



Department of Homeland Security

Information Analysis and Infrastructure Protection Directorate

CyberNotes

Issue #2003-21

October 20, 2003

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

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

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

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between October 2 and October 15, 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
Adiscon GmbH ¹	Windows	WinSyslog 4.21 SP1	A remote Denial of Service vulnerability exists when a malicious user submits UDP datagrams that contain arbitrary, overly large amounts of data to the interactive server (default port 10514/udp).	No workaround or patch available at time of publishing.	WinSyslog Long Syslog Message Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.

¹ Securiteam, October 14, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Adobe Systems Incorporated ²	Windows	SVG Viewer 3.0 & prior	A cross-domain security vulnerability exists in the 'alert()' command, which could let a remote malicious user execute arbitrary code. <i>Note: Any application that makes use of the WebBrowser control is vulnerable (Internet Explorer, AOL Browser, MSN Explorer, etc.).</i>	Patch available at: http://www.adobe.com/svg/viewer/install/mainframed.html	SVG Viewer Alert Method Code Execution	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Adobe Systems Incorporated ³	Windows	SVG Viewer 3.0 & prior	An information disclosure vulnerability exists because the non-standard 'postURL' and 'getURL' methods do not properly restrict cross-domain security controls, which could let a remote malicious user obtain sensitive information. <i>Note: Any application that makes use of the WebBrowser control is vulnerable (Internet Explorer, AOL Browser, MSN Explorer, etc.).</i>	Patch available at: http://www.adobe.com/svg/viewer/install/mainframed.html	SVG Viewer 'postURL' & 'getURL' Restriction Bypass	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Adobe Systems Incorporated ⁴	Windows	SVG Viewer 3.0 & prior	A vulnerability exists because the Active Scripting security settings can be bypassed, which could let a remote malicious user bypass security restrictions. <i>Note: Any application that makes use of the WebBrowser control is vulnerable (Internet Explorer, AOL Browser, MSN Explorer, etc.).</i>	Patch available at: http://www.adobe.com/svg/viewer/install/mainframed.html	SVG Viewer Active Scripting Security Bypass	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Ali ⁵	Windows, Unix	PayPal Store Front 3.0	A vulnerability exists in the 'index.php' script because the page parameter isn't properly verified, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	PayPal Store Front 'index.php'	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
America OnLine ⁶	Windows	Instant Messenger 5.2.3292	A buffer overflow vulnerability exists in the 'screenname' parameter, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.aim.com/get_aim/win/win_beta.adp	AOL Instant Messenger Screenname Buffer Overflow	High	Bug discussed in newsgroups and websites.

² GreyMagic Security Advisory, GM#004-MC, October 7, 2003.

³ GreyMagic Security Advisory, GM#003-MC, October 7, 2003.

⁴ GreyMagic Security Advisory, GM#002-MC, October 7, 2003.

⁵ Zone-H Security Team Advisory, ZH2003-28SA, October 8, 2003.

⁶ DigitalPranksters Security Advisory, October 15, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Apache Software Foundation ⁷ <i>Hewlett Packard issues advisory</i> ⁸	MacOS X 10.x, Unix	Apache 2.0a9, 2.0, 2.0.28, 2.0.32, 2.0.35-2.0.47	A Denial of Service vulnerability exists because the 'mod_cgi' doesn't handle output to STDERR correctly.	Mandrake: http://www.mandrakesecurity.net/en/ftp.php Hewlett Packard: http://itrc.hp.com/cki/bin/doc.pl/screen=ckiSecurityBulletin	Apache2 MOD_CGI Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Apache Software Foundation ⁹	Unix	Tomcat 4.0-4.0.6	A Denial of Service vulnerability exists due to a failure to handle multiple invalid or non-HTTP requests.	Debian: http://security.debian.org/pool/updates/contrib/t/tomcat4/	Tomcat Non-HTTP Request Denial of Service	Low	Bug discussed in newsgroups and websites.
Cisco Systems ¹⁰	Multiple	LEAP	A password disclosure vulnerability exists in LEAP (Lightweight Extensible Authentication Protocol), which could let a remote malicious user obtain authentication information.	The vendor has advised customers to use strong authentication and upgrade to PEAP (Protected Extensible Authentication Protocol). More information about PEAP can be found at: http://www.cisco.com/en/US/netsol/ns110/ns175/ns176/ns178/networking_solutions_package.html	Cisco LEAP Password Disclosure	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploits have been published. Vulnerability has appeared in the press and other public media.
Cisco Systems ¹¹	Multiple	PIX Firewall 6.2.2, 6.3 (3.102)	A remote Denial of Service vulnerability exists when global IP address pools are exposed to ICMP traffic.	Workaround: A workaround suggested by Cisco is to use a global PAT address.	Cisco PIX ICMP Echo Request Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Vulnerability may be exploited with one of numerous freely available tools.
Conectiva ¹²	Unix	Linux 7.0, 9.0	A Denial of Service vulnerability exists in the Vixie-Cron package when using 'cron.allow' and 'cron.deny' to access the 'crontab' application.	Upgrades available at: ftp://atualizacoes.conectiva.com.br/	Conectiva Vixie-Cron Package Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Conexant Systems, Inc. ¹³	Windows NT, XP	Access Runner DSL Console 3.21	A vulnerability exists in the authentication mechanism, which could let an unauthorized remote malicious user obtain administrative access.	No workaround or patch available at time of publishing.	AccessRunner Authentication Bypass	High	Bug discussed in newsgroups and websites. There is no exploit code required.

⁷ Mandrake Linux Security Update Advisory, MDKSA-2003:096, September 26, 2003.

⁸ Hewlett-Packard Company Security Bulletin, HPSBUX0310-285, October 7, 2003.

⁹ Debian Security Advisory, DSA 395-1, October 15, 2003.

¹⁰ Bugtraq, October 3, 2003.

¹¹ Cisco Security Notice, 44665 Revision 1.4, October 3, 2003.

¹² Conectiva Linux Security Announcement, CLA-2003:758, October 3, 2003.

¹³ SecurityTracker Alert, 1007883, October 5, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
DBMail ¹⁴	Unix	DBMail 1.0, 1.1	An input validation vulnerability exists because various parameters such as username and password aren't properly verified in the IMAP service, which could let a malicious user execute arbitrary code.	Upgrade available at: http://www.dbmail.org/tgz/dbmail-1.2.tgz	DBMail IMAP Input Validation	High	Bug discussed in newsgroups and websites.
DeskPro ¹⁵	Windows, Unix	DeskPro 1.1.0	A vulnerability exists due to insufficient validation of user-supplied input in a certain integer parameter, which could let a remote malicious user execute arbitrary code.	Update available at: http://www.deskpro.com/	DeskPro Remote Code Execution	High	Bug discussed in newsgroups and websites.
Divine ¹⁶	Windows	Divine Content Server 5.0	A Cross-Site Scripting vulnerability exists due to insufficient sanitation of input supplied to the 'pagename' parameter before it's included in an error page, which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	Divine Content Server Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Earth Station Five ¹⁷	Windows	ES5 2180, 1266	A vulnerability exists in the 'Search Service' packet handler, which could let a remote malicious user delete arbitrary files.	No workaround or patch available at time of publishing.	EarthStation 5 'Search Service' Remote File Deletion	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Eternal Mart ¹⁸	Windows, Unix	Guestbook 1.1 Mailing List Manager 1.32	A vulnerability exists in the 'admin/auth.php' and 'emml_email_func.php' scripts, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	EternalMart Multiple Remote File Include	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
File Sharing Software ¹⁹	Windows	Easy File Sharing Web Server 1.2	A vulnerability exists due to insecure default permissions on folders that contain the web server log and configuration files, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Easy File Sharing Web Server Information Disclosure	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Fortinet ²⁰	Multiple	FortiOS 2.5, 2.36	A Cross-Site Scripting vulnerability exists due to inadequate filtering of the log files, which could let a remote malicious user execute arbitrary HTML and script code.	Upgrades available at: http://support.fortinet.com/	FortiGate Firewall Remote Cross-Site Scripting	High	Bug discussed in newsgroups and websites. There is no exploit code required.

¹⁴ Secunia Advisory, SA10001, October 15, 2003.

¹⁵ SecurityTracker Alert, 1007890, October 7, 2003.

¹⁶ Secunia Advisory, SA9951, October 6, 2003.

¹⁷ Bugtraq, October 5, 2003.

¹⁸ Securiteam, October 9, 2003.

¹⁹ Bugtraq, October 4, 2003.

²⁰ Securiteam, October 9, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Francisco Burzi ²¹	Windows, Unix	PHP-Nuke 6.6	A vulnerability exists in the 'admin.php' file 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.	PHP-Nuke 'admin.php' SQL Injection	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Francisco Burzi ²²	Windows	PHP-Nuke 6.7	A vulnerability exists in the 'mailattach.php' script due to insufficient filtering of user-supplied input, which could let a remote malicious user execute arbitrary code	No workaround or patch available at time of publishing.	PHP-Nuke mailattach.php Code Execution	High	Bug discussed in newsgroups and websites.
FreeBSD ²³	Unix	FreeBSD 4.3-4.6, 4.6.2, 4.7, 4.8	A vulnerability exists in the 'readv(2)' system when a call to the 'fdrop()' function is missing, which could let a malicious user cause a Denial of Service or potentially obtain elevated privileges.	Patches available at: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-03:16/	FreeBSD Kernel Readv() Integer Overflow	Low/Medium (Medium if elevated privileges can be obtained)	Bug discussed in newsgroups and websites.
FreeBSD ²⁴	Unix	FreeBSD 5.1 & prior	Several vulnerabilities exist due to missing input validation of the 'UIO' offset parameter in the process file system (procfs) and Linux process file system (linprocfs), which could let a malicious user cause a Denial of Service or obtain sensitive information.	Patches available at: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-03:17/	FreeBSD Kernel ProcFS Handler UIO_Offset	Low/Medium (Medium if sensitive information can be obtained)	Bug discussed in newsgroups and websites.
Gallery Development Team ²⁵	Unix	Gallery 1.4, 1.4-pl1	A vulnerability exists in the 'index.php' script file due to a failure to verify the location in that it includes the 'util.php' script, which could let a remote malicious user execute arbitrary code.	Updates available at: http://sf.net/project/showfiles.php?group_id=7130&release_id=184028	Gallery index.php Remote Code Execution	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

²¹ Bugtraq, October 8, 2003.

²² SecurityTracker Alert, 1007886, October 5, 2003.

²³ FreeBSD Security Advisory, FreeBSD-SA-03:16, October 2, 2003.

²⁴ FreeBSD Security Advisory, FreeBSD-SA-03:17, October 3, 2003.

