



Department of Homeland Security

Information Analysis and Infrastructure Protection

Directorate CyberNotes

Issue #2003-11

June 2, 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 NIPC 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 May 14 and May 30, 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
access-remote-pc.com ¹	Windows	Remote PC Access 2.2	A Denial of Service vulnerability exists when a malicious user submits a spoofed client authorization code to the target server.	Upgrade available at: http://www.access-remote-pc.com/download.shtm
AMAX Information Technologies Inc. ²	Windows	Magic Winmail Server 2.3	A remote Denial of Service vulnerability exists due to insufficient validation of user-supplied input to the 'USER' and 'PASS' commands.	No workaround or patch available at time of publishing.

¹ SecurityFocus, May 26, 2003.

² Damage Hacking Group Security Advisory, May 23, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts
AnalogX ³	Windows, Unix	Proxy 4.13	A buffer overflow vulnerability exists due to insufficient bounds checking of client-supplied URIs, which could let a malicious user execute arbitrary code.	Upgrade available at: http://www.analogx.com/contents/download/network/proxy.htm
Apple ⁴	Unix	Darwin Streaming Server 4.1.3, Quicktime Streaming Server 4.1.3	A vulnerability exists in the 'QTSSReflector' module when the ANNOUNCE command is processed, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.
Apple ⁵	MacOS X 10.x	MacOS X 10.0-10.0.4, 10.1-10.1.5, 10.2-10.2.5, MacOS X Server 10.0, 10.2-10.2.5	A vulnerability exists when IPSec is enabled because some types of traffic are not handled properly, which could let a malicious user obtain unauthorized access.	Upgrade available at: http://www.apple.com/macosx/
Apple ⁶	Unix	Quicktime MP3 Broadcaster	A vulnerability exists because UD3 tags in MP3 files are not properly parsed, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.
ArGoSoft ⁷	Multiple	Mail Server FreeWare 1.8.2.6, 1.8.3.4	Several vulnerabilities exist: a vulnerability exists due to insufficient authentication in the user management interface, which could let a malicious user obtain sensitive information; and a remote Denial of Service vulnerability exists when a malicious user attempts to create a new user using an excessively long name.	No workaround or patch available at time of publishing.

³ NII Advisory, May 26, 2003.

⁴ @(#)Security Advisory, May 22, 2003.

⁵ Apple Security Update, 61798, May 16, 2003.

⁶ @(#)Security Advisory, May 22, 2003.

⁷ SecurityFocus, May 15, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts
<p>AStArt Technologies⁸</p> <p><i>RedHat issues advisory⁹</i></p> <p><i>More advisories issued^{10, 11}</i></p>	Unix	LPRng 3.8.10 .1	A vulnerability exists in the 'psbanner' filter because temporary files for debugging purposes are created insecurely, which could let a malicious user obtain elevated privileges.	<p>Debian: http://security.debian.org/pool/updates/main/l/lprng/</p> <p>RedHat: ftp://updates.redhat.com</p> <p>Mandrake: http://www.mandrakesecure.net/en/ftp.php</p>
Axis Communications ¹²	Multiple	2100 Network Camera 2.30-2.32, 2110 Network Camera 2.30-2.32, 2120 Network Camera 2.30-2.32, 2130 PTZ Network Camera 2.30-2.32, 2400 Video Server 2.30-2.32, 2401 Video Server 2.30-2.32, 2420 Network Camera 2.30-2.32	A vulnerability exists when a request is made for a specially formatted URL, which could let a remote malicious user bypass authentication mechanisms.	Upgrade available at: ftp://ftp.axis.com/pub_soft/cam_srv/
Baardsen Software ¹³	Windows	BaSoMail 1.24	Several vulnerabilities exist: a vulnerability exists because passwords are stored in plaintext, which could let a malicious user obtain unauthorized access; a remote Denial of Service vulnerability exists when a malicious user submits a LIST command that contains a negative integer parameter followed by a DEL with a negative integer parameter to the POP3 service; and a buffer overflow vulnerability exists in the SMTP server when a 'HELO,' 'MAIL FROM,' or 'RCPT TO' command contains a large amount of data, which could let a remote malicious user cause a Denial of Service.	No workaround or patch available at time of publishing.

⁸ Debian Security Advisory, DSA 285-1, April 14, 2003.

⁹ Red Hat Security Advisory, RHSA-2003:142-01, April 24, 2003.

¹⁰ Mandrake Linux Security Update Advisory, MDKSA-2003:060, May 21, 2003.

¹¹ RedHat Security Advisory, RHSA-2003:150-04, May 22, 2003.

¹² Core Security Technologies Advisory, May 27, 2003.

¹³ SecurityTracker Alert ID, 1006863, May 28, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts
Bandmin ¹⁴	Unix	Bandmin 1.4	A Cross-Site Scripting vulnerability exists due to insufficient filtering of HTML from user-supplied input, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.
Batalla Naval ¹⁵	Unix	Batalla Naval 1.04	A buffer overflow vulnerability exists when handling strings that are longer than 500 characters, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.
BitchX ¹⁶ <i>Vendors issue patches^{17, 18}</i>	Windows, Unix	IRC Client 1.0c19	Multiple vulnerabilities exist: a vulnerability exists when an excessively long hostname is supplied, which could let a remote malicious user execute arbitrary code; a vulnerability in Send_CTCP() when handling server-supplied data, which could let a remote malicious user execute arbitrary commands; a buffer overflow vulnerability exists in cannot_join_channel() when handling server-supplied data, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary commands; and a buffer overflow vulnerability exists in BX_compress_modes() when an excessive amount of data is supplied, which could let a remote malicious user execute arbitrary commands.	<u>Debian:</u> http://security.debian.org/pool/updates/main/i/ircii-pana/ <u>Slackware:</u> ftp://ftp.slackware.com/pub/slackware/

¹⁴ SecurityTracker Alert ID, 1006873, May 29, 2003.

¹⁵ Priv8security Advisory 1, May 26, 2003.

¹⁶ Bugtraq, March 13, 2003.

¹⁷ Debian Security Advisory, DSA 306-1, May 19, 2003.

¹⁸ Slackware Security Advisory, SSA:2003-141-02, May 21, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts
Blaine R Southam ¹⁹	Windows	Web Weaver 1.04	A remote Denial of Service exists when a malicious user submits an unusually long 'POST' or 'HEAD' request.	No workaround or patch available at time of publishing.
BNC ²⁰	Multiple	BNC 2.2.4, 2.4.6, 2.4.8, 2.6, 2.6.2	A Denial of Service vulnerability exists when two accounts connect to the service from the same IP address.	Upgrade to the latest version.
BZFlag ²¹	Unix	BZFlag 1.7g0	A remote Denial of Service vulnerability exists because a malicious user can connect to the server on two ports and flood those ports with random data.	No workaround or patch available at time of publishing.
Chrome-bob ²²	Unix	polymorph 0.4	A buffer overflow vulnerability exists in the 'file' argument due to insufficient bounds checking on user-supplied data, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.
Cisco Systems ²³	Multiple	Cisco IOS 12.x, R12.x	A remote Denial of Service vulnerability exists due to the way Service Assurance Agent (previously called Response Time Reporter, or RTR) packets are handled.	Affected users are advised to contact the vendor or authorized resellers for further information. See the advisory located at: http://www.cisco.com/warp/public/707/cisco-sa-20030515-saa.shtml
Cisco Systems ²⁴	Windows	VPN Client 3.x for Windows	A vulnerability exists in 'vpnclient.ini' when the VPN client is set to start prior to logon, which could let a malicious user obtain elevated privileges.	No workaround or patch available at time of publishing.
Compaq ²⁵	Windows	Insight Manager 5.0, Management Agents 4.36	A vulnerability exists in the authentication mechanism, which could let a remote malicious user obtain unauthorized access.	No workaround or patch available at time of publishing.

¹⁹ Bugtraq, May 27, 2003.

²⁰ Secunia Security Advisory, May 30, 2003.

²¹ Securiteam, May 21, 2003.

²² Bugtraq, May 22, 2003.

²³ Cisco Security Advisory, May 15, 2003.

²⁴ Secunia Security Advisory, May 19, 2003.

²⁵ SecurityFocus, May 21, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts
Demarc Security ²⁶	Windows NT 4.0/2000, XP, Unix	PureSecure 1.0.6	A vulnerability exists because the logging server password is stored in plaintext, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.
D-Link Systems, Inc. ²⁷	Multiple	DI-704P	A remote Denial of Service vulnerability exists in the web interface page when a malicious user submits multiple long malformed requests.	No workaround or patch available at time of publishing.
Easy Software Products ²⁸	Unix	CUPS 1.1.17, 1.1.18	A remote Denial of Service vulnerability exists due to an insufficient time-out process for malicious HTTP requests.	Patch available at: http://www.cups.org/strfiles/75/cups-1.1.18-str75.patchv2
Epic ²⁹ <i>Slackware issues update³⁰</i>	Unix	Epic4 1.0.1, 1.1.7 .20020907	A buffer overflow vulnerability exists in the status bar because server replies are not handled properly, which could let a malicious user obtain unauthorized access.	Debian: http://security.debian.org/pool/updates/main/e/epic/ Slackware: ftp://ftp.slackware.com/pub/slackware/
Epic ³¹ <i>Slackware issues update³²</i>	Unix	Epic4 1.0.1, 1.1.7 .20020907	A buffer overflow vulnerability exists in 'User_Cmd_Returned' because some types of server replies are not properly handled, which could let a malicious user obtain elevated privileges.	Debian: http://security.debian.org/pool/updates/main/e/epic/ Slackware: ftp://ftp.slackware.com/pub/slackware/
Epic ³³ <i>Slackware issues update³⁴</i>	Unix	Epic4 1.1.7 .20020907	A vulnerability exists in the 'PRIVMSG' command due to insufficient bounds checking, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary commands.	Debian: http://security.debian.org/pool/updates/main/e/epic/ Slackware: ftp://ftp.slackware.com/pub/slackware/

²⁶ SecurityTracker Alert ID, 1006826, May 23, 2003.

²⁷ Secunia Security Advisory, May 30, 2003.

²⁸ Turbolinux Security Advisory, TLSA-2003-33, May 20, 2003.

²⁹ Bugtraq, March 13, 2003.

³⁰ Slackware Security Advisory, SSA:2003-141-01, May 22, 2003.

³¹ SecurityFocus, March 14, 2003.

³² Slackware Security Advisory, SSA:2003-141-01, May 22, 2003.

³³ Bugtraq, March 13, 2003.

³⁴ Slackware Security Advisory, SSA:2003-141-01, May 22, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts
Erlend Berge ³⁵	Windows, Unix	Newsscript 1.0	A vulnerability exists in 'write.php' due to insufficient validation of user-supplied data to account editing input fields, which could let a remote malicious user obtain administrative access.	No workaround or patch available at time of publishing.
Eterm ³⁶	Unix	Eterm 0.9.1, 0.9.2	A buffer overflow vulnerability exists in the 'PATH_ENV' variable due to insufficient bounds checking, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.
eZ Systems ³⁷	Multiple	eZ publish 2.2	A Cross-Site Scripting vulnerability exists in the 'index.php' script due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code.	The vendor has released a patch to address this issue. Contact the vendor for information pertaining to obtaining and applying the patch.
Florian Sperber ³⁸	Windows, Unix	BLNews 2.1.3 - beta	A vulnerability exists in the 'admin/objects.inc.php4' script due to insufficient verification of the 'Server[path]' parameter, which could let a remote malicious user execute arbitrary PHP commands.	No workaround or patch available at time of publishing.
Francisco Burzi ³⁹	Windows, Unix	PHP-Nuke 5.0-5.6, 6.0, 6.5, 6.5 BETA 1, FINAL, RC1-RC3	A vulnerability exists in the 'Sections,' 'Avantgo,' 'Surveys,' 'Downloads,' 'Reviews,' and 'Web_Links' modules, which could let a remote malicious user execute arbitrary SQL code.	No workaround or patch available at time of publishing.
Francisco Burzi ⁴⁰	Windows, Unix	PHP-Nuke 5.5, 6.0	A Cross-Site Scripting vulnerability exists in the 'mainfile.php' script due to insufficient sanitization of URI parameters, which could let a malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.

³⁵ SecurityTracker Alert ID, 1006850, May 27, 2003.

