



Department of Homeland Security

Information Analysis and Infrastructure Protection Directorate

CyberNotes

Issue #2003-19

September 22, 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 September 4 and September 20, 2003. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
4D Inc. ¹	Windows	WebSTAR 5.2-5.2.4, 5.3, 5.3.1	A buffer overflow vulnerability exists in the 'PASS' command when handling excessive data due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	4D WebSTAR Remote Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit script has been published.

¹ Securiteam, September 16, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Aegis Group ²	Windows	FoxWeb 2.5	A buffer overflow vulnerability exists in the 'foxweb.dll' due to insufficient bounds checking of user-supplied data, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	FoxWeb Remote Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Andries Brouwer ³	Unix	man 1.5 m1, 1.5 m, 1.5 l, 1.5 k, 1.5 j, 1.5 i2, 1.5 i, 1.5 h1	A buffer overflow vulnerability exists in the 'MANPL' environment variable due to insufficient bounds checking, which could let a malicious user execute arbitrary code.	Upgrade available at: ftp://ftp.win.tue.nl/pub/linux-local/utills/man/man-1.5m2.tar.gz	Man Utility MANPL Environment Variable Buffer Overflow	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
b2evolution ⁴	Multiple	b2evolution 0.8.2	Several vulnerabilities exist: a Cross-Site Scripting vulnerability exists which could let a remote malicious user execute arbitrary HTML or script code; and multiple SQL injection vulnerabilities exist due to a failure to sanitize user-supplied input which could let a remote malicious user execute arbitrary code.	Update available at: Update to version 0.8.2.2: http://prdownloads.sourceforge.net/evocms/b2evolution-0.8.2.2-2003-09-02.zip?download	b2evolution Cross-Site Scripting & SQL Injection Vulnerabilities	High	Bug discussed in newsgroups and websites.
Cache Flow ⁵	Multiple	CacheOS 4.1.10016	A vulnerability exists because the 'HOST' header value can be misused, which could let a malicious user tunnel arbitrary TCP connections through a HTTP request.	No workaround or patch available at time of publishing.	CacheFlow CacheOS HTTP HOST Proxy	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

² SCAN Associates Sdn Bhd Security Advisory, September 5, 2003.

³ SecurityTracker Alert, 1007685, September 12, 2003.

⁴ SecurityFocus, September 10, 2003.

⁵ Bugtraq, September 10, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Cisco Systems ⁶ <i>Update regarding work-around⁷</i>	Multiple	WebNS 5.0 0.038s	A remote Denial of Service vulnerability exists in the Online Diagnostics Monitor (ONDM) when a malicious user submits a flood of TCP SYN packets to the System Controller Module (SCM) on Cisco Content Service Switches. <i>The vendor has reported that previous fix information advised by a third party to address this vulnerability was erroneous. Maintenance releases to address this issue are pending; customers who are affected by this issue are advised to apply the workaround until an appropriate vendor fix is made available.</i>	Upgrade available at: http://www.cisco.com/en/US/products/hw/contentw/ps789/prod_release_note09186a008014ee04.html <u>Workaround:</u> <i>The vendor has reported that affected customers may workaround this issue, by using ACLs on an upstream router to protect the circuit address.</i>	Content Service Switch ONDM Ping Remote Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Claudio Fontana ⁸	Multiple	CmdFTP 0.52, 0.62, 0.64	A heap overflow vulnerability exists in the 'store_line()' function due to insufficient boundary checks when handling FTP server directory listings, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://prdownloads.sourceforge.net/cmdftp/cmdftp-0.641.tar.gz?download	CmdFTP 'Store_Line()' Heap Overflow	High	Bug discussed in newsgroups and websites. Exploit has been published.
Craig Knudsen ⁹	Windows, Unix	Web Calendar 0.9.8, 0.9.11, 0.9.15, 0.9.16, 0.9.19-0.9.42	Multiple vulnerabilities exist: several input validation vulnerabilities exist in the 'includes/js/colors.php,' 'week.php,' 'day.php,' 'month.php,' 'week_details.php,' 'view_1.php,' 'view_m.php,' 'view_t.php,' 'view_v.php,' 'view_w.php,' and 'week_details.php' modules, which could let a remote malicious user execute arbitrary code; and multiple Cross-Site Scripting vulnerabilities exist in the 'view_t.php,' 'view_w.php,' 'view_v.php,' and 'login.php' modules due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	WebCalendar Multiple Input Validation & Cross-Site Scripting	High	Bug discussed in newsgroups and websites.

⁶ S 2 1 S E C Advisory, August 7, 2003.

⁷ SecurityFocus, September 8, 2003.

⁸ Secunia Advisory, SA9684, September 8, 2003.

⁹ Secunia Advisory, SA9672, September 4, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Digicraft Software ¹⁰	Windows	Yak! 2.0-2.0.2	A vulnerability exists when connecting to TCP port 3535 and logging into the FTP service using a standard username and password, which could let an unauthorized remote malicious user obtain access.	No workaround or patch available at time of publishing.	Yak! Chat Client FTP Server Default Credentials	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Digital Scribe ¹¹	Multiple	Digital Scribe 1.0-1.3	Several Cross-Site Scripting vulnerabilities exist in the 'login.php' and 'register.php' scripts due to insufficient validation, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Digital Scribe Error Function Cross-Site Scripting	High	Bug discussed in newsgroups and websites. There is no exploit code required, however, a Proof of Concept exploit has been published.
Donald R. Woods ¹²	Unix	Spider 1.1	Two vulnerabilities exist: a heap overflow vulnerability exists in 'util.c' in the remove_newlines() function, which could let a malicious user execute arbitrary code; and a buffer overflow vulnerability exists in 'vx_ui.c' in the spider_defaults_objects_initialize() function, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Spider Heap Overflow & Buffer Overflow	High	Bug discussed in newsgroups and websites.
EFS Software ¹³	Windows	Easy File Sharing Web Server 1.2	Several vulnerabilities exist: a Directory Traversal vulnerability exists due to insufficient verification of user-supplied requests, which could let a malicious user obtain sensitive information; a vulnerability exists in the 'users.sdb' file because passwords are stored in clear text, which could let a malicious user obtain sensitive information; and a vulnerability exists in the post icon, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Easy File Sharing Web Server Multiple Vulnerabilities	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

¹⁰ SecurityTracker Alert, 1007694, September 13, 2003.

¹¹ Secunia Advisory, SA9682, September 5, 2003.

¹² Zone-H Research Laboratories Advisory, ZH2003-27SA, September 14, 2003.

¹³ SecurityTracker Alert, 1007711, September 15, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Floosietek ¹⁴	Windows 2000, XP	FTGatePro 1.2 (1331)	Multiple vulnerabilities exist: a vulnerability exists in the WebAdmin Interface due to insufficient access controls, which could let an unauthorized malicious user obtain sensitive information; a vulnerability exists because the POP server returns different error messages in response to valid login attempts versus invalid login attempts, which could let a malicious user obtain sensitive information; and a vulnerability exists in the 'index.fts' script due to insufficient filtering of user-supplied HTML, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	FTGatePro Multiple Vulnerabilities	Medium/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. There is no exploit code required.
FreeBSD ¹⁵ <i>NetBSD issues advisory</i> ¹⁶	Unix	FreeBSD 4.0-4.8, 5.0, 5.1, 4.1.1 – STABLE-4.7 – STABLE, 4.1.1 – RELEASE - 4.3 – RELEASE , 4.5 – RELEASE - 4.7 – RELEASE , 4.3 – RELENG, 4.4 – RELENG	An information disclosure vulnerability exists due to the IBCS2 system call translator for "statfs()" erroneously using the user-supplied length parameter when copying kernel data structures, which could let a malicious user obtain sensitive information.	Patches available at: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-03:10/ibcs2.patch <i>NetBSD:</i> ftp://ftp.NetBSD.org/pub/NetBSD/security/patches/SA2003-013-ibcs2.patch	FreeBSD IBCS2 System Call Translator Information Disclosure	Medium	Bug discussed in newsgroups and websites.
FTP Solutions, Inc. ¹⁷	Windows	FTP Desktop 3.5	Several buffer overflow vulnerabilities exist when parsing 'Welcome' banner 220 messages or parsing 331 server responses from remote FTP servers, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	FTP Desktop Remote Buffer Overflows	High	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.

¹⁴ Bugtraq, September 10, 2003.

¹⁵ FreeBSD Security Advisory, FreeBSD-SA-03:10.ibcs2, August 11, 2003.

¹⁶ NetBSD Security Advisory, 2003-013, September 18, 2003.

¹⁷ SecurityTracker Alert, 1007659, September 8, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Future Wave Tech Inc. ¹⁸	Windows	WebX Lite, WebX Server 1.1	A Directory Traversal vulnerability exists due to insufficient verification of user-supplied input, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	WebX Server Directory Traversal	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
GameSpy Industries ¹⁹	Windows NT	Roger Wilco Dedicated Server (Linux, BSD) 0.26-0.30 a, Graphical Server 1.4.1.1-1.4.1.6	A buffer overflow vulnerability exists when processing malformed client packets, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Roger Wilco Remote Server Side Buffer Overflow	High	Bug discussed in newsgroups and websites.
GameSpy Industries ²⁰	Windows NT	Roger Wilco Graphical Server 1.4.1 .6	Remote Denial of Service vulnerability exists when a malicious user connects with an excessively long username.	No workaround or patch available at time of publishing.	Roger Wilco Remote Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Gordano ²¹	Windows, Unix	Gordano Messaging Suite 9.0	Several vulnerabilities exist: a remote Denial of Service vulnerability exists in 'WWW.exe' when a malicious user submits a malformed HTTP GET request; and a vulnerability exists in the 'alertlist.mml' script which could let a remote malicious user obtain sensitive information.	Patches available at <u>Linux</u> : ftp://ftp.gordano.com/gms/3138/hotfixes/h20030905/linux/www_h20030905.zip <u>Windows</u> : ftp://ftp.gordano.com/gms/3138/hotfixes/h20030905/windows/www_h20030905.zip	Gordano Messaging Suite Remote Denial of Service & Information Disclosure	Low/ Medium (Medium if sensitive information can be obtained)	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.

¹⁸ SecurityTracker Alert, 1007663, September 9, 2003.

¹⁹ Secunia Advisory, SA9693, September 10, 2003.

²⁰ Bugtraq, September 8, 2003.

²¹ Securiteam, September 16, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Hewlett Packard Company ²²	Unix	Compaq Tru64 4.0g, PK4 (BL22), PK3 (BL17), 4.0f, PK8 (BL22), PK7 (BL18), PK6 (BL17), 5.0, PK4 (BL18), PK4 (BL17), 5.1b, PK2 (BL22), PK1 (BL1), 5.1 a, PK5 (BL23), PK4 (BL21), PK3 (BL3), PK2 (BL2), PK1 (BL1), 5.1, PK6 (BL20), PK5 (BL19), PK4 (BL18), PK3 (BL17)	A Denial of Service vulnerability exists due to the way AdvFS files are handled.	Patches available at: http://ftp.support.compaq.com/patches/public/unix/	Tru64 NFS AdvFS File Denial of Service	Low	Bug discussed in newsgroups and websites.

²² SecurityFocus, September 13, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Hewlett Packard Company ²³	Unix	Compaq Tru64 4.0g, PK4 (BL22), PK3 (BL17), 4.0f, PK8 (BL22), PK7 (BL18), PK6 (BL17), 5.1b, PK2 (BL22), PK1 (BL1), 5.1a, PK5 (BL23), PK4 (BL21), PK3 (BL3), PK2 (BL2), PK1 (BL1), 5.1, PK6 (BL20), PK5 (BL19), PK4 (BL18), PK3 (BL17)	A local/remote Denial of Service vulnerability exists in the 'dterm' terminal emulator code.	Patches available at: http://ftp.support.compaq.com/patches/publis/unix	Tru64 UNIX DTerm Local/Remote Denial of Service CVE Name: CAN-2003-0064	Low	Bug discussed in newsgroups and websites.
HLSW ²⁴	Multiple	HLSW 1.0.0.8 beta, 1.0.0.7 beta, 1.0.0.6 beta, 1.0.0.5 beta, 1.0.0.4 beta	A vulnerability exists in the RCON game server console because passwords are not encrypted when exchanged between the client and server, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	HLSW RCON Console Password Disclosure	Medium	Bug discussed in newsgroups and websites.
IBM ²⁵	Unix	AIX 4.3.3, 5.1, 5.2	A format string vulnerability exists in the 'tsm' utility, which could let a malicious user obtain root privileges.	Patches available at: http://techsupport.services.ibm.com/server/aix.fdc	AIX tsm Utility Format String	High	Bug discussed in newsgroups and websites.
IBM ²⁶	Unix	AIX 4.3.3, 5.1, 5.2	A vulnerability exists due to a format string error in the 'LPD' Service, which could let a malicious user execute arbitrary code with root privileges.	Patches available at: http://techsupport.services.ibm.com/r	AIX lpd Format String	High	Bug discussed in newsgroups and websites.

²³ Hewlett-Packard Company Software Security Response Team Advisory, SSRT3507, September 10, 2003.

²⁴ Bugtraq, September 18, 2003.

²⁵ Secunia Advisory, SA9789, September 19, 2003.

²⁶ Secunia Advisory, SA9788, September 19, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
IBM ²⁷	Unix	DB2 Universal Database for Linux 7.2	Several vulnerabilities exist: a buffer overflow vulnerability exists in the 'db2dart' utility because long strings are not handled properly, which could let a malicious user execute arbitrary code; and a buffer overflow vulnerability exists in the 'db2licm' utility because long strings are not handled properly, which could let a malicious user execute arbitrary code.	Patch available at: ftp://ftp.software.ibm.com/products/db2/fixes/english-us/db2linuxv7/FP10a_U49517	DB2 'db2dart' & 'db2licm' Buffer Overflows CVE Names: CAN-2003-0758, CAN-2003-0759	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
ICQ Inc. ²⁸	Windows	Mirabilis ICQ 2003 a Build #3800, Build #3799, Build #3777	A Cross-Site Scripting vulnerability exists in the guestbook module due to insufficient sanitization of user-supplied data, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Webfront guestbook Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Ikonboard.com ²⁹	Windows NT 4.0/2000, Unix	Ikonboard 2.1 .0, 2.1.7b & previous, 2.1.8, 2.1.9, 2.17, 3.0 .1, 3.1.1, 3.1.2a	A vulnerability exists due to insufficient sanitization of user-supplied default cookie data, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	IkonBoard Arbitrary Command Execution	High	Bug discussed in newsgroups and websites.
Internet Security Systems ³⁰	Windows NT 4.0/2000	RealSecure Server Sensor 7.0 XPU 20.18, 7.0 XPU 20.16	A remote Denial of Service vulnerability exists when handling a malicious request over SSL. Execution of arbitrary code may also be possible.	Users should contact the vendor for details on obtaining upgrades.	RealSecure Remote Denial of Service CVE Name: CAN-2003-0702	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Vulnerability may be exploited via a web browser.
Invision Power Services ³¹	Multiple	Invision Board 1.0-1.2	A Cross-Site Scripting vulnerability exists in the 'index.php; script, which could let a remote malicious user execute arbitrary HTML or script code.	No workaround or patch available at time of publishing.	Invision Power Board Index.php Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
IpSwitch ³²	Windows	WS FTP Server 3.4, 4.0 1	A buffer overflow vulnerability exists in the 'APPE' and STAT FTP' commands when handling excessive data, which could let a remote malicious user execute arbitrary code or cause a Denial of Service.	No workaround or patch available at time of publishing.	WS_FTP Server Buffer Overflow	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

²⁷ Core Security Technologies Advisory, CORE-2003-0531, September 18, 2003.

²⁸ Exploitlabs.com Advisory, EXPL-A-2003-024 024, September 7, 2003.

²⁹ Bugtraq, September 9, 2003.

³⁰ Bugtraq, September 5, 2003.

³¹ SecurityFocus, September 9, 2003.

