backdoor.Evilbot.C	C	CyberNotes-2003-22
Backdoor.EZBot	N/A	CyberNotes-2003-18
Backdoor.Fatroj	N/A	CyberNotes-2003-10
Backdoor.Fatroj.Cli	Cli	CyberNotes-2003-10
Backdoor.Fluxay	N/A	CyberNotes-2003-07
Backdoor.Frango	N/A	CyberNotes-2003-22
Backdoor.FTP.Casus	N/A	CyberNotes-2003-02
Backdoor.FTP_Ana.C	C	CyberNotes-2003-07
Backdoor.FTP_Ana.D	D	CyberNotes-2003-08
Backdoor.Fxdoor	N/A	CyberNotes-2003-10
Backdoor.Fxdoor.Cli	Cli	CyberNotes-2003-10
Backdoor.Fxsvc	N/A	CyberNotes-2003-16
Backdoor.Graybird	N/A	CyberNotes-2003-07
Backdoor.Graybird.B	B	CyberNotes-2003-08
Backdoor.Graybird.C	C	CyberNotes-2003-08
Backdoor.Graybird.D	D	CyberNotes-2003-14
Backdoor.Graybird.G	G	CyberNotes-2003-19
Backdoor.Grobodor	N/A	CyberNotes-2003-12
Backdoor.Guzu.B	B	CyberNotes-2003-14
Backdoor.HackDefender	N/A	CyberNotes-2003-06
Backdoor.Hale	N/A	CyberNotes-2003-16
Backdoor.Hazzer	N/A	CyberNotes-2003-20
Backdoor.Helios.B	B	CyberNotes-2003-23
Backdoor.Hethat	N/A	CyberNotes-2003-01
Backdoor.Hipo	N/A	CyberNotes-2003-04
Backdoor.Hitcap	N/A	CyberNotes-2003-04
Backdoor.Hogle	N/A	CyberNotes-2003-22
Backdoor.Hornet	N/A	CyberNotes-2003-01
Backdoor.IRC.Aladinz	N/A	CyberNotes-2003-02

Trojan	Version	CyberNotes Issue #
Backdoor.IRC.Aladinz.C	C	CyberNotes-2003-14
Backdoor.IRC.Bobbins	N/A	CyberNotes-2003-18
Backdoor.IRC.Bot.B	B	CyberNotes-2003-22
Backdoor.IRC.Cloner	N/A	CyberNotes-2003-04
Backdoor.IRC.Comiz	N/A	CyberNotes-2003-11
Backdoor.IRC.Flood.F	F	CyberNotes-2003-16
Backdoor.IRC.Hatter	N/A	CyberNotes-2003-18
Backdoor.IRC.Jemput	N/A	CyberNotes-2003-19
Backdoor.IRC.Lampsy	N/A	CyberNotes-2003-10
Backdoor.IRC.PSK	PSK	CyberNotes-2003-16
Backdoor.IRC.Ratsou	N/A	CyberNotes-2003-10
Backdoor.IRC.Ratsou.B	B	CyberNotes-2003-11
Backdoor.IRC.Ratsou.C	C	CyberNotes-2003-11
Backdoor.IRC.RPCBot.B:	B	CyberNotes-2003-18
Backdoor.IRC.RPCBot.C	C	CyberNotes-2003-18
Backdoor.IRC.RPCBot.D	D	CyberNotes-2003-18
Backdoor.IRC.RPCBot.F	F	CyberNotes-2003-19
Backdoor.IRC.Tastyred	N/A	CyberNotes-2003-20
Backdoor.IRC.Whisper	N/A	Current Issue
Backdoor.IRC.Yoink	N/A	CyberNotes-2003-05
Backdoor.IRC.Yoink.A	A	CyberNotes-2003-23
Backdoor.IRC.Zcrew	N/A	CyberNotes-2003-04
Backdoor.IRC.Zcrew.B	B	CyberNotes-2003-19
Backdoor.Isen.Rootkit	N/A	CyberNotes-2003-23
Backdoor.Jittar	N/A	CyberNotes-2003-21
Backdoor.Kaitex.D	D	CyberNotes-2003-09
Backdoor.Kalasbot	N/A	CyberNotes-2003-09
Backdoor.Khaos	N/A	CyberNotes-2003-04
Backdoor.Kilo	N/A	CyberNotes-2003-04
Backdoor.Kodalo	N/A	CyberNotes-2003-14
Backdoor.Kol	N/A	CyberNotes-2003-06
Backdoor.Krei	N/A	CyberNotes-2003-03
Backdoor.Lala	N/A	CyberNotes-2003-01
Backdoor.Lala.B	B	CyberNotes-2003-16
Backdoor.Lala.C	C	CyberNotes-2003-16
Backdoor.Lanfilt.B	B	CyberNotes-2003-14
Backdoor.Lassrv	N/A	CyberNotes-2003-21
Backdoor.Lastras	N/A	CyberNotes-2003-17
Backdoor.LeGuardien.B	B	CyberNotes-2003-10
Backdoor.Litmus.203.c	c	CyberNotes-2003-09
Backdoor.LittleWitch.C	C	CyberNotes-2003-06
Backdoor.Lixy	N/A	CyberNotes-2003-21
Backdoor.Lixy.B	B	CyberNotes-2003-22
Backdoor.Longnu	N/A	CyberNotes-2003-06
Backdoor.Lorac	N/A	CyberNotes-2003-17
Backdoor.Madfind	N/A	CyberNotes-2003-23
Backdoor.Marotob	N/A	CyberNotes-2003-06
Backdoor.Massaker	N/A	CyberNotes-2003-02