³⁶ SecurityFocus, May 27, 2003.

³⁷ Bugtraq, May 16, 2003.

³⁸ Secunia Security Advisory, May 27, 2003.

³⁹ Bugtraq, May 18, 2003.

⁴⁰ Bugtraq, May 17, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts
GNU ⁴¹ <i>More vendors issue advisories</i> ^{42,43,44, 45}	Unix	GNU Privacy Guard 1.0-1.2.1	A vulnerability exists in the key validation code due to insufficient differentiation between the validity given to individual IDs on a public key that has multiple user IDs linked to it, which could let a malicious user obtain sensitive information.	Upgrade available at: http://www.gnupg.org/(en)/download/index.html#auto-ref-0 <i>Engarde:</i> http://www.linuxsecurity.com/advisories/engarde_advisory-3258.html <i>OpenPKG:</i> ftp://ftp.openpkg.org/release/ <i>RedHat:</i> ftp://updates.redhat.com/ <i>Mandrake:</i> http://www.mandrakesecure.net/en/ftp.php
Harakan Software ⁴⁶	PalmOS	PalmVNC 1.40	A vulnerability exists because password credentials are stored in plaintext, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.
Hewlett Packard Company ⁴⁷	Unix	Compaq Tru64 4.0g, PK3 (BL17), 4.0f, PK7 (BL17), PK6 (BL17), 5.1a, PK4 (BL21), PK3 (BL3), PK2 (BL2), PK1 (BL1), 5.1, PK6 (BL20), PK5 (BL19), PK4 (BL18), PK3 (BL17)	Several buffer overflow vulnerabilities exist in the Common Desktop Environment suite due to boundary errors, which could let a malicious user obtain unauthorized access.	Patches available at: http://ftp.support.compaq.com/patches/public/unix/
Hewlett Packard Company ⁴⁸	Unix	HP-UX 10.20, 11.0	A vulnerability exists in the Kermit implementation, which could let a malicious user obtain elevated privileges.	Workaround: The vendor has advised that until a fix is available customers should remove s permissions from /usr/bin/kermit. <i>Note: This action will have the adverse effect of limiting the functionality of k Full functionality will only be available to the root user.</i>
Hewlett Packard Company ⁴⁹	Unix	HP-UX 11.0	A buffer overflow vulnerability exists in the 'IPCS' utility due to insufficient bounds checking of user-supplied data, which could let a malicious user obtain elevated privileges.	Patch available at: ftp://ipcs:ipcs1@hprc.external.hp.com/

⁴¹ Bugtraq, May 4, 2003.

⁴² Guardian Digital Security Advisory, ESA-20030515-016, May 15, 2003.

⁴³ OpenPKG Security Advisory, OpenPKG-SA-2003.029, May 16, 2003.

⁴⁴ Red Hat Security Advisory, RHSA-2003:175-01, May 21, 2003.

⁴⁵ Mandrake Linux Security Update Advisory, DKSA-2003:061, May 22, 2003.

⁴⁶ Bugtraq, May 26, 2003.

⁴⁷ Secunia Security Advisory, May 30, 2003.

⁴⁸ Hewlett-Packard Company Security Bulletin, HPSBUX0305-259, May 19, 2003.

⁴⁹ Hewlett-Packard Company Security Bulletin, HPSBUX0305-260, May 19, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts
IBM ⁵⁰	Unix	AIX 4.3-4.3.3, 5.1, 5.2	A vulnerability exists in some of the printer commands due to a format string flaw in several command line utilities, which could let a malicious user obtain elevated privileges.	Patches available at: http://techsupport.services.ibm.com/
ifenslave ⁵¹	Unix	ifenslave .7	A buffer overflow vulnerability exists due to insufficient bounds checking, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.
iisProtect ⁵²	Windows NT 4.0/2000	iisProtect 2.1, 2.2	A vulnerability exists because authentication can be bypassed, which could let a remote malicious user obtain unauthorized access.	Upgrade available at: www.iisprotect.com
iisProtect ⁵³	Windows NT 4.0/2000	iisProtect 2.1, 2.2	A vulnerability exists in the web administration interface due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.iisprotect.com/
James Theiler ⁵⁴ <i>Exploit script has been published⁵⁵</i>	Unix	opt 3.12, 3.13, 3.16, 3.17, 3.18	A buffer overflow vulnerability exists in several Libopt.a error logging functions due to insufficient bounds checking of user-supplied data, which could let a malicious user execute arbitrary code.	Upgrade available at: http://nis-www.lanl.gov/~jt/Software/opt/opt-3.19.tar.gz
Kevin Lindsay ⁵⁶	Unix	slocate 2.1-2.7	A vulnerability exists in the 'SLOCATE_PATH' environment variable, which could let a malicious user obtain elevated privileges	No workaround or patch available at time of publishing.

⁵⁰ SecurityTracker Alert ID: 1006756, May 14, 2003.

⁵¹ SecurityFocus, May 26, 2003.

⁵² iDEFENSE Security Advisory, May 22, 2003.

⁵³ Bugtraq, May 23, 2003.

⁵⁴ Secure Network Operations, Inc. Advisory, SRT2003-04-24-1532, April 24, 2003.

⁵⁵ Bugtraq, May 23, 2003.

⁵⁶ SecurityTracker Alert ID, 1006800, May 20, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts
Lava Software Technologies ⁵⁷	Windows	ShareMail Pro 3.6.1	Several vulnerabilities exist: a vulnerability exists because the POP3 interface can be queried to determine whether a particular user account exists, which could let a remote malicious user obtain sensitive information; and a vulnerability exists because the server discloses some administrative information, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.
lv ^{58, 59}	Unix	lv 4.49.1- 4.49.4; RedHat lv-4.49.4-1.i386.rpm, lv-4.49.4-3.i386.rpm, lv-4.49.4-7.i386.rpm, lv-4.49.4-9.i386.rpm	A vulnerability exists in the lv multilingual file viewer, which could let a malicious user execute arbitrary commands.	Upgrade available at: http://www.ff.iiij4u.or.jp/~nrt/freeware/lv4495.tar.gz Debian: http://security.debian.org/pool/updates/main/l/lv/ RedHat: ftp://updates.redhat.com/
Meteor-soft ⁶⁰	Windows	Meteor FTP 1.5	A vulnerability exists due to the way the authentication procedure is handled by the FTP server, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.

⁵⁷ SecurityTracker, May 21, 2003.

⁵⁸ Debian Security Advisory, DSA 304-1, May 15, 2003.

⁵⁹ Red Hat Security Advisory, RHSA-2003:169-01, May 16, 2003.

⁶⁰ SecurityFocus, May 27, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts
Microsoft ⁶¹	Windows NT 4.0/2000, XP	IIS 4.0, 5.0, 5.1	Multiple vulnerabilities exist: a Cross-Site Scripting vulnerability exists involving the error message that's returned to advise that a requested URL has been redirected, which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability exists due to incorrect validation of requests for certain types of web pages known as server side includes, which could let a remote malicious user execute arbitrary code; a remote Denial of Service vulnerabilities exist when a malicious user submits an excessively long header in ASP pages; and a Denial of Service vulnerability exists due to a failure to properly handle large WebDav requests to the 'PROPFIND' and 'SEARCH' request methods.	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/MS03-018.asp
Microsoft ⁶²	Windows 95/98/ME/NT 4.0/2000	Internet Explorer 5.0, 5.0.1, 5.0.1 SP1-SP3, 5.5, 5.5 SP1&SP2, 6.0, 6.0 SP1	A Denial of Service exists when certain malformed or incomplete JavaScript statements are submitted.	No workaround or patch available at time of publishing.
Microsoft ⁶³	Windows 2000	ISA Server 2000, 2000 SP1, FP1	A Cross-Site Scripting vulnerability exists due to insufficient sanitization of certain HTTP header fields, which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.
Microsoft ⁶⁴	Windows 98/NT 4.0/2000, XP	Netmeeting 2.1, 3.0.1 4.4.3385	A remote Denial of Service vulnerability exists when a malicious user submits a malformed 'CallTo' URI.	No workaround or patch available at time of publishing.

⁶¹ Microsoft Security Bulletin, MS03-018 V1.1 May 30, 2003.

⁶² SecurityFocus, May 27, 2003.

⁶³ SecurityTracker Alert, 1006789, May 16, 2003.

⁶⁴ NTBugtraq, May 20, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts
Microsoft ⁶⁵	Windows NT 4.0/2000	Windows 2000 Advanced Server, SP1-SP3, 2000 Datacenter Server, SP1-SP3, 2000 Server, SP1-SP3, NT Enterprise Server 4.0, SP1-SP6a, NT Server 4.0, SP1-SP6a	A buffer overflow vulnerability exists in 'nsiislog.dll' due to the way incoming requests are processed, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-019.asp
Microsoft ⁶⁶	Windows 95/98/ME/NT 4.0/2000	Windows Media Player 7.0, 7.1	A vulnerability exists when a specially crafted XML Name Space URI is embedded within an HTML e-mail message, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.
Microsoft ⁶⁷	Windows 2000, XP	Windows Server 2003 Datacenter Edition, 64-bit, 2003 Enterprise Edition, 64-bit, 2003 Standard Edition, 2003 Web Edition, XP 64-bit Edition, SP1, 64-bit Edition Version 2003, XP Embedded, SP1, XP Home, SP1, XP Media Center Edition, XP Professional, SP1, XP Tablet PC Edition	A vulnerability exists for systems that have ICF enabled, which could let certain traffic bypass existing firewall filters.	No workaround or patch available at time of publishing.

⁶⁵ Microsoft Security Bulletin, MS03-019 V2.0, May 30, 2003.

⁶⁶ Bugtraq, May 21, 2003.

⁶⁷ SecurityFocus, May 22, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts
<p>Microsoft⁶⁸</p> <p><i>Proof of Concept exploit released⁶⁹</i></p> <p><i>Microsoft updates bulletin⁷⁰</i></p> <p><i>New exploit issued⁷¹</i></p>	<p>Windows 2000</p> <p><i>Windows NT 4.0</i></p>	<p>Windows 2000, ISS 5.0</p> <p><i>Windows NT 4.02, Windows NT 4.0 Terminal Server Edition</i></p>	<p>A buffer overflow vulnerability exists in the Windows component used by Web-based Distributed Authoring and Versioning (WebDAV) due to insufficient bounds checking on data, which could let a remote malicious user execute arbitrary code.</p> <p><i>Windows NT 4.0 also contains the vulnerability in ntdll.dll, however it does not support WebDAV and therefore the known exploit was not effective against Windows NT 4.0. Microsoft has now released a patch for Windows NT 4.0.</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/MS03-007.asp</p>
<p>Microsoft⁷²</p> <p><i>Microsoft updates bulletin⁷³</i></p>	<p>Windows NT 4.0/2000, XP</p>	<p>Windows 2000 Advanced Server, SP1-SP3, 2000 Data-center Server, SP1-SP3, 2000 Professional, SP1-SP3, 2000 Server, SP1-SP3, 2000 Terminal Services, SP1-SP3, NT Enterprise Server 4.0, SP1-SPa, NT Server 4.0, SP1-SP6a, NT Terminal Server 4.0, SP1-SP6a, NT Work-station 4.0, SP1-SP6a, XP 64-bit Edition, SP1, XP Home, SP1, XP Professional, SP1</p>	<p>A buffer overflow vulnerability exists in the way the kernel passes error messages to a debugger due to insufficient bounds checking, which could let a malicious user take any action on the system including deleting data, adding accounts with administrative access, execute arbitrary code, or reconfiguring the system.</p> <p><i>Bulletin updated to advise of availability of revised Windows XP SP1 patch to correct performance issues</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/MS03-013.asp</p>

⁶⁸ Microsoft Security Bulletin, MS03-007 V1.1, March 18, 2003.

⁶⁹ Bugtraq, March 25, 2003.

⁷⁰ Microsoft Security Bulletin, MS03-007 2.1, April 24, 2003.

⁷¹ Bugtraq, May 30, 2003.

⁷² Microsoft Security Bulletin, MS03-013, April 17, 2003.