²⁵ Securiteam, October 13, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Geeklog ²⁶	Windows, Unix	Geeklog 1.3, 1.3.5, sr2&sr2, 1.3.7, sr2&sr2, 1.3.8, sr2&sr2, 1.3.8 -1	Multiple vulnerabilities exist: a vulnerability exists because the password hash is stored in cookies to verify if users are logged in, which could let a malicious user obtain sensitive information; a vulnerability exists because when a user changes a password the old password is not needed, which could let a malicious user add, modify or delete user information; and a vulnerability exists because most functions in the forum do filter out normal '<SCRIPT>' tags, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Multiple GeekLog Vulnerabilities	Medium/ High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Hewlett Packard Company ²⁷	Unix	HP-UX 11.0, 11.11, 11.22	A buffer overflow vulnerability exists in 'dtpriinfo' due to insufficient validation of user-supplied input in the DISPLAY environment variable, which could let a malicious user execute arbitrary code with root privileges.	Patches available at: http://itrc.hp.com PHSS_29367, PHSS_29371, PHSS_29373	CDE DTPriInfo Display Environment Variable Buffer Overflow	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Hewlett Packard Company ²⁸	Windows	Openview Operations for Windows 7.0-7.2, OpenView Vantage Point for Windows 6.1, 6.2 Japanese OpenView Vantage Point for Windows 6.1, 6.2	A vulnerability exists in OpenView Operations for Windows (OVOW), which could let a local administrative user bypass security restrictions to obtain remote administrative privileges.	Updates available at: http://support.openview.hp.com/patches/patch_index.jsp	OpenView Operations for Windows Security Restriction Bypass	Medium	Bug discussed in newsgroups and websites.

²⁶ Secunia Advisory, SA9966, October 8, 2003.

²⁷ Hewlett-Packard Company Security Bulletin, HPSBUX0310-289, October 8, 2003.

²⁸ Hewlett-Packard Company Security Bulletin, HPSBMI0310-005, October 9, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Hewlett Packard Company ²⁹	Unix	Tru64 4.0g, PK4 (BL22), PK3 (BL17), 4.0f, PK8 (BL22), PK7 (BL18), PK6 (BL17), 5.1b, 5.1 a, PK5 (BL23), PK4 (BL21), PK3 (BL3), PK2 (BL2), PK1 (BL1), 5.1, PK6 (BL20), PK5 (BL19), PK4 (BL18), PK3 (BL17)	A vulnerability exists in 'dtmailpr' which could let a remote malicious user obtain unauthorized access.	Patches available at: http://www.itrc.hp.com/service/patch/	Tru64 CDE 'dtmailpr' Unauthorized Access	Medium	Bug discussed in newsgroups and websites.
Hummingbird LTD. ³⁰	Windows NT	CyberDOCS 3.1, 3.5.1	An input validation vulnerability exists in 'loginact.asp,' which could let a malicious user execute arbitrary SQL code.	Update and patch available at: ftp://fptlh.hummingbird.com/patches/cyberdocs/cyd40p4.exe ftp://fptlh.hummingbird.com/releasenotes/cyberdocs/cyd40p4readme.html	CyberDOCS 'loginact.asp' Code Execution	High	Bug discussed in newsgroups and websites. There is no exploit code required.
Hummingbird LTD. ³¹	Windows NT	CyberDOCS 3.1, 3.9. 4.0	A vulnerability exists because anonymous users can read the source code of programs, potentially revealing code, which is used to generate authentication certificates.	No workaround or patch available at time of publishing.	CyberDOCS Authentication Certificates	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Hummingbird LTD. ³²	Windows NT	CyberDOCS 3.1, 3.9. 4.0	A path disclosure vulnerability exists due to insecure default permissions on several script source code files ('.inc'), which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	CyberDOCS Path Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

²⁹ Hewlett-Packard Company Software Security Response Team Advisory, SSRT3589, October 10, 2003.

³⁰ ProCheckUp Security Bulletin ,PR03-04, October 6, 2003.

³¹ ProCheckUp Security Bulletin ,PR03-02, October 6, 2003.

³² ProCheckUp Security Bulletin ,PR03-03, October 6, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Hummingbird LTD. ³³	Windows NT	CyberDOCS 3.1, 3.9. 4.08	Cross-Site Scripting vulnerabilities exist in 'quickstart.asp,' 'sub_frameset.asp,' 'logindsp.asp,' 'loginandgoact.asp,' and 'cyberdocs.asp' scripts, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	CyberDOCS Cross-Site Scripting	High	Bug discussed in newsgroups and websites. There is no exploit code required.
IBM ³⁴	Unix	AIX 4.3, 5.1	A vulnerability exists because specific memory management performance tools fail to carry out sufficient access controls, which could let a malicious user obtain elevated privileges.	Updates available at: http://techsupport.services.ibm.com/server/aix.fixdist?wh ichFix=APAR&fixes=IY36422 http://techsupport.services.ibm.com/server/aix.fixdist?wh ichFix=APAR&fixes=IY35542	IBM VMM Performance Tools	Medium	Bug discussed in newsgroups and websites.
IBM ³⁵	Unix	AIX 4.3.3, 5.1	A vulnerability exists in the 'xglinfo' program, which could let a malicious user cause program instability.	Update available at: http://www.ibm.com/support	IBM OpenGL XGLInfo Program	Low	Bug discussed in newsgroups and websites.
IBM ³⁶	Unix	AIX 5.1	A buffer overflow vulnerability exists due to a lack of sufficient bounds checking performed on user supplied '-r' parameters before the data is copied into an insufficient reserved buffer in memory, which could let a malicious user execute arbitrary code.	Update available at: http://techsupport.services.ibm.com/server/aix.fixdist?wh ichFix=APAR&fixes=IY24231	IBM AIX UUQ Buffer Overflow	High	Bug discussed in newsgroups and websites.
IBM ³⁷	Unix	AIX 5.1	A vulnerability exists in the 'dump_smutil.sh' utility due to insecure creation of temporary files, which could let a malicious user execute arbitrary code.	Update available at: http://techsupport.services.ibm.com/server/aix.fixdist?wh ichFix=APAR&fixes=IY33055	IBM dump_smutil.sh Insecure Temporary File Creation	High	Bug discussed in newsgroups and websites. This issue can be exploited through the creation of a malicious symbolic link.
IBM ³⁸	Unix	AIX 5.1	A buffer overflow vulnerability exists in the 'cu' implementation due to insufficient boundary checks, which could let a malicious user execute arbitrary code.	Update available at: http://www-1.ibm.com/support/docview.wss?rs=0&q=jy27270&uid=isg1IY27270&loc=en_US&cs=utf-8&cc=us□=en	IBM 'cu' Buffer Overflow	High	Bug discussed in newsgroups and websites.

³³ ProCheckUp Security Bulletin ,PR03-05, October 6, 2003.

³⁴ SecurityFocus, October 9, 2003.

³⁵ SecurityFocus, October 10, 2003.

³⁶ SecurityFocus, October 9, 2003.

³⁷ SecurityFocus, October 9, 2003.

³⁸ SecurityFocus, October 9, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
IBM ³⁹	Unix	AIX 5.1	Multiple buffer overflow vulnerabilities exist in the 'MUXATMD' program, which could let a malicious user execute arbitrary code.	Update available at: http://techsupport.services.ibm.com/server/aix.fixdist?wh ichFix=APAR&fixes=IY23847	Multiple AIX MUXATMD Buffer Overflows	High	Bug discussed in newsgroups and websites.
IBM ⁴⁰	Unix	AIX 5.1	A vulnerability exists in 'bellmai' due to an insecure chown operation performed on a temporary file, which could let a malicious user execute arbitrary code.	Update available at: http://techsupport.services.ibm.com/server/aix.fixdist?wh ichFix=APAR&fixes=IY25661	AIX Bellmail Race Condition	High	Bug discussed in newsgroups and websites.
IBM ⁴¹	Unix	AIX 5.1	A vulnerability exists in 'ibdiag,' which could let a malicious user corrupt critical systems files.	Update available at: http://techsupport.services.ibm.com/server/aix.fixdist?wh ichFix=APAR&fixes=IY2268	AIX 'libdiag' File Corruption	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
IBM ⁴²	Unix	AIX 5.1	A vulnerability exists in the 'policyd' and 'rsvpd' daemons due to insecure file creation, which could let a malicious user obtain elevated privileges.	Update available at: http://www-1.ibm.com/support/docview.wss?rs=0&q=iy29758&uid=isg1IY29758&loc=en_US&cs=utf-8&cc=us&en	AIX 'policyd' & 'rsvpd' Insecure Temporary File Creation	Medium	Bug discussed in newsgroups and websites.
Inter7 ⁴³	Unix	vpopmail (vchkw) 5.2.1	A vulnerability exists due to insecure permissions on the vpopmail configuration file '/etc/vpopmail.conf' when merged with USE="mysql," which could let a malicious user obtain sensitive information.	Update Gentoo or set proper permissions (640) on the configuration file. emerge sync emerge -u vpopmail -pv emerge -u vpopmail emerge clean	VPopMail Configuration File Insecure Default Permissions	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
IRCNet ⁴⁴	Unix	IRCNet IRCD 2.10, 2.10.3 p3	A buffer overflow vulnerability exists in the 'm_join' function due to a boundary error, which could let a malicious user cause a Denial of Service and possibly execute arbitrary code.	Upgrade available at: ftp://ftp.irc.org/irc/server/irc2.10.3p4.tgz	IRCnet IRCD Buffer Overflow CVE Name: CAN-2003-0864	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.

³⁹ SecurityFocus, October 9, 2003.

⁴⁰ SecurityFocus, October 9, 2003.

⁴¹ SecurityFocus, October 9, 2003.

⁴² SecurityFocus, October 10, 2003.

⁴³ Gentoo Linux Security Announcement, October 2, 2003.

⁴⁴ Bugtraq, October 12, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
JBoss Group ⁴⁵	Windows, Unix	JBoss 3.0.8, 3.2.1	A vulnerability exists in the SQL database 'HSQLDB' used for managing JMS connections due to a combination of various errors in some classes in JDK and insecure default settings, which could let a remote malicious user manipulate data, obtain sensitive information, cause a Denial of Service, or execute arbitrary commands.	Workaround available at: http://sourceforge.net/docman/display_doc.php?docid=19314&group_id=22866	JBoss HSQLDB Remote Command Injection	Low/ Medium/ High Low if a DoS, Medium is sensitive information can be obtained; and High if arbitrary code can be executed)	Bug discussed in newsgroups and websites.
Juan Cespedes ⁴⁶	Unix	LTrace 0.3.10	A buffer overflow vulnerability exists in the 'search_for_command()' function in the 'options.c' file, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	LTrace 'options.c' Buffer Overflow	High	Bug discussed in newsgroups and websites.
Kevin Lindsay ⁴⁷	Unix	SLocate 2.1-2.6	A buffer overflow vulnerability exists in 'main.c' because dynamically allocated memory is not properly freed, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	SLocate Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Khaled Mardam-Bey ⁴⁸	Windows	mIRC 6.1, 6.11	A buffer overflow vulnerability exists in 'DCC SEND' requests due to insufficient bounds checking, which could let a remote malicious user cause a Denial of Service.	No workaround or patch available at time of publishing.	mIRC 'DCC SEND' Buffer Overflow	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Laurent Duveau ⁴⁹	Windows, Unix	Guppy 2.4 p3	Several vulnerabilities exist: a Cross-Site Scripting vulnerability exists in the 'postguest' module due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML or script code; and a vulnerability exists in the 'tinymsg.php' component, which could let a remote malicious user obtain sensitive information.	Update and patch available at: http://www.freeguppy.org/file/guppy_patch.zip http://www.freeguppy.org/file/guppy.zip	Guppy Cross-Site Scripting & Information Disclosure	Medium/ High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Exploits have been published.