Trojan	Version	CyberNotes Issue #
Backdoor.MeteorShell	N/A	CyberNotes-2003-21
Backdoor.MindControl	N/A	CyberNotes-2003-14
Backdoor.Monator	N/A	CyberNotes-2003-08
Backdoor.Mots	N/A	CyberNotes-2003-11
Backdoor.Mprox	N/A	CyberNotes-2003-20
Backdoor.MSNCorrupt	N/A	CyberNotes-2003-06
Backdoor.Mxsender	N/A	CyberNotes-2003-21
Backdoor.Netdevil.15	15	CyberNotes-2003-15
Backdoor.NetDevil.B	B	CyberNotes-2003-01
Backdoor.NetTrojan	N/A	CyberNotes-2003-01
Backdoor.Nibu	N/A	CyberNotes-2003-16
Backdoor.Nickser	N?A	CyberNotes-2003-14
Backdoor.Ohpass	N/A	CyberNotes-2003-01
Backdoor.OICQSer.165	N/A	CyberNotes-2003-01
Backdoor.OICQSer.17	17	CyberNotes-2003-01
Backdoor.Omygo	N/A	CyberNotes-2003-19
Backdoor.Optix.04.d	04.d	CyberNotes-2003-04
Backdoor.OptixDDoS	N/A	CyberNotes-2003-07
Backdoor.OptixPro.10.c	10.c	CyberNotes-2003-01
Backdoor.OptixPro.12.b	12.b	CyberNotes-2003-07
Backdoor.OptixPro.13	13	CyberNotes-2003-09
Backdoor.Peeper	N/A	CyberNotes-2003-20
Backdoor.Peers	N/A	CyberNotes-2003-10
Backdoor.Plux	N/A	CyberNotes-2003-05
Backdoor.Pointex	N/A	CyberNotes-2003-09
Backdoor.Pointex.B	B	CyberNotes-2003-09
Backdoor.Private	N/A	CyberNotes-2003-11
Backdoor.Prorat	N/A	CyberNotes-2003-13
Backdoor.PSpider.310	310	CyberNotes-2003-05
Backdoor.Pspider.310.b	310.b	CyberNotes-2003-18
Backdoor.Queen	N/A	CyberNotes-2003-06
Backdoor.Rado	N/A	CyberNotes-2003-18
Backdoor.Ranck	N/A	CyberNotes-2003-18
Backdoor.Ranck.C	C	CyberNotes-2003-22
Backdoor.Ratega	N/A	CyberNotes-2003-09
Backdoor.Recerv	N/A	CyberNotes-2003-09
Backdoor.Redkod	N/A	CyberNotes-2003-05
Backdoor.Remocy	N/A	CyberNotes-2003-22
Backdoor.Remohak.16	16	CyberNotes-2003-01
Backdoor.RemoteSOB	N/A	CyberNotes-2003-01
Backdoor.Rephlex	N/A	CyberNotes-2003-01
Backdoor.Roxy	N/A	CyberNotes-2003-16
Backdoor.Roxy.B	B	CyberNotes-2003-20
Backdoor.RPCBot.E	E	CyberNotes-2003-19
Backdoor.Rsbot	N/A	CyberNotes-2003-07
Backdoor.SchoolBus.B	B	CyberNotes-2003-04
Backdoor.Sdbot.C	C	CyberNotes-2003-02
Backdoor.Sdbot.D	D	CyberNotes-2003-03
Backdoor.Sdbot.E	E	CyberNotes-2003-06