³² Bugtraq, September 6, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
KDE ^{33, 34} 35, 36, 37	Unix	KDE 1.1-1.1.2, 1.2, 2.0 BETA, 2.0- 2.2.2, 3.0- 3.0.5, 3.1- 3.1.3	Two vulnerabilities exist: a vulnerability exists in the KDE Display Manager (KDM) when used in combination with Pluggable Authentication Modules (PAM), which could let an unauthorized remote malicious user obtain root access; and a vulnerability exists due to a weak session cookie algorithm that does not fully use the available 128 bits of entropy, which could let a remote malicious user obtain system access.	Patches available at: ftp://ftp.kde.org/pub/kde/security_patches Conectiva: ftp://atualizacoes.conectiva.com.br/ Debian: http://security.debian.org/pool/updates/main/k/kdebase/ Mandrake: http://www.mandrakesecure.net/en/advisories/ RedHat: ftp://updates.redhat.com/	KDM PAM Module PAM_SetCred Privilege Escalation CVE Names: CAN-2003- 0690, CAN-2003- 0692	High	Bug discussed in newsgroups and websites.
Kokesh CMS ³⁸	Multiple	Kokesh CMS 0.1 0.11	A vulnerability exists in 'edit.php' due to inadequate authentication before editing content, which could let a remote malicious user bypass security and manipulate data.	Upgrade available at: http://prdownloads.sourceforge.net/kokeshcms/KokeshCMS_0_2.zip?download	KokeshCMS Insufficient Authentication	Medium	Bug discussed in newsgroups and websites. Vulnerability may be exploited via a web browser.
Kukol ³⁹	Multiple	Kukol E.V. HTTP & FTP Server Suite 6.2	A Directory Traversal vulnerability exists in the web server component, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Kukol E.V. HTTP & FTP Server Suite Directory Traversal	Medium	Bug discussed in newsgroups and websites. Vulnerability may be exploited via a web browser.
Leafnode ⁴⁰	Unix	Leafnode 1.9.19- 1.9.27, 1.9.29- 1.9.31, 1.9.35- 1.9.41	A remote Denial of Service vulnerability exists in the fetchnews program when a malicious user posts malformed Usenet news articles.	Upgrade available at: http://sourceforge.net/projects/showfiles.php?group_id=57767&release_id=182196	Leafnode fetchnews Remote Denial of Service	Low	Bug discussed in newsgroups and websites.
Linux Support Services, Inc. ⁴¹	Unix	Asterisk 0.1.7- 0.1.9, 0.2, 0.3, 0.4	A buffer overflow vulnerability exists in the Session Initiation Protocol (SIP) implementation in the 'chan_sip.c' file due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code.	Patch available at: ftp://ftp.asterisk.org/pub/telephony	Asterisk SIP Request Buffer Overrun CVE Name: CAN-2003- 0761	High	Bug discussed in newsgroups and websites.

³³ KDE Security Advisory, September 16, 2003.

³⁴ Red Hat Security Advisory, RHSA-2003:269-01, September 16, 2003.

³⁵ Mandrake Linux Security Update Advisory, MDKSA-2003:091, September 17, 2003.

³⁶ Conectiva Linux Security Announcement, CLA-2003:747, September 19, 2003.

³⁷ Debian Security Advisory, DSA 388-1, September 19, 2003.

³⁸ Secunia Advisory, SA9685, September 9, 2003.

³⁹ SecurityFocus, September 8, 2003.

⁴⁰ LeafNode Security Advisory, leafnode-SA-2003:01, September 4, 2003.

⁴¹ @stake Inc. Security Advisory, September 4, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Linux Support Services, Inc. ⁴²	Unix	Asterisk 0.1.7-0.1.9, 0.2, 0.3, 0.4	A vulnerability exists in the Call Detail Record logging function due to insufficient validation of CDR data, which could let a remote malicious user execute SQL commands.	Update available at: http://www.asterisk.org/	Asterisk Call Detail Records SQL Injection CVE Name: CAN-2003-0779	High	Bug discussed in newsgroups and websites.
Lucent ⁴³	Multiple	MAX TNT Universal Gateway 8.0.1	A vulnerability exists due to the way hang-up and redial calls are handled, which could let a malicious user obtain unauthorized administrative access.	No workaround or patch available at time of publishing.	MAX TNT Universal Gateway Administrative Access	High	Bug discussed in newsgroups and websites. There is no exploit code required.
Mambo-server.com ⁴⁴	Windows, Unix	Mambo Site Server 4.0.14	Multiple vulnerabilities exist: a vulnerability exists in the '\$id' variable due to insufficient validation of user-supplied input, which could let a remote malicious user obtain sensitive information; a vulnerability exists when the target system has 'magic_quotes_gpc' turned off and is running MySQL version 4.x, which could let a remote malicious user execute arbitrary SQL commands; a vulnerability exists in the 'contact.php' script, which could let a remote malicious user send "anonymous" e-mail; and a vulnerability exists in the 'banners.php' script, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Multiple Mambo Server Vulnerabilities	Medium/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Michael Legart ⁴⁵	Unix	Apache::Gallery 0.4, 0.4.1, 0.5, 0.5.1, 0.6	A vulnerability exists in the 'Gallery.pm' module because shared libraries are created insecurely in a temporary directory, which could let a malicious user execute arbitrary code.	Upgrade available at: http://svn.apachegallery.dk/snapshots/	Apache::Gallery Code Execution	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Microsoft ⁴⁶	Windows NT	ASP.NET 1.1	A Cross-Site Scripting vulnerability exists in the 'Request Validation' feature due to insufficient sanitization of user-supplied input, which could let a malicious user bypass the security mechanism and execute arbitrary code.	No workaround or patch available at time of publishing.	ASP.NET Cross-Site Scripting	High	Bug discussed in newsgroups and websites. There is no exploit code required.

⁴² @stake, Inc. Security Advisory, a091103-1, September 11, 2003.

⁴³ SecurityFocus, September 17, 2003.

⁴⁴ Bugtraq, September 18, 2003.

⁴⁵ Bugtraq, September 7, 2003.

⁴⁶ WebCohort Research Advisory, September 8, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft ⁴⁷	Windows 95/98/SE/NT 4.0/2000, 2003	Internet Explorer 5.0.1, SP1-SP3, 5.5, SP1&SP2, 6.0, SP1	A vulnerability exists because object types are not handled properly when rendering malicious popup windows, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Internet Explorer Browser Popup Window	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Microsoft ⁴⁸	Windows 98/SE/NT 4.0/2000, 2003	Internet Explorer 6.0, SP1	A vulnerability exists due to a flaw in the media sidebar to cause IE to load a resource file in the "My Computer" zone, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Internet Explorer Media Sidebar	High	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published. Vulnerability has appeared in the press and other public media.
Microsoft ⁴⁹	Windows 98	Windows 98, SP1	A remote Denial of Service vulnerability exists when a malicious user submits a fragmented flood of spoofed UDP packets.	No workaround or patch available at time of publishing.	Windows 98 Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
Microsoft ⁵⁰	Windows 95/98/SE/NT. 40/2000, 2003	Internet Explorer 5.0.1, SP1-SP3, 5.5, SP1&SP2, 6.0, SP1	A vulnerability exists when rendering XML based web sites due to a failure to properly handle object types, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Internet Explorer XML Page Object Type Validation	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

⁴⁷ SecurityFocus, September 9, 2003.

⁴⁸ Bugtraq, September 10, 2003.

⁴⁹ Bugtraq, September 4, 2003.

⁵⁰ SecurityFocus, September 8, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft ⁵¹ <i>Microsoft updates bulletin</i> ⁵² <i>Bulletin updated again</i> ⁵³	Windows 95/98/ME/NT 4.0/2000, XP, 2003	Internet Explorer 5.01, SP1-SP3, 5.5, SP1-SP2, 6.0, SP1, 6.0 for Windows Server 2003	<p>Multiple vulnerabilities exist: a buffer overflow vulnerability exists in the 'BR549.dll' ActiveX control due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code; a Cross-Domain vulnerability exists in the way Internet Explorer retrieves files from the cache, which could let a remote malicious user execute arbitrary scripting in the "My Computer Zone;" and a vulnerability exists because Internet Explorer does not properly determine object types, which could let a remote malicious user execute arbitrary code.</p> <p><i>V1.1 Bulletin updated to add information regarding ASP.NET related issues with Windows XP patch. V1.2 Bulletin updated to add details to reboot information in Additional Information section.</i></p> <p><i>Added information regarding reports that the patch provided does not properly correct the Object Type Vulnerability (CAN-2003-0532)</i></p>	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-032.asp	Internet Explorer Multiple Vulnerabilities CVE Names: CAN-2003-0530, CAN-2003-0531, CAN-2003-0532	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published for the IE Object Type vulnerability.

⁵¹ Microsoft Security Bulletin, MS03-032, August 20, 2003.

⁵² Microsoft Security Bulletin, MS03-032 1.1 & 1.2, August 25 & 28, 2003

⁵³ Microsoft Security Bulletin, MS03-032 1.3, September 8, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft ⁵⁴	Windows NT 4.0/2000, XP, 2003	Windows 2000 Advanced Server, SP1-SP4, 2000 Datacenter Server, SP1-SP4, 2000 Professional, SP1-SP4, 2000 Server, SP1-SP4, NT Enterprise Server 4.0, SP1-SP6a, NT Server 4.0, SP1-SP6a, NT Terminal Server 4.0, SP1-SP6a, NT Workstation 4.0, SP1-SP6a, Server 2003 Datacenter Edition, 64-bit, 2003 Enterprise Edition, 64-bit, 2003 Standard Edition, 64-bit, 2003 Web Edition, XP 64-bit Edition, SP1, Version 2003, XP Home, SP1, XP Professional, SP1	Several vulnerabilities exist: a buffer overflow vulnerability exists in the Distributed Component Object Model (DCOM) interface in the RPCSS Service RPCSS Service and is related to code that handles RPC messages for DCOM activation due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary code with SYSTEM privileges; a buffer overflow vulnerability exists in the 'PerformScmStage' function via certain messages to the '_RemoteGetClassObject' interface, which could let a remote malicious user cause a Denial of Service; and a buffer overflow vulnerability exists in the Distributed Component Object Model (DCOM) interface in the RPCSS Service due to insufficient sanity checks when handling length values located within DCERPC DCOM object activation packets, which could let a remote malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-039.asp	Microsoft Multiple RPCSS DCOM Buffer Overflows CVE Names: CAN-2003-0528, CAN-2003-0605, CAN-2003-0715	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Exploit scripts have been published. Vulnerability has appeared in the press and other public media.

⁵⁴ Microsoft Security Bulletin, MS03-039, September 10, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
<p>Microsoft^{55, 56}</p> <p><i>Multiple exploits have been published and several Trojans circulating.⁵⁷</i></p> <p><i>Mblast worm circulating in the wild.</i></p> <p><i>Microsoft updates bulletin⁵⁸</i></p> <p><i>Microsoft updates bulletin⁵⁹</i></p>	Windows 98/NT 4.0/2000, 2003, XP	Windows 2000 Advanced Server, SP1-SP4, 2000 Datacenter Server, SP1-SP4, 2000 Professional, SP1-SP4, 2000 Server, SP1-SP4, NT Enterprise Server 4.0, SP1-SP6a, NT Server 4.0, SP1-SP6a, NT Terminal Server 4.0, SP1-SP6a, NT Workstation 4.0, SP1-SP6a, Server 2003 Datacenter Edition, 64-bit, 2003 Enterprise Edition, 64-bit, Server 2003 Standard Edition, Server 2003 Web Edition, Windows XP 64-bit Edition, SP1, XP Home, SP1, XP Professional, SP1	<p>A buffer overflow vulnerability exists in the RPC interface that implements the Distributed Component Object Model services (DCOM) due to insufficient bounds checking of client DCOM object activation requests, which could let a malicious user install programs, view, change or delete data, create new accounts with full privileges or execute arbitrary code.</p> <p><i>V1.4 Bulletin has been updated to include information about Windows 2000 Service Pack 2 support for this patch and updated bulletin with additional workaround information.</i></p> <p><i>V1.5 Added details for scanner tool.</i></p> <p><i>V1.6 Updated download links, removed the word "Server" from the NT4 link.</i></p> <p><i>V1.7 Corrected minor formatting errors in the Frequently Asked Questions section.</i></p> <p><i>V1.8 Updated supercedence information in the Additional Information section.</i></p> <p><i>Bulletin updated to include information about the release of MS03-039 an updated scanning tool that supersedes this bulletin and the original scanning tool provided with it.</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/MS03-026.asp</p> <p><i>New bulletin available at:</i> http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-039.asp</p>	Windows DCOM RPC Buffer Overflow	High	<p>Bug discussed in newsgroups and websites.</p> <p>Vulnerability has appeared in the press and other public media.</p> <p><i>Multiple exploit scripts have been published. There is currently at least one autorooter-enabled IRC bot circulating that exploits this vulnerability. Also multiple Trojans are circulating that exploit the vulnerability.</i></p> <p><i>Another exploit script has been published.</i></p>

⁵⁵ Microsoft Security Bulletin, MS03-026 V1.2, July 21, 2003.

⁵⁶ Department of Homeland Security Advisory, July 24, 2003.

⁵⁷ SecurityFocus, August 8, 2003.

⁵⁸ Microsoft Security Bulletin, MS03-026 V1.4-V1.8, August 12, 14, 15, 18, & 21, 2003.

⁵⁹ Microsoft Security Bulletin, MS03-026 V2.0, September 10, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Mini HTTP Server ⁶⁰	Windows 2000, XP	File-Sharing for NET 1.5 WebForum Server 1.5	A Directory Traversal vulnerability exists due to insufficient sanitization of user-supplied data, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	WebForums/ File-Sharing for NET Servers Directory Traversal	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Mini HTTP Server ⁶¹	Windows 2000, XP	WebForum Server 1.0, 1.5, 1.6	A vulnerability exists due to insufficient validation of administrative credentials, which could let a remote malicious user obtain unauthorized administrative access.	No workaround or patch available at time of publishing.	WebForum Server Unauthorized Administrative Access	High	Bug discussed in newsgroups and websites. There is no exploit code required.
Mini HTTP Server ⁶²	Windows 2000, XP	WebForum Server 1.5	A vulnerability exists because the login script does not properly validate the password variable, which could let a remote malicious user obtain administrative access.	No workaround or patch available at time of publishing.	WebForums Server Default Password	High	Bug discussed in newsgroups and websites. There is no exploit code required.
Mondo Soft ⁶³	Multiple	Mondo Search 4.4, 5.0, 5.1	An access validation vulnerability exists which could let an unauthorized remote malicious user obtain access.	Patch available at: http://www.mondosoft.com/security/msp0903a.zip	MondoSearch Access Validation Error	Medium	Bug discussed in newsgroups and websites.
Mozilla ⁶⁴	Windows, Unix	ChatZilla Remote Denial of Service	A remote Denial of Service vulnerability exists when a malicious user acting as an IRC server submits a specially crafted request containing a long string.	No workaround or patch available at time of publishing.	ChatZilla Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Multiple Vendors ⁶⁵ <i>RedHat issues advisory⁶⁶</i>	Unix	Linux kernel 2.4.20	A remote Denial of Service vulnerability exists in kernels built supporting the 'CONFIG_IP_NF_CONNT RACK' option or with the 'IP_conntrack' module loaded.	Patch available at: http://downloads.securityfocus.com/vulnerabilities/patches/netfilter-ipconntrack.patch <i>RedHat:</i> http://rhn.redhat.com/	Netfilter Connection Tracking Remote Denial of Service CVE Name: CAN-2003-0187	Low	Bug discussed in newsgroups and websites.

⁶⁰ SecurityFocus, September 15, 2003.

⁶¹ SecurityFocus, September 16, 2003.

⁶² SecurityFocus, September 15, 2003.

⁶³ SecurityFocus, September 18, 2003.

⁶⁴ M00 Security Advisory #003, September 14, 2003.

⁶⁵ Netfilter Core Team Security Advisory, August 2, 2003.

⁶⁶ SecurityFocus, September 5, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors ⁶⁷	Unix	Systems running versions of OpenSSH prior to 3.7.1, Systems that use or derive code from vulnerable versions of OpenSSH	A buffer mismanagement vulnerability exists in the 'buffer.c' source file, which could let a remote malicious user execute arbitrary code.	<p>Cisco: Workaround & fixes available at: http://www.cisco.com/warp/public/707/cisco-sa-20030917-openssh.shtml</p> <p>Conectiva: ftp://atualizacoes.conectiva.com.br/</p> <p>Debian: http://security.debian.org/pool/updates/main/o/openssh/</p> <p>Engarde: http://infocenter.guardiandigital.com/advisories/</p> <p>FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-03:12/</p> <p>IBM: http://www-1.ibm.com/servers/aix/products/aixos/linux/download.html</p> <p>Immunix: http://download.immunix.org/ImmunixOS/7+/Updates/RPMS/</p> <p>Mandrake: http://www.mandrakesecure.net/en/advisorie</p> <p>NetBSD: http://www-1.ibm.com/servers/aix/products/aixos/linux/download.html</p> <p>OpenPKG: ftp://ftp.openpkg.org/release/</p> <p>OpenSSH: http://www.openssh.com/txt/buffer.adv</p> <p>RedHat: http://rhn.redhat.com</p> <p>Slackware: ftp://ftp.slackware.com/pub/slackware/s</p> <p>SuSE: ftp://ftp.suse.com/pub/suse/i386/update/</p> <p>TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/Server/8/updates/</p> <p>Trustix: http://www.trustix.net/pub/Trustix/updates/</p> <p>YellowDog: Ftp.yellowdoglinux.com/pub/yellowdog/updates/yellowdog-3.0/</p>	OpenSSH Buffer Mismanagement Vulnerabilities CVE Name: CAN-2003-0693	High	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.