⁴⁵ Illegalaccess.org Security Alert, October 5, 2003.

⁴⁶ BFI Security Research Group Advisory, October 8, 2003.

⁴⁷ Security Advisory 20031006, October 6, 2003.

⁴⁸ Secunia Advisory, SA10000, October 13, 2003.

⁴⁹ SecurityFocus, October 5, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Linksys ⁵⁰	Multiple	BEFSX41 1.44.3	A remote Denial of Service vulnerability exists when a malicious user submits an invalid value for the 'Log_Page_Num' parameter.	Upgrade available at: ftp://ftp.linksys.com/pub/befsr41/befsx41_1453_fw.zip	Linksys BEFSX41 'Log_Page_Num' Remote Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Macro media ⁵¹	Multiple	ColdFusion MX 6.0	A Cross-Site Scripting vulnerability exists due to improper handling of error messages, which could let a malicious user execute arbitrary HTML or script code.	No workaround or patch available at time of publishing.	ColdFusion MX Error Message Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Microsoft ⁵²	Windows NT 4.0/2000	Exchange Server 5.5, SP1-SP4	A Cross-Site Scripting vulnerability exists due to the way that Outlook Web Access (OWA) performs HTML encoding in the Compose New Message form, 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/MS03-047.asp	Exchange Server 5.5 Outlook Web Access Cross-Site Scripting CVE Name: CAN-2003-0712	High	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Microsoft ⁵³	Windows 98/ME/NT 4.0/2000, 2003, XP	Internet Explorer 6.0, SP1, Outlook 2002, SP1&SP2; Qualcomm Eudora 6.0	A remote Denial of Service vulnerability exists when absolute positioning is used. It has been reported that the exploit code for this issue may also cause Eudora to crash.	No workaround or patch available at time of publishing.	Internet Explorer Absolute Position Block Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Microsoft ⁵⁴	Windows NT 4.0/2000	Exchange Server 5.5, SP1-SP4 Exchange 2000 Server, SP1-SP3	A buffer overflow vulnerability exists due to a failure to handle certain SMTP extended verbs correctly.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-046.asp	Exchange Server Buffer Overflow CVE Name: CAN-2003-0714	High	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.

⁵⁰ DigitalPranksters Security Advisory, October 15, 2003.

⁵¹ SecurityFocus, October 15, 2003.

⁵² Microsoft Security Bulletin, MS03-047, October 15, 2003.

⁵³ SecurityFocus, October 4, 2003.

⁵⁴ Microsoft Security Bulletin, MS03-046, October 15, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft ⁵⁵ <i>Microsoft issues bulletin</i> ⁵⁶ <i>Microsoft updates bulletin</i> ⁵⁷	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. <i>Microsoft updates Knowledge Base article link, install platforms information, and administrator logon information.</i>	<i>Frequently asked questions regarding this vulnerability and the patch can be found at:</i> http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-040.asp	Internet Explorer XML Page Object Type Validation CVE Name: CAN-2003-0809	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Microsoft ⁵⁸ <i>Microsoft issues bulletin</i> ⁵⁹	Windows 95/98/ME/NT 4.0/2000, XP, 2003, MacOS 7.x, 8.x, Unix	Internet Explorer 5.0, 5.0 for Windows 95, 5.0 for Windows 98, 5.0 for Windows NT 4.0, 5.0 for Windows 2000, 5.0.1, SP1-SP3, 5.0.1 for Windows 95, 5.0.1 for Windows 98, 5.0.1 for Windows NT 4.0, 5.0.1 for Windows 2000, 5.5, SP1-SP2, 5.5 preview, 6.0, SP1, Windows Media Player XP, 6.3, 6.4, 7.0, 7.1, 8.0, 9.0	A vulnerability exists because the Zone based access control model can be evaded due to a flaw that allows untrusted content to access the Local Zone, which could let a remote malicious user execute arbitrary code.	<i>Frequently asked questions regarding this vulnerability and the patch can be found at:</i> http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-040.asp	Media Player IE Zone Access Control Bypass	High	Bug discussed in newsgroups and websites. Exploit has been published.

⁵⁵ SecurityFocus, September 8, 2003.

⁵⁶ Microsoft Security Bulletin MS03-040, October 3, 2003.

⁵⁷ Microsoft Security Bulletin MS03-040 V1.1, October 6, 2003.

⁵⁸ SecurityTracker Alert ID, 1007287, July 24, 2003.

⁵⁹ Microsoft Security Bulletin, MS03-040, 1.1 October 6, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft ⁶⁰ <i>Microsoft issues bulletin</i> ⁶¹	Windows 95/98/ME/NT 4.0/2000, XP, 2003, MacOS 7.x, 8.x, Unix	Internet Explorer 5.0, 5.0 for Windows 95, 5.0 for Windows 98, 5.0 for Windows NT 4.0, 5.0 for Windows 2000, 5.0.1, SP1-SP3, 5.0.1 for Windows 95, 5.0.1 for Windows 98, 5.0.1 for Windows NT 4.0, 5.0.1 for Windows 2000, 5.5, SP1-SP2, 5.5 preview, 6.0, SP1, Windows Media Player XP, 6.3, 6.4, 7.0, 7.1, 8.0, 9.0	A vulnerability exists because the Zone based access control model can be evaded due to a flaw that allows untrusted content to access the Local Zone, which could let a remote malicious user execute arbitrary code.	<i>Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-040.asp</i>	Media Player IE Zone Access Control Bypass	High	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft ⁶² <i>Microsoft issues bulletin</i> ⁶³ <i>Microsoft updates bulletin</i> ⁶⁴	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. <i>Microsoft updates Knowledge Base article link, install platforms information, and administrator logon information.</i>	<i>Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-040.asp</i>	Internet Explorer Browser Popup Window CVE Name: CAN-2003-0838	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

⁶⁰ SecurityTracker Alert ID, 1007287, July 24, 2003.

⁶¹ Microsoft Security Bulletin, MS03-040, 1.1 October 6, 2003.

⁶² SecurityFocus, September 9, 2003.

⁶³ Microsoft Security Bulletin MS03-040, October 3, 2003.

⁶⁴ Microsoft Security Bulletin MS03-040 V1.1, October 6, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft ⁶⁵ <i>Microsoft issues bulletin</i> ⁶⁶ <i>Microsoft updates bulletin</i> ⁶⁷	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. <i>Microsoft updates Knowledge Base article link, install platforms information, and administrator logon information.</i>	<i>Frequently asked questions regarding this vulnerability and the patch can be found at:</i> http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-040.asp	Internet Explorer XML Page Object Type Validation CVE Name: CAN-2003-0809	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Microsoft ⁶⁸	Windows 2000, XP	Windows 2000 Advanced Server, SP1-SP4, 2000 Datacenter Server, SP1-SP4, 2000 Professional, SP1-SP4, 2000 Server, SP1-SP4, XP Home, SP1, XP Media Center Edition, XP Professional, SP1	A multi-threaded race condition vulnerability exists in the Windows RPC DCOM functionality with the MS03-039 patch installed when handling a large number of RPC requests, which could let a remote malicious user cause a Denial of Service. <i>Note: This vulnerability exists in the most current patch-levels of the Windows operating systems, including computers patched against the issues described in Microsoft Security Bulletin MS03-039.</i>	Due to the possibility of the existence of working exploit being distributed in the wild, users are advised to apply all available workarounds until the vendor can acknowledge and patch the issue. Workarounds available at: http://xforce.iss.net/xforce/alerts/id/155	Windows RPCSS Multi-thread Race Condition CVE Name: CAN-2003-0813	Low	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Microsoft ⁶⁹	Windows 2000	Windows 2000 Advanced Server, SP1-SP4, Datacenter Server, SP1-SP4, Professional, SP1-SP4, 2000 Server, SP1-SP4	A buffer overflow vulnerability exists in the TroubleShooter ActiveX control, 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/MS03-042.asp	Windows 2000 TroubleShooter ActiveX Control Buffer Overflow CVE Name: CAN-2003-0662	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published. Vulnerability has appeared in the press and other public media.

⁶⁵ SecurityFocus, September 8, 2003.

⁶⁶ Microsoft Security Bulletin MS03-040, October 3, 2003.

⁶⁷ Microsoft Security Bulletin MS03-040 V1.1, October 6, 2003.

⁶⁸ Internet Security Systems Security Advisory, October 14, 2003.

⁶⁹ Microsoft Security Bulletin, MS03-042, October 15, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft ⁷⁰	Windows NT 4.0/2000, 2003, XP	Windows 2000 Advanced Server, SP1-SP4, Datacenter Server, SP1-SP4, Professional, SP1-SP4, 2000 Server, SP1-SP4, Windows ME, NT Enterprise Server 4.0, SP1-SP6a, NT Terminal Server 4.0, SP1-SP6a, NT Workstation 4.0, SP1-SP6a, 2003 Datacenter Edition, 64-bit, 2003 Enterprise Edition, 64-bit, 2003 Standard Edition, 2003 Web Edition, XP 64-bit Edition, SP1, XP Home, SP1, XP Professional, SP1	A buffer overflow vulnerability exists because the length of messages is not verified, 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/MS03-043.asp	Messenger Service Buffer Overflow CVE Name: CAN-2003-0717	High	Bug discussed in newsgroups and websites. Exploit scripts have been published.

⁷⁰ Microsoft Security Bulletin, MS03-043, October 15, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft ⁷¹	Windows NT 4.0/2000, 2003, XP	Windows 2000 Advanced Server, SP1-SP4, Datacenter Server, SP1-SP4, Professional, SP1-SP4, 2000 Server, SP1-SP4, Windows ME, NT Enterprise Server 4.0, SP1-SP6a, NT Terminal Server 4.0, SP1-SP6a, NT Workstation 4.0, SP1-SP6a, 2003 Datacenter Edition, 64-bit, 2003 Enterprise Edition, 64-bit, 2003 Standard Edition, 2003 Web Edition, XP 64-bit Edition, SP1, XP Home, SP1, XP Professional, SP1	A buffer overflow vulnerability exists because the 'ListBox' and 'ComboBox' controls due to insufficient validation of user-supplied parameters, which could let a remote malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-045.asp	Windows ListBox & ComboBox Control Buffer Overflow CVE Name: CAN-2003-0659	High	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.