Trojan	Version	CyberNotes Issue #
Backdoor.Sdbot.F	F	CyberNotes-2003-07
Backdoor.Sdbot.G	G	CyberNotes-2003-08
Backdoor.Sdbot.H	H	CyberNotes-2003-09
Backdoor.Sdbot.L	L	CyberNotes-2003-11
Backdoor.Sdbot.M	M	CyberNotes-2003-13
Backdoor.Sdbot.P	P	CyberNotes-2003-17
Backdoor.SDBot.Q	Q	CyberNotes-2003-21
Backdoor.Sdbot.R	R	CyberNotes-2003-21
Backdoor.Semes	N/A	CyberNotes-2003-20
Backdoor.Serpa	N/A	CyberNotes-2003-03
Backdoor.Servsax	N/A	CyberNotes-2003-01
Backdoor.Sheldor	N/A	CyberNotes-2003-18
Backdoor.SilverFTP	N/A	CyberNotes-2003-04
Backdoor.Simali	N/A	CyberNotes-2003-09
Backdoor.Sincom	N/A	CyberNotes-2003-21
Backdoor.Sinit	N/A	CyberNotes-2003-21
Backdoor.Sixca	N/A	CyberNotes-2003-01
Backdoor.Slao	N/A	CyberNotes-2003-11
Backdoor.Smokodoor	N/A	CyberNotes-2003-21
Backdoor.Smother	N/A	CyberNotes-2003-20
Backdoor.Snami	N/A	CyberNotes-2003-10
Backdoor.Snowdoor	N/A	CyberNotes-2003-04
Backdoor.Socksbot	N/A	CyberNotes-2003-06
Backdoor.Softshell	N/A	CyberNotes-2003-10
Backdoor.Sokacaps	N/A	CyberNotes-2003-18
Backdoor.Spotcom	N/A	Current Issue
Backdoor.Stealer	N/A	CyberNotes-2003-14
Backdoor.SubSari.15	15	CyberNotes-2003-05
Backdoor.SubSeven.2.15	2.15	CyberNotes-2003-05
Backdoor.Sumtax	N/A	CyberNotes-2003-16
Backdoor.Surdux	N/A	CyberNotes-2003-20
Backdoor.Syskbot	N/A	CyberNotes-2003-08
Backdoor.SysXXX	N/A	CyberNotes-2003-06
Backdoor.Talex	N/A	CyberNotes-2003-02
Backdoor.Tankedoor	N/A	CyberNotes-2003-07
Backdoor.Tinydog	N/A	Current Issue
Backdoor.Translat	N/A	CyberNotes-2003-20
Backdoor.Trynoma	N/A	CyberNotes-2003-08
Backdoor.Turkojan	N/A	CyberNotes-2003-07
Backdoor.Udps.10	1	CyberNotes-2003-03
Backdoor.UKS	N/A	CyberNotes-2003-11
Backdoor.Unifida	N/A	CyberNotes-2003-05
Backdoor.Upfudoor	N/A	CyberNotes-2003-01
Backdoor.Urat.b	b	CyberNotes-2003-18
Backdoor.Usirf	N/A	CyberNotes-2003-21
Backdoor.Uzbet	N/A	CyberNotes-2003-15
Backdoor.VagrNocker	N/A	CyberNotes-2003-01
Backdoor.Vmz	N/A	CyberNotes-2003-01
Backdoor.Winet	N/A	CyberNotes-2003-11

Trojan	Version	CyberNotes Issue #
Backdoor.WinJank	N/A	CyberNotes-2003-15
Backdoor.Winker	N/A	CyberNotes-2003-15
Backdoor.WinShell.50	N/A	CyberNotes-2003-16
Backdoor.Wolf.16	16	CyberNotes-2003-18
Backdoor.Xenozbot	N/A	CyberNotes-2003-01
Backdoor.Xeory	N/A	CyberNotes-2003-03
Backdoor.XTS	N/A	CyberNotes-2003-08
Backdoor.Zdemon	N/A	CyberNotes-2003-02
Backdoor.Zdemon.126	126	CyberNotes-2003-10
Backdoor.Zdown	N/A	CyberNotes-2003-05
Backdoor.Zinx	N/A	CyberNotes-2003-23
Backdoor.Zix	N/A	CyberNotes-2003-02
Backdoor.Zombam	N/A	CyberNotes-2003-08
Backdoor.Zombam.B	B	CyberNotes-2003-20
Backdoor.Zvrop	N/A	CyberNotes-2003-03
Backdoor-AFC	N/A	CyberNotes-2003-05
Backdoor-AOK	N/A	CyberNotes-2003-01
BackDoor-AQL	N/A	CyberNotes-2003-05
BackDoor-AQT	N/A	CyberNotes-2003-05
BackDoor-ARR	ARR	CyberNotes-2003-06
Backdoor-ARU	ARU	CyberNotes-2003-06
BackDoor-ARX	ARX	CyberNotes-2003-06
BackDoor-ARY	ARY	CyberNotes-2003-06
BackDoor-ASD	ASD	CyberNotes-2003-07
BackDoor-ASL	ASL	CyberNotes-2003-07
BackDoor-ASW	ASW	CyberNotes-2003-08
BackDoor-ATG	ATG	CyberNotes-2003-09
BackDoor-ATM.gen	N/A	Current Issue
BackDoor-AUP	N/A	CyberNotes-2003-11
BackDoor-AVF	AVF	CyberNotes-2003-12
BackDoor-AVH	AVH	CyberNotes-2003-12
BackDoor-AVO	AVO	CyberNotes-2003-12
BackDoor-AXC	AXC	CyberNotes-2003-14
BackDoor-AXQ	AXQ	CyberNotes-2003-15
Backdoor-AXR	AXR	CyberNotes-2003-16
Backdoor-AZF	AZF	CyberNotes-2003-20
BackDoor-BAE	BAE	CyberNotes-2003-21
BackDoor-BBO	BBO	CyberNotes-2003-22
BDS/AntiPC	N/A	CyberNotes-2003-02
BDS/Backstab	N/A	CyberNotes-2003-02
BDS/CheckESP	N/A	CyberNotes-2003-12
BDS/Ciadoor.10	10	CyberNotes-2003-07
BDS/Evilbot.A	A	CyberNotes-2003-09
BDS/Evolut	N/A	CyberNotes-2003-03
BDS/GrayBird.G	G	CyberNotes-2003-17
BDS/IRCBot.82779	82779	CyberNotes-2003-23
BDS/PowerSpider.A	A	CyberNotes-2003-11
BDS/SdBot.76870	76870	CyberNotes-2003-21