⁶⁷ CERT® Advisory, CA-2003-24, September 18, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors ^{68, 69, 70, 71, 72, 73, 74, 75}	Unix	Sendmail 8.12.9 & prior	A buffer overflow vulnerability exists when parsing non-standard rulesets, which could possibly let a remote malicious user execute arbitrary code.	<p>SendMail: ftp://ftp.sendmail.org/pub/sendmail/</p> <p>Conectiva: ftp://atualizacoes.conectiva.com.br/</p> <p>Debian: http://security.debian.org/pool/updates/main/s/sendmail/</p> <p>Immunix: http://download.immunix.org/ImmunixOS/7+/Updates/RPMS/</p> <p>OpenPKG: ftp://ftp.openpkg.org/release/</p> <p>RedHat: ftp://updates.redhat.com/</p> <p>Slackware: ftp://ftp.slackware.com/pub/slackware/</p> <p>TurboLinux: Ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/</p> <p>YellowDog: ftp://ftp.yellowdoglinux.com/pub/yellowdog/updates/yellowdog-3.0/</p>	Sendmail Ruleset Parsing Buffer Overflow CVE Name: CAN-2003-0681	High	Bug discussed in newsgroups and websites.
Multiple Vendors ^{76, 77, 78, 79} <i>Conectiva issues advisory⁸⁰</i>	Unix	pam_smb 1.1-1.1.6, 2.0 -rc4,; RedHat pam_smb-1.1.6-2.i386. rpm, 1.1.6-2.ia64. rpm, 1.1.6-5.i386 .rpm, 1.1.6-7.i386.rpm	A buffer overflow vulnerability exists due to a boundary error when handling passwords, which could let a remote malicious user execute arbitrary code with root privileges.	<p>Debian: http://security.debian.org/pool/updates/main/libpam-smb/</p> <p>RedHat: ftp://updates.redhat.com/SuSE: ftp://ftp.suse.com/pub/suse/</p> <p>TurboLinux: ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/</p> <p>Conectiva: ftp://atualizacoes.conectiva.com.br/</p>	Pam_SMB Remote Buffer Overflow CVE Name: CAN-2003-0686	High	Bug discussed in newsgroups and websites. Exploit script has been published.

⁶⁸ Debian Security Advisory. DSA 384-1, September 17, 2003.

⁶⁹ Immunix Secured OS Security Advisory, IMNX-2003-7+-021-01, September 17, 2003.

⁷⁰ Yellow Dog Linux Security Announcement, YDU-20030917-2, September 17, 2003.

⁷¹ Slackware Security Advisory, SSA:2003-260-02, September 17, 2003.

⁷² Conectiva Linux Security Announcement, CLA-2003:742, September 18, 2003.

⁷³ TurboLinux Security Advisor, TLSA-2003-52, September 18, 2003.

⁷⁴ Red Hat Security Advisory, RHSA-2003:283-01, September 18, 2003.

⁷⁵ OpenPKG Security Advisory, OpenPKG-SA-2003.04, September 19, 2003.

⁷⁶ Debian Security Advisory, DSA 374-1, August 26, 2003.

⁷⁷ Red Hat Security Advisories, RHSA-2003:261-01 & RHSA-2003:262-07, August 26, 2003.

⁷⁸ Turbo Linux Security Announcement, TLSA-2003-50, August 29, 2003.

⁷⁹ SuSE Security Announcement, SuSE-SA:2003:036, September 3, 2003.

⁸⁰ Conectiva Linux Security Announcement, CLA-2003:734, September 5, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
<p>Multiple Vendors 81, 82, 83, 84, 85, 86, 87, 88</p> <p><i>More advisories issued^{89, 90, 91}</i></p> <p><i>HP releases updates⁹²</i></p> <p><i>HP updates bulletin⁹³</i></p>	MacOS X, Unix	<p>FreeBSD 4.0, alpha, 4.0.x, 4.1, 4.1.1, Stable, Release, 4.2, Release, Stable, Stablepre0 50201, pre122300, 4.3, Release, Releng, Stable, 4.4, Releng, Stable, 4.5, Release, Stable, 4.5 Stablepre2 002-03-07, 4.6, Release, Stable, 4.6.2, 4.7, Release, Stable, 4.8, PreRelease 5.0, alpha; NetBSD 1.5-1.5.3, 1.6, 1.6.1; OpenBSD 2.0-2.9, 3.0-3.3; RedHat wu-ftp-2.6.1-16.i386.rpm, 16.ppc.rpm, 18.i386.rpm, 18.ia64.rpm, -2.6.2-5.i386.rpm, 8.i386.rpm Washington University wu-ftp 2.5.0, 2.6.0-2.6.3</p>	<p>A buffer overflow vulnerability exists due to an off-by-one error in the 'fb_realpath()' function when calculating the length of a concatenated string, which could let a remote malicious user obtain root privileges.</p> <p><i>HP bulletin updates to reflect more upgrades.</i></p>	<p>Conectiva: http://atualizacoes.conectiva.com.br/</p> <p>Debian: http://security.debian.org/pool/updates/main/w/wu-ftp/</p> <p>FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-03:08/realpath.patch</p> <p>Mandrake: http://www.mandrakesecure.net/en/ftp.php</p> <p>NetBSD: ftp://ftp.netbsd.org/pub/NetBSD/security/patches/SA2003-011-realpath.patch</p> <p>OpenBSD: ftp://ftp.OpenBSD.org/pub/OpenBSD/patches/</p> <p>RedHat: ftp://updates.redhat.com/</p> <p>SuSE: ftp://ftp.suse.com/pub/use</p> <p>Apple: http://docs.info.apple.com/article.html?artnum=61798</p> <p>Immunix: http://download.immunix.org/ImmunixOS/7+/Updates/RPMS/wu-ftp-2.6.1-6_imnx_8.i386.rpm</p> <p>Sun: http://sunsolve.sun.com/patches/linux/security.html</p> <p>Hewlett Packard: ftp://ftp.itrc.hp.com/export/patches/hp-ux_patch_matrix/</p> <p>Hewlett Packard: http://itrc.hp.com/cki/bin/doc.pl?screen=ckiSecurityBulletin</p>	<p>Multiple Vendor realpath() Off-By-One Buffer Overflow</p> <p>CVE Name: CAN-2003-0466</p>	<p>High</p>	<p>Bug discussed in newsgroups and websites. Exploit scripts have been published.</p> <p><i>Another exploit script has been published.</i></p>

⁸¹ Debian Security Advisory, 357-1, July 31, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts	
<p>Multiple Vendors 94, 95, 96, 97, 98, 99, 100, 101, 102</p> <p><i>More advisories issued¹⁰³</i></p>	MacOS X 10.2x nix	<p>FreeBSD 4.6-4.8, 5.0;</p> <p>OpenBSD 3.2;</p> <p>RedHat sendmail-8.12.5-7.i386. rpm, 8.12.8-4.i386. rpm, cf-8.12.5-7.i386. rpm, cf-8.12.8-4.i386. rpm, devel-8.12.5-7.i386. rpm, devel-8.12.8-4.i386.rpm , doc-8.12.5-7.i386. rpm, oc-8.12.8-4.i386. rpm;</p> <p>Sendmail Consortium Sendmail 8.12.1-8.12.8;</p> <p>SGI IRIX 6.5.19-.5.21</p>	A vulnerability exists when implementing the use of DNS Maps due to a failure to properly initialize dynamically allocated data, which could let a malicious user cause a Denial of Service and possibly execute arbitrary code.	<p><u>SendMail Consortium:</u> ftp://ftp.sendmail.org/pub/sendmail/sendmail.8.12.9.tar.gz</p> <p><u>Conectiva:</u> ftp://atualizacoes.conectiva.com.br/</p> <p><u>FreeBSD:</u> ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/S-A-03:11/sendmail.patch</p> <p><u>Hewlett Packard:</u> http://www.securityfocus.com/advisories/5774</p> <p><u>Mandrake:</u> http://www.mandrakesecurity.net/en/ftp.php</p> <p><u>OpenBSD:</u> ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.2/common/016_sendmail.patch</p> <p><u>OpenPKG:</u> ftp.openpkg.org</p> <p><u>RedHat:</u> ftp://updates.redhat.com/</p> <p><u>SGI:</u> ftp://patches.sgi.com/support/free/security/patches/</p> <p><u>SOT Linux:</u> ftp://ftp.sot.com/updates/2003/</p> <p><u>SuSE:</u> ftp://ftp.suse.com/pub/suse/i386/update/</p> <p><u>Hewlett Packard:</u> http://www.itrc.hp.com/service/patch/patchDetail.do?patchid=T64V51AB-IX6-SENDMAIL-58-61-SSRT3612</p>	Sendmail DNS Maps Remote Denial of Service	CVE Name: CAN-2003-0688	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites.

⁸² Mandrake Linux Security Update Advisory, MDKSA-2003:080, July 31, 2003.

⁸³ Red Hat Security Advisory, RHSA-2003:245-01, July 31, 2003.

⁸⁴ SuSE Security Announcement, SuSE-SA:2003:032, July 31, 2003.

⁸⁵ Conectiva Linux Security Announcement, CLA-2003:715, August 1, 2003.

⁸⁶ FreeBSD Security Advisory, FreeBSD-SA-03:08, August 4, 2003.

⁸⁷ NetBSD Security Advisory 2003-01, August 4, 2003.

⁸⁸ TurboLinux Security Advisory, TLSA-2003-46, August 4, 2003.

⁸⁹ Immunix Secured OS Security Advisory, IMNX-2003-7+-019-01, August 7, 2003.

⁹⁰ Apple Security Update, 61798, August 14, 2003.

⁹¹ Sun Advisory, August 18, 2003.

⁹² Hewlett-Packard Company Security Bulletin, HPSBUX0309-277, September 2, 2003.

⁹³ Hewlett-Packard Company Security Bulletin, HPSBUX0309-277, September 15, 2003.

⁹⁴ SGI Security Advisory, 20030803-01-P, August 25, 2003.

⁹⁵ FreeBSD Security Advisory, FreeBSD-SA-03:11, August 26, 2003.

⁹⁶ SuSE Security Announcement, SUSE-SA:2003:035, August 26, 2003.

⁹⁷ Mandrake Linux Security Update Advisory, MDKSA-2003:086, August 26, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors 104, 105, 106, 107108, 109, 110, 111, 112, 113	Windows NT 4.0/2000, MacOS X 10.x, Unix	Systems running open-source SendMail versions prior to 8.12.10, Commercial releases of Sendmail including Sendmail Switch, Advanced Message Server (SAMS), & Sendmail for NT	A buffer overflow vulnerability exists in the 'prescan()' function, which could let local/remote malicious user execute arbitrary code.	SendMail: ftp://ftp.sendmail.org/pub/sendmail/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Debian: http://security.debian.org/pool/updates/main/s/sendmail/ FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-03:13/sendmail_patch Immunix: http://download.immunix.org/ImmunixOS/7+/Updates/RPMS/ OpenPKG: ftp://ftp.openpkg.org/ RedHat: ftp://updates.redhat.com Slackware: Ftp://ftp.slackware.com/pub/slackware/slackware-9.0/patches/packages/ SuSE: ftp://ftp.suse.com/pub/suse/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ YellowDog: ftp://ftp.yellowdoglinux.com/pub/yellowdog/updates/yellowdog-3.0/	Sendmail Prescan() Buffer Overflow CVE Name: CAN-2003-0694	High	Bug discussed in newsgroups and websites.
myServer 114	Windows 98/2000, Unix	myServer 0.4.1-0.4.3	A buffer overflow vulnerability exists in the 'cgi-lib.dll' MFCGI library because long URL variables are not processed properly, which could let a remote malicious user execute arbitrary code.	Patch available at: http://myserverweb.sourceforge.net/cvs.php	MyServer 'cgi-lib.dll' Remote Buffer Overflow	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

⁹⁸ OpenPKG Security Advisory, OpenPKG-SA-2003.037, August 28, 2003.

⁹⁹ Red Hat Security Advisory, RHSA-2003:265-01, August 28, 2003.

¹⁰⁰ Conectiva Linux Security Announcement, CLA-2003:727, August 29, 2003.

¹⁰¹ SOT Linux Security Advisory, SLSA-2003:39, August 29, 2003.

¹⁰² Hewlett-Packard Security Advisory, SSRT3612, September 5, 2003.

¹⁰³ Hewlett-Packard Company Software Security Response Team, SSRT3612, September 9, 2003.

¹⁰⁴ Debian Security Advisory, DSA 384-1, September 17, 2003.

¹⁰⁵ FreeBSD Security Advisory, FreeBSD-SA-03:13, September 17, 2003.

¹⁰⁶ Slackware Security Advisory, SSA:2003-260-02, September 17, 2003.

¹⁰⁷ Yellow Dog Linux Security Announcement, YDU-20030917-2, September 17, 2003.

¹⁰⁸ Conectiva Linux Security Announcement, CLA-2003:742, September 18, 2003.

¹⁰⁹ Immunix Secured OS Security Advisory, IMNX-2003-7+-021-01, September 18, 2003.

¹¹⁰ Red Hat Security Advisory RHSA-2003:283-01, September 18, 2003.

¹¹¹ TurboLinux Security Advisory, TLSA-2003-52, September 18, 2003.

¹¹² OpenPKG Security Advisory, OpenPKG-SA-2003.041, September 19, 2003.

¹¹³ SuSE Security Announcement, SuSE-SA:2003:040, September 20, 2003.

¹¹⁴ Moozatech Advisory, September 12, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
MySQL AB ^{115, 116, 117}	Unix	MySQL 3.23.x, 3.23.2-3.23.5, 3.23.8-3.23.10, 3.23.22-3.23.34, 3.23.36-3.23.56, 4.0.0-4.0.14, 4.1.0-alpha, 4.1.0-0	A buffer overflow vulnerability exists when handling user passwords of excessive size due to insufficient bounds checking, which could let a malicious user execute arbitrary code.	Patch available at: http://www.mysql.com/downloads/mysql-4.0.html Debian: http://security.debian.org/pool/updates/main/m/mysql/ OpenPKG: Ftp://ftp.openpkg.org/releases/ Trustix: http://www.trustix.net/pub/Trustix/updates/	MySQL Password Handler Buffer Overflow CVE Name: CAN-2003-0780	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published. An exploit script has also been published.
NetBSD ¹¹⁸	Unix	NetBSD 1.5-1.5.3, 1.6, 1.6.1	Multiple vulnerabilities exist: a vulnerability exists because a pointer variable is used for both user-level and kernel addresses, which could let a malicious user cause a Denial of Service; a vulnerability exists if the process ID of a zombie process is passed to the system call, which could let a malicious user cause a Denial of Service; and a vulnerability exists because some sysctl nodes do not implement sufficient range checking, which could let a malicious user obtain sensitive information.	Patches available at: ftp://ftp.NetBSD.org/pub/NetBSD/security/advisories/NetBSD-SA2003-014.txt.asc	NetBSD Multiple Vulnerabilities	Low/Medium (Medium if sensitive information can be obtained)	Bug discussed in newsgroups and websites.
Net-SNMP ¹¹⁹	Unix	Net-SNMP 5.0.1, 5.0.3, 5.0.4.pre2, 5.0.5, 5.0.6, 5.0.7, 5.0.8	A vulnerability exists which could let an unauthorized malicious user obtain access to MIB objects.	Upgrade available at: http://sourceforge.net/project/showfiles.php?group_id=12694	Net-SNMP Unauthorized Access	Medium	Bug discussed in newsgroups and websites.
NetWin ¹²⁰	Windows, Unix	DBabble 2.5 i	A Cross-Site Scripting vulnerability exists in the 'dbabble' script due to insufficient verification of user-supplied input, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	DBabble Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
New Era Scripts ¹²¹	Windows, Unix	EZ-WEB Site Builder 1.5	A Directory Traversal vulnerability exists because the 'selectedpage' parameter isn't properly verified, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	EZ-WEB Site Builder Directory Traversal	Medium	Bug discussed in newsgroups and websites.

¹¹⁵ Debian Security Advisory, DSA 381-1, September 14, 2003.

¹¹⁶ OpenPKG Security Advisory, OpenPKG-SA-2003.038, September 15, 2003.

¹¹⁷ Trustix Secure Linux Security Advisory, TSLSA-2003-09-17, September 17, 2003.

¹¹⁸ NetBSD Security Advisory, 2003-014, September 18, 2003.

¹¹⁹ Secunia Advisory, SA9697, September 9, 2003.

¹²⁰ SecurityTracker Alert, 1007700, September 14, 2003.