⁷³ Microsoft Security Bulletin, MS03-013 V2.0 May 28, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts
Mirko De Grandis ⁷⁴	Unix	WSMP3 .7-.10	A buffer overflow vulnerability exists in the 'parse_request()' function due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.
Mirko De Grandis ⁷⁵	Unix	WSMP3 .1-.10	Several vulnerabilities exist: a Directory Traversal vulnerability exists due to insufficient sanitization of HTTP GET requests, which could let a remote malicious user obtain sensitive information; and a vulnerability exists due to insufficient sanitization of HTTP POST requests, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.
mod_auth_any ⁷⁶ <i>Sun issues patch</i> ⁷⁷	Unix	mod_auth_any 1.2.2	A vulnerability exists in the mod_auth_any Apache module due to insufficient sanitization of user-supplied arguments, which could let a remote malicious user execute arbitrary commands.	Upgrade available at: http://rhn.redhat.com/ <i>Sun:</i> http://sunsolve.sun.com/patches/linux/security.html
Mozilla ⁷⁸ <i>Conectiva issues advisory</i> ⁷⁹	Unix	Bugzilla 2.10, 2.12, 2.14- 2.14.5, 2.16- 2.16.2, 2.17, 2.17.1, 2.17.3	A vulnerability exists because temporary files are insecurely created, which could let a malicious user corrupt or overwrite files.	Patches available at: http://ftp.mozilla.org/pub/webtools/ <i>Conectiva:</i> ftp://atualizacoes.conectiva.com.br/
Multiple Vendors ⁸⁰	Windows	Deerfield VisNetic FTPServer 2.0; South River Technologies Titan FTP Server 2.02	A Directory Traversal vulnerability exists, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.

⁷⁴ INetCop Security Advisory, 2003-0x82-017.b, May 21, 2003.

⁷⁵ INetCop Security Advisory, 2003-0x82-017.a, May 21, 2003.

⁷⁶ RedHat Security Advisory, RHSA-2003:114-09, April 28, 2003.

⁷⁷ SecurityFocus, May 26, 2003.

⁷⁸ Bugzilla Security Advisory, April 24, 2003.

⁷⁹ Conectiva Linux Security Announcement, CLA-2003:653, May 21, 2003.

⁸⁰ Damage Hacking Group Security Advisory, May 29, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts
Multiple Vendors ⁸¹	Windows 95/98/ME/NT 4.0/2000, XP	Grokster Grokster 1.3, 1.3.3; iMesh.Com iMesh 1.0 2 & previous, 3.1; KaZaA KaZaA Media Desktop 1.3-1.3.2, 1.6.1, 2.0, 2.0.2; Music City Networks Morpheus 1.3, 1.3.3, 1.9	A buffer overflow vulnerability exists in the FastTrack P2P Supernode Packet Handler due to insufficient bounds checking, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.	No workaround or patch available at time of publishing.
Multiple Vendors ⁸²	Multiple	Microsoft Outlook Express 6.0; Mozilla Browser 1.3, 1.4a; Qualcomm Eudora 5.2.1; Sylpheed Sylpheed 0.8.11; University of Washington IMAP 2002b, Pine 4.53; Ximian Evolution 1.2.4	Integer flow vulnerabilities exist due to insufficient boundary checks on literal size values, which could let a remote malicious user execute arbitrary code.	This issue has reportedly been addressed in University of Washington imap-2 Ximian Evolution 1.3.2 (beta) and Mozilla 1.3.1 and 1.4b. Users should contact relative vendor to obtain an upgraded version. Outlook Express 6.00.2800.1 reported to be fixed with the next OE service pack.
Multiple Vendors ⁸³	Unix	RedHat kernel-utils-2.4-8.13.i386.rpm; User-Mode Linux uml_utilities	A vulnerability exists in 'uml_net.c' due to insufficient bounds checking, which could let a malicious user execute arbitrary code.	RedHat: http://updates.redhat.com/8.0/en/os/i386/kernel-utils-2.4-8.28.i386.rpm
Multiple Vendors ^{84,85}	Unix	Apache Software Foundation Apache 2.0.37-2.0.45; RedHat httpd-2.0.40-21.i386.rpm, 40-8.i386.rpm, httpd-devel-2.0.40-21.i386.rpm, 2.0.40-8.i386.rpm, httpd-manual-2.0.40-21.i386.rpm, 2.0.40-8.i386.rpm, mod_ssl-2.0.40-21.i386.rpm, 2.0.40-8.i386.rpm	A vulnerability exists in the 'apr_password_validate()' function due to improper use of specific thread-safe functions, which could let a remote malicious user cause a Denial of Service.	Apache: http://www.apache.org/dist/httpd/ Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: http://updates.redhat.com/

⁸¹ Bugtraq, May 25, 2003.

⁸² Bugtraq, May 14, 2003.

⁸³ Bugtraq, May 24, 2003.

⁸⁴ Red Hat Security Advisory, RHSA-2003:186-01, May 28, 2003.

⁸⁵ iDEFENSE Security Advisory, May 30, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts
Multiple Vendors ^{86, 87, 88} <i>More updates issued⁸⁹</i> <i>Mandrake issues update⁹⁰</i>	Unix	BSD lpr 2000.05.07, 0.48; FreeBSD FreeBSD 2.2-2.2.6; lpr-ppd lpr-ppd 0.72; lprold lprold 3.0.48; OpenBSD OpenBSD 2.0-2.9, 3.0-3.2	A buffer overflow vulnerability exists in the 'lpr' printer spooling system, which could let a malicious user execute arbitrary code as root.	Debian: http://security.debian.org/pool/updates/main/l/lpr/ SuSE: ftp://ftp.suse.com/pub/suse/ OpenBSD: ftp://ftp.openbsd.org/pub/OpenBSD/patches/ SGI: http://support.sgi.com/ Mandrake: http://www.mandrakesecure.net/en/ftp.php
Multiple Vendors ^{91, 92}	Unix	Linux kernel 2.4-2.4.20	A Denial of Service vulnerability exists because a low volume flood of some types of traffic is not handled properly.	Engarde: http://www.linuxsecurity.com/advisories/engarde_advisory-3259.html RedHat: ftp://updates.redhat.com/
Multiple Vendors ^{93, 94, 95}	Multiple	Apache Software Foundation Apache 2.0.37-2.0.45; RedHat httpd-2.0.40-21.i386.rpm, 40-8.i386.rpm, httpd-devel-2.0.40-21.i386.rpm, 2.0.40-8.i386.rpm, httpd-manual-2.0.40-21.i386.rpm, 2.0.40-8.i386.rpm, mod_ssl-2.0.40-21.i386.rpm, 2.0.40-8.i386.rpm	A vulnerability exists in the 'apr_psprintf()' Apache Portable Runtime (APR) library, which could let a remote malicious user execute arbitrary code.	Apache: http://www.apache.org/dist/httpd/ Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: ftp://updates.redhat.com/

⁸⁶ SuSE Security Announcement, SuSE-SA:2003:0014, March 13, 2003.

⁸⁷ Debian Security Advisory, DSA 267-1, March 24, 2003.

⁸⁸ Debian Security Advisory, DSA 275-1, April 2, 2003.

⁸⁹ SGI Security Advisory, 20030406-02-P, April 25, 2003.

⁹⁰ Mandrake Linux Security Update Advisory, MDKSA-2003:059, May 21, 2003.

⁹¹ Red Hat Security Advisory, RHSA-2003:172-00, May 14, 2003.

⁹² Guardian Digital Security Advisory, ESA-20030515-017, May 15, 2003.

⁹³ Red Hat Security Advisory, RHSA-2003:186-01, May 28, 2003.

⁹⁴ iDEFENSE Security Advisory, May 30, 2003.

⁹⁵ Mandrake Linux Security Update Advisory, MDKSA-2003:063, May 30, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts
MySQL AB ^{96, 97, 98} <i>Engarde releases upgrade⁹⁹</i> <i>More advisories issued^{100, 101}</i>	Unix	MySQL 3.23.52	A vulnerability exists in the 'mysqld' service, which could let a malicious user obtain elevated privileges as root.	Upgrade available at: http://www.mysql.com/downloads/mysql-3.23.html OpenPKG: ftp.openpkg.org Trustix: http://www.trustix.net/pub/Trustix/updates/ Engarde: http://ftp.engadelinux.org/pub/engarde/stable/updates/ Mandrake: http://www.mandrakesecure.net/en/advisories/ Debian: http://security.debian.org/pool/updates/main/m/mysql
Netpbm ¹⁰² <i>More vendors release upgrades^{103, 104}</i> <i>Conectiva issues advisory¹⁰⁵</i>	Unix	Netpbm 10.0-10.14	Multiple buffer overflow vulnerabilities exist due to math overflow errors, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.	Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: ftp://updates.redhat.com Conectiva: ftp://atualizacoes.conectiva.com.br/
OneOr Zero ¹⁰⁶	Multiple	Helpdesk 1.4 rc4	Two vulnerabilities exist: a vulnerability exists in the 'supporter/tupdate.php' script due to insufficient validation, which could let a remote malicious user execute arbitrary SQL or obtain administrative access; and a vulnerability exists in the 'install.php' script when creating a new administrative account due to insufficient sanitization of user-supplied input, which could let a remote malicious user obtain administrative access.	No workaround or patch available at time of publishing.

⁹⁶ OpenPKG Security Advisory, OpenPKG-SA-2003.022, March 18, 2003.

⁹⁷ Gentoo Linux Security Announcement, 200303-14, March 18, 2003.

⁹⁸ Trustix Secure Linux Security Advisory, 2003-0009, March 18, 2003.

⁹⁹ EnGarde Secure Linux Security Advisory, ESA-20030324-012, March 24, 2003.

¹⁰⁰ Mandrake Linux Security Update Advisory, MDKSA-2003:057, May 14, 2003.

¹⁰¹ Debian Security Advisory, DSA 303-1, May 16, 2003.

¹⁰² Bugtraq, February 28, 2003.

¹⁰³ Mandrake Linux Security Update Advisory, MDKSA-2003:036, March 25, 2003.

¹⁰⁴ Red Hat Security Advisory, RHSA-2003:060-01, April 2, 2003.

¹⁰⁵ Conectiva Linux Security Announcement, CLA-2003:656, May 27, 2003.

¹⁰⁶ SecurityFocus, May 15, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts
Open LDAP ¹⁰⁷	Unix	OpenLDAP 2.0-2.0.23, 2.0.25, 2.0.27, 2.1.10-2.1.16	A remote Denial of Service vulnerability exists when the server attempts to free an uninitialized structure during authentication.	Upgrade available at: ftp://ftp.OpenLDAP.org/pub/OpenLDAP/openldap-release/openldap-2.1.20.tgz
Owl ¹⁰⁸	Windows, Unix	Owl Intranet Engine 0.6, 0.7, 0.71	A Cross-Site Scripting vulnerability exists due to insufficient sanitization of search queries, which could let a malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.
PHP-Banner Exchange ¹⁰⁹	Multiple	PHP-Banner Exchange 1.2	A path disclosure vulnerability exists when requesting the directory for the software, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.
Platform ¹¹⁰	Windows NT 4.0/2000, Unix	Platform LSF 4.0, 4.2, 5.0, 5.1	A vulnerability exists because input environmental variables are not properly handled, which could let a malicious user obtain elevated privileges.	Patch available at: ftp://ftp.platform.com/patches/5.1/patch/sup_by_dev33993/
PostNuke Development Team ¹¹¹	Windows, Unix	PostNuke Phoenix 0.721- 0.723	Several vulnerabilities exist: path disclosure vulnerabilities exist in the 'Download,' 'Web Links,' 'Sections,' 'FAQ,' 'Search,' 'Reviews,' and 'Glossary' modules, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.
PostNuke Development Team ¹¹²	Windows, Unix	PostNuke Phoenix 0.721- 0.723	A remote Denial of Service vulnerability due to a failure to handle some submissions to the rating system.	No workaround or patch available at time of publishing.
PpoPn ¹¹³	Windows, Unix	P-News 1.16	A vulnerability exists in the 'p-news.php' file due to insufficient validation of data, which could let a remote malicious user obtain administrative access.	No workaround or patch available at time of publishing.

¹⁰⁷ SecurityFocus, May 22, 2003.

¹⁰⁸ AngryPacket Security Advisory, May 21, 2003.

¹⁰⁹ SecurityFocus, May 20, 2003.

¹¹⁰ Secunia Security Advisory, May 23, 2003.

¹¹¹ SecurityFocus, May 29, 2003.