Trojan	Version	CyberNotes Issue #
BKDR_LITH.103.A	A	CyberNotes-2003-17
Cardown	N/A	CyberNotes-2003-19
CoolFool	N/A	CyberNotes-2003-17
Daysun	N/A	CyberNotes-2003-06
DDoS-Stinkbot	N/A	CyberNotes-2003-08
Delude	N/A	CyberNotes-2003-19
Desex	N/A	CyberNotes-2003-20
DoS-iFrameNet	N/A	CyberNotes-2003-04
Download.Aduent.Trojan	N/A	CyberNotes-2003-18
Download.Magicon	N/A	CyberNotes-2003-22
Download.Trojan.B	B	CyberNotes-2003-13
Downloader.BO.B	B	CyberNotes-2003-10
Downloader.BO.B.dr	B.dr	CyberNotes-2003-10
Downloader.Dluca	N/A	CyberNotes-2003-17
Downloader.Dluca.B	B	CyberNotes-2003-19
Downloader.Dluca.C	C	CyberNotes-2003-20
Downloader.Dluca.D	D	CyberNotes-2003-22
Downloader.Mimail	N/A	CyberNotes-2003-16
Downloader.Slime	N/A	CyberNotes-2003-21
Downloader.Tooncom	N/A	CyberNotes-2003-22
Downloader-BN.b	BN.b	CyberNotes-2003-13
Downloader-BO.dr.b	N/A	CyberNotes-2003-02
Downloader-BS	N/A	CyberNotes-2003-02
Downloader-BW	N/A	CyberNotes-2003-05
Downloader-BW.b	BW.b	CyberNotes-2003-06
Downloader-BW.c	BW.c	CyberNotes-2003-07
Downloader-BW.h	BW.h	CyberNotes-2003-23
Downloader-CY	CY	CyberNotes-2003-16
Downloader-DM	DM	CyberNotes-2003-16
Downloader-DN.b	DN.b	CyberNotes-2003-17
Downloader-EB	EB	CyberNotes-2003-18
DownLoader-EG	EG	CyberNotes-2003-20
Downloader-ES	ES	CyberNotes-2003-22
Downloader-EU	EU	CyberNotes-2003-22
Downloader-EV	EV	CyberNotes-2003-22
ELF_TYPOT.A	A	CyberNotes-2003-13
ELF_TYPOT.B	B	CyberNotes-2003-13
Enocider	N/A	CyberNotes-2003-22
Exploit-IISInjector	N/A	CyberNotes-2003-03
Gpix	N/A	CyberNotes-2003-08
Hacktool.Keystal	N/A	CyberNotes-2003-19
Hacktool.PWS.QQPass	N/A	CyberNotes-2003-06
ICQPager-J	N/A	CyberNotes-2003-05
IgetNet.dr	dr	CyberNotes-2003-21
IRC.Trojan.Fgt	Fgt	CyberNotes-2003-22
IRC/Backdoor.e	E	CyberNotes-2003-01
IRC/Backdoor.f	f	CyberNotes-2003-02
IRC/Backdoor.g	g	CyberNotes-2003-03
IRC/Flood.ap	N/A	CyberNotes-2003-05

Trojan	Version	CyberNotes Issue #
IRC/Flood.bi	N/A	CyberNotes-2003-03
IRC/Flood.br	br	CyberNotes-2003-06
IRC/Flood.bu	bu	CyberNotes-2003-08
IRC/Flood.cd	cd	CyberNotes-2003-11
IRC/Flood.cm	cm	CyberNotes-2003-13
IRC/Fyle	N/A	CyberNotes-2003-16
IRC-BBot	N/A	CyberNotes-2003-16
IRC-Emoz	N/A	CyberNotes-2003-03
IRC-OhShootBot	N/A	CyberNotes-2003-01
IRC-Vup	N/A	CyberNotes-2003-09
JS.Fortnight.B	B	CyberNotes-2003-06
JS.Fortnight.D	D	CyberNotes-2003-22
JS.Seeker.J	J	CyberNotes-2003-01
JS.Seeker.K	K	CyberNotes-2003-20
JS/Fortnight.c@M	c	CyberNotes-2003-11
JS/Seeker-C	C	CyberNotes-2003-04
JS/StartPage.dr	dr	CyberNotes-2003-11
JS_WEBLOG.A	A	CyberNotes-2003-05
Keylogger.Cone.Trojan	N/A	CyberNotes-2003-14
KeyLog-Kerlib	N/A	CyberNotes-2003-05
Keylog-Keylf	N/A	CyberNotes-2003-17
Keylog-Kjie	N/A	CyberNotes-2003-12
Keylog-Mico	N/A	CyberNotes-2003-20
Keylog-Perfect.dr	dr	CyberNotes-2003-09
Keylog-Razytimer	N/A	CyberNotes-2003-03
KeyLog-TweakPan	N/A	CyberNotes-2003-02
Keylog-Yeehah	N/A	CyberNotes-2003-12
Linux/DDoS-Ferlect	N/A	CyberNotes-2003-17
Linux/Exploit-SendMail	N/A	CyberNotes-2003-05
Lockme	N/A	CyberNotes-2003-15
MouseLog-Ladora	N/A	CyberNotes-2003-22
MultiDropper-FD	N/A	CyberNotes-2003-01
OF97/ExeDrop-B	N/A	CyberNotes-2003-19
Pac	N/A	CyberNotes-2003-04
Petala	N/A	CyberNotes-2003-20
PHP.Rumaz.Trojan	N/A	CyberNotes-2003-23
ProcKill-AE	N/A	CyberNotes-2003-05
ProcKill-AF	N/A	CyberNotes-2003-05
ProcKill-AH	AH	CyberNotes-2003-08
ProcKill-AJ	AJ	CyberNotes-2003-13
ProcKill-Z	N/A	CyberNotes-2003-03
Proxy-Guzu	N/A	CyberNotes-2003-08
Proxy-Migmaf	N/A	CyberNotes-2003-14
Proxy-Regate	N/A	CyberNotes-2003-22
PWS-Aileen	N/A	CyberNotes-2003-04
PWS-Bugmaf	N/A	CyberNotes-2003-21
PWS-Mob	N/A	CyberNotes-2003-22
PWS-Moneykeeper	N/A	CyberNotes-2003-18
PWS-Sincom.dr	dr	CyberNotes-2003-17