¹²¹ SecurityTracker, 1007606, September 3, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Nicolas Boullis ¹²²	Unix	Mah-Jong 1.4	Several vulnerabilities exist: a buffer overflow vulnerability exists when a specially crafted command is submitted to the server, which could let a remote malicious user execute arbitrary code; and a remote Denial of Service vulnerability exists due to the way escaped characters are processed.	Debian: http://security.debian.org/pool/updates/main/m/mah-jong/	Mah-Jong Server Remote Buffer Overflow & Denial of Service CVE Names: CAN-2003-0705, CAN-2003-0706	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites.
Nokia ¹²³	Windows	Nokia Electronic Documentation 5.0	Multiple vulnerabilities exist: a vulnerability exists in the default configuration of the NED application (and the associated WebLogic application server) because the web root directory and installation path can be viewed by a remote malicious user; a vulnerability exists because the 'location' parameter isn't properly verified, which could let a remote malicious user obtain sensitive information; and a Cross-Site Scripting vulnerability exists because HTML code is not properly filtered from user-supplied input, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing. Nokia has planned to release a new version early 2004. They state that NED shouldn't be accessible except for trusted staff and is designed to be placed on a separate network.	Nokia Electronic Documentation Multiple Vulnerabilities	Medium/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Web root directory & installation path vulnerability may be exploited via a web browser. There is no exploit code required for the Connection Redirection vulnerability. Exploit has been published for the Cross-Site Scripting vulnerability.
Novell ¹²⁴	Multiple	Netware 6.0, SP1-SP3	A new version of the TCP implementation is available which address bugs and potential security vulnerabilities. Of particular importance is a flaw in ISN generation that could make it plausible for remote malicious users anticipate sequence numbers in packets, allowing for man-in-the-middle attacks.	Upgrade available at: http://support.novell.com/cgi-bin/search/searchtid.cgi?/2966665.htm	NetWare TCP Potential Vulnerabilities	Medium	Bug discussed in newsgroups and websites.
NullSoft ¹²⁵	Windows	Winamp 2.81, 2.91, 3.0, 3.1	A buffer overflow vulnerability exists in the 'IN_MIDI.DLL' plugin due to a boundary error, which could let a remote malicious user create malformed MIDI files that, when loaded, will execute arbitrary code.	No workaround or patch available at time of publishing.	Winamp 'IN_MIDI.DLL' Remote Buffer Overflow	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

¹²² Debian Security Advisory, DSA 378-1, September 7, 2003.

¹²³ @stake, Inc. Security Advisory, a091503-1, September 15, 2003.

¹²⁴ Novell Technical Information Document, TID2966665, September 18, 2003.

¹²⁵ Bugtraq, September 8, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
OpenBSD ¹²⁶ <i>Proof of Concept exploits published</i> ¹²⁷	Unix	OpenBSD 3.3	A Denial of Service vulnerability exists in the semget() system call due to insufficient bounds checking.	Upgrade available at: http://www.openbsd.org/errata.html	OpenBSD semget() Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published. <i>Proofs of Concept exploits have been published.</i>
Oracle Corporation ¹²⁸ <i>Oracle updates bulletin</i> ¹²⁹	Windows NT 4.0/2000, XP, Unix, OpenVMS	Oracle9i Release 2; Oracle9i Release 1 Oracle8i (8.1.x all releases)	Several buffer overflow vulnerabilities exist in the 'EXTPROC' application, which could let a remote malicious user execute arbitrary code. <i>Updated bulletin available at: http://otn.oracle.com/deploy/security/pdf/2003alert57.pdf</i>	Patches available at: http://metalink.oracle.com	Oracle Database Server EXTPROC Buffer Overflow	High	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
OSSIM ¹³⁰	Multiple	os-sim 0.1-alpha - 0.3-alpha	Multiple SQL injection vulnerabilities exist due to insufficient input validation, which could let a remote malicious user obtain sensitive information, bypass security restrictions, or execute arbitrary code.	Upgrade available at: http://prdownloads.sourceforge.net/os-sim/os-sim-0.3.1-alpha.tgz?download	Multiple Unspecified OSSIM SQL Injection	Medium/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites.
phpBB Group ¹³¹	Windows, Unix	phpBB 2.0.6	A Cross-Site Scripting vulnerability exists in the '[url]' BBCode tag due to insufficient sanitization of user-supplied URL BBCode tags, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	PHPBB URL BBCode Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
phpPortals ¹³²	Windows, Unix	vbPortal 2.0 alpha 8.1	A vulnerability exists in the 'auth.inc.php' script due to insufficient validation of user-supplied input, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	vbPortal 'auth.inc.php' SQL Injection	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

¹²⁶ SecurityTracker Alert, 1007543, August 20, 2003.

¹²⁷ SecurityFocus, September 10, 2003.

¹²⁸ NGSSoftware Insight Security Research Advisory, #NISR25072003, July 25, 2003.

¹²⁹ Bugtraq, September 12, 2003.

¹³⁰ Secunia Advisory, SA9695, September 9, 2003.

¹³¹ Bugtraq, September 8, 2003.

¹³² SecurityTracker Alert, 1007695, September 13, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Plug and Play Software ¹³³	Windows NT 4.0/2000, XP	Plug and Play Web Server 1.0 002c	Two vulnerabilities exist: a Directory Traversal vulnerability exists due to insufficient validation, which could let a remote malicious user obtain sensitive information; and a buffer overflow vulnerability exists when a specially crafted argument is submitted to the FTP service, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Plug and Play Web Server Directory Traversal & Buffer Overflow	Medium/ High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Python Publishing Accessories ¹³⁴	Windows, Unix	Python Publishing Accessories 0.2.1	A Cross-Site Scripting vulnerability exists due to insufficient sanitization of user-supplied data, which could let a remote malicious user execute arbitrary code.	Update available at: http://prdownloads.sourceforge.net/ppa/PPA-0.2.2.tar.gz?download	Python Publishing Accessories Cross-Site Scripting	High	Bug discussed in newsgroups and websites.
RARLAB ¹³⁵	Windows	UnRAR 2.71, WinRAR 2.90, 3.0.0, 3.10, beta 5, beta 3, 3.11, 3.20	A vulnerability exists in the '.rar' header because values are trusted without adequate verification of the actual file size, which could let a user expect that a compressed file is a certain size and decompress it based on this assumption.	This issue is addressed in UnRAR 3.2.3. It is not known if WinRAR fixes are available.	WinRAR Compressed File Size	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Real Networks ¹³⁶ <i>Upgrade now available</i> ¹³⁷	Windows NT 4.0/2000, XP, Unix	Helix Universal Server 8.01, 9.01, 9.0, Real Server 7.0, 7.0.1, 7.0.2, 8.0 Beta, 8.0, 8.01, 8.02, G21.0	A buffer overflow vulnerability exists because the 'vsrclin.so' and 'vsrclin.dll' plugins fail to handle long requests, which could let a remote malicious user execute arbitrary code with root privileges.	Workaround available at: http://www.service.real.com/help/faq/security/rootexploit082203.html <i>Upgrade available at:</i> http://www.service.real.com/help/faq/security/rootexploit091103.html	Helix Universal Server Remote Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Real Networks ¹³⁸	Unix	RealOne Player Alpha for Linux 2.2	A vulnerability exists because configuration files are stored in the home directory with insecure permissions, which could let a malicious user obtain elevated privileges.	No workaround or patch available at time of publishing.	RealOne Player Insecure Configuration File Permission Local Privilege Escalation	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.

¹³³ Bugtraq, September 18, 2003.

¹³⁴ Secunia Advisory, SA9681, September 5, 2003.

¹³⁵ Bugtraq, September 10, 2003.

¹³⁶ Securiteam, August 26, 2003.

¹³⁷ SecurityFocus, September 12, 2003.

¹³⁸ Securiteam, September 17, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Research In Motion ¹³⁹	Windows	Blackberry Enterprise Server 2.1, 3.5, 3.6	Multiple vulnerabilities exist: a Denial of Service vulnerability exists when handling extremely large .pdf documents; a vulnerability exists due to the way password protected attachments are handled, which could let a malicious user obtain sensitive information; and a vulnerability exists when a password protected attachment is received and the correct password is provided because all subsequent e-mails with the same attachment can be viewed without supplying a password.	Patch available at: https://www.blackberry.com/SoftwareDownload/user.jsp?code-1305	Multiple Blackberry Enterprise Server	Low/ Medium (Medium if sensitive information can be obtained)	Bug discussed in newsgroups and websites.
SANE ¹⁴⁰	Unix	SANE 1.0.0-1.0.9, sane-backend 1.0.10	Multiple vulnerabilities exist: a vulnerability exists because the identity (IP address) of the remote host is not checked during the SANE_NET_INIT RPC call, which could let a remote malicious user obtain unauthorized access; a vulnerability exists because connection drops are not handled properly, which could let a remote malicious user obtain sensitive information and cause a Denial of Service; a vulnerability exists when a connection is dropped before the size value of malloc is set, which could let a remote malicious user cause a Denial of Service; a vulnerability exists because the validity of RPC numbers it gets before getting the parameters; a vulnerability exists when debug messages are enabled dropped connections are not properly handled, which could let a remote malicious user cause a Denial of Service; and a vulnerability exists because memory is not properly allocated in some cases, which could let a remote malicious user cause a Denial of Service.	Debian: http://security.debian.org/pool/updates/main/s/sane-backends/	Multiple Sane Package Remote Vulnerabilities CVE Names: CAN-2003-0773, CAN-2003-0774, CAN-2003-0775, CAN-2003-0776, CAN-2003-0777, CAN-2003-0778	Low/ Medium (Medium if unauthorized access or sensitive information can be obtained)	Bug discussed in newsgroups and websites.

¹³⁹ Secunia Security Advisory, SA9663, September 4, 2003.

¹⁴⁰ Debian Security Advisory DSA 379-1, September 11, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
SCO ¹⁴¹	Unix	Open Server 5.0.5-5.0.7	A vulnerability exists in the 'mana' process 'PATH_INFO' and 'REMOTE_ADDR' environment variables because authentication can be bypassed, which could let a malicious user obtain administrative privileges and possibly execute arbitrary code.	Patches available at: ftp://ftp.sco.com/pub/updates/OpenServer/CSSA-2003-SCO.19	OpenServer 'mana' Process Authentication Bypass CVE Name: CAN-2003-0742	High	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
SGI ¹⁴²	Unix	IRIX 6.5.21m, 6.5.21f, 6.5.21	A vulnerability exists because under certain conditions a NFS client can avoid read-only restrictions on filesystems exported via NFS, which could let a malicious user bypass "read-only" access restrictions.	Patches & upgrade available at: http://support.sgi.com/	IRIX NFS Export Security Bypass CVE Name: CAN-2003-0680	Medium	Bug discussed in newsgroups and websites.
SGI ¹⁴³ <i>SGI issues another advisory</i> ¹⁴⁴	Unix	IRIX 6.5-6.5.16, 6.5.17 m-6.5.19 m, 6.5.17 f-6.5.19 f	A remote Denial of Service vulnerability exists in the NFS daemon (nsfd) due to an error in the XDR decoding routines.	Patches available at: ftp://patches.sgi.com/support/free/security/patches/ <i>More patches available at: ftp://patches.sgi.com/support/free/security/advisories/20030801-02-P</i>	IRIX NFSD XDR Decoding Remote Denial of Service CVE Name: CAN-2003-0576	Low	Bug discussed in newsgroups and websites.
Squished Mosquito, Inc. ¹⁴⁵	Windows, Unix	Escapade 0.2.1 Beta	A Cross-Site Scripting vulnerability exists due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML or script code.	Upgrade available at:	Escapade Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Stunnel ¹⁴⁶	Windows 98/ 2000, Unix	Stunnel 3.20, 3.10, 3.3, 3.4 a, 3.7-3.9, 3.11-3.19, 3.21, a, b, c, 3.22, 3.24, 4.0	A vulnerability exists in the 'listen()' call because returned file descriptors are made available to unprivileged processes, which could let a malicious user hijack the Stunnel Server.	STunnel: http://www.stunnel.org/download/stunnel/src/stunnel-4.04.tar.gz	Stunnel Leaked File Descriptor CVE Name: CAN-2003-0740	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Sun Microsystems, Inc. ¹⁴⁷	Unix	Solaris2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86, 9.0, 9.0_x86	A vulnerability exists in the sadmin service when a sequence of specially crafted Remote Procedure Call (RPC) requests is submitted to the sadmind daemon, which could let a remote malicious user obtain root access.	Workaround available at: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F56740	Solaris SAdmin Client Credentials Remote Root Access	High	Bug discussed in newsgroups and websites. Exploit script has been published.

¹⁴¹ SCO Security Advisory, CSSA-2003-SCO.19, September 10, 2003.

¹⁴² SGI Security Advisory, 0030901-01-P, September 17, 2003.

¹⁴³ SGI Security Advisory, 20030801-01-P, August 13, 2003.

¹⁴⁴ SGI Security Advisory, 20030801-02-P, September 9, 2003.

¹⁴⁵ SecurityTracker Alert, 1007666, September 9, 2003.

¹⁴⁶ Connectiva Linux Security Announcement, CLA-2003:736, September 5, 2003.

¹⁴⁷ Sun(sm) Alert Notification, 56740, September 15, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
The DSPAM Project ¹⁴⁸	Unix	DSPAM 2.6.5 .1 DSPAM 2.6.5	A vulnerability exists because DSPAM is installed world executable and setgid by default, which could let a malicious user execute arbitrary code.	Upgrade available at:	DSPAM Insecure Default Permissions	High	Bug discussed in newsgroups and websites. There is no exploit code required.
U-Foot ¹⁴⁹	Unix	Liquid War 5.4.5	A buffer overflow vulnerability exists in the 'HOME' environment variable due to insufficient bounds checking, which could let a malicious user execute arbitrary code.	Upgrade available at: http://www.ufoot.org/liquidwar/download.php3	Liquid War HOME Environment Variable Buffer Overflow	High	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
University of Washington ^{150, 151, 152, 153, 154}	Unix	Pine 3.98, 4.0.2, 4.0.4, 4.10, 4.20, 4.21, 4.30, 4.33, 4.44, 4.50, 4.52, 4.543, 4.56	Two vulnerabilities exist: a buffer overflow vulnerability exists when handling 'message/external body type' attributes due to a boundary error, which could let a remote malicious user execute arbitrary code; and an integer overflow vulnerability exists in the 'rfc2231_get_param()' function when parsing e-mail headers, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.washington.edu/pine/getpine/ Conectiva: ftp://atualizacoes.conectiva.com.br/7 Engarde: http://infocenter.guardiandigital.com/advisories/ RedHat: ftp://updates.redhat.com/ Slackware: ftp://ftp.slackware.com/pub/slackware/ SuSE: ftp://ftp.suse.com/pub/suse/	Pine Buffer Overflow & Integer Overflow CVE Names: CAN-2003-0720, CAN-2003-0721	High	Bug discussed in newsgroups and websites. Exploit script has been published for the buffer overflow vulnerability.
Wintel Corporation ¹⁵⁵	Windows 98/NT 4.0/2000, XP	Wide Chapter 3.0	A buffer overflow vulnerability exists when handling excessive length HTTP requests, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	WideChapter HTTP Request Buffer Overflow	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Yahoo! ¹⁵⁶	Windows	Webcam ActiveX Control 2.0 .0.107	A buffer overflow vulnerability exists in the 'TargetName' parameter due to insufficient verification, which could let a remote malicious user execute arbitrary code.	Patch available at: http://messenger.yahoo.com/messenger/security/	Webcam ActiveX Control 'TargetName' Buffer Overflow	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

¹⁴⁸ Securiteam, September 16, 2003.

¹⁴⁹ Securiteam, September 17, 2003.

¹⁵⁰ Slackware Security Advisory, SSA:2003-253-01, September 10, 2003.

¹⁵¹ SuSE Security Announcement, SuSE-SA:2003:037, September 10, 2003.

¹⁵² Guardian Digital Security Advisory, ESA-20030911-022, September 11, 2003

¹⁵³ Red Hat Security Advisory, RHSA-2003:273-01, September 11, 2003.

¹⁵⁴ Conectiva Linux Security Announcement, CLA-2003:738, September 12, 2003.

¹⁵⁵ Bugtraq, September 13, 2003.

¹⁵⁶ Secunia Advisory, SA9760, September 17, 2003.

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

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

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

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

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between September 5 and September 19, 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, 31 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
September 19, 2003	rainbowcrack-1.1-win.tgz	An instant Microsoft Windows password cracker based on Philippe Oechslin's faster time-memory trade-off technique..
September 18, 2003	gyan_pine.c	Script that exploits the Remote Pine versions 4.56 and below vulnerability.
September 18, 2003	liquidwar-exploit.c	Script that exploits the Liquid War HOME Environment Variable Buffer Overflow vulnerability.
September 18, 2003	MS03-039-linux.c	Script that exploits the Microsoft Multiple RPCSS DCOM Buffer Overflows vulnerability.
September 18, 2003	rootdown.pl	Perl script that exploits the Solaris SAdmin Client Credentials Remote Root Access vulnerability.
September 17, 2003	mouny.c	Remote root exploit for rpc.mountd that makes use of the xlog off-by-one vulnerability.
September 16, 2003	09.14.mysql.c	Exploit for the MySQL Password Handler Buffer Overflow vulnerability.
September 16, 2003	DominoHunter-0.92.zip	A Lotus Domino web server scanner, written in Perl, that attempts to access default NSF databases, as well as crawl user-defined bases. It tries to enumerate the database structure, enumerate available views, available documents, and ACLs set on documents.
September 16, 2003	MS03-039-exp.c	Script that exploits the Microsoft Multiple RPCSS DCOM Buffer Overflows vulnerability.
September 16, 2003	sorpine.c	Script that exploits the Pine Buffer Overflow vulnerability.
September 14, 2003	chatzilla_dos.c	Script that exploits the ChatZilla Remote Denial of Service vulnerability.
September 14, 2003	mysql.c	Script that exploits the MySQL Password Handler Buffer Overflow vulnerability.
September 13, 2003	4DWS_ftp.c	Exploit for the 4D WebSTAR Remote Buffer Overflow vulnerability.