¹¹² SecurityFocus, May 26, 2003.

¹¹³ SecurityFocus, May 26, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts
Prishtina Soft ¹¹⁴	Windows	Prishtina FTP 1.0, 1.1, 1.2	A remote Denial of Service vulnerability exists when FTP server banners of excessive length are processed.	No workaround or patch available at time of publishing.
Privacy ware ¹¹⁵	Multiple	Private firewall 3.0	A vulnerability exists because TCP traffic with certain flag settings are not properly handled, which could let a remote malicious user circumvent firewall filtering.	No workaround or patch available at time of publishing.
Qual-comm ¹¹⁶	Multiple	Eudora 5.2.1	A vulnerability exists because it is possible to refer to other files or attachments through specially formatted inline text, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.
RedHat ¹¹⁷	Unix	Enterprise Linux WS 2.1 IA64, 2.1, ES 2.1 IA64, ES 2.1, AS 2.1 IA64, AS 2.1, Linux Advanced Work Station 2.1	A vulnerability exists in the up2date mechanism that may result in a segmentation fault during Migration.	Update available at: ftp://updates.redhat.com/enterprise/
RedHat ¹¹⁸	Unix	Linux 7.1, 7.1 k i386, ia64, i386, alpha, 7.2, 7.2 ia64, i386, alpha, 7.3 i386, 8.0 i386, 9.0 i386, tcpdump-3.4-39.i386.rpm, tcpdump-3.6.2-12.i386.rpm, tcpdump-3.6.2-9.i386.rpm, tcpdump-3.6.2-9.ia64.rpm, tcpdump-3.6.3-3.i386.rpm, tcpdump-3.7.2-.i386.rpm	A vulnerability exists due to a compilation error design in tcpdump, which would let tcpdump continue running as "root" rather than the less privileged user "pcap." <i>Note: This is not a vulnerability in itself, since it could only be exploited if another vulnerability is present.</i>	Upgrade available at: ftp://updates.redhat.com/

¹¹⁴ Damage Hacking Group Security Advisory, May 21, 2003.

¹¹⁵ Ukr Security Advisory, May 24, 2003.

¹¹⁶ Bugtraq, May 22, 2003.

¹¹⁷ Red Hat Security Advisory, RHSA-2003:177-01, May 28, 2003.

¹¹⁸ Red Hat Security Advisory, RHSA-2003:174-01, May 15, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts
Renaud et al Deraison ¹¹⁹	Unix	Nessus 2.0-2.0.5	Several vulnerabilities exist in the 'libnsal' library due to some boundary errors, which could let a malicious user execute arbitrary commands. <i>Note: The malicious script must be a legitimate plugin that has been uploaded to the Nessus server.</i>	Upgrade available at: http://www.nessus.org/nessus_2_0.html
Sam Lantinga ¹²⁰	Unix	Maelstrom 3.0.3, 3.0.5, 3.0.6	A buffer overflow vulnerability exists due to insufficient bounds checking of user-supplied data, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.
sd ¹²¹	Unix	Encrypted Virtual Filesystem 0.2	A vulnerability exists in the 'efs' utility due to insufficient size calculations when allocating heap memory, which could let a malicious user execute arbitrary instructions with root privileges.	Upgrade available at: http://hysteria.sk/evfs/f/evfs-0.3.tgz
Selom Ofori ¹²²	Windows 2000, XP	FTP Server 2.6	Several vulnerabilities exist: a vulnerability exists in the 'blackmoon.mdb' file because authentication credentials are stored in plaintext, which could let a malicious user obtain sensitive information; and an information disclosure vulnerability exists due to the way the authentication procedure is handled, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.
Sendmail Consortium ¹²³	Unix	Sendmail 8.9.3, 8.12.3, 8.12.9	A vulnerability exists in the 'expn,' 'checksendmail,' and 'doublebounce.pl' scripts because insecure temporary files are created, which could let a malicious user obtain elevated privileges.	Debian: http://security.debian.org/pool/updates/main/s/sendmail/

¹¹⁹ Securiteam, May 26, 2003.

¹²⁰ Bugtraq, May 18, 2003.

¹²¹ SecurityFocus, May 24, 2003.

¹²² Telhack 026 Inc. Security Advisory #4, May 21, 2003.

¹²³ Debian Security Advisory, DSA 305-1, May 15, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts
SGI ¹²⁴	Unix	IRIX 5.0-6.5.19	A buffer overflow vulnerability exists in the MediaMail binary, which could let a malicious user obtain elevated privileges and possibly execute arbitrary code.	SGI has stated that MediaMail is an expired product, and patches will not be issued. Additionally, SGI has stated that affected users should uninstall the program, and use an alternative mail client.
Slackware ¹²⁵	Unix	Linux 9.0	A vulnerability exists in the 'rc.M runlevel' script due to the use of an incorrect flag, which could result in a false sense of security.	Upgrade available at: ftp://ftp.slackware.com/pub/slackware/slackware-9.0/patches/packages/sysvinit-2.84-13
Snort Project ¹²⁶	Windows, Unix	Snort 2.0.0rc2	A vulnerability exists because a malicious spoofed packet can be submitted that causes Snort to modify the state of an established TCP session, which could let a remote malicious user continue with a TCP session without detection.	No workaround or patch available at time of publishing.
Snow-blind ¹²⁷	Windows	Snowblind Web Server 1.0, 1.01	Several vulnerabilities exist: a Directory Traversal vulnerability exists due to insufficient filtering, which could let a remote malicious user obtain sensitive information; a remote Denial of Service vulnerability exists when malformed HTTP requests are processed; and a buffer overflow vulnerability exists when the web server attempts to process HTTP requests of excessive length, which could possibly let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.

¹²⁴ SecurityFocus, May 26, 2003.

¹²⁵ Slackware Security Advisory, SSA:2003-141-06a, May 22, 2003.

¹²⁶ SecurityTracker Alert ID, 1006835, May 23, 2003.

¹²⁷ Secunia Security Advisory, May 21, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts
Softrex ¹²⁸	Windows	Tornado www-Server 1.2	Several vulnerabilities exist: a Directory Traversal vulnerability exists due to insufficient sanitization of client requested paths, which could let a remote malicious user obtain sensitive information; and a buffer overflow vulnerability exists when overly long HTTP requests are processed, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code.	No workaround or patch available at time of publishing.
STSoft ¹²⁹	Multiple	ST FTP Service 3.0	A Directory Traversal vulnerability exists, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.
SudBox ¹³⁰	Multiple	SudBox Boutique 1.2	A vulnerability exists in the 'login.php' script due to insufficient initialization of variables, which could let an unauthorized malicious user obtain administrative access.	No workaround or patch available at time of publishing.

¹²⁸ Damage Hacking Group Security Advisory, May 28, 2003.

¹²⁹ Damage Hacking Group Security Advisory, May 23, 2003.

¹³⁰ SecurityFocus, May 21, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts
Sun Microsystems, Inc. ¹³¹	Windows 2000, XP	Sun One Application Server 7.0 Standard Edition, 7.0 Platform Edition	Multiple vulnerabilities exist: a vulnerability exists due the way the case of a file extension is handled, which could let a remote malicious user obtain sensitive information; a Cross-Site Scripting vulnerability exists due to insufficient filtering of script code from URL parameters, which could let a remote malicious user execute arbitrary code; a vulnerability exists because requests are not properly logged, which could let a remote malicious user obscure attacks from the view of administrators; and a vulnerability exists because the username and password for the administrative server is stored in a world-readable file during installation, which could let a remote malicious user obtain unauthorized access to the administrative server.	No workaround or patch available at time of publishing.
Sun Microsystems Inc. ¹³²	Windows, Unix	Java Media Framework (Linux) 2.1.1, 2.1.1 a- 2.1.1 c, Sun Java Media Framework (Solaris) 2.1.1, 2.1.1 a- 2.1.1 c, Sun Java Media Framework (Windows) 2.1, 2.1.1 a- 2.1.1 c.	A vulnerability exists in the Java Virtual Machine, which could let a remote malicious user cause a Denial of Service or obtain unauthorized privileges.	Upgrades available at: http://java.sun.com/products/java-media/jmf/2.1.1/download.html
Sun Microsystems, Inc. ¹³³	Unix	Cluster 2.2	A vulnerability exists because user names and passwords are stored in a plaintext cluster configuration file, which could let a malicious user obtain sensitive information.	Patches available at: http://sunsolve.sun.com

¹³¹ SPI Labs Advisory, May 27, 2003.

¹³² Sun(sm) Alert Notification , 54760, May 14, 2003.

¹³³ Sun(sm) Alert Notification, 51340, May 20, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts
Sun Microsystems, Inc. ¹³⁴	Windows NT 4.0/2000, Unix	iPlanet Messaging Server 5.0-5.2	A Cross-Site Scripting vulnerability exists when processing HTML attachments that are received via e-mail, which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.
Super-M ¹³⁵	Windows	Son hServer 0.2	A Directory Traversal vulnerability exists due to insufficient sanitization of client requested paths, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.
TextPortal ¹³⁶	Unix	TextPortal 0.8, 0.77, 0.76	A vulnerability exists due to a weak undocumented password, which could let a remote malicious user obtain unauthorized administrative access.	No workaround or patch available at time of publishing.
The Uptimes Project ¹³⁷	Unix	upclient 5.0b7	A buffer overflow vulnerability exists due to a failure to handle command line arguments that are an excessive length, which could let a malicious user execute arbitrary code.	Upgrade available at: http://uptimes.wonko.com/download.php
ttCMS ¹³⁸	Multiple	ttCMS 2.3, 2.2	A vulnerability exists in the 'header.php' script due to insufficient sanitization of user-supplied variables, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.
ttCMS ¹³⁹	Multiple	ttCMS 2.3, 2.2, 1.1	A vulnerability exists in the Instant-Messages script due to insufficient sanitization of input, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.

¹³⁴ SecurityTracker Alert ID, 1006859, May 28, 2003.

¹³⁵ Damage Hacking Group Security Advisory, May 29, 2003.

¹³⁶ Securiteam, May 26, 2003.

¹³⁷ NUX-ACID ADVISORY #002, May 27, 2003.

¹³⁸ Bugtraq, May 17, 2003.

¹³⁹ Bugtraq, May 20, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts
Ultimate PHP Board ¹⁴⁰	Unix	Ultimate PHP Board Ultimate PHP Board 1.9	A vulnerability exists in 'admin_iplog.PHP' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary PHP commands.	No workaround or patch available at time of publishing.
Venturi Wireless ¹⁴¹	Multiple	Venturi Client 2.1	A vulnerability exists because proxying requests are honored from unauthorized external hosts, which could let a malicious user relay traffic using the host running Venturi Client.	Upgrade available at: http://www.venturiwireless.com/tech_support/Q_and_A/Q_A_09.htm
Vignette ¹⁴²	Windows NT 4.0/2000, Unix	Content Suite V5-V7, StoryServer 4.0, 4.1, 5.0, 6.0	Multiple Cross-Site Scripting vulnerabilities exist due to insufficient sanitization of HTML characters from user-supplied data, which could let a malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.
Vignette ¹⁴³	Windows NT 4.0/2000, Unix	Content Suite V5-V7, StoryServer 4.0, 4.1, 5.0, 6.0	A vulnerability exists because several templates are installed in the /vgn directory, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.
Vignette ¹⁴⁴	Windows NT 4.0/2000, Unix	Content Suite V5-V7, StoryServer 4.0, 4.1, 5.0, 6.0	A vulnerability exists in the 'NEEDS' and 'VALID_PATHS' commands, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.
Vignette ¹⁴⁵	Windows NT 4.0/2000, Unix	Content Suite V5-V7, StoryServer 4.0, 4.1, 5.0, 6.0	A vulnerability exists in the login template, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.
Vignette ¹⁴⁶	Windows NT 4.0/2000, Unix	Content Suite V5-V7, StoryServer 4.0, 4.1, 5.0, 6.0	A remote Denial of Service vulnerability exists because several templates are installed in the /vgn directory.	No workaround or patch available at time of publishing.

¹⁴⁰ Securiteam, May 26, 2003.

¹⁴¹ Secunia Security Advisory, May 21, 2003.

¹⁴² S 2 1 S E C Advisory, S21SEC-023, May 26, 2003.