Trojan	Version	CyberNotes Issue #
PWSteal.ABCHlp	N/A	CyberNotes-2003-12
PWSteal.ALight	N/A	CyberNotes-2003-01
PWSteal.Bancos	N/A	CyberNotes-2003-15
PWSteal.Bancos.B	B	CyberNotes-2003-16
PWSteal.Bancos.C	C	CyberNotes-2003-22
PWSteal.Banpaes	N/A	CyberNotes-2003-21
PWSteal.Banpaes.B	B	Current Issue
PWSteal.Finero	N/A	CyberNotes-2003-21
PWSteal.Firum	N/A	CyberNotes-2003-22
PWSteal.Hukle	N/A	CyberNotes-2003-08
PWSteal.Kipper	N/A	CyberNotes-2003-10
PWSteal.Ldpinch	N/A	CyberNotes-2003-23
PWSteal.Lemir.105	105	CyberNotes-2003-10
PWSteal.Lemir.C	C	CyberNotes-2003-17
PWSteal.Lemir.D	D	CyberNotes-2003-18
PWSteal.Lemir.E	E	CyberNotes-2003-20
PWSteal.Lemir.F	F	CyberNotes-2003-20
PWSteal.Nikana	N/A	CyberNotes-2003-21
PWSteal.Reanet	N/A	CyberNotes-2003-21
PWSteal.Rimd	N/A	CyberNotes-2003-01
PWSteal.Rimd.B	B	CyberNotes-2003-10
PWSteal.Salira	N/A	CyberNotes-2003-21
PWSteal.Senhas	N/A	CyberNotes-2003-03
PWSteal.Snatch	N/A	CyberNotes-2003-10
PWSteal.Sysrater	N/A	CyberNotes-2003-12
PWSteal.Tarno	N/A	CyberNotes-2003-22
PWS-Tenbot	N/A	CyberNotes-2003-01
PWS-Train	N/A	CyberNotes-2003-17
PWS-Truebf	N/A	CyberNotes-2003-13
PWS-Watsn	N/A	CyberNotes-2003-10
PWS-Wexd	N/A	CyberNotes-2003-14
PWS-WMPatch	N/A	CyberNotes-2003-07
PWS-Yipper	N/A	CyberNotes-2003-10
QDel359	359	CyberNotes-2003-01
QDel373	373	CyberNotes-2003-06
Qdel374	374	CyberNotes-2003-06
Qdel375	375	CyberNotes-2003-06
Qdel376	376	CyberNotes-2003-07
QDel378	378	CyberNotes-2003-08
QDel379	369	CyberNotes-2003-09
QDel390	390	CyberNotes-2003-13
QDel391	391	CyberNotes-2003-13
QDel392	392	CyberNotes-2003-13
QDial11	1	CyberNotes-2003-14
QDial15	15	CyberNotes-2003-22
QDial6	6	CyberNotes-2003-11
Renamer.c	N/A	CyberNotes-2003-03
Reom.Trojan	N/A	CyberNotes-2003-08
StartPage-G	G	CyberNotes-2003-06