Date of Script (Reverse Chronological Order)	Script name	Script Description
September 13, 2003	defeating-w2k3-stack-protection.pdf	A paper that discusses how to defeat the stack based buffer overflow prevention mechanism in Microsoft Windows 2003 Server.
September 13, 2003	oc192-bof.c	Program for testing weak binaries for basic overflows. It can test command line overflows, ENV and basic format string vulnerabilities as well.
September 12, 2003	elfsh-0.51b3-portable.tgz	an automated reverse engineering tool with read/write capability for the ELF format. Sophisticated output with cross references using .got, .ctors, .dtors, .symtab, .dynsym, .dynamic, .rel.* and many other with an integrated hexdump.
September 10, 2003	mana-root.sh	Script that exploits the OpenServer 'mana' Process Authentication Bypass vulnerability.
September 10, 2003	rp9-priv-esc.c	Script that exploits the RealOne Player Insecure Configuration File Permission Local Privilege Escalation vulnerability.
September 10, 2003	rw.c	Script that exploits the OpenBSD semget() Denial of Service vulnerability.
September 10, 2003	set.c	Script that exploits the OpenBSD semget() Denial of Service vulnerability.
September 9, 2003	ethereal-0.9.15.tar.gz	A GTK+-based network protocol analyzer, or sniffer, that lets you capture and interactively browse the contents of network frames.
September 9, 2003	libShellCode-0.2.0.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.
September 9, 2003	sp-myserver.c	Remote Denial of Service exploit for MyServer 0.4.3.
September 9, 2003	StackOverflow-en.pdf	White paper discussing stack overflows, ways to exploit them.
September 8, 2003	augustiner.c	Script that exploits the Windows 98 Remote Denial of Service vulnerability.
September 8, 2003	leak-splloit.c	Script that exploits the Stunnel Leaked File Descriptor vulnerability.
September 7, 2003	Gallery_4033.c	Script that exploits the Apache:: Gallery Code Execution vulnerability.
September 7, 2003	gspoof-3.0.tar.gz	A GTK+ program written in C which makes easy and accurate the building and the sending of TCP packets with or without a data payload.
September 6, 2003	elfdoctor.c	Scanner to look up infection techniques that can be used in ELF modules. Includes function hijacking, relocation files, etc.
September 5, 2003	bazooka_penaka.pl	Perl script that exploits the FoxWeb Remote Buffer Overflow vulnerability.
September 5, 2003	word.zip	Exploit for the Microsoft Converter for WordPerfect Remote Buffer Overflow vulnerability.

Trends

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

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

Viruses

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

BAT.Deav.Worm (Batch File Worm): This is a batch file worm that spreads using the KaZaA and iMesh file-sharing networks. This worm also deletes files from the system.

PHP.Virdrus (Alias: PHP.Virdrus) (File Prepending Virus): PHP.Virdrus is a virus that prepends itself to the .php files. It is written in PHP. When PHP.Virdrus is executed, it searches the current folder for files with a .php extension and opens .php files to determine whether they are already infected. If a .php file is not infected, it prepends the viral code to the infected file.

VBS/Ryon@MM (Visual Basic Script Worm): When the virus is executed, it will copy itself to the following locations:

- C:\message.vbs [windows directory]
- \tasksys.vbs [windows directory]
- \message.vbs [windows SYSTEM directory]
- \message.vbs [windows SYSTEM directory]
- \helpdesk.vbs [windows SYSTEM directory]
- \asl.vbs [windows SYSTEM directory]
- \welcome.vbs [windows SYSTEM directory]
- \fwtwih.dll T

The following registry key will be added:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
 \tasksys,"[windows directory]\tasksys.vbs"

It will create the file C:\readme.html that contains a message. The VBScript will then drop C:\embryon.dll and C:\embryon.vbs . These files are detected as VBS/Generic@MM. This file edits the registry key:

- HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Start Page,
 "http://www.greenpeace.org."

Embryon.vbs will copy the file C:\message.vbs to all fixed and network drives as "readme.vbs ." It will also search to see if mIRC is installed and if so, edits script.ini to send infected files through this chat program. Using Outlook, it mails out to first 101 recipients in the address list and logs the addresses sent, to the registry key:

- HKEY_CURRENT_USER\Software\Microsoft\Notepad\

The e-mail characteristics are shown below:

- Subject : Mail delivery failed: returning message to sender.
- Attachment : message.vbs

It drops the file flps.vbs in the windows system directory which intends to copy the infected file fwtwih.dll to A:\message.vbs. This payload is not executed due to bug in code. The files C:\embryon.vbs and C:\embryon.dll are deleted and the registry key added:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\flps,
 "[windows SYSTEM directory]\flps.vbs"

W32/Blurt@MM (Aliases: I-Worm.Blar, W32.Blare@mm, WORM_BLAIRE.A) (Win32 Worm): This worm attempts to spread via Microsoft Outlook, and Internet Relay Chat. It also terminates security software, contains a Denial of Service attack payload, a web page overwriting payload, and disables the registry editor and task manager. The virus may be received in an e-mail message with various subjects, bodies, and attachments. When the attachment is run (manually accessed with the mouse or keyboard), the virus attempts to copy itself to the PROGRA~1 (Program Files) directory as ACCOUNT_DETAILS.DOC.exe. A registry key is created to load this, non-existent, file:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "Windows Task Manager" = c:\progra~1\ACCOUNT_DETAILS.DOC.exe

A file named WIN32.SORT-IT-OUT-BLAIR.TXT is created on the root directory of the C: drive. This file contains the following text: "Infected by the WIN32.SORT-IT-OUT-BLAIR Virus!" The virus contains a payload to overwrite the following files with this text:

- C:\inetpub\wwwroot\default.asp
- C:\inetpub\wwwroot\default.htm
- C:\inetpub\wwwroot\default.html
- C:\inetpub\wwwroot\index.asp
- C:\inetpub\wwwroot\index.htm
- C:\inetpub\wwwroot\index.html

The mIRC script is overwritten with instructions to send the virus to users who join the same channel as the infected user. The following registry keys are created to disable the registry editor and task manager:

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

On the 11th of the month, an ICMP denial of service attack is launched on the domain www.number-10.gov.uk.

W32.Dumaru.F@mm (Alias: Dumaru.F) (Win32 Worm): Dumaru.F is very similar to Dumaru.B with the following differences:

- File infection routine has been removed
- IRC backdoor component has been removed
- Uses different e-mail address to post the stolen data
- The e-mail address where it sends the stolen data is updateable through the TCP backdoor
- FTP uploading of stolen data has been enabled. This feature was disabled in Dumaru.B. The FTP site it would use is inaccessible at this point.

W32.HLLW.Cake (Alias: W32/Cake.worm!p2p, Worm/P2P.Cake, W32/Cake.worm) (Win32 Worm): This is a worm that attempts to spread through file-sharing networks, such as KaZaA, Grokster, and iMesh. It is written in the Microsoft Visual C++ programming language and is compressed with tElock.

W32.HLLW.Caspid (Win32 Worm): This is a worm that spreads through file-sharing networks, such as Morpheus and KaZaA. It is a virus that infects HTML files. This worm may also spread through e-mail by setting itself as the default stationery used in e-mail messages. It takes advantage of a vulnerability described in MS03-14, which allows for the execution of a MIME-encoded program inside an HTML file. It is written in Visual Basic and is packed with UPX. The existence of %Windir%\Capside.exe or %Windir%\Capside.htm is an indication of infection.

W32.HLLW.Gaobot.AE (Aliases: W32.HLLW.Gaobot.AA, Backdoor.Agobot.3.f, W32/Agobot.AA, W32.HLLW.Gaobot.AF) (Win32 Worm): This is a minor variant of W32.HLLW.Gaobot.AA that attempts to spread to the network shares with weak passwords. The worm also allows for a malicious user to access an infected computer through IRC. It uses the following vulnerabilities: The DCOM RPC vulnerability, described in Microsoft Security Bulletin MS03-026, using TCP port 135. The worm specifically targets Windows XP machines using this exploit. The RPC locator vulnerability, described in Microsoft Security Bulletin MS03-001, using TCP port 445. It is compressed with UPX.

W32.HLLW.Syney@mm (Alias: W32/Syney@MM) (Win32 Worm): This is a mass-mailing worm that deletes Windows system files and spreads through Microsoft Outlook. The e-mail message will have the following characteristics:

- Subject: Fwd:None
- Attachment: Attach.exe

W32.HLLW.Torvel@mm (Win32 Worm): This is a worm that spreads itself through Microsoft Outlook, Outlook Express, and through file-sharing networks.

W32.HLLW.Vuxer@mm (Win32 Worm): This is a mass-mailing worm that replicates using e-mail. It uses Microsoft Outlook to send itself to the contacts in the Outlook Address Book. The e-mail message has the following characteristics:

- Subject: Here it is!
- Attachment: Setup.exe (9,216 Bytes)

It is a Visual Basic application and is packed with UPX v0.76.1-1.24.

W32.Jonbarr.D@mm (Alias: W32/Pepex@MM) (Win32 Worm): This is a variant of the W32.Jonbarr@mm worm and is a mass-mailing worm that uses its own SMTP engine to send itself to all the e-mail addresses it finds in the .htm files and in temporary Internet files. Additionally, the worm attempts to terminate the processes of various antiviral programs. The e-mail has the following characteristics:

- Subject: Microsoft Windows Patch or Re:hya From: "Microsoft" support@microsoft.com
- Reply-To: "Microsoft" microsoft@microsoft.com
- Attachment: install.exe

When the attachment is opened, W32.Jonbarr.D@mm displays the message: "Happy Birthday My! Merdeka!" It is written in the Microsoft C++ programming language and is compressed with UPX.

W32.Marjor (Alias: W32/Marjor.A) (Win32 Virus): This is a virus that overwrites opened files on an infected system. The virus is written in the Microsoft Visual Basic programming language.

W32.Mexer.D.Worm (Alias: Worm.P2P.Harex.c) (Win32 Worm): This is a worm that attempts to spread across file-sharing networks such as KaZaA and iMesh. It also attempts to download an executable from a hard-coded Web link. It is packed with FSG. W32.Mexer.D.Worm is a variant of W32.Mexer.C.Worm.

W32.Moks (Win32 Virus): This is a virus that deletes every file and folder on drive C, on the 10th day of the month. It spreads itself by copying itself to A:\WildRose.exe. The virus is written in Microsoft Visual Basic and is packed with UPX.

W32/Nexiv.worm (Alias: HellFire) (Win32 Worm): This is an IRC-based worm which propagates via poorly secured network shares. It also takes advantage of the following vulnerability: MS03-026 (Dcom RPC)

W32/Opaserv-D (Aliases: Worm.Win32.Opasoft.d, BackDoor-ALB trojan) (Win32 Worm): This is a variant of W32/Opaserv-A and is a worm that spreads via network shares. When executed, the worm will create a file called scrsvr.exe in the Windows folder on the current drive. W32/Opaserv-D then adds the following registry entry to run itself when the system starts:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\ScrSvr = C:\WINDOWS\ScrSvr.exe

The worm attempts to copy itself to the Windows folder on networked computers with open shared drives. It then modifies the win.ini file on the remote machine to ensure the copied file will be run on system start. It also searches local IP addresses for open C: shares and attempts to copy itself to the Windows folder of the share. Once the local area network has been scanned, the worm will start performing the same search on the Internet starting at a randomly generated IP address. As a result, anyone connected to the Internet who has file sharing enabled and who enables NETBIOS over TCP/IP is potentially vulnerable to this worm. It also attempts to connect to a website that is currently unavailable. This attempted connection is most likely intended as a means of updating the worm executable. The following three non-viral files may be found in the root folder of infected systems: tmp.ini scrsin.dat scrsout.dat

W32.Patoo@mm (Alias: Bloodhound.W32.50) (Win32 Worm): This is a mass-mailing worm that attempts to use Microsoft Outlook to e-mail itself to all the contacts in the Address Book. The e-mail has the following characteristics:

- Subject: hey..
- Attachment: Stop Messenger Popups

It is written in Microsoft Visual Basic.

W32/Raleka.B (Aliases: Raleka.B, Worm.Win32.Raleka.B, W32/Raleka.B.worm, WORM_RALEKA.B) (Win32 Worm): Raleka.B is minor variant of the Raleka.A worm. In this variant the update URL was changed.

W32/Raleka.C (Aliases: Raleka.C, Worm.Win32.Raleka.C, W32/Raleka.C.worm, WORM_RALEKA.C) (Win32 Worm): Raleka.C is minor variant of the Raleka.A worm. In this variant the update URL was changed.

W32.Randex.J (Aliases: W32.Randex.F, W32/Randex.J, Worm.Randex.G) (Win32 Worm): This is a network-aware worm that will copy itself as `c$\winnt\system32\spolds.exe`. It will receive instructions from an IRC channel on a specific IRC server. One such command will trigger it to spread across the network.

W32.Repad.Worm (Win32 Worm): This is a worm that attempts to spread through the KaZaA file sharing network. The existence of the file `st01b.reb` or `SysTray32.dat` is an indication of a possible infection. The first time the worm is executed it will shut down the computer.

W32/Sluter-B (Aliases: W32.Randex.F, W32/Sdbot.worm.gen.b, W32/Sluter.worm.b) (Win32 Worm): This worm has been reported in the wild. It is a worm that propagates over network shares with weak passwords. The worm copies itself to the Windows system folder as `netd32.exe` and sets the following registry entries so as to run on system startup:

- `HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Microsoft Network Daemon for Win32 = netd32.exe`

and

- `HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\Microsoft Network Daemon for Win32 = netd32.exe`

Additionally W32/Sluter-B acts as an IRC based backdoor Trojan, allowing a remote intruder unlimited access to the affected computer.

W32/SobigF-Dam (Aliases: I-Worm.Sobig.f.dam, W32/Sobig.dam, WORM_SOBIG.F.DAM, W32.Sobig.F.Dam) (Win32 Virus): This virus has been reported in the wild. It is a damaged version of W32/Sobig-F. This version does not work and any files can simply be deleted.

W32.Strano (Win32 Virus): This is a virus that spreads through Microsoft Word documents. It is also a worm that spreads through IRC using "dcc send" commands. The existence of the file, "stb.dat," in the system folder is a sign of possible infection. When W32.Strano is executed, it infects the default Microsoft Word document template, `Normal.dot`, with the `W97M.Strano` macro virus. The virus creates the file, `%Sysdir%\stb.dat`, which contains source code for the macro virus. It locates the Mirc installation folder, for example, `C:\Program Files\Mirc`, and creates the file, `Strangerbox.ini`, in this folder. It also modifies the `Mirc.ini` file in this folder, adding "[StrangerBox]" to the top of the file and "n=strangerbox.ini" to the bottom of the file. The virus adds the value, "Strng32" = "`%Sysdir%\strngbox.exe`," to the registry key:

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

W32/Swen.A@mm (Aliases: I-Worm.Swen, WORM_SWEN.A, Swen, Worm Swen.A, W32/Gibe.e@MM, W32/Swan, W32/Gibe-F, Win32.HLLM.Gibe.2) (Win32 Worm): This worm has been reported in the wild. It is a worm which spreads by e-mailing itself via its own SMTP engine to addresses extracted from various sources on the victim's drives (e.g. MBX and DBX files). The worm also spreads using the KaZaA peer-to-peer shared folders and via IRC channels. It may also attempt to spread via Usenet newsgroups (NNTP). If the worm is run with a filename that starts with a P,Q,U or I (regardless of the case), it displays the message, "Microsoft Internet Update Pack This update does not need to be installed on this system" or "This will install Microsoft Security Update. Do you wish to continue?" and may also pretend to be an installation package by displaying an installation window with various messages in the title bar. If W32/Swen.A detects the installation of a debugger active in memory, it displays the message "Try to pull my legs?." The worm copies itself to the Windows folder as a randomly-named lowercase executable (e.g. `jlfsm.exe`) and adds an entry to the registry at:

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

to run itself on system restart. The worm also changes the entries in the registry at:

- `HKCR\exefile\shell\open\command HKCR\regfile\shell\open\command`
- `HKCR\comfile\shell\open\command HKCR\batfile\shell\open\command`

- HKCR\pifile\shell\open\command HKCR\scrfile\shell\open\command
- HKCR\scrfile\shell\config\command

so that it is run before EXE, COM, PIF, BAT, SCR files and to display a false error message (e.g. "Error occurred Memory access violation in module kernel32 at :") when REG files are opened. The worm sets several entries in the registry to signify installation, confirm KaZaA infection and to prevent REGEDIT.EXE from running. It may also create a file called SWEN1.DAT in the Windows folder containing a list of several IP addresses and domain names that may be NNTP servers. W32.Swen.A may attempt to exploit the IFRAME vulnerability in certain versions of Microsoft Internet Explorer and Outlook Express that allows automatic execution of attachments while viewing the message. It copies itself to the KaZaA shared folder and to the Windows folder with various EXE or ZIP filenames randomly constructed and attempts to terminate various processes related to anti-virus or security software (e.g. Sweep95, Zonealarm and Blackice).