¹⁴³ S 2 1 S E C Advisory, S21SEC-019, May 26, 2003.

¹⁴⁴ S 2 1 S E C Advisory, S21SEC-024, May 26, 2003.

¹⁴⁵ S 2 1 S E C Advisory, S21SEC-020, May 26, 2003.

¹⁴⁶ S 2 1 S E C Advisory, S21SEC-020, May 21, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts
Vignette ¹⁴⁷	Unix	Content Suite V7, V6, StoryServer 4.0, 4.1, 5.0, 6.0	A vulnerability exists due to a flaw in the way the size of certain characters in URI variables are calculated, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.
Vignette ¹⁴⁸	Windows NT 4.0/2000, Unix	Content Suite V7, V6, StoryServer 4.0, 4.1, 5.0, 6.0	A vulnerability exists in the Legacy Tool application due to insufficient access restrictions, which could let an unauthorized remote malicious user execute database queries.	No workaround or patch available at time of publishing.
Vignette ¹⁴⁹	Windows NT 4.0/2000, Unix	Content Suite V7, V6, StoryServer 4.0, 4.1, 5.0, 6.0	A vulnerability exists which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.
Working Resources Inc. ¹⁵⁰	Windows 95/98/ME/NT 4.0/2000, XP	BadBlue Enterprise Edition 1.7, 1.7.2-1.7.4, 2.0-2.2, 2.15, Personal Edition 1.7, 1.7.2-1.7.4, 2.0-2.2, 2.15, 2.16	A vulnerability exists in the administration interface due to insufficient validation of user-supplied requests for non-HTML files, which could let a remote malicious user bypass security restrictions and obtain unauthorized administrative access.	Upgrade available at: http://www.badblue.com/down.htm

¹⁴⁷ S 2 1 S E C Advisory, S21SEC-018, May 26, 2003.

¹⁴⁸ S 2 1 S E C Advisory, S21SEC-017, May 26, 2003.

¹⁴⁹ S 2 1 S E C Advisory, S21SEC-016, May 26, 2003.

¹⁵⁰ Bugtraq, May 20, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts
Ximian ^{151, 152} <i>Conectiva issues upgrade</i> ¹⁵³	Unix	Evolution 1.0.3-1.0.8, 1.1.1, 1.2-1.2.2	Multiple vulnerabilities exist: a remote Denial of Service vulnerability exists in the parsing component when a malicious user includes a specially crafted UUE header as part of an e-mail; a remote Denial of Service vulnerability exists in the Mail User Agent (MUA) when a malicious user submits a specially encoded e-mail message; and a vulnerability exists due to insufficient validation of MIME image/* Content-Type fields, which could let a remote malicious user execute arbitrary code or bypass the "Don't connect to remote hosts to fetch images" option.	RedHat: ftp://updates.redhat.com/ Mandrake: http://www.mandrakesecure.net/en/ftp.php <i>Conectiva:</i> ftp://atualizacoes.conectiva.com.br/
Xinetd ¹⁵⁴ <i>Vendors issue advisories</i> ^{155, 156, 157}	Unix	Xinetd 2.3-2.3.10	A remote Denial of Service vulnerability exists in the 'sve_request' function when connection attempts to some services are rejected.	Upgrade available at: http://www.xinetd.org/xinetd-2.3.11.tar.gz RedHat: ftp://updates.redhat.com Mandrake: http://www.mandrakesecure.net/en/ftp.php
Xmb-forum.com ¹⁵⁸	Windows, Unix	Forum 1.8, 1.8 SP1	A Cross-Site Scripting vulnerability exists in the 'member.php' script due to insufficient filtering of script code from URL parameters, which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.

¹⁵¹ Core Security Technologies Advisory, CORE-20030304-01, March 19, 2003.

¹⁵² Red Hat Security Advisory, RHSA-2003:108-01, March 21, 2003.

¹⁵³ Conectiva Linux Security Announcement, CLA-2003:648, May 14, 2003.

¹⁵⁴ Bugtraq, April 18, 2003.

¹⁵⁵ Red Hat Security Advisory, RHSA-2003:160-01, May 13, 2003.

¹⁵⁶ Mandrake Linux Security Update Advisory, MDKSA-2003:056, May 14, 2003.

¹⁵⁷ Red Hat Security Advisory, RHSA-2003:161-07, May 22, 2003.

¹⁵⁸ Bugtraq, May 22, 2003.

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

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

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

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

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between May 15 and May 28, 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, 37 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
May 28, 2003	guess-who-0.44.tgz	A password brute force utility for SSH2.
May 28, 2003	priv8gbn.pl	Perl script that exploits the Batalla Naval Remote Buffer Overflow vulnerability.
May 28, 2003	kripp-0.5.tar.gz	A simple and light-weight network password sniffer written in Perl that uses TCPDump to intercept traffic.
May 28, 2003	nikto-1.30.tar.gz	A PERL, open source web server scanner that supports SSL and checks for (and if possible attempts to exploit) over 2000 remote web server vulnerabilities and misconfigurations.
May 28, 2003	openssh-3.6p2-bd.diff	A backdoor that logs all logins and passwords to a file.
May 28, 2003	libShellCode-0.1.0.tar.gz	A library that can be included when writing linux/i386 exploits by providing functions that generate shellcode with user given parameters during runtime.
May 28, 2003	thcrut-1.2.4g.tar.gz	A local network discovery tool developed to brute force its way into wlan access points and offers arp-request on ip-ranges and identifies the vendor of the NIC, spoofed DHCP, BOOTP and RARP requests, icmp-address mask request and router discovery techniques.
May 27, 2003	fadvWWhtdos.py	Exploit for the WebWeaver 'POST' & 'HEAD' Remote Denial of Service vulnerability.
May 27, 2003	upclient-exp.c	Script that exploits the Upclient Buffer Overflow vulnerability.

Date of Script (Reverse Chronological Order)	Script name	Script Description
May 26, 2003	rpcasrc.c	Script that exploits the Remote PC Access Denial of Service vulnerability.
May 26, 2003	batnav_exploit.pl	Perl script that exploits the Batalla Naval Remote Buffer Overflow vulnerability.
May 26, 2003	expl-ifenslave.pl	Perl script that exploits the Ifenslave Buffer Overflow vulnerability.
May 26, 2003	jsk-ifenslave-exp.c	Script that exploits the Ifenslave Buffer Overflow vulnerability.
May 24, 2003	sm00ny-uml_net.c	Script that exploits the UML_NET Integer Mismanagement Code Execution vulnerability.
May 23, 2003	0x333maelstrom.c	Script that exploits the Maelstrom Server & Player Argument Buffer Overflow vulnerability.
May 23, 2003	maelx.pl	Perl script that exploits the Maelstrom Server & Player Argument Buffer Overflow vulnerability.
May 23, 2003	maelst0x00.c.gz	Script that exploits the Maelstrom Server & Player Argument Buffer Overflow vulnerability.
May 23, 2003	b-WsMP3dvuln.txt	Technique for exploiting the WSMP3 Request Data Buffer Overflow vulnerability.
May 23, 2003	ethersniff.c	A simple utility to probe for the etherleak vulnerability where multiple platforms have Ethernet Network Interface Card (NIC) device drivers that incorrectly handle frame padding, allowing a malicious user to view slices of previously transmitted packets or portions of kernel memory due to poor programming practices.
May 23, 2003	RE_papers.tgz	Two articles that present an introduction to reverse engineering a disassembly dump from gdb into an accurate C program.
May 23, 2003	Pi3web-DoS.c	Script that exploits the Pi3Web Malformed GET Request Denial of Service vulnerability.
May 23, 2003	aimhol.zip	A simply utility that will allow an end user to query OSCAR/BOS servers on a large scale to retrieve multitudes of screen names.
May 23, 2003	vuln.c	Script that exploits the Libopt.a Error Logging Buffer Overflow vulnerability.
May 23, 2003	lsadmin-ex.sh	Script that exploits the Platform Load Sharing Facility Escalated Privileges vulnerability.
May 23, 2003	elfsh-0.5b8-linux.tgz	An interactive and scriptable reverse engineering tool with advanced read/write capabilities for the ELF format.
May 23, 2003	bsd-airtools-v0.2.tgz	A package that provides a complete tool set for wireless 802.11b auditing. It currently contains a bsd-based wep cracking application, called dweputils (as well as kernel patches for NetBSD, OpenBSD, and FreeBSD) and also contains a curses based ap detection application similar to netstumbler (dstumbler) that can be used to detect wireless access points and connected nodes, view signal to noise graphs, and interactively scroll through scanned ap's and view statistics for each.
May 23, 2003	unmaskv1.1.tar.gz	A simple md5 cracking utility that will attempt to find the true IP address.
May 22, 2003	nessus-installer.sh	A free, up-to-date, and full featured remote vulnerability scanner for Linux, BSD, Solaris and other systems that is multithreaded, plugin-based, has a nice GTK interface, and currently performs over a thousand remote security checks.
May 22, 2003	c-polymorph.c	Script that exploits the Polymorph Buffer Overflow vulnerability.

Date of Script (Reverse Chronological Order)	Script name	Script Description
May 21, 2003	bzdeath.c	Script that exploits the BZFlag Reconnect Remote Denial of Service vulnerability.
May 21, 2003	but.its.free.zip	Exploit for the Windows Media Player Automatic File Download and Execution vulnerability.
May 21, 2003	0x82-Remote.WsMp3d.again.c	Script that exploits the WSMP3 Request Data Buffer Overflow vulnerability.
May 21, 2003	prishtina-dos.pl	Perl script that exploits the Prishtina Remote Denial of Service vulnerability.
May 18, 2003	Maelstrom-exp.c	Script that exploits the Maelstrom Server & Player Argument Buffer Overflow vulnerability.
May 18, 2003	maelort.pl	Script that exploits the Maelstrom Server & Player Argument Buffer Overflow vulnerability.
May 16, 2003	nmap-matrix2log.jpg	An exploit for the SSH CRC-32 vulnerability in the new movie Matrix Reloaded.
May 15, 2003	oneorzero-poc.py	Exploit for the Helpdesk 'TUpdate.php' & 'Install.php' SQL Injection vulnerability.

Trends

- A new version of the network worm "Sobig" has been detected, Sobig.c. There here have been numerous registered infections from the new version of this malicious program. For more information, see "Virus Section."
- Sobig.B (Aliases: Palyh or Mankx) infections have been reported from over 80 countries worldwide. This worm is spreading at an increasing pace. The largest infections seem to be in UK and USA. It spreads via e-mail attachments and Windows network shares. The e-mails sent by the worm pretend to come from support@microsoft.com and they contain the message text "All information is in the attached file." Windows users everywhere are urged to update their anti-virus definitions.
- According to new research, nearly three-quarters of malicious connections to wireless networks are used for sending spam. A survey found that almost a quarter of unauthorized connections to the wireless LANs were intentional, and 71 per cent of those were used to send e-mails.
- The Department of Homeland Security (DHS), Information Analysis and Infrastructure Protection (IAIP) has issued an advisory to heighten awareness of a recently discovered Snort(TM) vulnerability, a heap overflow in the Snort "stream4" preprocessor (CAN-2003-0029). For more information see 'Bugs, Holes, & Patches Table (CyberNotes 2003-08) and DHS/IAIP Advisory 03-018, located at: <http://www.nipc.gov/warnings/advisories/2003/03-018.htm>
- The number of security events detected by companies in the first quarter of 2003 jumped nearly 84 percent over the preceding three months. The increase in events, which can include minor probes for holes in network security as well as major attacks, stems mainly from an increase in worms and automated attack software.
- Over the past few weeks, there have been an increased number of reports of intruder activity involving the exploitation of Null (i.e., non-existent) or weak Administrator passwords on Server Message Block (SMB) file shares used on systems running Windows 2000 or Windows XP. This activity has resulted in the successful compromise of thousands of systems, with home broadband users' systems being a prime target. Recent examples of such activity are the attack tools known as W32/Deloder, GT-bot, sdbot, and W32/Slackor. For more information, see CERT® Advisory CA-2003-08, located at: <http://www.cert.org/advisories/CA-2003-08.html>.