Trojan	Version	CyberNotes Issue #
Startpage-N	N	CyberNotes-2003-13
StartPage-U	U	CyberNotes-2003-20
StartPage-W	W	CyberNotes-2003-22
Stash	N/A	CyberNotes-2003-23
Stealthther	N/A	CyberNotes-2003-16
Stoplete	N/A	CyberNotes-2003-06
Swizzor	N/A	CyberNotes-2003-07
Tellafriend.Trojan	N/A	CyberNotes-2003-04
Tr/Decept.21	21	CyberNotes-2003-07
Tr/Delf.r	r	CyberNotes-2003-16
Tr/DelWinbootdir	N/A	CyberNotes-2003-07
TR/Fake.YaHoMe.1	N/A	CyberNotes-2003-02
TR/Gaslide.C	C	CyberNotes-2003-17
Tr/SpBit.A	A	CyberNotes-2003-04
Tr/VB.t	T	CyberNotes-2003-11
TR/WinMx	N/A	CyberNotes-2003-02
Troj/Apdoor-A	A	CyberNotes-2003-19
Troj/Ataka-E	E	CyberNotes-2003-15
Troj/Autoroot-A	A	CyberNotes-2003-16
Troj/Backsm-A	A	CyberNotes-2003-19
Troj/Bdoor-AAG	AAG	CyberNotes-2003-21
Troj/Bdoor-RQ	RQ	CyberNotes-2003-17
Troj/CoreFloo-C	C	CyberNotes-2003-22
Troj/Dloader-BO	BO	CyberNotes-2003-02
Troj/DownLdr-DI	DI	CyberNotes-2003-15
Troj/Eyeveg-A	A	CyberNotes-2003-19
Troj/Golon-A	A	CyberNotes-2003-15
Troj/HacDef-084	N/A	Current Issue
Troj/Hackarmy-A	A	CyberNotes-2003-20
Troj/Hacline-B	B	CyberNotes-2003-13
Troj/IRCBot-C	C	CyberNotes-2003-11
Troj/Ircbot-M	M	CyberNotes-2003-21
Troj/IRCBot-P	P	CyberNotes-2003-22
Troj/Litmus-AS	AS	Current Issue
Troj/Manifest-A	N/A	CyberNotes-2003-03
Troj/Migmaf-A	A	CyberNotes-2003-15
Troj/Mystri-A	A	CyberNotes-2003-13
Troj/PcGhost-A	A	CyberNotes-2003-13
Troj/Peido-B	B	CyberNotes-2003-10
Troj/Qhosts-1	N/A	CyberNotes-2003-20
Troj/QQPass-A	A	CyberNotes-2003-16
Troj/Qzap-248	N/A	CyberNotes-2003-01
Troj/SadHound-A	N/A	CyberNotes-2003-03
Troj/Sandesa-A	A	CyberNotes-2003-14
Troj/Slacker-A	A	CyberNotes-2003-05
Troj/Slanret-A	N/A	CyberNotes-2003-03
Troj/Sysbug-A	A	Current Issue
Troj/TKBot-A	A	CyberNotes-2003-04

Trojan	Version	CyberNotes Issue #
Troj/Tofger-A	A	Current Issue
Troj/Webber-A	A	CyberNotes-2003-15
Troj/Webber-C	C	CyberNotes-2003-23
TROJ_JBELLZ.A	A	CyberNotes-2003-02
TROJ_KILLBOOT.B	B	CyberNotes-2003-01
TROJ_RACKUM.A	A	CyberNotes-2003-05
Trojan.Abaxo	N/A	CyberNotes-2003-20
Trojan.Ailati	N/A	CyberNotes-2003-15
Trojan.Analogx	N/A	CyberNotes-2003-17
Trojan.Androv	N/A	CyberNotes-2003-23
Trojan.AprilFool	N/A	CyberNotes-2003-08
Trojan.Barjac	N/A	CyberNotes-2003-05
Trojan.Bedrill	N/A	CyberNotes-2003-23
Trojan.Bootconf	N/A	CyberNotes-2003-21
Trojan.Boxer	N/A	CyberNotes-2003-19
Trojan.Cuydoc	N/A	CyberNotes-2003-21
Trojan.Dasmin	N/A	CyberNotes-2003-01
Trojan.Dasmin.B	B	CyberNotes-2003-03
Trojan.Downloader.Aphe	N/A	CyberNotes-2003-06
Trojan.Downloader.Inor	N/A	CyberNotes-2003-02
Trojan.Fwin	N/A	CyberNotes-2003-18
Trojan.Gaslide.Intd	N/A	CyberNotes-2003-20
Trojan.Grepape	N/A	CyberNotes-2003-05
Trojan.Guapeton	N/A	CyberNotes-2003-08
Trojan.Idly	N/A	CyberNotes-2003-04
Trojan.Ivanet	N/A	CyberNotes-2003-02
Trojan.Kaht	N/A	CyberNotes-2003-10
Trojan.Kalshi	N/A	CyberNotes-2003-21
Trojan.KillAV.B	B	CyberNotes-2003-19
Trojan.KillAV.C	C	CyberNotes-2003-23
Trojan.KKiller	N/A	CyberNotes-2003-01
Trojan.Lear	N/A	CyberNotes-2003-10
Trojan.Loome	N/A	CyberNotes-2003-22
Trojan.Mumuboy	N/A	CyberNotes-2003-13
Trojan.Mumuboy.B	B	CyberNotes-2003-20
Trojan.Myet	N/A	CyberNotes-2003-12
Trojan.Myss.B	B	CyberNotes-2003-21
Trojan.Naldem	N/A	CyberNotes-2003-23
Trojan.Norio	N/A	CyberNotes-2003-19
Trojan.Obsorb	N/A	CyberNotes-2003-22
Trojan.OptixKiller	N/A	CyberNotes-2003-16
Trojan.Poetas	N/A	CyberNotes-2003-14
Trojan.Poldo.B	B	CyberNotes-2003-02
Trojan.Poot	N/A	CyberNotes-2003-05
Trojan.PopSpy	N/A	CyberNotes-2003-11
Trojan.Progent	N/A	CyberNotes-2003-16
Trojan.ProteBoy	N/A	CyberNotes-2003-04
Trojan.PSW.Gip	N/A	CyberNotes-2003-06