W32.Titog.C.Worm (Win32 Worm): This is a mass-mailing worm that uses Microsoft Outlook and IRC to distribute itself. The e-mail message has the following characteristics:

- Subject: Speed up your connection!
- Attachment: t_dsl.exe

The worm attempts to delete many files and registry values.

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

- Subject: Microsoft Pack3, ;o)

It is written in Borland Delphi. When W32.Vybab@mm is executed, it creates the file %Windir%\123.txt, which is a text file with the message: "babyv ; made of Ran." The worm creates the batch file, %Windir%\<random three-letters>.bat, for example, Windows\xxx.bat. This batch file contains only references itself. If this file is executed, it causes a recursive-forever loop. It also attempts to delete some randomly selected files.

W32.Yaha.AB@mm (Aliases: I-Worm.Lentin.q, W32/Lentin.S@mm) (Win32 Worm): This worm is a variant of W32.Yaha.T@mm. It terminates some antiviral and firewall processes and uses its own SMTP engine to e-mail itself to all the contacts in the Windows Address Book, MSN Messenger, .NET Messenger, Yahoo Pager, ICQ Pager, as well as in all the files whose extensions contain the letters HT. The worm installs a keylogger and e-mails the logs to its author. It contains a destructive payload, which may be triggered if the system timezone is GMT+5. The worm also performs a Denial of Service (DoS) attack to some specified hosts and random hosts on ports 80, 135, 139, and 445. The e-mail message has a randomly chosen subject line, message, and attachment name. The attachment will have a .com, .exe, .scr, or .zip file extension. It is written in the Microsoft C++ language and is compressed with FSG.

W97M.Plonky (Word 97 Macro Virus): This is a Microsoft Word macro virus that spreads by infecting Microsoft Word documents and the Normal.dot global template. It disables access to the Control Toolbox toolbar and prevents you from editing Visual Basic code. When a document that is infected with W97M.Plonky is opened or closed, the macro virus replicates itself into active documents and the Normal.dot template. The virus may change the following Word options: When you open a document that contains a macro, the warning message no longer appears by default. The menu option that controls the macro settings is disabled.

W97M.Riosys (Alias: VBA/Generic.src) (Word 97 Macro Virus): This is a macro virus that infects Microsoft Word documents and templates when they are closed. When W97M.Riosys runs, it infects the Microsoft Word templates and any opened documents. The virus ends any running processes that contain the text "NAV" or "ANTIVIRUS" in their file names and disables the following Microsoft Word features:

- DisplayAlerts
- EnableCancelKey
- VirusProtection
- ConfirmConversions

- SaveNormalPrompt

The virus creates the following files:

- %Windir%\rioPHOsis.sYS
- %Windir%\rIOPHosIs.vBS

It also creates the subkey, "nAv AGENT, under the key:

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

The virus adds the values, "rIophosIs"="rIOPHosIs.vBS," to the registry key:

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

W97M.Rochitz.A (Word 97 Macro Virus): This is a macro virus that infects Microsoft Word documents when they are opened or closed. When a document infected with W97M.Rochitz.A is opened, it checks for signs on a previous infection in both the Active document code modules and the Normal template code modules. The virus displays a message box if it infects the Normal Template. It infects documents from the Normal Template for 50% of the time. If the document that the virus infected contains macros, it displays another message box. It does not infect documents for 50% of the time.

W97M.Strano (Alias: W97M/Dropbox) (Word 97 Macro Virus): This is a macro virus that infects Microsoft Word documents using the Normal.dot template. It creates and runs W32.Strano as %Sysdir%\Stbox32.exe.

WM97/Oragon-A (Aliases: W97M.Ping.A, W97M_ORAGON.A) (Word 97 Macro Virus): WM97/Oragon-A removes the Macro option from the Word Tools drop-down menu. On the first day of the month WM97/Oragon-A sets the caption of the active document so that it displays the username of the current user and attempts to bring up an animation of the Office Assistant application.

WM97/Simuleek-C (Aliases: Macro.Word97.Omni, W97M.Radnet, W97M_BUHAY, W97M/Simuleek) (Word 97 Macro Virus): This is a macro virus that drops a VBS script. VBS/Simuleek-C is added to the WIN.INI so that the script runs on startup. The virus has the ability to re-infect the Word environment. WM97/Simuleek-C may attempt to replace occurrences of the word "Ranuya" with the word "John."

Worm/Capsid (Alias: W32.Capsid) (Internet Worm): This is a memory resident Internet worm that spreads through various file sharing programs including KaZaA. If executed, the worm copies itself to the following locations:

- C:\WINDOWS\CAPSID.EXE
- C:\WINDOWS\SYSTEM\HVECVO.SCR
- C:\WINDOWS\CAPSIDERED.PIF
- C:\WINDOWS\CAPSID.HTM

Numerous files will be copied to the directories C:\PROGRAM FILES\KAZAA\MY SHARED FOLDER\ and C:\PROGRAM FILES\EDONKEY2000\INCOMING. It will also modify the file "C:\windows\system.ini" as follows: shell=Explorer.exe shell=Explorer.exe C:\WINDOWS\Capsid.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
"W32Load"="C:\\WINDOWS\\SYSTEM\\celKSng.scr"

Finally, the following keys are added:

- HKEY_CURRENT_USER\Identities\{A2BC20C0-875F-11D7-A0A4-D56AE6C02E32}\Software\Microsoft\Outlook Express\5.0\Mail
"Wide Stationery Name"="C:\\WINDOWS\\Capsid.htm"
"Stationery Name"="C:\\WINDOWS\\Capsid.htm"

Worm/Dumaru.J (Aliases: I-Worm.Dumaru.e, W32/Dumaru.j@MM) (Internet Worm): This is an Internet worm that spreads through e-mail addresses it collects in the files with the following extensions, .HTM .WAB .HTML .DBX .TBB .ABD and sends itself via its own SMTP engine. The worm arrives through e-mail in the following format:

- Subject: <no subject>

- Attachment: patch.exe

If executed, the worm creates copies of itself at different locations:

- C:\%windows%\dllreg.exe
- C:\windows%\system%\load32.exe
- C:\windows%\system%\vxdmgr32.exe
- C:\windows\Start Menu\Programs\Startup\RUNDLLW.EXE

Additionally, the following files are also created: C:\%windows%\GUID32.DLL 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 "load32" = "C:\WINNT%\System%\load32.exe"

Additionally, the following registry keys also get created:

- HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Run "run"="C:\windows\DLLREG.EXE"
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon "Shell"="Explorer.exe" "Shell"="Explorer.exe C:\windows%\system%\vxdmgr32.exe"

Worm/Dumar.J will also modify the files "win.ini" and "System.ini" files so that it gets loaded at startup.

Worm/Icebut.A (Internet Worm): This is an Internet worm that spreads through e-mail by using addresses it collects in the Windows Address Book. The worm arrives through e-mail in the following format:

- Subject: It's Near 911!
- Attachment: nerোসys.exe

If executed, the worm copies itself in C:\%windows%\ under the filename "nerოსys.exe." The file "system.ini" is then modified: system.ini shell=Explorer.exe shell=Explorer.exe nerოსys.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 NT\CurrentVersion\Winlogon "Shell"="Explorer.exe" "Shell"="Explorer.exe nerოსys.exe"

The registry key is just created on NT-based systems. Worm/Icebut.A is UPX packed but you can read the following string in the unpacked file: "This is Neroma Worm for :::911 : 119::"

WORM_NEROMA.B (Alias: W32.Neroma.B@mm, Worm/Icebut.B, I-Worm.Nearby.b, W32/Neroma-B, W32.Neroma.B@mm) (Internet Worm): This mass-mailing worm sends itself out to all e-mail addresses in the Microsoft Outlook address book. It sends out e-mail with the following details: Subject: Time to 911! Message body: Hi, Nice butt! Attachment: 119.gif It runs on Windows 95, 98, ME, NT, 2000, and XP.

Worm/Opasoft.L (Alias: W32.Opaserv.L) (Internet Worm): This is a variant of Worm/Opasoft, a network aware Internet worm that spreads through the use of network shares. If executed, the worm copies itself in the \windows\ directory under the following filenames "VACAS!" and "VAGABU!." The file "C:\PUTAS!!" then gets created. 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 "PutAS!"="C:\\WINDOWS\\PutA!.com"

Worm/Opasoft.L copies itself on shared "C" drives on other machines to \windows\ directory under VACAS!. Due to a vulnerability the virus has the ability to copy itself on password protected machines as well. This vulnerability only exists under Windows 95/98/ME machines.

Worm/Sefex (Alias: Trojan.Sefex) (Internet Worm): This is a memory resident Internet worm that if executed will copy itself in the \windows\ directory under the filename "RESUEM.EXE." 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 "putil"="C:\\WINDOWS\\RESUEM.EXE"

Worm/Stepaik (Alias: I-Worm.Stepaik) (Internet Worm): This is an Internet worm that if executed will copy itself in the \windows%\system% directory under the filename "asrss.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 "System Recovery Agent"="C:\WINDOWS\SYSTEM\asrss.exe"

Additionally, the following key is added:

- HKEY_CLASSES_ROOT\grp

WORM_VOTE.K (Aliases: W32.Vote.K@mm, Win32:WTC-Voted [Wrm], Bloodhound.W32.VBWORM) (Internet Worm): This worm propagates via e-mail, Internet Relay Chat (IRC), and the KaZaA peer-to-peer file-sharing network. It deletes several files and replaces .EXE files with a copy of itself. It arrives as an attachment in an e-mail message with following details:

- Subject: %Email address%. %s%
- Attachments: WTC32.SCR, WTC32.DLL

This worm is written in Visual Basic and runs on Windows 95, 98, ME, NT, 2000, and XP.

WORM_YAHA.U (Internet Worm): Similar to other worm YAHA variants, this mass-mailing worm propagates via e-mail using its own Simple Mail Transfer Protocol (SMTP) engine. It obtains target e-mail addresses from the following files: *HoTMaiL*. *ht* files, ICQ Databases, MSN Messenger and .NET Messenger data files, Windows Address Book (WAB), and Yahoo Messenger profiles. It also sends an e-mail to randomly generated addresses. It further arrives as a file attachment with the following extensions: ZIP, EXE, SCR, and COM. This worm also spreads via shared network drives. It logs keystrokes and sends them to a predefined e-mail address. It performs a Denial of Service (DoS) attack on the following sites by sending HyperText Transfer Protocol (HTTP) requests every few seconds:

- klc.org.pk
- ummah.org.uk
- ak.gov.pk
- ahore.gov.pk
- jamaat.org

Additionally, it is designed to remove several variants of the file infector, LOVGATE and also, WORM_SOBIG.A, from the system. This worm is also designed to terminate certain processes that are mostly security programs, such as antiviral and firewall applications. It runs on Windows 95, 98, ME, NT, 2000 and XP.

WORM_YAHA.W (Internet Worm): This YAHA variant attempts to propagate via e-mail and shared network drives. It terminates antiviral-related processes on the system. It tries to launch denial of service (DoS) attacks against the following Web sites:

- jamaat.org
- pak.gov.pk
- klc.org.pk
- ummah.org.
- uk piac.com.pk

Aside from propagating via shared network drives, this worm uses its own Simple Mail Transfer Protocol (SMTP) engine to send copies of itself via e-mail to addresses found in the following: Windows Address Book, ListCache of .NET messenger, ListCache of MSN messenger, Yahoo profiles, ICQ profiles, **HoTMaiL*. *ht* (All files with file names containing the string "HoTMaiL" and extensions containing "ht".), and * *. *ht* (All files with file names containing the extension "ht".) This malware runs on Windows 95, 98, ME, NT, 2000 and XP.

WORM_YAHA.X (Internet Worm): This mass-mailing worm propagates via e-mail using its own SMTP engine. It obtains target e-mail addresses from the following files: *HoTMaiL*. *ht* files, .HTM and .HTML files from the INETPUB and WWWROOT folders, ICQ Databases, MSN Messenger and .NET Messenger data files, Windows Addressbook (WAB), and Yahoo Messenger profiles. It also sends e-mail to randomly generated addresses. These e-mail messages are designed to contain two known vulnerabilities in Internet Explorer, the IFRAME and Incorrect MIME Header exploits. Additional information regarding these vulnerabilities are available at: (Microsoft Security Bulletin MS01-020) <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-020.asp>. This worm also spreads via shared network drives. It logs keystrokes and sends them to a predefined e-mail

address. It performs a denial of service attack on the following sites by sending HTTP requests every few seconds: jamaat.org klc.org.pk pak.gov.pk piac.com.pk ummah.org.uk This worm terminates antiviral processes and some Windows applications. It runs on Windows 95, 98, ME, 2000, and, XP.

W32/Yaha.y@MM (Win32 Worm): This variant of W32/Yaha is packed using ASPack and written in MSVC. It propagates via e-mail and over network shares. It uses its own built-in SMTP engine for constructing messages. It terminates specific processes if they are running (AV/security related), and contains code to deliver a denial of service attack against remote machines (various targets are hard-coded within the worm). Upon execution, the Trojan installs itself into the %Sysdir% directory as: MSEXEC.EXE MSUPDAT.EXE TASKMGR32.DLL (Where %Windir% is the Windows directory, for example C:\WINDOWS) (Where %Sysdir% is the Windows System directory, for example C:\WINDOWS\SYSTEM) The following Registry key is added to hook system startup:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run"MicrosoftService Manager " = "C:\%sysdir%\msupdat.exe"

The following registry is modified so that it runs whenever an .EXE, .BAT and .COM file is executed:

- HKEY_CLASSES_ROOT\exefile\shell\open\command "Default " = "%Sysdir%\MSEXEC.EXE""%1"%"*"
- HKEY_CLASSES_ROOT\batfile\shell\open\command "Default " = "%Sysdir%\MSEXEC.EXE""%1"%"*"
- HKEY_CLASSES_ROOT\comfile\shell\open\command "Default " = "%Sysdir%\MSEXEC.EXE""%1"%"*"

The worm looks for a WIN.INI file in specific folders (hardcoded within worm) on remote shares (only on mapped network drives in testing). If found, it copies itself to that folder as REG32.EXE, and adds a hook into the WIN.INI file: [windows] run=REGP32.EXE This worm uses its own SMTP Engine to send out messages from an infected system. The messages are constructed in the same way as mentioned for the description of W32/Yaha.x@MM . The files, HOSTS and LMHOSTS, in the Windows folder are modified to prevent the user from accessing the following Web sites:

- www.symantec.com
- www.kaspersky.com
- www.mcafee.com
- www.microsoft.com
- www.nai.com www.sophos.com
- www.avp.ru

This worm performs a denial of service attack on the following sites:

- jamaat.org
- klc.org.pk
- pak.gov.pk
- piac.com.pk
- ummah.org.uk

Trojans

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

Trojan	Version	CyberNotes Issue #
A97M/AcceV	N/A	CyberNotes-2003-18

Trojan	Version	CyberNotes Issue #
AdwareDropper-A	A	CyberNotes-2003-04
Adware-SubSearch.dr	dr	CyberNotes-2003-14
AIM-Canbot	N/A	CyberNotes-2003-07
AprilNice	N/A	CyberNotes-2003-08
Backdoor.Acidoor	N/A	CyberNotes-2003-05
Backdoor.Amitis	N/A	CyberNotes-2003-01
Backdoor.Amitis.B	B	CyberNotes-2003-11
Backdoor.AntiLam.20.K	K	CyberNotes-2003-10
Backdoor.AntiLam.20.Q	20.Q	CyberNotes-2003-18
Backdoor.Apdoor	N/A	CyberNotes-2003-12
Backdoor.Assasin.D	D	CyberNotes-2003-01
Backdoor.Assasin.E	E	CyberNotes-2003-04
Backdoor.Assasin.F	F	CyberNotes-2003-09
Backdoor.Badcodor	N/A	CyberNotes-2003-12
Backdoor.Beasty	N/A	CyberNotes-2003-02
Backdoor.Beasty.B	B	CyberNotes-2003-03
Backdoor.Beasty.C	C	CyberNotes-2003-05
Backdoor.Beasty.Cli	Cli	CyberNotes-2003-10
Backdoor.Beasty.D	D	CyberNotes-2003-06
Backdoor.Beasty.dr	dr	CyberNotes-2003-16
Backdoor.Beasty.E	E	CyberNotes-2003-06
Backdoor.Beasty.G	G	CyberNotes-2003-16
Backdoor.Beasty.Kit	N/A	CyberNotes-2003-18
Backdoor.Bigfoot	N/A	CyberNotes-2003-09
Backdoor.Bmbot	N/A	CyberNotes-2003-04
Backdoor.Bridco	N/A	CyberNotes-2003-06
Backdoor.CamKing	N/A	CyberNotes-2003-10
Backdoor.CHCP	N/A	CyberNotes-2003-03
Backdoor.Cmjspy	N/A	CyberNotes-2003-10
Backdoor.Cmjspy.B	B	CyberNotes-2003-14
Backdoor.CNK.A	A	CyberNotes-2003-10
Backdoor.CNK.A.Cli	Cli	CyberNotes-2003-10
Backdoor.Colfuser	N/A	CyberNotes-2003-01
Backdoor.Coreflood.dr	Dr	Current Issue
Backdoor.Cow	N/A	CyberNotes-2003-01
Backdoor.CrashCool	N/A	Current Issue
Backdoor.Cybspy	N/A	CyberNotes-2003-01
Backdoor.Dani	N/A	CyberNotes-2003-04
Backdoor.Darmenu	N/A	CyberNotes-2003-05
Backdoor.Death.Cli	Cli	CyberNotes-2003-10
Backdoor.Deftcode	N/A	CyberNotes-2003-01
Backdoor.Delf.Cli	Cli	CyberNotes-2003-10
Backdoor.Delf.F	F	CyberNotes-2003-07
Backdoor.Drator	N/A	CyberNotes-2003-01
Backdoor.Dsklite	N/A	CyberNotes-2003-14
Backdoor.Dsklite.cli	cli	CyberNotes-2003-14
Backdoor.Dvlldr	N/A	CyberNotes-2003-06
Backdoor.EggDrop	N/A	CyberNotes-2003-08
Backdoor.Evilbot.B	B	Current Issue