⁷¹ Microsoft Security Bulletin MS03-045, October 15, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft ⁷²	Windows NT 4.0/2000, 2003, XP	Windows 2000 Advanced Server, SP1-SP4, Datacenter Server, SP1-SP4, Professional, SP1-SP4, 2000 Server, SP1-SP4, Windows ME, NT Enterprise Server 4.0, SP1-SP6a, NT Terminal Server 4.0, SP1-SP6a, NT Workstation 4.0, SP1-SP6a, 2003 Datacenter Edition, 64-bit, 2003 Enterprise Edition, 64-bit, 2003 Standard Edition, 2003 Web Edition, XP 64-bit Edition, SP1, XP Home, SP1, XP Professional, SP1	A vulnerability exists in 'Authenticode' because under certain low memory conditions an ActiveX control can be downloaded and installed without presenting the user with an approval dialog, 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/MS03-041.asp	Microsoft ActiveX Authenticode Verification Bypass CVE Name: CAN-2003-0660	High	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Microsoft ⁷³	Windows 2003	Windows Server 2003	A Directory Traversal vulnerability exists because HTML can be created that references various 'shell folders' on the system, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Windows Server 2003 Directory Traversal	Medium	Bug discussed in newsgroups and websites.

⁷² Microsoft Security Bulletin, MS03-041, October 15, 2003.

⁷³ SecurityTracker Alert, 1007905, October 8, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft ⁷⁴	Windows NT 4.0/2000, XP, 2003	Windows 2000 Advanced Server, SP1-SP4, Datacenter Server, SP1-SP4, Professional, SP1-SP4, 2000 Server, SP1-SP4, Windows ME, NT Enterprise Server 4.0, SP1-SP6a, NT Terminal Server 4.0, SP1-SP6a, NT Workstation 4.0, SP1-SP6a, 2003 Datacenter Edition, 64-bit, 2003 Enterprise Edition, 64-bit, 2003 Standard Edition, 2003 Web Edition, XP 64-bit Edition, SP1, XP Home, SP1, XP Professional, SP1	A buffer overflow vulnerability exists in the URI Handler in the Help and Support Center (HSC) due to insufficient bounds checking when handling 'hpc://' URI links, 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/MS03-044.asp	Windows Help And Support Center URI Handler Remote Buffer Overflow CVE Name: CAN-2003-0711	High	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Microsoft ⁷⁵ <i>Microsoft issues bulletin</i> ⁷⁶	Windows 95/98/ME/ NT 4.0/2000	Windows Media Player 7.0, 7.1	A vulnerability exists when a specially crafted XML Name Space URI is embedded within an HTML e-mail message, which could let a malicious user execute arbitrary code.	<i>Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-040.asp</i>	Windows Media Player Automatic File Download and Execution	High	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.

⁷⁴ Microsoft Security Bulletin MS03-044, October 15, 2003.

⁷⁵ Bugtraq, May 21, 2003.

⁷⁶ Microsoft Security Bulletin, MS03-040, 1.1 October 6, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft ⁷⁷	Windows 95/98/ME/NT 4.0/2000, XP	Word 2000, SR1, SR1a, SP2&SP3, 2002, SP1&SP2, Word 97, SR1&SR2, Word 98, 98 Japanese Version	A remote Denial of Service vulnerability exists when a malicious user modifies the memory structure of a document. It may also be possibly to execute arbitrary code.	No workaround or patch available at time of publishing.	Word Malformed Document Remote Denial of Service	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Microsoft ⁷⁸	Windows 95/98/ME/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, XP 64-bit Edition, SP1, XP Embedded, SP1, XP Home, SP1, XP Media Center Edition, XP Professional, SP1, XP Tablet PC Edition	A Denial of Service vulnerability exists in the 'PostThreadMessage()' API because any program can send a 'WM_QUIT,' 'WM_CLOSE,' or 'WM_DESTROY' message to another program's thread on the same desktop.	No workaround or patch available at time of publishing.	Windows PostThread Message() Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.

⁷⁷ SecurityFocus, October 3, 2003.

⁷⁸ NTBugtraq, October 2, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft ⁷⁹	Windows 95/98/SE/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, Windows 95, SR2, 98, 98SE, 98 ME, 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, Windows Server 2003 Datacenter Edition, 64-bit, 2003 Enterprise Edition, 64-bit, 2003 Standard Edition, 2003 Web Edition, XP Home, SP1, XP Media Center Edition, XP Professional, SP1	A heap overflow vulnerability exists due to a boundary error in Microsoft Message Queuing Service ("mqsvc.exe") when handling search criteria in 'MQLocateBegin' packets, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Windows Message Queuing Service Heap Overflow	High	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.

⁷⁹ Secunia Advisory, SA9991, October 11, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft ⁸⁰ <i>More exploit scripts published</i> ⁸¹	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. <i>More exploit scripts have been published.</i>

⁸⁰ Microsoft Security Bulletin, MS03-039, September 10, 2003.

⁸¹ SecurityFocus, October 10, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft ⁸²	Windows 95/98/SE/NT 4.0, 2000	Word 200, SR1, SR1a, SP2&SP3, Word 2000 Chinese Version, Japanese Version, Korean Version, Word 97, SR1&SR2, Word 97 Chinese Version, Japanese Version, Korean Version, Word 98, Word 98 Chinese Version, Japanese Version, Korean Version	A buffer overflow vulnerability exists due to a boundary error when handling macro names, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code.	No workaround or patch available at time of publishing.	Word Macro Name Handler Remote Buffer Overflow	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites.
Mini HTTP Server ⁸³	Multiple	WebForum Server 1.5	A vulnerability exists due to missing input validation in the 'Subject' and 'Your Message' fields when posting new messages in the message forum, which could let a remote malicious user execute arbitrary HTML or script code.	No workaround or patch available at time of publishing.	WebForums Code Execution	High	Bug discussed in newsgroups and websites. Vulnerability may be exploited via a web browser.
MPlayer ⁸⁴ <i>Conectiva issues advisory</i> ⁸⁵	Unix	MPlayer 0.9 0rc4, 9.1, 0.90 rc series, 0.90 pre series, 0.90, 0.91, 9.2, 1.0 pre1	A buffer overflow vulnerability exists in 'asf_http_request() due to a boundary error when parsing ASX Headers, which could let a remote malicious user execute arbitrary code.	<u>Mandrake:</u> http://www.mandrakesecurity.net/en/mlist.php <u>Conectiva:</u> ftp://atualizacoes.conectiva.com.br/	MPlayer Remote Buffer Overflow CVE Name: CAN-2003-0835	High	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.

⁸² Secunia Advisory, SA10020, October 15, 2003.

⁸³ Bugtraq, October 6, 2003.

⁸⁴ Mandrake Linux Security Update Advisory, MDKSA-2003:097, September 30, 2003.

⁸⁵ Conectiva Linux Security Announcement, CLA-2003:760, October 6, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
<p>Multiple Vendors 86, 87, 88, 89, 90, 91, 92, 93</p> <p><i>More advisories issued^{84, 95}</i></p> <p><i>Hewlett Packard updates bulletin⁹⁶</i></p>	Unix	Sendmail 8.12.9 & prior	<p>A buffer overflow vulnerability exists when parsing non-standard rulesets, which could possibly let a remote malicious user execute arbitrary code.</p> <p><i>Bulletin revised because the previous 11.22 SendMail file failed to work properly. It has been replaced by sendmail.811.11.22.r5.</i></p>	<p>SendMail: ftp://ftp.sendmail.org/pub/sendmail/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Debian: http://security.debian.org/pool/updates/main/s/sendmail/ Immunix: http://download.immunix.org/ImmunixOS/7+/Updates/RPMS/ OpenPKG: ftp://ftp.openpkg.org/release/ RedHat: ftp://updates.redhat.com/ Slackware: ftp://ftp.slackware.com/pub/slackware/ TurboLinux: Ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ YellowDog: ftp://ftp.yellowdoglinux.com/pub/yellowdog/updates/yellowdog-3.0/</p> <p>Hewlett Packard: ftp://hprc.external.hp.com Sun: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F56922</p>	Sendmail Ruleset Parsing Buffer Overflow	High	Bug discussed in newsgroups and websites.

⁸⁶ Debian Security Advisory. DSA 384-1, September 17, 2003.

⁸⁷ Immunix Secured OS Security Advisory, IMNX-2003-7+-021-01, September 17, 2003.

⁸⁸ Yellow Dog Linux Security Announcement, YDU-20030917-2, September 17, 2003.

⁸⁹ Slackware Security Advisory, SSA:2003-260-02, September 17, 2003.

⁹⁰ Conectiva Linux Security Announcement, CLA-2003:742, September 18, 2003.

⁹¹ TurboLinux Security Advisor, TLSA-2003-52, September 18, 2003.

⁹² Red Hat Security Advisory, RHSA-2003:283-01, September 18, 2003.

⁹³ OpenPKG Security Advisory, OpenPKG-SA-2003.041, September 19, 2003.

⁹⁴ Hewlett-Packard Company Security Bulletin, HPSBUX0309-281, September 29, 2003.

⁹⁵ Sun(sm) Alert Notification, 56922, September 30, 2003.

⁹⁶ Hewlett-Packard Company Security Bulletin, HPSBUX0309-281, October 6, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
<p>Multiple Vendors 97, 98, 99, 100, 101, 102, 103, 104, 105, 106</p> <p><i>More advisories issued¹⁰⁷, 108, 109, 110</i></p> <p><i>NetBSD issues advisory 111</i></p> <p><i>Hewlett Packard updates advisory 112</i></p>	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	<p>A buffer overflow vulnerability exists in the 'prescan()' function, which could let local/remote malicious user execute arbitrary code.</p> <p><i>Hewlett Packard bulletin revised because the previous 11.22 SendMail file failed to work properly. It has been replaced by sendmail.811.11.22.r5.</i></p>	<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>FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/S-A-03:13/sendmail.patch</p> <p>Immunix: http://download.immunix.org/ImmunixOS/7+/Updates/RPMS/</p> <p>OpenPKG: ftp://ftp.openpkg.org/</p> <p>RedHat: ftp://updates.redhat.com</p> <p>Slackware: Ftp://ftp.slackware.com/pub/slackware/slackware-9.0/patches/packages/</p> <p>SuSE: ftp://ftp.suse.com/pub/suse</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> <p>Hewlett Packard: Ftp://hprc.external.hp.com</p> <p>IBM: ftp://aix.software.ibm.com/aix/efixes/security/sendmail_4_efix.tar.Z</p> <p>SGL: ftp://patches.sgi.com/support/free/security/advisories/20030903-01-P.asc</p> <p>Sun: http://sunsolve.sun.com/pub/cgi/</p> <p>NetBSD: ftp://ftp.NetBSD.org/pub/NetBSD/security/advisories/NetBSD-SA2003-016.txt.asc</p>	Sendmail Prescan() Buffer Overflow	High	Bug discussed in newsgroups and websites.