Trojan	Version	CyberNotes Issue #
Trojan.PSW.Platan.5.A	N/A	CyberNotes-2003-01
Trojan.PWS.QQPass.D	N/A	CyberNotes-2003-02
Trojan.PWS.QQPass.E	E	CyberNotes-2003-20
Trojan.Qforager	N/A	CyberNotes-2003-02
Trojan.Qforager.Dr	N/A	CyberNotes-2003-02
Trojan.Qwe	N/A	CyberNotes-2003-02
Trojan.Retsam	N/A	CyberNotes-2003-22
Trojan.Sarka	N/A	CyberNotes-2003-14
Trojan.Sidea	N/A	CyberNotes-2003-12
Trojan.Sinkin	N/A	CyberNotes-2003-21
Trojan.Snag	N/A	CyberNotes-2003-02
Trojan.Unblockee	N/A	CyberNotes-2003-01
Trojan.Vardo	N/A	CyberNotes-2003-20
Trojan.Visages	N/A	CyberNotes-2003-15
Trojan.Windelete	N/A	CyberNotes-2003-14
Trojan.Gaslid	N/A	CyberNotes-2003-18
Uploader-D	D	CyberNotes-2003-06
Uploader-D.b	D.b	CyberNotes-2003-07
VBS.Bootconf	N/A	CyberNotes-2003-23
VBS.ExitWin	N/A	CyberNotes-2003-12
VBS.Flipe	N/A	CyberNotes-2003-17
VBS.Kasnar	N/A	CyberNotes-2003-06
VBS.Moon.B	B	CyberNotes-2003-02
VBS.Noex.Trojan	N/A	CyberNotes-2003-23
VBS.StartPage	N/A	CyberNotes-2003-02
VBS.Trojan.Lovcx	N/A	CyberNotes-2003-05
VBS.Zizarn	N/A	CyberNotes-2003-09
VBS/Fourcourse	N/A	CyberNotes-2003-06
W32.Adclicker.C.Trojan	C	CyberNotes-2003-09
W32.Adclicker.G.Trojan	G	CyberNotes-2003-22
W32.Bambo	N/A	CyberNotes-2003-14
W32.Benpao.Trojan	N/A	CyberNotes-2003-04
W32.CVIH.Trojan	N/A	CyberNotes-2003-06
W32.Hostidel.Trojan	N/A	Current Issue
W32.Hostidel.Trojan.B	B	Current Issue
W32.Laorenshen.Trojan	N/A	CyberNotes-2003-14
W32.Noops.Trojan	N/A	CyberNotes-2003-09
W32.Petch.B	B	CyberNotes-2003-23
W32.Socay.Worm	N/A	CyberNotes-2003-02
W32.Spybot.dr	dr	CyberNotes-2003-15
W32.Systemtry.Trojan	N/A	CyberNotes-2003-03
W32.Tofazzol	N/A	CyberNotes-2003-22
W32.Trabajo	N/A	CyberNotes-2003-14
W32.Xilon.Trojan	N/A	CyberNotes-2003-01
W32.Yinker.Trojan	N/A	CyberNotes-2003-04
W32/Igloo-15	N/A	CyberNotes-2003-04
W97M.Tabi.Trojan	N/A	CyberNotes-2003-20
Woodcot	N/A	CyberNotes-2003-16
X97M.Sysbin	N/A	CyberNotes-2003-22

Trojan	Version	CyberNotes Issue #
Xin	N/A	CyberNotes-2003-03

Backdoor.Asoxy: This is a Trojan horse that runs as a proxy server. When Backdoor.Asoxy runs, it copies itself as %System%\MCP<random 4 characters>.exe and opens two randomly chosen ports.

Backdoor..Asoxy adds the value, "ieupdate" = %System%\MCP<random 4 characters>.exe, to the registry key:

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

so that the Trojan runs when you start Windows. It also attempts to connect to a predetermined IP address and alert the malicious user of the IP address and open ports on the infected computer.

BackDoor-ATM.gen (Alias: Backdoor.Padmin): This is a generic detection for a remote access Trojan written in Visual Basic. As this description is meant to be generic, filenames and registry keys may differ.

Backdoor.Ciador.B (Aliases: Backdoor.Ciador.12.b, Backdoor-ASB): This is a Trojan Horse that gives unauthorized access to a compromised computer. When Backdoor.Ciador.B is executed, it copies itself as %Windir%\Spoolsv.exe, with attributes set to hidden and add a value, "Print Spooler" = Windir%\Spoolsv.exe, to the following registry keys:

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

The Trojan registers itself as a process and adds the following lines to the [windows] section of the Win.ini file:

- load=%Windir%\Spoolsv.exe
- run=%Windir%\Spoolsv.exe

It modifies the [boot] section of the System.ini file to look similar to, "shell=Explorer.exe %Windir%\Spoolsv.exe" and opens a port and listens for commands from the malicious user. The default port is 1987.

Backdoor.IRC.Whisper: This is a backdoor Trojan Horse that allows a malicious user to use IRC to remotely control your computer. It is written in Delphi and usually packed with ASPack. Upon execution Backdoor.IRC.Whisper adds the value, "Network Host Controller" = "<path to Trojan>," to the registry key

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

It attempts to connect to a predetermined Web site and requests a file, start2.txt. However, the HTTP request has been specially crafted to accept a large range of files. If an executable file is passed back to the infected computer, the Trojan then attempts to execute the file. The Trojan connects to a predetermined IRC server and waits for further instructions from a malicious user on the IRC channel.