Viruses

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. **To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available.** The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported during the latest three months), and approximate date first found. During this month, a number of anti-virus vendors have included information on Trojan Horses and Worms. Following this table are descriptions of new viruses and updated versions discovered in the last two weeks. *NOTE: At times, viruses may contain names or content that may be considered offensive.*

Ranking	Common Name	Type of Code	Trends	Date
1	W32/Klez	Worm	Stable	January 2002
2	W32/Fizzer	Worm	New to table	May 2003
3	W32/Yaha	Worm	Slight Decrease	February 2002
4	W32/Sobig	Worm	Slight Decrease	January 2003
5	W32/Lovegate	Virus	Slight Decrease	February 2003
6	Elkern	File Infector	Slight Decrease	October 2001
7	W32/Sobig	Worm	New to table	May 2003
8	W32/Bugbear	File	Slight Decrease	September 2002
9	W32/SQLSlammer	Worm	Slight Increase	January 2003
10	JS/NoClose	Trojan	Decrease	May 2002

Note: Virus reporting may be weeks behind the first discovery of infection. A total **212** distinct viruses are currently considered "in the wild" by anti-virus experts, with another **320** viruses suspected. "In the wild" viruses have been reported to anti-virus vendors by their clients and have infected user machines. The additional suspected number is derived from reports by a single source.

SWF.LFM.926 (Aliases: Flash virus, ACTS.LFM, SWScript.LFM) (File Infector): This Flash infector infects Macromedia Flash files with SWF extension. This is the first virus of its kind. The only way it can successfully spread is when the SWF file is downloaded manually, placed to a directory which contains clean SWF files and then executing the file with Macromedia Flash Player. SWF.LFM.926 uses the Macromedia Flash's ActionScript scripting system to spread. While infecting other files, it shows a display saying "Loading Flash Movie."

VBS.Omni (Alias: VBA/Generic.src) (Visual Basic Script Worm): This simple VBS script infects Microsoft Word documents.

W32.Erah.A@mm (Win32 Worm): This mass-mailing worm sends itself to all the addresses in the Windows Address Book. The e-mail message has the following characteristics:

- Subject: The subject line will be one of the following:
- Attachment: <original worm filename>

The above e-mail routine will occur on the following days only: January 1, February 14, April 1, April 21, July 4, August 12, October 1, November 14, and December 25.

W32.HLLP.65542 (Win32 Worm): This virus infects files in the folders belonging to popular file-share programs and is written in Visual Basic.

W32.HLLW.Narith (Alias: Worm.P2P.Ritan)(Win32 Worm): This simple worm attempts to spread itself through the KaZaA file-sharing network. It is written in the Microsoft Visual Basic (VB) programming language. The VB run-time libraries are required to execute this worm.

W32.HLLW.Redist@mm (Aliases: W32/Gant.b@mm, W32/Gant.b@MM, W32/Outsider.A, Worm/Outsider, I-Worm.Generic) (Win32 Worm) This mass-mailing worm attempts to e-mail itself to all the contacts in the Windows Address Book. The e-mail will have a subject line and attachment chosen from a predetermined list. The attachment will have a .exe, .pif, or .scr file extension. The worm also attempts to spread itself through the KaZaA file-sharing network. It attempts to steal information from an infected computer and send it to a specified e-mail address. The worm will attempt to terminate the processes of various programs, including antivirus and firewall programs. This threat is written in the Microsoft Visual Basic (VB) programming language and is compressed with UPX. The VB run-time libraries are required to execute W32.HLLW.Redist@mm.

W32.HLLW.Shynet (Win32 Worm): This worm attempts to spread itself through the KaZaA file-sharing network. Due to a bug in the code, the worm's filename must be Regstr.exe to execute. This threat is written in the Microsoft Visual Basic (VB) programming language and is compressed with UPX. The VB run-time libraries are required to execute W32.HLLW.Shynet.

W32.HLLW.SsdX (Win32 Worm): This worm spreads using the KaZaA file-sharing program. It copies itself as the following files:

- C:\MSDOS.EXE C:\My Documents\Windows.EXE A:\NewFolder.EXE

Win32.Initx (Win32 Worm): This harmless per-process resident virus infects Windows Portable executable (PE) files that have the ".EXE" filename extension. The virus consists of two parts: its startup routine stored in infected files, and the dynamic link library (DLL) file called "initx.dat." The virus searches for suitable files with the ".EXE" extension in the Windows and Windows System directories, and all computers' network shares and tries to infect them. If the computer's name begins with "CT" in any case, the virus replicates only in the shared directories.

W32.Naco@mm (Alias: W32/Naco@MM) (Win32 Worm): This mass-mailing worm is written in Visual Basic (VB). It can spread via e-mail, peer-to-peer file-sharing applications, such as KaZaA, as well as network shares. This worm is 29,184 bytes in size. However, it has been packed with a known run-time compression utility, that is, UPX. The size of the unpacked worm is close to 100 KB. The worm also contains a functionality to run as a Backdoor Trojan Horse. It can also replace HTML files on Microsoft IIS servers. NOTE: W32.Naco@mm contains many bugs, and therefore, may not work as its author intended.

W32.Sobig.C@mm (Aliases: W32/Sobig.c@MM, Win32/Sobig.C, Sobig.C, I-Worm.Sobig.c, WORM_SOBIG.C, Win32.Sobig.C, W32/Sobig-C Win32 Virus): This virus has been reported in the wild and is rapidly spreading. It is a mass-mailing worm that sends itself to all the e-mail addresses that it finds in files with the following extensions: .wab, .dbx, .htm, .html, .eml, and .txt The e-mail falsely purports that Microsoft sent it (bill@microsoft.com). NOTE: The worm de-activates on June 8, 2003, and therefore, the last day on which the worm will spread is June 7, 2003.

W32.Vote.E@mm (Aliases: PE_DER.B, PE_VOTE.E) (Win 32 Worm): This mass-mailing worm attempts to use Microsoft Outlook to e-mail itself to all the contacts in the Windows Address Book. It also attempts to overwrite and delete numerous files on an infected system. The e-mail has the following characteristics:

- Subject: <Recipients.name>, <Random message>
- Attachment: USA.VS.IRAQ.scr, Plug-In_EXT.dll

This worm is written in Microsoft Visual Basic (VB). The VB run-time libraries must be installed for the worm to execute.

W32/Anacon-B (Aliases: I-Worm.Anacon, Win32.Naco.b, W32/Naco.b@mm, W32.Naco.B@mm, WORM_NACO.B, Naco.B, I-Worm.Nocana.b, Nocana, Naco_B, Naco, Anacon, W32/Anacon-B, Worm/Anacon, Nocana.b) (Win32 Worm): This mass mailing worm has a backdoor component that attempts to spread via e-mail using Outlook address book, network shares and popular P2P networks. The worm may arrive in an e-mail with a variety of subject lines and attachments. When executed, the worm extracts, runs, and deletes ANACON.BAT. ANACON.BAT copies and registers MSWINSCK.OCX to C:\Progra~1 folder, executes an extracted unpacked copy of the worm, copies itself to the Windows System folder and extracts an unpacked copy called SysAna32.exe, Anacon.exe or Syspoly32.exe.

W32/Auric@MM (Aliases: W32.HLLW.Magold@mm, I-Worm.Magold, Magold, Maya Gold, Auric) (Win32 Worm): This virus spreads via E-mail and comes as an attachment called "Maya Gold.scr." There are two forms of the same worm known - UPXed (240kb in size) and uncompressed (622kb). E-mail has the following characteristics:

- From: EROTIKA.LAP.HU
- Subject: May Gold-os kepernyokimelo!

The body of the E-mail is static and is in Hungarian.

W32/Duksten.o@MM (Alias: WORM_DUKSTEN.O) (Win32 Worm): This worm propagates via e-mailing itself to recipients listed in the Windows Address Book (WAB) on infected machines. It contains its own SMTP engine to construct outgoing messages, attaching itself within a ZIP file (similarly to previous W32/Duksten@MM variants). The worm also attempts to connect to a specific channel on a remote IRC server.

W32/Holar-H (Aliases: I-Worm.Hawawi.e, W32/Holar.h@MM, Win32/Holar.H, W32/Wlots, Holar.H, Worm/Holar.H, Win32-Holar.h@mm) (Win32 Worm): This Internet worm spreads via file sharing on P2P networks and by e-mailing itself to addresses found on the local computer. The e-mail subject line and message text can have many combinations. The worm copies itself to P2P shared folders and creates two files in the Windows system folder on the current drive: SMTP.ocx and explore.exe. The worm then adds the following registry entry to ensure it is run at system startup:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Explore = <Current drive:>\<Windows system folder>\Explore.exe

W32/Holar-H stores a counter of the number of times it has been run (typically the number of reboots) under the registry entry HKCU\DeathTime. When the value of this registry entry reaches 30, the worm attempts to delete files from the current drive and then displays a series of message boxes with the text "LOVE," "PEACE," "HOME," "HAPPINESS," "These things Can't be Found as long as Bush & Jews Are aLive :)," "Made By ZaCker In 2003-03-30 :)." When the user clicks OK to the last of these message boxes, Windows is shutdown.

W32/Lovgate-L (Win32 Worm): This worm has been reported in the wild. It is a minor variant of W32/Lovgate-J.

W32/Melare-A (Aliases: I-Worm.Melare, WORM_MELARE.A, W32/Melare@MM, Win32/Melare.A, W32.Ahlem.A@mm, Worm/Melare, Win32.Melare.A@mm) (Win32 Worm): This worm arrives in an e-mail with the following characteristics:

- Subject line: Alert! SARS Is being Spread!
- Attached file: The name of the executable that sent the worm.

When it is first executed, a copy is created in the Windows folder with the filename csrss.exe and the following registry entry is created so that the worm is run when Windows starts up:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\ SystemSARS32 = csrss.exe

On the 1, 4, 8, 12, 16, 20, 24, and 28 of any month this worm will attempt to delete DLL, NLS and OCX files on the infected computer.

W32/Tarit.worm (Alias: Bloodhound.w32.5) (Win32 Worm): This worm spreads purely through KaZaA networks by making multiple copies of itself into the default shared folder of KaZaA. This path is hardcoded as:

- C:\PROGRAM FILES\KAZAA\MY SHARED FOLDER

Users who use the KaZaA software are at risk. The worm has a variety of filenames.

W97M.Omni (Word 97 Macro Virus): This simple macro virus spreads by infecting Microsoft Word documents and the global template, Normal.dot.

W97M.Tchau (Word 97 Macro Virus): This simple macro virus spreads by infecting Microsoft Word documents and the global template, Normal.dot.

WM97/Lazy-C (Word 97 Macro Virus): This virus is created when a document infected with WM/Lazy is converted from Office 95 to Office 97/2000/XP format. The virus does not spread in the Office 97/2000/XP environment.

WM97/Panjang-A (Aliases: W97M/Bandung.ap, W97M/Panjang.A) (Word 97 Macro Virus): This virus is created when a document infected with WM/Panjang is converted from Office 95 to Office 97/2000/XP format. The virus does not spread in the Office 97/2000/XP environment.

Wdialupd (Aliases: W32/Wdialupd.Adware, PornDial-177, Dialer.Porno.J, TROJ_WDIALUPD.A) (Win32 Worm): The 'From:' field always consists of a seemingly random sequence of alphanumeric characters followed by '@yahoo.com.' The 'Subject:' field looks like those from common SPAM (unsolicited e-mail), referring to porn and other miscellaneous topics. In all the messages the attachment is named 'movies.zip.' The zip file contains an executable that is the actual installer/downloader of the adware. When run, the Wdialupd asks a user to select his/her location and then attempts to download and activate additional components from Internet without asking a permission.

WORM_LOVELORN.B (Aliases: W32/Lovelorn@MM, I-Worm.Lovelorn.b, Win32.Lovelorn.B worm) (Win32 Worm): This variant of WORM_LOVELORN.A similarly spreads via e-mail using its built-in SMTP (Simple Mail Transfer Protocol) engine. It sends an e-mail using a variety of subjects, message bodies, attachments and senders. This mailer gets its target recipients from files with names that contain any of these strings:

- .EML
- ITEM
- BOX
- .DBX
- .HTM

It also carries file infection routines but due to bugs in its codes, this intended routine is not always triggered. This mass-mailer also tries to copy itself to floppy disks and steals the user's passwords.