⁹⁷ Debian Security Advisory, DSA 384-1, September 17, 2003.

⁹⁸ FreeBSD Security Advisory, FreeBSD-SA-03:13, September 17, 2003.

⁹⁹ Slackware Security Advisory, SSA:2003-260-02, September 17, 2003.

¹⁰⁰ Yellow Dog Linux Security Announcement, YDU-20030917-2, September 17, 2003.

¹⁰¹ Conectiva Linux Security Announcement, CLA-2003:742, September 18, 2003.

¹⁰² Immunix Secured OS Security Advisory, IMNX-2003-7+-021-01, September 18, 2003.

¹⁰³ Red Hat Security Advisory RHSA-2003:283-01, September 18, 2003.

¹⁰⁴ TurboLinux Security Advisory, TLSA-2003-52, September 18, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors ^{113, 114}	Unix	OpenSSL Project OpenSSL 0.9.6-0.9.6e; EnGarde Secure Community 1.0.1, Secure Professional 1.1, 1.2; Red Hat Linux 7.1, 7.1 for iSeries, 7.1 for pSeries, 7.2, 7.3, 8.0	A remote Denial of Service vulnerability exists when processing a specially crafted malicious CLIENT_MASTER_KEY message.	OpenSSL Project: http://www.openssl.org/source/ EnGarde: http://www.linuxsecurity.com/advisories/engarde_advisory-3709.html RedHat: ftp://updates.redhat.com/	OpenSSL SSLv2 Client_Master_Key Remote Denial of Service	Low	Bug discussed in newsgroups and websites.
MyPHP Calendar ¹¹⁵	Windows, Unix	MyPHP Calendar 10192k Build 1 Beta	Vulnerabilities exists in the 'admin.php,' 'contacts.php,' and 'convert-date.php' files due to insufficient sanitization of user-supplied values, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Multiple MyPHP Calendar File Include Vulnerabilities	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

¹⁰⁵ OpenPKG Security Advisory, OpenPKG-SA-2003.041, September 19, 2003.

¹⁰⁶ SuSE Security Announcement, SuSE-SA:2003:040, September 20, 2003.

¹⁰⁷ SGI Security Advisory, 20030903-01-P, September 29, 2003.

¹⁰⁸ Hewlett-Packard Company Security Bulletin, HPSBUX0309-281, September 29, 2003.

¹⁰⁹ IBM, MSS-OAR-E01-2003:1235.1, September 28, 2003.

¹¹⁰ Sun(sm) Alert Notification, 56860 & 56922, September 30, 2003.

¹¹¹ NetBSD Security Advisory, 2003-016, October 6, 2003.

¹¹² Hewlett-Packard Company Security Bulletin, HPSBUX0309-281, October 6, 2003.

¹¹³ RedHat Security Advisory, RHSA-2003:291-11, September 30, 2003.

¹¹⁴ Guardian Digital Security Advisory, ESA-20031003-028, October 3, 2003.

¹¹⁵ Securiteam, October 13, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
MySQL AB ^{116, 117, 118} <i>More advisories issued</i> ^{119, 120, 121, 122} <i>More advisories issued</i> ^{123, 124, 125}	Unix	MySQL 3.23.x, 3.23.2- 3.23.5, 3.23.8- 3.23.10, 3.23.22- 3.23.34, 3.23.36- 3.23.56, 4.0.0- 4.0.14, 4.1.0- alpha, 4.1. .0-0	A buffer overflow vulnerability exists when handling user passwords of excessive size due to insufficient bounds checking, which could let a malicious user execute arbitrary code.	Patch available at: http://www.mysql.com/downloads/mysql-4.0.html Debian: http://security.debian.org/pool/updates/main/m/mysql/ OpenPKG: Ftp://ftp.openpkg.org/release/ Trustix: http://www.trustix.net/pub/Trustix/updates/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Engarde: http://www.linuxsecurity.com/advisories/engarde_advisory-3650.html Mandrake: http://www.mandrakesecure.net/en/ftp.php SuSE: ftp://ftp.suse.com/pub/suse RedHat: Ftp://updates.redhat.com/ TurboLinux: ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/	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.

¹¹⁶ Debian Security Advisory, DSA 381-1, September 14, 2003.

¹¹⁷ OpenPKG Security Advisory, OpenPKG-SA-2003.038, September 15, 2003.

¹¹⁸ Trustix Secure Linux Security Advisory, TSLSA-2003-09-17, September 17, 2003.

¹¹⁹ Conectiva Linux Security Announcement, CLA-2003:743, September 18, 2003.

¹²⁰ Guardian Digital Security Advisory, ESA-20030918-025, September 18, 2003.

¹²¹ Mandrake Linux Security Update Advisory, MDKSA-2003:094, September 18, 2003.

¹²² SuSE Security Announcement, SuSE-SA:2003:042, October 1, 2003

¹²³ TurboLinux Security Advisory, TLSA-2003-56, October 7, 2003.

¹²⁴ Red Hat Security Advisory, RHSA-2003:281-01, October 9, 2003.

¹²⁵ Conectiva Linux Security Announcement, CLSA-2003:764, October 16, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
NetScreen ¹²⁶	Multiple	ScreenOS 3.1.1r2, 3.1.0r9, 3.1.0r2, 3.1.0r1, 3.1.0, 3.0.0r1- 3.0.0r4, 3.0.0, 2.6, 2.6.1 r5, 2.6.1 r1- 2.6.1 r4, 2.6.1, 3.0.1r2&r2, 3.0.1, 3.0.2, 3.0.3 r1.1, 3.0.3, 4.0 – DIAL, 4.0, 4.0.1	A vulnerability exists because a buffer used for holding the contents of the last HTTP management session is being re-used for generating DHCP Offer messages without being cleared first, which could let a malicious user obtain sensitive information.	Patches will be available at: http://www.netscreen.com/cso	ScreenOS DHCP Packet Buffer Padding Information Leakage	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited by transmitting DHCP requests to a target appliance and recording the data stored within the responses.
Nicolas Boullis ¹²⁷ <i>Exploit script published</i> ¹²⁸	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.	<u>Debian:</u> 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. <i>Exploit script has been published.</i>
Open Office ¹²⁹	Unix	OpenOffice 1.0.1	A remote Denial of Service vulnerability exists because the UNO (Universal Network Objects) service can't handle malformed input.	No workaround or patch available at time of publishing.	OpenOffice Remote Access Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Open Text Corporation ¹³⁰	Windows NT, Unix	Centrinity FirstClass 5.50, 5.77, 7.0, 7.1	A remote Denial of Service vulnerability exists due to a boundary error in 'fcintsv.exe' when handling HTTP requests.	Upgrades available at: http://www.firstclass.com/Downloads/Server/Windows%20Download%20Page	FirstClass Remote Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit script has been published.

¹²⁶ NetScreen Advisory, 57983, October 2, 2003.

¹²⁷ Debian Security Advisory, DSA 378-1, September 7, 2003.

¹²⁸ SecurityFocus, October 16, 2003.

¹²⁹ Illegalaccess.org Security Alert, October 8, 2003.

¹³⁰ SecurityTracker Alert, 1007899, October 8, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
OpenBSD ¹³¹	Unix	OpenBSD 3.2, 3.3	A remote Denial of Service vulnerability exists when active scrub rules are in use.	Patches available at: ftp://ftp.openbsd.org/pub/OpenBSD/patches/	OpenBSD Active Scrub Remote Denial of Service	Low	Bug discussed in newsgroups and websites.
OpenSSH ^{132, 133, 134, 135} <i>More vendors issue advisories^{136, 137}</i>	Unix	OpenSSH 3.7 p1, 3.7.1 p1	Multiple vulnerabilities exist in the Portable OpenSSH PAM support implementation: a vulnerability exists when Privilege Separation is disabled due to insufficient authentication checking, which could let a remote malicious user obtain root access; and a vulnerability exists because an array of structures is interpreted as an array of pointers, which could let a remote malicious user obtain elevated privileges.	Upgrade available at: http://www.openssh.org/portable.html <u>OpenPKG:</u> ftp://ftp.openpkg.org <u>Slackware:</u> ftp://ftp.slackware.com/pub/slackware <u>TurboLinux:</u> ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/ <u>Sun Microsystems:</u> http://sunsolve.sun.com/pub/cgi/retrieve.pl?doc=fsalert%2F56862 <u>FreeBSD:</u> ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/S-A-03:15/ <u>SCO:</u> ftp://ftp.sco.com/pub/updates/OpenServer	Multiple Portable OpenSSH PAM Vulnerabilities CVE Names: CAN-2003-0786, CAN-2003-0787	Medium/High (High if root access can be obtained)	Bug discussed in newsgroups and websites.
PeopleSoft ¹³⁸	Unix	PeopleTools 8.4, 8.10- 8.19, 8.40-8.42	Several vulnerabilities exist: an information disclosure vulnerability exists in the <Control><J> hot key, which could let a malicious user obtain sensitive information; a Denial of Service vulnerability exists in the 'LONGCHAR' and 'VARCHAR' field when a malicious user uploads large amounts of data; and a vulnerability exists due to missing user authentication when accessing temporary search files on a web server when using the 'grid' option, which could let a malicious user obtain sensitive information.	The vendor has issued a script available at: (see Solution ID: 200749183). http://www.peoplesoft.com	PeopleTools Multiple Vulnerabilities	Low/Medium (Medium if sensitive information can be obtained)	Bug discussed in newsgroups and websites. Vulnerability may be exploited via a web browser.

¹³¹ SecurityFocus, October 7, 2003.

¹³² OpenPKG Security Advisory, OpenPKG-SA-2003.042, September 24, 2003.

¹³³ Slackware Security Advisory, SSA:2003-266-01, September 24, 2003.

¹³⁴ TurboLinux Security Advisory, TLSA-2003-53, September 24, 2003.

¹³⁵ Sun(sm) Alert Notification, 56862, September 24, 2003.

¹³⁶ SCO Security Advisories, CSSA-2003-SCO.24 & CSSA-2003-027.0., October 2, 2003.

¹³⁷ FreeBSD Security Advisory, FreeBSD-SA-03:15, October 6, 2003.