Backdoor.Spotcom: This is a Backdoor Trojan Horse that injects itself into Internet Explorer. When the installer for Backdoor.Spotcom is executed, it creates the following files in the %System% folder:

- msrsvp.exe
- olegui.dll

It runs a hidden instance of Internet Explorer (IExplore.exe) and injects olegui.dll into the process as a thread. This action allows the Trojan to access the Internet, appearing as though Internet Explorer was making the outgoing connection and attempts to contact a predetermined IP address on UDP port 53. It also modifies the value, "ImagePath" = "%SYSTEM%\msrsvp.exe," in the registry key:

- HKEY_LOCAL_MACHINE\System\Services\RSVP

which adds the Trojan to the OS services as "QoS RSVP," replacing the legitimate service, if it exists.

Backdoor.Spotcom accepts backdoor commands from the IP address, including opening a command prompt with administrative access on an arbitrary port and logs all the created and deleted files on all the drives, which the author of the Trojan can retrieve.

Backdoor.Tinydog: This is a Backdoor Trojan Horse that creates a remote shell on your system. It is based on the open source project for TinyShell. In addition to standard remote shell functionality, Backdoor.Tinydog also recognizes a hidden password. When Backdoor.Tinydog is executed, it opens a listening port, as the malicious user specifies. Backdoor.Tinydog will accept connections through this port as long as the connecting party supplies the correct password, which the malicious user also supplies. In addition to the user-supplied password, Backdoor.Tinydog also recognizes a hard-coded password, which the creator of the remote shell program placed there. The Trojan launches cmd.exe with a hidden window, which it will redirect all future send/receive requests of that connection. It allows the remote user the same access as a logged-on user, as it is a remote shell program. For example, making FTP connections, execute programs, delete files, and so on.

PWSteal.Banpaes.B: This is a Trojan Horse that attempts to steal online banking information. The Trojan is written in the Delphi language and is packed with UPX. When PWSteal.Banpaes.B is executed, it creates the following files:

- %Windir%\Wmsys32.exe
- %Windir%\Syshook.dll
- %Windir%\Syskeybrd.dll

The Trojan adds the value, "wmsys32"="%Windows%\wmsys32.exe," to the registry key:

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

so that PWSteal.Banpaes.B runs when you start Windows. It logs keystrokes with various strings in the title, and then sends them to a predetermined e-mail address.

Troj/HacDef-084 (Aliases: Backdoor.Hacdef.084, Backdoor.HackDefender, BKDR_HACDEF.C): This Trojan has been reported in the wild. It is backdoor Trojan that is targeted at NT/2000/XP operating systems. As well as allowing unauthorized remote access to the victim's computer, it is also able to hide information about the victim's system including files, folders, processes, services and registry entries.

Troj/Litmus-AS (Aliases: Backdoor.Litmus.203, BackDoor-JZ, Win32/Litmus.203.AsPack, Backdoor.Litmus.203.b): This Trojan has been reported in the wild. It is a backdoor Trojan that runs in the background as a system process and allows unauthorized remote access to the computer via an IRC network connection. The Trojan copies itself to C:\Windows\Server as svchost.EXE and adds an entry to the registry at HKCU\Software\Microsoft\Windows\CurrentVersion\Run\LTM2 to run itself on system restart. The Trojan may also attempt to steal passwords.

Troj/Sysbug-A (Aliases: Backdoor-CAG, Backdoor.Sysbug, TrojanSpy.Win32.Sysbug, TR/Sysbug.A1, Trj/Sysbug.A, Trojan.PWS.Sysbug.A, TROJ_SYDEB.A, Win32.PSW.LdPinch.G): This Trojan has been reported in the wild. It is a Trojan that retrieves system information and allows unauthorized access to the compromised computer. This Trojan horse has been distributed in the form of an e-mail with the following characteristics:

- From: james2003@hotmail.com
- Subject line: Re[2]: Mary
- Attached file: Private.zip (contains wendynaked.jpg.exe)

Troj/Sysbug-A will copy itself to the Windows folder as sysdeb32.exe and adds the following registry entry to ensure it gets run at system logon:

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

It creates the files svc.sav in the Windows folder and C:\temp35.txt. These files are not malicious and can simply be deleted.

Troj/Tofger-A (Aliases: MultiDropper-GP.a, TrojanDropper.JS.Mimail.b, Trojan.Sefex): This is a keylogging Trojan. In order to run automatically when Windows starts up the Trojan copies itself to the file system.exe in the Windows folder and adds the following registry entry pointing to this file:

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

The Trojan also drops the utility library file msin32.dll and creates the text file sysini.ini in the Windows folder. When the Trojan detects an active Internet connection it captures keystrokes typed into Internet Explorer and sends the information to a remote Internet address. Troj/Tofger-A is spread as an e-mail

attachment MyProfile.zip. The ZIP archive contains a HTML page Profile.html that uses the codebase and MHTML vulnerabilities in Internet Explorer and Outlook/Outlook Express to drop and execute the Trojan binary automatically as the file \dating.exe. For more information please see the Microsoft security bulletins MS02-015 and MS02-014.

W32.Hostidel.Trojan: This is a Trojan horse that overwrites the Windows Hosts files, which are used for name resolution. It also modifies the Windows registry to change the Internet Explorer home page and the default search page in Internet Explorer.

W32.Hostidel.Trojan.B: This is a variant of W32.Hostidel.Trojan that overwrites the Windows Hosts files. The Trojan also changes the Internet Explorer home page and search page and drops Backdoor.Daemonize in the %System% folder.