WORM.P2p.SpyBot (P2P Worm): This peer-to-peer worm has backdoor capabilities that can also spread via computers infected with some Backdoor programs. The worm is a Windows PE EXE file that is written in Visual C++. While installing itself the worm copies itself to the Windows system directory and sets the Hidden attribute for its copy. This file is then registered in the system registry in the following auto-run key entries:

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

On Windows 9x machines the worm hides itself from the task list. SpyBot also tries to kill some firewalls and ant-virus programs.

WORM_MAAx.B (Aliases: Win32.Maax.B worm, I-Worm.Axam.e) (Win32 Worm): This mass-mailing worm spreads by sending copies of itself via MAPI to all addresses found in the Outlook Addressbook. It can have a variety of subjects and the following attachment:

- Attachment: INITIAL.MSI

Note: The "click here" statement has a hyperlink to the malicious user site at:

<http://vx.netlux.org/~melhacker/axamtips.exe>. Currently, this file is unavailable for download. It deletes all files in the root directory of drive A and every 11th day of the month, the worm deletes all files with the following extension on the root directory of all local and mapped network drives: dll, jpg, doc, mdb, bmp, lnk, sys, bin, mp3, xls, pif, zip, cab, avi, mpg, vbs, gif, reg, wma, wmv. The worm has the ability to terminate antivirus processes and overwrite some system files.

Worm/Benatic.B (Alias: I-Worm.Benatic.B) (Internet Worm): When executed, this Internet worm copies itself to C:\Windows\System\<%computername%>32.exe. So that it gets run each time a user restart their computer the following registry key gets added:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
"<%loginname%>"="C:\\WINDOWS\\SYSTEM\\<%computername%>32.exe"

Worm/Druagz.P2P (Alias: Worm.P2P.Druagz) (P2P Worm): This Peer-2-Peer (P2P) worm spreads through the use of various file-sharing programs including KaZaA. If executed, the worm copies itself to

- C:\WINDOWS\SYSTEM\druagz.exe.

So that it gets run each time a user restart their computer the following registry key gets added:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
"Druagz"="C:\\WINDOWS\\SYSTEM\\Druagz.exe"

The worm copies itself and then creates a registry run key, Windows will then close it.

Worm/Pendex (Alias: Worm.Win32.Pendex) (Internet Worm): When executed, this Internet worm adds the following new files:

- SH.BAT
- SH2.BAT
- SH3.BAT

Worm/Outsider.B (Internet Worm): This Internet worm spreads through e-mail, as well as, through various file-sharing programs like KaZaA, eDonkey2000 and Bearshare. The worm arrives through e-mail in the following format:

- Subject: Re:
- Attachment: Card_05.pif

Each time a user restarts their computer the following registry key gets added:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "Windows Explorer Shell"="C:\\WINDOWS\\Winexec32.exe"
- [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices "Winhlp32"="Wscript.exe C:\\WINDOWS\\SYSTEM\\Msexec32.vbs %1"
- HKEY_CURRENT_USER\Software\Zed\Outsider "Outsider2"="W32/Outsider.B by Zed"

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 #
AdwareDropper-A	A	CyberNotes-2003-04
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	Current Issue
Backdoor.AntiLam.20.K	K	CyberNotes-2003-10
Backdoor.Assasin.D	D	CyberNotes-2003-01
Backdoor.Assasin.E	E	CyberNotes-2003-04
Backdoor.Assasin.F	F	CyberNotes-2003-09
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.E	E	CyberNotes-2003-06
Backdoor.Bigfoot	N/A	CyberNotes-2003-09
Backdoor.Bmbot	N/A	CyberNotes-2003-04
Backdoor.Bridco	N/A	CyberNotes-2003-06
Backdoor.CamKing	N/A	CyberNotes-2003-10
Backdoor.CHCP	N/A	CyberNotes-2003-03
Backdoor.Cmjspy	N/A	CyberNotes-2003-10
Backdoor.CNK.A	A	CyberNotes-2003-10
Backdoor.CNK.A.Cli	Cli	CyberNotes-2003-10
Backdoor.Colfuser	N/A	CyberNotes-2003-01
Backdoor.Cow	N/A	CyberNotes-2003-01
Backdoor.Cybspy	N/A	CyberNotes-2003-01
Backdoor.Dani	N/A	CyberNotes-2003-04
Backdoor.Darmenu	N/A	CyberNotes-2003-05
Backdoor.Death.Cli	Cli	CyberNotes-2003-10
Backdoor.Deftcode	N/A	CyberNotes-2003-01
Backdoor.Delf.Cli	Cli	CyberNotes-2003-10
Backdoor.Delf.F	F	CyberNotes-2003-07
Backdoor.Drator	N/A	CyberNotes-2003-01
Backdoor.Dvldr	N/A	CyberNotes-2003-06
Backdoor.EggDrop	N/A	CyberNotes-2003-08
Backdoor.Fatroj	N/A	CyberNotes-2003-10
Backdoor.Fatroj.Cli	Cli	CyberNotes-2003-10
Backdoor.Fluxay	N/A	CyberNotes-2003-07

Trojan	Version	CyberNotes Issue #
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.Graybird	N/A	CyberNotes-2003-07
Backdoor.Graybird.B	B	CyberNotes-2003-08
Backdoor.Graybird.C	C	CyberNotes-2003-08
Backdoor.HackDefender	N/A	CyberNotes-2003-06
Backdoor.Hethat	N/A	CyberNotes-2003-01
Backdoor.Hipo	N/A	CyberNotes-2003-04
Backdoor.Hitcap	N/A	CyberNotes-2003-04
Backdoor.Hornet	N/A	CyberNotes-2003-01
Backdoor.IRC.Aladinz	N/A	CyberNotes-2003-02
Backdoor.IRC.Cloner	N/A	CyberNotes-2003-04
Backdoor.IRC.Comiz	N/A	Current Issue
Backdoor.IRC.Lampsy	N/A	CyberNotes-2003-10
Backdoor.IRC.Ratsou	N/A	CyberNotes-2003-10
Backdoor.IRC.Ratsou.B	B	Current Issue
Backdoor.IRC.Ratsou.C	C	Current Issue
Backdoor.IRC.Yoink	N/A	CyberNotes-2003-05
Backdoor.IRC.Zcrew	N/A	CyberNotes-2003-04
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.Kol	N/A	CyberNotes-2003-06
Backdoor.Krei	N/A	CyberNotes-2003-03
Backdoor.Lala	N/A	CyberNotes-2003-01
Backdoor.LeGuardien.B	B	CyberNotes-2003-10
Backdoor.Litmus.203.c	c	CyberNotes-2003-09
Backdoor.LittleWitch.C	C	CyberNotes-2003-06
Backdoor.Longnu	N/A	CyberNotes-2003-06
Backdoor.Marotob	N/A	CyberNotes-2003-06
Backdoor.Massaker	N/A	CyberNotes-2003-02
Backdoor.Monator	N/A	CyberNotes-2003-08
Backdoor.Mots	N/A	Current Issue
Backdoor.MSNCorrupt	N/A	CyberNotes-2003-06
Backdoor.NetDevil.B	B	CyberNotes-2003-01
Backdoor.NetTrojan	N/A	CyberNotes-2003-01
Backdoor.Ohpass	N/A	CyberNotes-2003-01
Backdoor.OICQSer.165	N/A	CyberNotes-2003-01
Backdoor.OICQSer.17	17	CyberNotes-2003-01
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

Trojan	Version	CyberNotes Issue #
Backdoor.Peers	N/A	CyberNotes-2003-10
Backdoor.Plux	N/A	CyberNotes-2003-05
Backdoor.Pointex	N/A	CyberNotes-2003-09
Backdoor.Pointex.B	B	CyberNotes-2003-09
Backdoor.Private	N/A	Current Issue
Backdoor.PSpider.310	310	CyberNotes-2003-05
Backdoor.Queen	N/A	CyberNotes-2003-06
Backdoor.Ratega	N/A	CyberNotes-2003-09
Backdoor.Recevr	N/A	CyberNotes-2003-09
Backdoor.Redkod	N/A	CyberNotes-2003-05
Backdoor.Remohak.16	16	CyberNotes-2003-01
Backdoor.RemoteSOB	N/A	CyberNotes-2003-01
Backdoor.Rephlex	N/A	CyberNotes-2003-01
Backdoor.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
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	Current Issue
Backdoor.Serpa	N/A	CyberNotes-2003-03
Backdoor.Servsax	N/A	CyberNotes-2003-01
Backdoor.SilverFTP	N/A	CyberNotes-2003-04
Backdoor.Simali	N/A	CyberNotes-2003-09
Backdoor.Sixca	N/A	CyberNotes-2003-01
Backdoor.Slao	N/A	Current Issue
Backdoor.Snami	N/A	CyberNotes-2003-10
Backdoor.Snowdoor	N/A	CyberNotes-2003-04
Backdoor.Socksbot	N/A	CyberNotes-2003-06
Backdoor.Softshell	N/A	CyberNotes-2003-10
Backdoor.SubSari.15	15	CyberNotes-2003-05
Backdoor.SubSeven.2.15	2.15	CyberNotes-2003-05
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.Trynoma	N/A	CyberNotes-2003-08
Backdoor.Turkojan	N/A	CyberNotes-2003-07
Backdoor.Udps.10	10	CyberNotes-2003-03
Backdoor.UKS	N/A	Current Issue
Backdoor.Unifida	N/A	CyberNotes-2003-05
Backdoor.Upfudoor	N/A	CyberNotes-2003-01
Backdoor.VagrNocker	N/A	CyberNotes-2003-01
Backdoor.Vmz	N/A	CyberNotes-2003-01
Backdoor.Winet	N/A	Current Issue
Backdoor.Xenozbot	N/A	CyberNotes-2003-01
Backdoor.Xeory	N/A	CyberNotes-2003-03

Trojan	Version	CyberNotes Issue #
Backdoor.XTS	N/A	CyberNotes-2003-08
Backdoor.Zdemon	N/A	CyberNotes-2003-02
Backdoor.Zdemon.126	126	CyberNotes-2003-10
Backdoor.Zdown	N/A	CyberNotes-2003-05
Backdoor.Zix	N/A	CyberNotes-2003-02
Backdoor.Zombam	N/A	CyberNotes-2003-08
Backdoor.Zvrop	N/A	CyberNotes-2003-03
Backdoor-AFC	N/A	CyberNotes-2003-05
Backdoor-AOK	N/A	CyberNotes-2003-01
BackDoor-AQL	N/A	CyberNotes-2003-05
BackDoor-AQT	N/A	CyberNotes-2003-05
BackDoor-ARR	ARR	CyberNotes-2003-06
Backdoor-ARU	ARU	CyberNotes-2003-06
BackDoor-ARX	ARX	CyberNotes-2003-06
BackDoor-ARY	ARY	CyberNotes-2003-06
BackDoor-ASD	ASD	CyberNotes-2003-07
BackDoor-ASL	ASL	CyberNotes-2003-07
BackDoor-ASW	ASW	CyberNotes-2003-08
BackDoor-ATG	ATG	CyberNotes-2003-09
BackDoor-AUP	N/A	Current Issue
BDS/AntiPC	N/A	CyberNotes-2003-02
BDS/Backstab	N/A	CyberNotes-2003-02
BDS/Ciadoor.10	10	CyberNotes-2003-07
BDS/Evilbot.A	A	CyberNotes-2003-09
BDS/Evolut	N/A	CyberNotes-2003-03
BDS/PowerSpider.A	A	Current Issue
Daysun	N/A	CyberNotes-2003-06
DDoS-Stinkbot	N/A	CyberNotes-2003-08
DoS-iFrameNet	N/A	CyberNotes-2003-04
Downloader.BO.B	B	CyberNotes-2003-10
Downloader.BO.B.dr	B.dr	CyberNotes-2003-10
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
Exploit-IISInjector	N/A	CyberNotes-2003-03
Gpix	N/A	CyberNotes-2003-08
Hacktool.PWS.QQPass	N/A	CyberNotes-2003-06
ICQPager-J	N/A	CyberNotes-2003-05
IRC/Backdoor.e	E	CyberNotes-2003-01
IRC/Backdoor.f	f	CyberNotes-2003-02
IRC/Backdoor.g	g	CyberNotes-2003-03
IRC/Flood.ap	N/A	CyberNotes-2003-05
IRC/Flood.bi	N/A	CyberNotes-2003-03
IRC/Flood.br	br	CyberNotes-2003-06
IRC/Flood.bu	bu	CyberNotes-2003-08
IRC/Flood.cd	cd	Current Issue