¹³⁸ Securiteam, October 8, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
PHP Prayer Board ¹³⁹	Windows, Unix	PHP Prayer Board 0.51	Vulnerabilities exist due to missing input validation in 'prayerboard.php' and 'prayerboard_db.php,' which could let a malicious user execute arbitrary HRML or script code.	Update available at: http://prdownloads.sourceforge.net/phpprayerboard/phpprayerboard-0.52.tar.bz2?download	PHP Prayer Board Code Execution	High	Bug discussed in newsgroups and websites. Vulnerability may be exploited via a web browser.
PLANET Technology Corp. ¹⁴⁰	Multiple	WGSD-1020	A vulnerability exists because an undocumented administrative account exists and the username and password are visible in the configuration file, which could let an unauthorized remote malicious user obtain administrative access.	No workaround or patch available at time of publishing.	WGSD-1020 Switch Unauthorized Remote Administrative Access	High	Bug discussed in newsgroups and websites. There is no exploit code required.
ProFTPD Project ^{141, 142, 143, 144, 145, 146, 147} <i>Exploit scripts published</i> ¹⁴⁸	Unix	ProFTPD 1.2.7, rc1-rc3, 1.2.8, rc1&rc2, 1.2.9 rc1&rc2	A buffer overflow vulnerability exists due to the way incoming ACSII transfer files are handled, which could let a remote malicious user execute arbitrary code.	Upgrade available at: ftp: ftp://ftp.proftpd.org/Conectiva: ftp://atualizacoes.conectiva.com.br/9/ Mandrake: http://www.mandrakesecurity.net/en/advisories/ OpenPKG: ftp://ftp.openpkg.org/release TurboLinux: ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/ Trustix: http://www.trustix.net/pub/Trustix/updates/ Slackware: http://www.slackware.org/security/viewer.php?l=slackware-security&y=2003&m=slackware-security.392320	ProFTPD ASCII File Transfer Remote Buffer Overflow CVE Name: CAN-2003-0831	High	Bug discussed in newsgroups and websites. <i>Exploit scripts have been published.</i>

¹³⁹ Secunia Advisory, SA9939, October 6, 2003.

¹⁴⁰ SECURITY.NNOV, October 14, 2003.

¹⁴¹ Internet Security Systems Security Advisory, September 23, 2003.

¹⁴² Slackware Security Advisory, SSA:2003-259-02, September 23, 2003.

¹⁴³ Conectiva Linux Security Announcement, CLA-2003:750, September 29, 2003.

¹⁴⁴ Mandrake Linux Security Update Advisory, MDKSA-2003:095, September 29, 2003.

¹⁴⁵ OpenPKG Security Advisory, OpenPKG-SA-2003.043, September 29, 2003.

¹⁴⁶ Trustix Secure Linux Security Advisory, TSLSA-2003-0037, September 29, 2003.

¹⁴⁷ TurboLinux Security Advisory, TLSA-2003-54, September 30, 2003.

¹⁴⁸ SecurityFocus, October 14, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Real Networks ¹⁴⁹	Windows 95/98/ME/NT 4.0/2000, XP, Unix	RealOne Desktop Manager, Enterprise Desktop 6.0.11.774, RealOne Player 6.0.11.853, 6.0.11.841, 6.0.11.830, 6.0.11.818, 2.0, RealOne Player Gold for Windows 6.0.10 .505	A vulnerability exists due to the way temporary files are handled, which could let an unauthorized remote malicious user execute arbitrary code.	Patches available at: http://service.real.com/help/faq/security/securityupdate_october2003.html	RealOne Player Insecure Temporary File Handling	High	Bug discussed in newsgroups and websites.
Real Networks ¹⁵⁰ <i>Exploit has been published</i> ¹⁵¹	Windows 95/98/ME/NT 4.0/2000, XP, Unix	RealOne Desktop Manager, RealOne Enterprise Desktop 6.0.11.774, RealOne Player 6.0.11.853, 6.0.11.841, 6.0.11.830, 6.0.11.818, 2.0, RealOne Player Gold for Windows 6.0.10 .505	A vulnerability exists due to an unspecified error in the handling of SMIL files, which could let a remote malicious user execute arbitrary code.	Updates available at: http://www.service.real.com/help/faq/security/securityupdate_august2003.html	RealOne Player SMIL File Script Execution	High	Bug discussed in newsgroups and websites. <i>Exploit has been published.</i>
RedHat ¹⁵² <i>Conectiva issues advisory</i> ¹⁵³	Unix	Enterprise Linux WS 2.1 IA64, 2.1, ES 2.1 IA64, 2.1, AS 2.1 IA64, 2.1	A buffer overflow vulnerability exists in the 'getgrouplist' function if the size of the group list is too small to hold all the user's groups, which could let a malicious user cause a Denial of Service.	Patches available at: http://rhn.redhat.com/errata/RHSA-2003-249.html <i>Conectiva:</i> ftp://atualizacoes.conectiva.com.br/	Glibc Getgrouplist Function Buffer Overflow CVE Name: CAN-2003-0689	Low	Bug discussed in newsgroups and websites.
Rit Research Labs ¹⁵⁴	Windows	TinyWeb 1.9	A remote Denial of Service vulnerability exists when a malicious user submits a /cgi-bin/.%00./dddd.html HTTP GET request.	No workaround or patch available at time of publishing.	TinyWeb Server Remote Denial of Service	Low	Bug discussed in newsgroups and websites.

¹⁴⁹ SecurityFocus, October 15, 2003.

¹⁵⁰ RealNetworks Security Advisory, August 19, 2003.

¹⁵¹ SecurityFocus, October 15, 2003.

¹⁵² RedHat Security Advisory, RHSA-2003:249-11, August 22, 2003.

¹⁵³ Conectiva Linux Security Announcement, CLA-2003:762, October 14, 2003.

¹⁵⁴ Securiteam, October 9, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
SANE ¹⁵⁵ <i>More advisories issued^{156, 157}</i>	Unix	SANE 1.0.0-1.0.9, sane-backend 1.0.10	Multiple vulnerabilities exist: a vulnerability exists because the identity (IP address) of the remote host is not checked during the SANE_NET_INIT RPC call, which could let a remote malicious user obtain unauthorized access; a vulnerability exists because connection drops are not handled properly, which could let a remote malicious user obtain sensitive information and cause a Denial of Service; a vulnerability exists when a connection is dropped before the size value of malloc is set, which could let a remote malicious user cause a Denial of Service; a vulnerability exists because the validity of RPC numbers it gets before getting the parameters; a vulnerability exists when debug messages are enabled dropped connections are not properly handled, which could let a remote malicious user cause a Denial of Service; and a vulnerability exists because memory is not properly allocated in some cases, which could let a remote malicious user cause a Denial of Service.	<u>Debian:</u> http://security.debian.org/pool/updates/main/s/sane-backends/ <u>Mandrake:</u> http://www.mandrakesecurity.net/en/ftp.php <u>RedHat:</u> ftp://updates.redhat.com/	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.
SNAP Innovation ¹⁵⁸	Unix	PrimeBase SQL Database Server 4.2	Two vulnerabilities exist: a vulnerability exists in the installation process because the '/tmp/PrimeBase.log' file is created insecurely, which could let a malicious user overwrite or corrupt sensitive files; and a vulnerability exists because the '/usr/local/primebase' folder is created with insecure permissions, which could let a malicious user obtain elevated privileges.	No workaround or patch available at time of publishing.	PrimeBase SQL Database Server Insecure Installation & Permissions	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

¹⁵⁵ Debian Security Advisory DSA 379-1, September 11, 2003.

¹⁵⁶ Red Hat Security Advisories, RHSA-2003:278-01 & RHSA-2003:285-03, October 7, 2003.

¹⁵⁷ Mandrake Linux Security Update Advisory, MDKSA-2003:099, October 10, 2003.

¹⁵⁸ Secunia Advisory, SA9964, October 7, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Snert. Com ¹⁵⁹	Multiple	mod_throttle 3.0	A vulnerability exists due to the incorrect storage of critical data within shared memory, which could let a malicious user obtain elevated privileges.	No workaround or patch available at time of publishing.	Apache Mod_Throttle Module Shared Memory	Medium	Bug discussed in newsgroups and websites.
Software 602 ¹⁶⁰ <i>Upgrade now available</i> ¹⁶¹	Windows 98/ME/NT 4.0/2000, XP	602Pro LAN SUITE 2002, 2003	Several vulnerabilities exist which could let an unauthorized remote malicious user obtain elevated privileges and access.	<i>Upgrade available at:</i> http://www.software602.com/download/	602Pro LAN SUITE 2003 Multiple Remote Vulnerabilities	Medium	Bug discussed in newsgroups and websites.
Squirrel Mail ¹⁶²	Multiple	Squirrel Mail 1.4	A vulnerability exists due to insufficient filtering of script code, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	SquirrelMail CSS JavaScript Expression MSIE Script Code Injection	High	Bug discussed in newsgroups and websites. There is no exploit code required.
Sun Micro-systems, Inc. ¹⁶³	Unix	2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86, 9.0	A vulnerability exists in the 'sysinfo(2)' system, which could let a malicious user obtain sensitive information.	Patches available at: http://sunsolve.sun.com	Solaris SysInfo System Call Kernel Memory Reading	Medium	Bug discussed in newsgroups and websites.
Sun Micro-systems, Inc. ¹⁶⁴	Unix	2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86, 9.0, 9.0_x86	A Denial of Service vulnerability exists in the pipe function and 'STREAMS' routine.	Patches available at: http://sunsolve.sun.com	Solaris Pipe Function Denial of Service	Low	Bug discussed in newsgroups and websites.
Sun Micro-systems, Inc. ¹⁶⁵	Unix	Cobalt RaQ 1.1, 2.0, 3.0, 4.0	A Cross-Site Scripting vulnerability exists in the 'message.cgi' script due to improper validation of user-supplied input in the 'info' parameter, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Cobalt RaQ 'Message.CGI' Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
SuSE ¹⁶⁶	Unix	Linux Professiona 1 7.3	A vulnerability exists in the JavaRunt configuration file used by SuSEConfig, which could let a malicious user obtain elevated privileges.	No workaround or patch available at time of publishing.	SuSE Linux JavaRunt Configuration File	Medium	Bug discussed in newsgroups and websites.

¹⁵⁹ SecurityFocus, October 14, 2003.

¹⁶⁰ Bugtraq, September 25, 2003.

¹⁶¹ SecurityFocus, October 10, 2003.

¹⁶² Bugtraq, October 3, 2003.

¹⁶³ Sun Advisory, 57340, October 15, 2003.

¹⁶⁴ Sun Advisory, 57080, October 15, 2003.

¹⁶⁵ SecurityTracker Alert, 1007876, October 3, 2003.