Trojan	Version	CyberNotes Issue #
Backdoor.EZBot	N/A	CyberNotes-2003-18
Backdoor.Fatroj	N/A	CyberNotes-2003-10
Backdoor.Fatroj.Cli	Cli	CyberNotes-2003-10
Backdoor.Fluxay	N/A	CyberNotes-2003-07
Backdoor.FTP.Casus	N/A	CyberNotes-2003-02
Backdoor.FTP_Ana.C	C	CyberNotes-2003-07
Backdoor.FTP_Ana.D	D	CyberNotes-2003-08
Backdoor.Fxdoor	N/A	CyberNotes-2003-10
Backdoor.Fxdoor.Cli	Cli	CyberNotes-2003-10
Backdoor.Fxsvc	N/A	CyberNotes-2003-16
Backdoor.Graybird	N/A	CyberNotes-2003-07
Backdoor.Graybird.B	B	CyberNotes-2003-08
Backdoor.Graybird.C	C	CyberNotes-2003-08
Backdoor.Graybird.D	D	CyberNotes-2003-14
Backdoor.Graybird.G	G	Current Issue
Backdoor.Grobodor	N/A	CyberNotes-2003-12
Backdoor.Guzu.B	B	CyberNotes-2003-14
Backdoor.HackDefender	N/A	CyberNotes-2003-06
Backdoor.Hale	N/A	CyberNotes-2003-16
Backdoor.Hethat	N/A	CyberNotes-2003-01
Backdoor.Hipo	N/A	CyberNotes-2003-04
Backdoor.Hitcap	N/A	CyberNotes-2003-04
Backdoor.Hornet	N/A	CyberNotes-2003-01
Backdoor.IRC.Aladinz	N/A	CyberNotes-2003-02
Backdoor.IRC.Aladinz.C	C	CyberNotes-2003-14
Backdoor.IRC.Bobbins	N/A	CyberNotes-2003-18
Backdoor.IRC.Cloner	N/A	CyberNotes-2003-04
Backdoor.IRC.Comiz	N/A	CyberNotes-2003-11
Backdoor.IRC.Flood.F	F	CyberNotes-2003-16
Backdoor.IRC.Hatter	N/A	CyberNotes-2003-18
Backdoor.IRC.Jemput	N/A	Current Issue
Backdoor.IRC.Lampsy	N/A	CyberNotes-2003-10
Backdoor.IRC.PSK	PSK	CyberNotes-2003-16
Backdoor.IRC.Ratsou	N/A	CyberNotes-2003-10
Backdoor.IRC.Ratsou.B	B	CyberNotes-2003-11
Backdoor.IRC.Ratsou.C	C	CyberNotes-2003-11
Backdoor.IRC.RPCBot.B:	B	CyberNotes-2003-18
Backdoor.IRC.RPCBot.C	C	CyberNotes-2003-18
Backdoor.IRC.RPCBot.D	D	CyberNotes-2003-18
Backdoor.IRC.RPCBot.F	F	Current Issue
Backdoor.IRC.Yoink	N/A	CyberNotes-2003-05
Backdoor.IRC.Zcrew	N/A	CyberNotes-2003-04
Backdoor.IRC.Zcrew.B	B	Current Issue
Backdoor.Kaitex.D	D	CyberNotes-2003-09
Backdoor.Kalasbot	N/A	CyberNotes-2003-09
Backdoor.Khaos	N/A	CyberNotes-2003-04
Backdoor.Kilo	N/A	CyberNotes-2003-04
Backdoor.Kodalo	N/A	CyberNotes-2003-14
Backdoor.Kol	N/A	CyberNotes-2003-06

Trojan	Version	CyberNotes Issue #
Backdoor.Krei	N/A	CyberNotes-2003-03
Backdoor.Lala	N/A	CyberNotes-2003-01
Backdoor.Lala.B	B	CyberNotes-2003-16
Backdoor.Lala.C	C	CyberNotes-2003-16
Backdoor.Lanfilt.B	B	CyberNotes-2003-14
Backdoor.Lastras	N/A	CyberNotes-2003-17
Backdoor.LeGuardien.B	B	CyberNotes-2003-10
Backdoor.Litmus.203.c	c	CyberNotes-2003-09
Backdoor.LittleWitch.C	C	CyberNotes-2003-06
Backdoor.Longnu	N/A	CyberNotes-2003-06
Backdoor.Lorac	N/A	CyberNotes-2003-17
Backdoor.Marotob	N/A	CyberNotes-2003-06
Backdoor.Massaker	N/A	CyberNotes-2003-02
Backdoor.MindControl	N/A	CyberNotes-2003-14
Backdoor.Monator	N/A	CyberNotes-2003-08
Backdoor.Mots	N/A	CyberNotes-2003-11
Backdoor.MSNCorrupt	N/A	CyberNotes-2003-06
Backdoor.Netdevil.15	15	CyberNotes-2003-15
Backdoor.NetDevil.B	B	CyberNotes-2003-01
Backdoor.NetTrojan	N/A	CyberNotes-2003-01
Backdoor.Nibu	N/A	CyberNotes-2003-16
Backdoor.Nickser	N?A	CyberNotes-2003-14
Backdoor.Ohpass	N/A	CyberNotes-2003-01
Backdoor.OICQSer.165	N/A	CyberNotes-2003-01
Backdoor.OICQSer.17	17	CyberNotes-2003-01
Backdoor.Omygo	N/A	Current Issue
Backdoor.Optix.04.d	04.d	CyberNotes-2003-04
Backdoor.OptixDDoS	N/A	CyberNotes-2003-07
Backdoor.OptixPro.10.c	10.c	CyberNotes-2003-01
Backdoor.OptixPro.12.b	12.b	CyberNotes-2003-07
Backdoor.OptixPro.13	13	CyberNotes-2003-09
Backdoor.Peers	N/A	CyberNotes-2003-10
Backdoor.Plux	N/A	CyberNotes-2003-05
Backdoor.Pointex	N/A	CyberNotes-2003-09
Backdoor.Pointex.B	B	CyberNotes-2003-09
Backdoor.Private	N/A	CyberNotes-2003-11
Backdoor.Prorat	N/A	CyberNotes-2003-13
Backdoor.PSpider.310	310	CyberNotes-2003-05
Backdoor.PSpider.310.b	310.b	CyberNotes-2003-18
Backdoor.Queen	N/A	CyberNotes-2003-06
Backdoor.Rado	N/A	CyberNotes-2003-18
Backdoor.Ranck	N/A	CyberNotes-2003-18
Backdoor.Ratega	N/A	CyberNotes-2003-09
Backdoor.Receiv	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

Trojan	Version	CyberNotes Issue #
Backdoor.Roxy	N/A	CyberNotes-2003-16
Backdoor.RPCBot.E	E	Current Issue
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	CyberNotes-2003-11
Backdoor.Sdbot.M	M	CyberNotes-2003-13
Backdoor.Sdbot.P	P	CyberNotes-2003-17
Backdoor.Serpa	N/A	CyberNotes-2003-03
Backdoor.Servsax	N/A	CyberNotes-2003-01
Backdoor.Sheldor	N/A	CyberNotes-2003-18
Backdoor.SilverFTP	N/A	CyberNotes-2003-04
Backdoor.Simali	N/A	CyberNotes-2003-09
Backdoor.Sixca	N/A	CyberNotes-2003-01
Backdoor.Slao	N/A	CyberNotes-2003-11
Backdoor.Snami	N/A	CyberNotes-2003-10
Backdoor.Snowdoor	N/A	CyberNotes-2003-04
Backdoor.Socksbot	N/A	CyberNotes-2003-06
Backdoor.Softshell	N/A	CyberNotes-2003-10
Backdoor.Sokacaps	N/A	CyberNotes-2003-18
Backdoor.Stealer	N/A	CyberNotes-2003-14
Backdoor.SubSari.15	15	CyberNotes-2003-05
Backdoor.SubSeven.2.15	2.15	CyberNotes-2003-05
Backdoor.Sumtax	N/A	CyberNotes-2003-16
Backdoor.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	1	CyberNotes-2003-03
Backdoor.UKS	N/A	CyberNotes-2003-11
Backdoor.Unifida	N/A	CyberNotes-2003-05
Backdoor.Upfudoor	N/A	CyberNotes-2003-01
Backdoor.Urat.b	b	CyberNotes-2003-18
Backdoor.Uzbek	N/A	CyberNotes-2003-15
Backdoor.VagrNocker	N/A	CyberNotes-2003-01
Backdoor.Vmz	N/A	CyberNotes-2003-01
Backdoor.Winet	N/A	CyberNotes-2003-11
Backdoor.WinJank	N/A	CyberNotes-2003-15
Backdoor.Winker	N/A	CyberNotes-2003-15
Backdoor.WinShell.50	N/A	CyberNotes-2003-16
Backdoor.Wolf.16	16	CyberNotes-2003-18
Backdoor.Xenozbot	N/A	CyberNotes-2003-01

Trojan	Version	CyberNotes Issue #
Backdoor.Xeory	N/A	CyberNotes-2003-03
Backdoor.XTS	N/A	CyberNotes-2003-08
Backdoor.Zdemon	N/A	CyberNotes-2003-02
Backdoor.Zdemon.126	126	CyberNotes-2003-10
Backdoor.Zdown	N/A	CyberNotes-2003-05
Backdoor.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	CyberNotes-2003-11
BackDoor-AVF	AVF	CyberNotes-2003-12
BackDoor-AVH	AVH	CyberNotes-2003-12
BackDoor-AVO	AVO	CyberNotes-2003-12
BackDoor-AXC	AXC	CyberNotes-2003-14
BackDoor-AXQ	AXQ	CyberNotes-2003-15
Backdoor-AXR	AXR	CyberNotes-2003-16
BDS/AntiPC	N/A	CyberNotes-2003-02
BDS/Backstab	N/A	CyberNotes-2003-02
BDS/CheckESP	N/A	CyberNotes-2003-12
BDS/Ciadoor.10	10	CyberNotes-2003-07
BDS/Evilbot.A	A	CyberNotes-2003-09
BDS/Evolut	N/A	CyberNotes-2003-03
BDS/GrayBird.G	G	CyberNotes-2003-17
BDS/PowerSpider.A	A	CyberNotes-2003-11
BKDR_LITH.103.A	A	CyberNotes-2003-17
Cardown	N/A	Current Issue
CoolFool	N/A	CyberNotes-2003-17
Daysun	N/A	CyberNotes-2003-06
DDoS-Stinkbot	N/A	CyberNotes-2003-08
Delude	N/A	Current Issue
DoS-iFrameNet	N/A	CyberNotes-2003-04
Download.Aduent.Trojan	N/A	CyberNotes-2003-18
Download.Trojan.B	B	CyberNotes-2003-13
Downloader.BO.B	B	CyberNotes-2003-10
Downloader.BO.B.dr	B.dr	CyberNotes-2003-10
Downloader.Dluca	N/A	CyberNotes-2003-17
Downloader.Dluca.B	B	Current Issue

Trojan	Version	CyberNotes Issue #
Downloader.Mimail	N/A	CyberNotes-2003-16
Downloader-BN.b	BN.b	CyberNotes-2003-13
Downloader-BO.dr.b	N/A	CyberNotes-2003-02
Downloader-BS	N/A	CyberNotes-2003-02
Downloader-BW	N/A	CyberNotes-2003-05
Downloader-BW.b	BW.b	CyberNotes-2003-06
Downloader-BW.c	BW.c	CyberNotes-2003-07
Downloader-CY	CY	CyberNotes-2003-16
Downloader-DM	DM	CyberNotes-2003-16
Downloader-DN.b	DN.b	CyberNotes-2003-17
Downloader-EB	EB	CyberNotes-2003-18
ELF_TYPOT.A	A	CyberNotes-2003-13
ELF_TYPOT.B	B	CyberNotes-2003-13
Exploit-IISInjector	N/A	CyberNotes-2003-03
Gpix	N/A	CyberNotes-2003-08
Hacktool.Keystaal	N/A	Current Issue
Hacktool.PWS.QQPass	N/A	CyberNotes-2003-06
ICQPager-J	N/A	CyberNotes-2003-05
IRC/Backdoor.e	E	CyberNotes-2003-01
IRC/Backdoor.f	f	CyberNotes-2003-02
IRC/Backdoor.g	g	CyberNotes-2003-03
IRC/Flood.ap	N/A	CyberNotes-2003-05
IRC/Flood.bi	N/A	CyberNotes-2003-03
IRC/Flood.br	br	CyberNotes-2003-06
IRC/Flood.bu	bu	CyberNotes-2003-08
IRC/Flood.cd	cd	CyberNotes-2003-11
IRC/Flood.cm	cm	CyberNotes-2003-13
IRC/Fyle	N/A	CyberNotes-2003-16
IRC-BBot	N/A	CyberNotes-2003-16
IRC-Emoz	N/A	CyberNotes-2003-03
IRC-OhShootBot	N/A	CyberNotes-2003-01
IRC-Vup	N/A	CyberNotes-2003-09
JS.Fortnight.B	B	CyberNotes-2003-06
JS.Seeker.J	J	CyberNotes-2003-01
JS/Fortnight.c@M	c	CyberNotes-2003-11
JS/Seeker-C	C	CyberNotes-2003-04
JS/StartPage.dr	dr	CyberNotes-2003-11
JS_WEBLOG.A	A	CyberNotes-2003-05
Keylogger.Cone.Trojan	N/A	CyberNotes-2003-14
KeyLog-Kerlib	N/A	CyberNotes-2003-05
Keylog-Keylf	N/A	CyberNotes-2003-17
Keylog-Kjie	N/A	CyberNotes-2003-12
Keylog-Perfect.dr	dr	CyberNotes-2003-09
Keylog-Razytimer	N/A	CyberNotes-2003-03
KeyLog-TweakPan	N/A	CyberNotes-2003-02
Keylog-Yeehah	N/A	CyberNotes-2003-12
Linux/DDoS-Ferlect	N/A	CyberNotes-2003-17
Linux/Exploit-SendMail	N/A	CyberNotes-2003-05
Lockme	N/A	CyberNotes-2003-15

Trojan	Version	CyberNotes Issue #
MultiDropper-FD	N/A	CyberNotes-2003-01
OF97/ExeDrop-B	N/A	Current Issue
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-AJ	AJ	CyberNotes-2003-13
ProcKill-Z	N/A	CyberNotes-2003-03
Proxy-Guzu	N/A	CyberNotes-2003-08
Proxy-Migmaf	N/A	CyberNotes-2003-14
PWS-Aileen	N/A	CyberNotes-2003-04
PWS-Moneykeeper	N/A	CyberNotes-2003-18
PWS-Sincom.dr	dr	CyberNotes-2003-17
PWSteal.ABCHlp	N/A	CyberNotes-2003-12
PWSteal.AILight	N/A	CyberNotes-2003-01
PWSteal.Bancos	N/A	CyberNotes-2003-15
PWSteal.Bancos.B	B	CyberNotes-2003-16
PWSteal.Hukle	N/A	CyberNotes-2003-08
PWSteal.Kipper	N/A	CyberNotes-2003-10
PWSteal.Lemir.105	105	CyberNotes-2003-10
PWSteal.Lemir.C	C	CyberNotes-2003-17
PWSteal.Lemir.D	D	CyberNotes-2003-18
PWSteal.Rimd	N/A	CyberNotes-2003-01
PWSteal.Rimd.B	B	CyberNotes-2003-10
PWSteal.Senhas	N/A	CyberNotes-2003-03
PWSteal.Snatch	N/A	CyberNotes-2003-10
PWSteal.Sysrater	N/A	CyberNotes-2003-12
PWS-Tenbot	N/A	CyberNotes-2003-01
PWS-Train	N/A	CyberNotes-2003-17
PWS-Truebf	N/A	CyberNotes-2003-13
PWS-Watsn	N/A	CyberNotes-2003-10
PWS-Wexd	N/A	CyberNotes-2003-14
PWS-WMPatch	N/A	CyberNotes-2003-07
PWS-Yipper	N/A	CyberNotes-2003-10
QDel359	359	CyberNotes-2003-01
QDel373	373	CyberNotes-2003-06
Qdel374	374	CyberNotes-2003-06
Qdel375	375	CyberNotes-2003-06
Qdel376	376	CyberNotes-2003-07
QDel378	378	CyberNotes-2003-08
QDel379	369	CyberNotes-2003-09
QDel390	390	CyberNotes-2003-13
QDel391	391	CyberNotes-2003-13
QDel392	392	CyberNotes-2003-13
QDial11	1	CyberNotes-2003-14
QDial6	6	CyberNotes-2003-11
Renamer.c	N/A	CyberNotes-2003-03
Reom.Trojan	N/A	CyberNotes-2003-08
StartPage-G	G	CyberNotes-2003-06