Trojan	Version	CyberNotes Issue #
IRC-Emoz	N/A	CyberNotes-2003-03
IRC-OhShootBot	N/A	CyberNotes-2003-01
IRC-Vup	N/A	CyberNotes-2003-09
JS.Fortnight.B	B	CyberNotes-2003-06
JS.Seeker.J	J	CyberNotes-2003-01
JS/Fortnight.c@M	c	Current Issue
JS/Seeker-C	C	CyberNotes-2003-04
JS/StartPage.dr	dr	Current Issue
JS_WEBLOG.A	A	CyberNotes-2003-05
KeyLog-Kerlib	N/A	CyberNotes-2003-05
Keylog-Perfect.dr	dr	CyberNotes-2003-09
Keylog-Razytimer	N/A	CyberNotes-2003-03
KeyLog-TweakPan	N/A	CyberNotes-2003-02
Linux/Exploit-SendMail	N/A	CyberNotes-2003-05
MultiDropper-FD	N/A	CyberNotes-2003-01
Pac	N/A	CyberNotes-2003-04
ProcKill-AE	N/A	CyberNotes-2003-05
ProcKill-AF	N/A	CyberNotes-2003-05
ProcKill-AH	AH	CyberNotes-2003-08
ProcKill-Z	N/A	CyberNotes-2003-03
Proxy-Guzu	N/A	CyberNotes-2003-08
PWS-Aileen	N/A	CyberNotes-2003-04
PWSteal.ALlight	N/A	CyberNotes-2003-01
PWSteal.Hukle	N/A	CyberNotes-2003-08
PWSteal.Kipper	N/A	CyberNotes-2003-10
PWSteal.Lemir.105	105	CyberNotes-2003-10
PWSteal.Rimd	N/A	CyberNotes-2003-01
PWSteal.Rimd.B	B	CyberNotes-2003-10
PWSteal.Senhas	N/A	CyberNotes-2003-03
PWSteal.Snatch	N/A	CyberNotes-2003-10
PWS-Tenbot	N/A	CyberNotes-2003-01
PWS-Watsn	N/A	CyberNotes-2003-10
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
QDial6	6	Current Issue
Renamer.c	N/A	CyberNotes-2003-03
Reom.Trojan	N/A	CyberNotes-2003-08
StartPage-G	G	CyberNotes-2003-06
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

Trojan	Version	CyberNotes Issue #
Tr/DelWinbootdir	N/A	CyberNotes-2003-07
TR/Fake.YaHoMe.1	N/A	CyberNotes-2003-02
Tr/SpBit.A	A	CyberNotes-2003-04
Tr/VB.t	T	Current Issue
TR/WinMx	N/A	CyberNotes-2003-02
Troj/Dloader-BO	BO	CyberNotes-2003-02
Troj/IRCBot-C	C	Current Issue
Troj/Manifest-A	N/A	CyberNotes-2003-03
Troj/Peido-B	B	CyberNotes-2003-10
Troj/Qzap-248	N/A	CyberNotes-2003-01
Troj/SadHound-A	N/A	CyberNotes-2003-03
Troj/Slacker-A	A	CyberNotes-2003-05
Troj/Slanret-A	N/A	CyberNotes-2003-03
Troj/TKBot-A	A	CyberNotes-2003-04
TROJ_JBELLZ.A	A	CyberNotes-2003-02
TROJ_KILLBOOT.B	B	CyberNotes-2003-01
TROJ_RACKUM.A	A	CyberNotes-2003-05
Trojan.AprilFool	N/A	CyberNotes-2003-08
Trojan.Barjac	N/A	CyberNotes-2003-05
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.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.KKiller	N/A	CyberNotes-2003-01
Trojan.Lear	N/A	CyberNotes-2003-10
Trojan.Poldo.B	B	CyberNotes-2003-02
Trojan.Poot	N/A	CyberNotes-2003-05
Trojan.PopSpy	N/A	Current Issue
Trojan.ProteBoy	N/A	CyberNotes-2003-04
Trojan.PSW.Gip	N/A	CyberNotes-2003-06
Trojan.PSW.Platan.5.A	N/A	CyberNotes-2003-01
Trojan.PWS.QQPass.D	N/A	CyberNotes-2003-02
Trojan.Qforager	N/A	CyberNotes-2003-02
Trojan.Qforager.Dr	N/A	CyberNotes-2003-02
Trojan.Qwe	N/A	CyberNotes-2003-02
Trojan.Snag	N/A	CyberNotes-2003-02
Trojan.Unblockee	N/A	CyberNotes-2003-01
Uploader-D	D	CyberNotes-2003-06
Uploader-D.b	D.b	CyberNotes-2003-07
VBS.Kasnar	N/A	CyberNotes-2003-06
VBS.Moon.B	B	CyberNotes-2003-02
VBS.StartPage	N/A	CyberNotes-2003-02
VBS.Trojan.Lovcx	N/A	CyberNotes-2003-05

Trojan	Version	CyberNotes Issue #
VBS.Zizam	N/A	CyberNotes-2003-09
VBS.Fourcourse	N/A	CyberNotes-2003-06
W32.Adclicker.C.Trojan	C	CyberNotes-2003-09
W32.Benpao.Trojan	N/A	CyberNotes-2003-04
W32.CV1H.Trojan	N/A	CyberNotes-2003-06
W32.Noops.Trojan	N/A	CyberNotes-2003-09
W32.Socay.Worm	N/A	CyberNotes-2003-02
W32.Systemtry.Trojan	N/A	CyberNotes-2003-03
W32.Xilon.Trojan	N/A	CyberNotes-2003-01
W32.Yinker.Trojan	N/A	CyberNotes-2003-04
W32/Igloo-15	N/A	CyberNotes-2003-04
Xin	N/A	CyberNotes-2003-03

Backdoor.Amitis.B (Aliases: BackDoor-AKZ, Backdoor.Amitis.13): This Backdoor Trojan Horse allows unauthorized access to the infected computer. By default, the Trojan opens TCP ports 12345, 3547, 47387, 44390, 7823, 13173, 64429, and 44280. This threat is written in Borland Delphi and compressed with UPX. The unpacked size is approximately 808 KB.

BackDoor-AUP (Aliases: Backdoor.Delf.fr, BackDoor.LMR.20, Win32.LMR.20): This is a remote access backdoor Trojan. There are several versions of this Trojan existed. When the server is run on victim's machine, it copies itself to Windows system directory as %SysDir%\Svced.exe. It creates the following registry key in order to load itself at Windows start up:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "svced" = C:\WINDOWS\SYSTEM\svced.exe
- Once the server is running, it opens port 25226, 45672 and listens on these ports.

Backdoor.IRC.Comiz: This Backdoor Trojan Horse gives its creator full control over your computer.

Backdoor.IRC.Ratsou.B: This Backdoor Trojan Horse gives its creator full control over your computer. The Trojan may be downloaded by Trojan.Downloader.Aphe from the Web site, <http://amateur.freegayspace.com>.

Backdoor.IRC.Ratsou.C: This Backdoor Trojan Horse gives its creator full control over your computer. The Trojan may be downloaded by Trojan.Downloader.Aphe from the Web site, <http://www.3raby.com>.

Backdoor.Mots: This Backdoor Trojan Horse will connect to an IRC server to receive remote commands.

Backdoor.Private: This Backdoor Trojan Horse allows unauthorized access to a compromised system. It allows the intruder access to files and machine functions. The Trojan also causes machine instability and possible system crashes. The Trojan is written in the Delphi programming language and is packed. Communication to the intruder is done via the ICQ and mIRC channels. The Trojan uses port 666, by default.

Backdoor.Sdbot.L (Alias: Backdoor.Sdbot): This Backdoor Trojan Horse is a variant of Backdoor.Sdbot. It allows the Trojan's creator to use Internet Relay Chat (IRC) to gain access to an infected computer. This threat is written in the Microsoft Visual Basic (VB) programming language. The VB run-time libraries are required to execute Backdoor.Sdbot.L.

Backdoor.Slao: This Backdoor Trojan Horse allows unauthorized access to an infected computer. This threat is written in the Microsoft Visual Basic (VB) programming language. The VB run-time libraries are required to execute Backdoor.Slao.

Backdoor.UKS (Alias: Backdoor.UKS.Client): This Backdoor Trojan Horse allows unauthorized access to an infected computer. Both the server and client programs are written in Visual Basic.

Backdoor.Winet (Alias: Trojan Horse): This Backdoor Trojan Horse will install itself in the System directory. It receives instructions from a hard-coded URL.

BDS/PowerSpider.A (Alias: Backdoor.PowerSpider.A): Like other backdoors, this Trojan could potentially allow someone with malicious intent remote access to your computer. If executed, the Trojan adds the following file to the \windows\%system% directory, "IEXPLORE .EXE." So that it gets run each time a user restart their computer the following registry key gets added:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices]
"mssysint"="IEXPLORE .EXE"

IRC/Flood.cd (Alias: Backdoor.IRC.Flood.E): This detection is for an Internet Relay Chat (IRC) bot/DDoS tool. Exact details will vary according to the specific actions desired by the malicious user who creates the package, which is delivered via a dropper file. The main dropper file is approximately 850kB in length. When run, a series of files are dropped into a specific directory on the local disk. Typically, the mIRC client will be installed to run at system startup, via a Registry key. For example:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "taskdebug" = C:\WINNT\INF\TSKDBG.EXE

JS/Fortnight.c@M: This Trojan spreads by inserting a bit of HTML code into every message sent through Microsoft Outlook Express. This is accomplished by creating a new HTML file, and setting it as the default signature file used by Outlook Express. This virus exploits an Internet Explorer vulnerability in order to propagate.

JS/StartPage.dr (Alias: TrojanDropper.JS.Mimail): The purpose of this Trojan is to extract and run another program. This extracted program changes the default start page of Internet Explorer. This Trojan arrives in an e-mail message with a ZIP file called reg.zip. The ZIP file contains the file reg.html. If the reg.html file is opened (it does not open automatically in known e-mail attachments), it creates a file named reg.exe, which is contained inside reg.html in MIME-encoded format, and runs it. This reg.exe file is a Start Page changing Trojan.

QDial6 (Alias: Dial/Top-A): This generic detection for a Trojan tries to use an installed Modem to place a call. The phone number that is dialed may get changed. After execution, the Trojan starts dialing without displaying any dialog or warning messages. It does not make any changes to the registry or system files.

Tr/VB.t (Alias: TrojanWin32.VB.t): This Trojan could potentially allow someone with malicious intent backdoor access to your computer. If executed, the Trojan adds the following files to the root directory, "write.js" and "programacion.html." So that it gets run each time a user restart their computer the following registry key gets added:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
"gpvcwar"="c:\windows\java\jaVirginiaexe"

Tr/VB.t was originally received as "programacion.exe."

Troj/IRCBot-C: This backdoor Trojan allows a remote intruder to access and control a computer via IRC channels. The installation executable for Troj/IRCBot-C typically arrives via e-mail or via IRC channels as a DCC send. When run, the installation executable for Troj/IRCBot-C drops the files listed below to the C:\WINNT\SYSTEM32\ folder. If this folder does not exist (i.e. on Win9x), it will be created.

- exe32.exe MIRC.INI REMOTE.INI secure.bat server.txt win.dll wind.bat

The following clean utility programs are also dropped to the C:\WINNT\SYSTEM32\ folder:

- NB.EXE bnc.exe fnet.exe libparse.exe psexec.exe rpcserv.exe SYS32.EXE wget.exe

The installation executable launches exe32.exe, an MS-DOS program that simply launches C:\WINNT\SYSTEM32\NB.EXE. Exe32.exe is copied to the folder C:\Documents and Settings\All Users\Start Menu\Programs\Startup\ so that exe32.exe, and thus NB.EXE, are launched automatically each time Windows is started. NB.EXE is a clean mIRC client that connects to a remote IRC server and joins a

specific channel. The remote intruder will then be able to gain access and control over the computer using a regular IRC client. NB.EXE sets a number of IRC, mIRC and ChatFile registry entries, overriding any previous installations and making itself the default IRC client.

Trojan.PopSpy: This program gathers system information on a compromised system and sends information and screenshots to predetermined addresses.