¹⁶⁶ Bugtraq, October 6, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
SuSE ¹⁶⁷	Unix	Linux Professional 1 8.2	A vulnerability exists in the SuSEWM configuration file used by SuSEConfig, which could let a malicious user obtain elevated privileges.	No workaround or patch available at time of publishing.	SuSE Linux SuSEWM Configuration File	Medium	Bug discussed in newsgroups and websites.
The Creative Assembly Limited ¹⁶⁸	Windows	Medieval: Total War 1.0, 1.1	Two vulnerabilities exist: a remote Denial of Service vulnerability exists when a malicious user submits a malformed nickname value consisting of 0 Unicode characters during the initial authentication process; and a remote Denial of Service vulnerability exists when a malicious user submits a nickname that is longer than 76 unicode characters during the 'Lobby' screen.	No workaround or patch available at time of publishing.	Medieval Total War Remote Denial of Service Vulnerabilities	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
University of Washington ^{169, 170, 171, 172, 173} <i>Turbo Linux issues advisory</i> ¹⁷⁴	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 TurboLinux: ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/	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.
WordPress ¹⁷⁵	Unix	WordPress 0.7, 0.71, WordPress (B2) 0.6.2.1, 0.6.2	Multiple vulnerabilities exist in the 'blog.header.php' script due to insufficient sanitization on the 'cat' and 'order_by' URI parameters, which could let a malicious user execute arbitrary SQL code.	Patch available at: http://cvs.sourceforge.net/viewcvs.py/cafelog/wordpress/blog.header.php.diff?r1=text&tr1=1.18&r2=text&tr2=1.21&diff_format=u	WordPress Multiple Blog.Header. PHP SQL Injection	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

¹⁶⁷ Bugtraq, October 6, 2003.

¹⁶⁸ Securiteam, October 8, 2003.

¹⁶⁹ Slackware Security Advisory, SSA:2003-253-01, September 10, 2003.

¹⁷⁰ SuSE Security Announcement, SuSE-SA:2003:037, September 10, 2003.

¹⁷¹ Guardian Digital Security Advisory, ESA-20030911-022, September 11, 2003

¹⁷² Red Hat Security Advisory, RHSA-2003:273-01, September 11, 2003.

¹⁷³ Conectiva Linux Security Announcement, CLA-2003:738, September 12, 2003.

¹⁷⁴ TurboLinux Security Advisory, TLSA-2003-57, October 8, 2003.

¹⁷⁵ Securiteam, October 9, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
WREN SOFT ¹⁷⁶	Windows	Zoom Search Engine 2.0 Build: 1018	A Cross-Site Scripting vulnerability exists due to improper verification of search queries, which could let a remote malicious user execute arbitrary HTML or script code.	Upgrade available at: http://www.wrensoft.com/ftp/zoomsearch.exe	Zoom Search Engine Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
XShisen ¹⁷⁷	Windows, Unix	XShisen 1.5.1	Two vulnerabilities exist: a buffer overflow vulnerability exists when handling the 'XSHISENLIB' environment variable due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code; and a buffer overflow vulnerability exists in the '-KCONV' command line parameter due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	XShisen -KCONV & XSHISENLIB Buffer Overflows	High	Bug discussed in newsgroups and websites.

*"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 October 2 and October 15, 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, 40 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.*

¹⁷⁶ Secunia Advisory, SA10002, October 15, 2003.

¹⁷⁷ Secunia Advisory, SA9950, October 6, 2003.

Date of Script (Reverse Chronological Order)	Script name	Script Description
October 15, 2003	dosmj.pl	Perl script that exploits the Mah-Jong Server Remote Denial of Service vulnerability.
October 15, 2003	gaimexploit.txt	Notes on how to exploit GAIM via the festival plugin.
October 15, 2003	ms03-043.c	Exploit for the Messenger Service Buffer Overflow vulnerability.
October 15, 2003	MS03-043_poc.c	Exploit for the Messenger Service Buffer Overflow vulnerability.
October 15, 2003	nessus-installer.sh	A free, up-to-date, and full featured remote vulnerability scanner for Linux, BSD, Solaris and other systems that is multithreaded, plugin-based, has a nice GTK interface, and currently performs over a thousand remote security checks.
October 14, 2003	10.04.proftpd_xforce.c	Script that exploits the ProFTPD ASCII File Transfer Remote Buffer Overflow vulnerability.
October 14, 2003	10.14.pfpoc.c	Script that exploits the ProFTPD ASCII File Transfer Remote Buffer Overflow vulnerability.
October 14, 2003	MS-DCOM-Uni.asm	Script that exploits the Windows RPCSS Multi-thread Race Condition vulnerability.
October 14, 2003	MS-DCOM-Uni.c	Script that exploits the Windows RPCSS Multi-thread Race Condition vulnerability.
October 14, 2003	proft_put_down.c	Script that exploits the ProFTPD ASCII File Transfer Remote Buffer Overflow vulnerability.
October 14, 2003	rpc3.zip	Script that exploits the Windows RPCSS Multi-thread Race Condition vulnerability.
October 14, 2003	winsyslog-DoS.pl	Perl script that exploits the WinSyslog Long Syslog Message Remote Denial of Service vulnerability.
October 13, 2003	proftpd00t.c	Remote root exploit for the ProFTPD ASCII File Transfer Remote Buffer Overflow vulnerability.
October 13, 2003	SFPDisable.zip	A utility that disable Microsoft Windows' File Protection by patching sfc.dll under Windows 2000 and sfc_os.dll in Windows XP. This allows a remote malicious user to delete, manipulate, and backdoor any file on the system without Windows noticing upon reboot.
October 13, 2003	venom-win32-1_1_5.zip	A tool to run dictionary password attacks against Windows accounts by using the Windows Management Instrumentation (WMI) service.
October 12, 2003	mauer.c	Exploit for the IRCnet IRCD Buffer Overflow vulnerability.
October 11, 2003	allchin.cpp	Script that exploits the Windows Message Queuing Service Heap Overflow vulnerability.
October 8, 2003	fcex.c	Script that exploits the FirstClass Remote Denial of Service vulnerability.
October 8, 2003	mtwdos-server.zip	Exploit for the Medieval Total War Remote Denial of Service Vulnerabilities.
October 7, 2003	IE6XMLbypass.txt	Exploit for the Internet Explorer 6 XML bypass vulnerability.
October 7, 2003	wmpphp.txt	Exploit that swaps the Windows Media Player with a message from Mindlock by making use of the Internet Explorer 6 XML bypass vulnerability.
October 6, 2003	slocate-heap-ex.c	Exploit for the SLocate Buffer Overflow vulnerably.
October 5, 2003	ES5.cpp	Exploit for the EarthStation 5 'Search Service' Remote File Deletion vulnerability.
October 3, 2003	chaptest.c	Script that exploits the Cisco LEAP Password Disclosure vulnerability.
October 3, 2003	ciscoLEAP.txt	A document that describes the shortcomings of Cisco's LEAP authentication used on their wireless access points and how to score root on them.
October 3, 2003	clean.sh	Script that exploits the Cisco LEAP Password Disclosure vulnerability.

Date of Script (Reverse Chronological Order)	Script name	Script Description
October 3, 2003	compile.sh	Script that exploits the Cisco LEAP Password Disclosure vulnerability.
October 3, 2003	des.h	Script that exploits the Cisco LEAP Password Disclosure vulnerability.
October 3, 2003	deskey.c	Script that exploits the Cisco LEAP Password Disclosure vulnerability.
October 3, 2003	desport.c	Script that exploits the Cisco LEAP Password Disclosure vulnerability.
October 3, 2003	leap.tgz	Exploit that brute forces Microsoft's Active Directory authentication used in conjunction with the Cisco LEAP authentication on Cisco wireless access points.
October 3, 2003	md4.c	Script that exploits the Cisco LEAP Password Disclosure vulnerability.
October 3, 2003	md4.h	Script that exploits the Cisco LEAP Password Disclosure vulnerability.
October 3, 2003	mschap.c	Script that exploits the Cisco LEAP Password Disclosure vulnerability.
October 3, 2003	mschap.h	Script that exploits the Cisco LEAP Password Disclosure vulnerability.
October 2, 2003	AppShutdown.c	Script that exploits the Windows PostThread Message() Denial of Service vulnerability.
October 2, 2003	gspoof-3.1.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.
October 2, 2003	login-back.c	Backdoor for login where the original binary must be renamed and only gets called whenever the remote user's TERM variable is not set to the magic password.
October 2, 2003	metacoretex-0.8.0.tar.gz	MetaCoreTex is an entirely JAVA based vulnerability scanning framework which puts special emphasis on databases.
October 2, 2003	prockill.txt	Exploit for the Windows PostThread Message() Denial of Service vulnerability.

Trends

- The SANS Twenty Most Critical Internet Security Vulnerabilities list has been published. This updated SANS Top Twenty is actually two Top Ten lists: the ten most commonly exploited vulnerable services in Windows and the ten most commonly exploited vulnerable services in UNIX and Linux. For more information see the list located at: <http://www.sans.org/top20/>.
- **The National Cyber Security Division (NCS) of the Department of Homeland Security (DHS) / Information Analysis and Infrastructure Protection (IAIP) Directorate has issued an advisory in consultation with the Microsoft Corporation to heighten awareness of potential Internet disruptions resulting from the possible spread of malicious software exploiting the Microsoft Operating Systems' Remote Procedure Call Server Service (RPCSS) vulnerability. For more information, see "Bugs, Holes & Patches" Table and advisory located at: <http://www.nipc.gov/warnings/advisories/2003/Advisory9102003.htm>. The Microsoft advisory is located at: http://www.microsoft.com/security/security_bulletins/ms03-039.asp. Tools have been developed to exploit this vulnerability and there is an increased likelihood that new viruses will emerge soon.**
- 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.
- 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/>.

Viruses

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

Ranking	Common Name	Type of Code	Trends	Date
1	W32.Mimail	Worm	Increase	July 2003
2	W32/Swen	Worm	New to Table	September 2003
3	Worm_Msblast.A	Worm	New to Table	August 2003
4	W32/Klez	Worm	Decrease	January 2002
5	W32/Sobig	Worm	Slight Decrease	May 2003
6	W32/Bugbear	File	Decrease	September 2002
7	W32/Dumaru-A	Worm	New to Table	August 2003
8	W32/Yaha	Worm	Decrease	February 2002
9	W32/Lovegate	Virus	Slight Decrease	February 2003
10	W32/SQLSlammer	Worm	Slight Decrease	January 2003

Note: Note: Virus reporting may be weeks behind the first discovery of infection. A total 632 distinct viruses are currently considered "in the wild" by anti-virus experts, with another 253 viruses suspected. "In the wild" viruses have been reported to anti-virus vendors by their clients and have infected user machines. The additional suspected number is derived from reports by a single source.