Trojan	Version	CyberNotes Issue #
Startpage-N	N	CyberNotes-2003-13
Stealther	N/A	CyberNotes-2003-16
Stoplete	N/A	CyberNotes-2003-06
Swizzor	N/A	CyberNotes-2003-07
Tellafriend.Trojan	N/A	CyberNotes-2003-04
Tr/Decept.21	21	CyberNotes-2003-07
Tr/Delf.r	r	CyberNotes-2003-16
Tr/DelWinbootdir	N/A	CyberNotes-2003-07
TR/Fake.YaHoMe.1	N/A	CyberNotes-2003-02
TR/Gaslide.C	C	CyberNotes-2003-17
Tr/SpBit.A	A	CyberNotes-2003-04
Tr/VB.t	T	CyberNotes-2003-11
TR/WinMx	N/A	CyberNotes-2003-02
Troj/Apdoor-A	A	Current Issue
Troj/Ataka-E	E	CyberNotes-2003-15
Troj/Autoroot-A	A	CyberNotes-2003-16
Troj/Backsm-A	A	Current Issue
Troj/Bdoor-RQ	RQ	CyberNotes-2003-17
Troj/Dloader-BO	BO	CyberNotes-2003-02
Troj/DownLdr-DI	DI	CyberNotes-2003-15
Troj/Eyeveg-A	A	Current Issue
Troj/Golon-A	A	CyberNotes-2003-15
Troj/Hacline-B	B	CyberNotes-2003-13
Troj/IRCBot-C	C	CyberNotes-2003-11
Troj/Manifest-A	N/A	CyberNotes-2003-03
Troj/Migmaf-A	A	CyberNotes-2003-15
Troj/Mystri-A	A	CyberNotes-2003-13
Troj/PcGhost-A	A	CyberNotes-2003-13
Troj/Peido-B	B	CyberNotes-2003-10
Troj/QQPass-A	A	CyberNotes-2003-16
Troj/Qzap-248	N/A	CyberNotes-2003-01
Troj/SadHound-A	N/A	CyberNotes-2003-03
Troj/Sandesa-A	A	CyberNotes-2003-14
Troj/Slacker-A	A	CyberNotes-2003-05
Troj/Slanret-A	N/A	CyberNotes-2003-03
Troj/TKBot-A	A	CyberNotes-2003-04
Troj/Webber-A	A	CyberNotes-2003-15
TROJ_JBELLZ.A	A	CyberNotes-2003-02
TROJ_KILLBOOT.B	B	CyberNotes-2003-01
TROJ_RACKUM.A	A	CyberNotes-2003-05
Trojan.Ailati	N/A	CyberNotes-2003-15
Trojan.Analogx	N/A	CyberNotes-2003-17
Trojan.AprilFool	N/A	CyberNotes-2003-08
Trojan.Barjac	N/A	CyberNotes-2003-05
Trojan.Boxer	N/A	Current Issue
Trojan.Dasmin	N/A	CyberNotes-2003-01
Trojan.Dasmin.B	B	CyberNotes-2003-03
Trojan.Downloader.Aphe	N/A	CyberNotes-2003-06

Trojan	Version	CyberNotes Issue #
Trojan.Downloader.Inor	N/A	CyberNotes-2003-02
Trojan.Fwin	N/A	CyberNotes-2003-18
Trojan.Grepage	N/A	CyberNotes-2003-05
Trojan.Guapeton	N/A	CyberNotes-2003-08
Trojan.Idly	N/A	CyberNotes-2003-04
Trojan.Ivanet	N/A	CyberNotes-2003-02
Trojan.Kaht	N/A	CyberNotes-2003-10
Trojan.KillAV.B	B	Current Issue
Trojan.KKiller	N/A	CyberNotes-2003-01
Trojan.Lear	N/A	CyberNotes-2003-10
Trojan.Mumuboy	N/A	CyberNotes-2003-13
Trojan.Myet	N/A	CyberNotes-2003-12
Trojan.Norio	N/A	Current Issue
Trojan.OptixKiller	N/A	CyberNotes-2003-16
Trojan.Poetas	N/A	CyberNotes-2003-14
Trojan.Poldo.B	B	CyberNotes-2003-02
Trojan.Poot	N/A	CyberNotes-2003-05
Trojan.PopSpy	N/A	CyberNotes-2003-11
Trojan.Progent	N/A	CyberNotes-2003-16
Trojan.ProteBoy	N/A	CyberNotes-2003-04
Trojan.PSW.Gip	N/A	CyberNotes-2003-06
Trojan.PSW.Platan.5.A	N/A	CyberNotes-2003-01
Trojan.PWS.QQPass.D	N/A	CyberNotes-2003-02
Trojan.Qforager	N/A	CyberNotes-2003-02
Trojan.Qforager.Dr	N/A	CyberNotes-2003-02
Trojan.Qwe	N/A	CyberNotes-2003-02
Trojan.Sarka	N/A	CyberNotes-2003-14
Trojan.Sidea	N/A	CyberNotes-2003-12
Trojan.Snag	N/A	CyberNotes-2003-02
Trojan.Unblockee	N/A	CyberNotes-2003-01
Trojan.Visages	N/A	CyberNotes-2003-15
Trojan.Windelete	N/A	CyberNotes-2003-14
TrojanGaslid	N/A	CyberNotes-2003-18
Uploader-D	D	CyberNotes-2003-06
Uploader-D.b	D.b	CyberNotes-2003-07
VBS.ExitWin	N/A	CyberNotes-2003-12
VBS.Flipe	N/A	CyberNotes-2003-17
VBS.Kasnar	N/A	CyberNotes-2003-06
VBS.Moon.B	B	CyberNotes-2003-02
VBS.StartPage	N/A	CyberNotes-2003-02
VBS.Trojan.Lovcx	N/A	CyberNotes-2003-05
VBS.Zizarn	N/A	CyberNotes-2003-09
VBS/Fourcourse	N/A	CyberNotes-2003-06
W32.Adclicker.C.Trojan	C	CyberNotes-2003-09
W32.Bambo	N/A	CyberNotes-2003-14
W32.Benpao.Trojan	N/A	CyberNotes-2003-04
W32.CVIH.Trojan	N/A	CyberNotes-2003-06
W32.Laorenshen.Trojan	N/A	CyberNotes-2003-14

Trojan	Version	CyberNotes Issue #
W32.Noops.Trojan	N/A	CyberNotes-2003-09
W32.Socay.Worm	N/A	CyberNotes-2003-02
W32.Spybot.dr	dr	CyberNotes-2003-15
W32.Systentry.Trojan	N/A	CyberNotes-2003-03
W32.Trabajo	N/A	CyberNotes-2003-14
W32.Xilon.Trojan	N/A	CyberNotes-2003-01
W32.Yinker.Trojan	N/A	CyberNotes-2003-04
W32.Igloo-15	N/A	CyberNotes-2003-04
Woodcot	N/A	CyberNotes-2003-16
Xin	N/A	CyberNotes-2003-03

Backdoor.Coreflood.dr: Backdoor.Coreflood.dr is an HTML file containing VBScript. If a Web site has been compromised, some of its pages may contain iframe links to Backdoor.Coreflood.dr. The dropper uses an exploit described in Microsoft Security Bulletin MS03-032 to allow execution of arbitrary code from a Web page. When the page is loaded by a browser that has not been patched against the remote execution exploit, the script creates and executes a file called malware***.exe (where *** represents any digits, 0-9). The malware***.exe file then extracts and downloads the other components of the backdoor.

Backdoor.CrashCool (Alias: Backdoor.CrashCool.a): This is a Trojan Horse that allows unauthorized access to the victim machine. By default it opens port 9898 for listening. It is written in the Microsoft Visual Basic programming language.

Backdoor.Evilbot.B (Aliases: Backdoor.Evilbot.a, W32/Cult.worm.gen): This is a variant of Backdoor.Evilbot that allows unauthorized access to an infected computer. This Trojan Horse could also allow a malicious user to launch a remote attack using an infected computer. When Backdoor.Evilbot.B runs, it copies itself as one of the following file names:

- %Windir%\Setup_32.exe
- %Windir%\WinSetup.exe

The Trojan adds one of the following values: "win32"="%Windir%\Setup_32.exe" "win32"="%Windir%\WinSetup.exe" to registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\

It also communicates to the author via mIRC, using the user name "psychothug."

Backdoor.Graybird.G (Alias: Backdoor.GrayBird.f): This is a variant of Backdoor.Graybird that allows unauthorized access to a compromised system. The Trojan is written in Borland Delphi and is compressed with ASPack.

Backdoor.IRC.Jemput: This is a Backdoor Trojan Horse that installs an mIRC client, with backdoor capabilities, which gives the Trojan's author unlimited access to a computer.

Backdoor.IRC.RPCBot.F: This is an Internet Relay Chat (IRC) Trojan Horse that allows its creator to control a computer through IRC. It is also a worm that can use the DCOM RPC vulnerability (described in Microsoft Security Bulletin MS03-026) to spread itself.

Backdoor.IRC.Zcrew.B: This is a Backdoor Trojan Horse that may allow remote control of an infected system through IRC and FTP. The Trojan may arrive as a self-extracting archive, approximately 1.5 megabytes in size. When Backdoor.IRC.Zcrew.B is executed, it drops various files in the C:\WINNT\system32\wbem\repository\fs\macromed folder and adds the hidden attribute to these files. It also adds the value, "print sharing" = "<path>\hidden32.exe <path>\explorer.exe," to the registry key:

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

This Trojan starts the Serv-U and Iroffer applications as service processes.

Backdoor.Omygo (Aliases: Backdoor.Trojan, Backdoor.VB.ke): This is a Backdoor Trojan Horse that provides unauthorized remote access to an infected computer. Another program detected as Backdoor.Omygo.dr usually drops this Trojan. It is written in Microsoft Visual Basic and is usually packed with a run-time packer, such as ASPack or PECO.

Backdoor.RPCBot.E: This is an Internet Relay Chat (IRC) Trojan horse that allows its creator to control a computer through IRC. It also uses the DCOM RPC vulnerability, described in Microsoft Security Bulletin MS03-026, to spread itself.

Cardown (Aliases: Java/Cardown.A, TrojanDownloader.Java.DummyMod): This is a Java applet based Trojan that downloads and installs the Startpage.Y Trojan on the system. Cardown activates when a user views a web page or HTML e-mail that contains reference to the Trojan file. Cardown is a Java applet that is heavily obfuscated and uses scrambling in its strings. The Trojan is not packaged in to a Jar file so each component class file is individually loaded when Trojan executes, so in most cases the user will get a warning about the first component file and will not receive the rest of the malware. When the Trojan is executed it uses Microsoft Internet Explorer VerifierBug vulnerability to get full privileges by escaping the Java security, and execute its code. Then the Trojan downloads bootconf.exe into Windows directory (default C:\Windows) and modifies registry so that the Trojan starts automatically at Windows startup. Further information about the vulnerability in the Microsoft Java VM, including a fix, is available at: <http://www.microsoft.com/technet/security/bulletin/ms03-011.asp>.

Delude (Alias: Trojan.BAT.Startpage.a): Delude is a Trojan that is available on a web page. The web page contains a code that uses a vulnerability in the Internet Explorer (MS03-032) to execute. More information about the vulnerability, including a fix, is available from Microsoft at: http://www.microsoft.com/security/security_bulletins/ms03-032.asp.

Downloader.Dluca.B: This is a variant of the Downloader.Dluca Trojan Horse that sends information about your computer to a specific Web site. When Downloader.Dluca.B is executed, it copies itself to the System directory and adds a value, "%System%\<filename>.exe /noconnect," to the registry key:

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

The Trojan adds the values: "UninstallString"="%System%\<filename>-uninstall.exe /uninstall" "DisplayName"="<filename>" to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\uninstall\<filename>

It adds the value, "MIMETYPE_DESCRIPTION"=".wxx," to the registry key:

- HKEY_CURRENT_USER\Software\<filename>

Hacktool.Keysteel (Aliases: Trojan.PSW.VB.aq, Generic PWS): This is a hacktool that collects CD keys and other user information about selected products. This information is written to a file that could be retrieved at a later date. NOTE: Because the file is not sent to another source, and because the software does not perform actions other than gathering information, this threat is classified as a hacktool rather than a Trojan Horse.

OF97/ExeDrop-B (Aliases: TrojanDropper.Macro.AcceV, A97M/AcceV, A2KM_GRYBIRD.DRP): This is a macro that drops and runs Troj/Graybird-A. It requires a double-byte version of Office 2000 (or above) and is received by being spammed with an Access Database named SEP 2003 POM.mdb.

Troj/Apdoor-A (Aliases: Backdoor.Apdoor.c, CoreFlood trojan, Win32/Apdoor.C, Backdoor.Coreflood.B): This Trojan has been reported in the wild. It is a backdoor Trojan that drops a DLL with a random name into the Windows temporary folder and executes it. The Trojan DLL attempts to inject itself into the Program Manager process, then copies itself and the Trojan EXE into the Windows system or temporary folder and sets the following registry entry or the corresponding HKCU entry:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\<randomstring> = <Path to the Trojan exe>

It monitors this registry entry and attempts to reset it if the entry is modified or removed. A malicious script hosted on a website typically distributes it. The script will drop a downloader EXE file and run it. The

dropped EXE program drops a DLL into the Windows temporary folder with a random name and executes it. The dropped DLL attempts to inject itself into the Program Manager process, copies itself and its dropper EXE into the Windows system or temporary folder and sets the following HKLM or HKCU registry key:

- \Software\Microsoft\Windows\CurrentVersion\Run\<randomstring>
- = <Path to the downloader exe>

The DLL then attempts to download Troj/Apdoor-A from a predefined website onto the user's machine and run it.

Troj/Backsm-A (Aliases: Backdoor.Small.c, Backdoor.Sdbot): This Trojan has been reported in the wild. It is a backdoor Trojan. When executed, the Trojan initiates a background process and attempts to connect to a remote IRC server and provide unauthorized access to the infected computer. Troj/Backsm-A sets the following registry entry in an attempt to run the Trojan when Windows starts up:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run "winlogin"=<System>\Winlogin.exe

Troj/Eyeveg-A (Aliases: Backdoor.Lorac,BKDR_LORAC.A,Backdoor_AYU): This is a password stealing Trojan and network worm. It attempts to send cached passwords and system information to a remote location. Troj/Eyeveg-A spreads to shared drives on the local network, copying itself as Explore.exe to the startup folder specified in the registry entry:

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Common Startup

When first run, Troj/Eyeveg-A copies itself to the Windows System folder using a random filename and adds its pathname to the registry entry:

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

so that it is run automatically each time the computer is started.

Trojan.Boxer (Alias: PWS-Runbox): This is a Trojan Horse that records keystrokes in a log file and then sends the information to a predetermined e-mail address. It is packed with FSG. Note: Trojan.Boxer may arrive as an attachment in an e-mail that uses the HTML codebase exploit, mentioned in Microsoft Security Bulletins MS02-015 and MS03-014, which allows the Trojan to be executed automatically.

Trojan.KillAV.B (Alias: Trojan.Win32): This Trojan attempts to kill Norton Antivirus and Norton Internet Security processes. It also makes the Task Manager and Registry Editor tools inaccessible to the user of an infected machine. When Trojan.KillAV.B runs, it copies itself as C:\Winnt\Java\Java\iexplore.exe and ends the Norton Antivirus Auto-Protect and Norton Internet Security proxy services. The Trojan adds the value, "DisableTaskMgr"="0x00000001," to the registry key:

- HKey_Current_User\Software\Microsoft\Windows\CurrentVersion\Policies\System\

which disables the Task Manager. It also adds the value, "DisableRegistryTools"="0x00000001," to the registry key:

- HKey_Current_User\Software\Microsoft\Windows\CurrentVersion\Policies\System\

which disables the Registry Editing tools. It also sets the value, "Java Runtimes"="C:\Winnt\Java\Java\iexplore.exe," in the registry key:

- HKey_Local_Machine\Software\Microsoft\Windows\CurrentVersion\Run\

so that the Trojan runs when you start Windows. The following values are modified:

- "ApplicationAccess1"="0x00000001"
- "ApplicationList1"="C:\Winnt\Java\Java\iexplore.exe"

in the registry key:

- HKey_Local_Machine\Software\Symantec\IAM\FirewallObjects\ Applications\iexplore.exe\

Trojan.Norio: This is a Trojan horse that modifies browser and network settings to direct you to pornographic Web sites. It includes a component that can download and execute arbitrary code on your computer.