PP97M.Lacoph (PowerPoint 97 Macro Virus): This is a simple PowerPoint macro virus that spreads by copying itself to any other open SlideShow presentations on the host system. Upon execution, it drops the registry file, C:\Power.reg. The virus then executes C:\Power.reg, which adds the value, "MacroVirusProtection"="0," to the registry key:

- HKEY_CURRENT_USER\Software\Microsoft\Office\8.0\PowerPoint\Options

JS.Rad@mm (JavaScript Worm): This is a JavaScript-based worm that e-mails itself to contacts in the Microsoft Outlook address book. It arrives as an attachment with a variable name, which may have different double extensions, such as .jpg, .jpeg, .bmp, .gif, .png, .tif, .tiff, or .jif followed by .js.

VBS.Notup.A@mm (Alias: Bloodhound.VBS.Worm, I-Worm.WCGen, VBS/Pica.worm.gen)(Visual Basic Script Worm): This is a mass-mailing worm that sends itself to all the recipients in the Outlook Address Book. The e-mail message has the following characteristics:

- Subject: Symantec notification
- Attachment: SymantecUpdates.vbs

W32/Agobot-AE (Aliases: Backdoor.Agobot.3.m, W32.HLLW.Gaobot.AE, WORM_AGOBOT.AD, W32/Gaobot.worm.ai) (Win32 Worm): This worm has been reported in the wild. It is a network worm that also allows unauthorized remote access to the computer via IRC channels. W32/Agobot-AE copies itself to network shares with weak passwords and attempts to spread to computers using the DCOM RPC and the RPC locator vulnerabilities. These vulnerabilities allow the worm to execute its code on target computers with System level privileges. For further information on these vulnerabilities and for details on how to protect/patch the computer against such attacks please see Microsoft security bulletins MS03-026 and MS03-001. W32/Agobot-AE drops a copy of itself to the Windows system folder and creates the following registry entries to run itself on system restart:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Config Loader = "<copy of the worm>"
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\Config Loader = "<copy of the worm>"

It also attempts to terminate various processes related to anti-virus and security software (e.g. SWEEP95.EXE, BLACKICE.EXE and ZONEALARM.EXE).

W32.Gramos (Win32 Worm): This is a network-aware worm that is written in Microsoft Visual C++ and is packed with ASPack. When W32.Gramos is executed, it adds the value, "Messenger start-up"="Msgran.exe," to the registry key:

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

so that the worm runs when you start Windows. It downloads the Trojan proxy, Backdoor.Ranck, from a hard-coded URL, copies it to C:\winnt\Mh.exe, and then executes it and registers itself as a service process on Windows 95/98/ME systems to hide itself from the task list. Next, it calculates a random IP address, enumerates the users on the remote server, and then attempts to connect using these usernames with a blank password. The Trojan copies itself to \\<authenticated IP>\c\$\winnt\system32\Msgran.exe and remotely schedules a task to run the worm on the newly infected computer.

W32/Headout (Alias: TROJ_XOOMCIAO.A) (Win32 Worm): This virus exists as an executable file that was being distributed from a xoom.virgilio.it user page. This site was removed prior to the analysis of this virus and therefore the exact content of that user's site is unknown. A link directing users to the infectious site may be received in the following e-mail message:

- Subject: non ci posso credere ahahaa...

When a user clicks the hyperlink contained in the e-mail message, they are directed to the website that contained the executable file. When that file, Lisa.avi.exe is run, it sends an e-mail message to all users in the Windows Address Book containing the aforementioned message. The from address is forged, or spoofed, concealing the truly infected user from recipients of the message. The executable directs users to another page on the same Xoom user site, as well as downloading a pornographic video, bbcrissy.asx, from a specified IP address.

W32.HLLW.Donk.C (Alias: Backdoor.SdBot.gen): This is a network-aware worm that attempts to connect to a predetermined IRC server to receive instructions from its author.

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

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

It is compressed with UPX.

W32.HLLP.Gogo (Alias: W32/Gogo) (Win32 Virus): This is a 32-bit Windows virus. It may also display a message box, depending on the current time and date. When W32.HLLP.Gogo is executed, it extracts and runs the original host file, with the extension .viv, in the current folder and searches the entire C:\ drive for files with the .exe extension and prepends itself to these files. Depending on the time and date, the virus may display a message box with the text:

- I am The Virus oF Happy

along with some additional double-byte characters.

W32.HLLW.Kazwin (Win32 Worm): This is a worm that spreads itself through the KaZaA file-sharing network. It also downloads a file from a predefined Web site. It is written in the Borland Delphi programming language.

W32.HLLW.Logpole (Win32 Worm): This is a worm that spreads through the KaZaA file-sharing network. It is written in Borland Delphi. When W32.HLLW.Logpole runs, it copies itself to the C:\Windows\Backup directory as various files and adds the value, "Dir0"="012345:C:\WINDOWS\Backup," to the registry key:

- HKEY_CURRENT_USER\Software\Kazaa\LocalContent

which allows C:\Windows\Backup to be shared via KaZaA. It also adds the value, "DirectX"="C:\Windows\Backup\DirectX.exe," to the registry key:

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

so the worm runs when you start Windows.

W32.HLLW.Moega.D (Aliases: Backdoor.Sdbot.gen, W32/Sdbot.worm.gen) (Win32 Worm): This is a worm with backdoor capabilities that attempts to spread through the local area network. The worm attempts to open ports 139 and 445, and to steal sensitive information. The executable for W32.HLLW.Moega.D looks similar to the icon for Windows XP's Windows Update executable, Wupdmgr.exe. It is packed with FSG.

W32.HLLW.Repsan (Win32 Worm): This is a worm that spreads through file-sharing networks. It does not contain a destructive payload.

W32.HLLW.Syney.B@mm (Alias: W32/Syney@MM): This is a mass-mailing worm that attempts to delete antiviral files and spreads through Microsoft Outlook. The e-mail message has the following characteristics:

- Subject: Fwd:None
- Attachment: Me.exe, Mess.exe, or Mes.exe

W32.HLLW.Wanado (Win32 Worm): This is a worm that spreads through the eMule file-sharing network. It is written in Borland Delphi and is packed with FSG.

W32/Inmotecd-A (Aliases: Trojan.Win32.Inmota, TROJ_INMOTECD.A, W32.Inmota.Worm, W32/Inmota.dll) (Win32 Worm): This is an Internet worm that spreads by replying to mail messages on computers using MAPI-based e-mail clients such as Microsoft Outlook or Outlook Express. The subject of the e-mail is "Re: 0!~" and the attached file is default.htm<SPACES>.pif where <SPACES> is a large number of space characters, aimed at hiding the file's true extension of PIF. When default.htm<SPACES>.pif is run, a message box is displayed with the text "Welcome," "Welcome Microsoft CD Key web site Press OK to open the Web" and Microsoft Internet Explorer is launched with the URL <http://omnitechdesign.com/cdkey.html>. The worm copies itself to the Windows and Windows System folders as default.htm<SPACES>.pif, drops the files rundl132.exe and Gate.dll to both the Windows and System folders and sets or creates one of the following registry entries to run rundl132.exe automatically on startup:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\<variable> = rundl132.exe powrprof.dll,loadcurrentpwrscheme
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\PowerProfile = rundl132 kernel.dll,PowerProfileEnable

It changes all sub-keys of HKLM\Software\Microsoft\Windows\CurrentVersion\Run\ whose data contains the string "Rundll."

W32.Kromber (IRC Worm): This is an IRC worm that attempts to get mIRC users to visit a malicious URL. When an unsuspecting user visits the URL, a malicious HTML page loads a .php file, using an exploit to avoid any security warnings. Microsoft has released a cumulative patch for this vulnerability, available in Microsoft Security Bulletin MS03-40.

W32.Ogid (Win32 Worm): This is a worm that copies itself to multiple places on the hard disk and mapped drives. In particular, the worm attempts to copy itself to directories that popular file-sharing programs share.

W32.Spacearm (Win32 Worm): This is a worm that copies itself to the local drive and mapped drives as variable file names. It is written in Visual Basic.

W32/Spybot-R (Aliases: W32.Spybot.Worm, Worm.P2P.SpyBot.gen) (P2P Worm): This is a P2P worm that spreads via the KaZaA file sharing network. Upon execution, W32/Spybot-R displays the fake error message: "Runtime Error," "Unable to locate Smartinstl32.dll. Re-installing the application may fix the problem." The worm creates the folder <system>\kazaabackupfiles and copies itself there using several different filenames. To enable sharing of these files the registry entry:

- HKCU\Software\Kazaa\LocalContent\Dir0 is updated to point to this location.

In order to be run automatically on system startup, the worm copies itself to explorer64.exe in the Windows system folder and adds the following registry entries that point to this file:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Microsoft Explorer(64)
- HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce\Microsoft Explorer(64)

W32/Spybot-R has an IRC backdoor component that has keylogging and backdoor capabilities. The worm connects to an IRC server announcing the infection and allows a malicious user remote access to the computer.

W32.Wintoo.Worm (Win32 Worm): This is a mass-mailing worm that sends itself to all the recipients in the Windows Address Book. It sends itself using the MAPI interface. The e-mail will have the following characteristics:

- Subject: <Cyrilic text that loosely translates to "Look at this">
- Attachment: win2drv.exe

The worm also modifies the Windows background to a bitmap containing a message in Cyrilic.

WORM_ACEBOT.A (Aliases: Win32:Acebo-B [Trj], Worm/AceBot, Worm/Newbiero, I-Worm.Win32.Acebot.172032, W32.HLLW.Acebo, W32/AceBot.worm, Win32/NewBiero.0_34.worm, Worm.Newbiero.034, Win32.Acebot.041) (Win32 Worm): This memory-resident malware exhibits characteristics of both a network worm and a backdoor program. As a worm, it propagates through drives connected to a local network. As a backdoor server program, it allows a remote user to perform various action on the infected systems. Aside from having backdoor capabilities, it also steals passwords and shuts down certain personal firewall applications.

WORM_RANDEX.Q (Aliases: I-Worm.Simbolos, W32.Randex.Q) (Internet Worm): This malware has both worm and backdoor capabilities. To propagate, it looks for random target machines with weak IPC\$ share passwords and then drops and executes a copy of itself on these compromised systems. As a backdoor, it allows a remote user to gain access to a target system via IRC (Internet Relay Chat). This malware also deletes the system file NETSTAT.EXE from the Windows system folder. It is developed in Visual C++ and usually arrives as a Win32 executable file compressed with the Aspack utility and runs on Windows 95, 98, ME, NT, 2000, and XP.

WORM_REDIST.E (Internet Worm): This worm spreads via e-mail using Microsoft Outlook. It sends e-mail with varying details to all addresses in the user address book. It also has password-stealing capabilities and is able to propagate via peer-to-peer file-sharing networks. It is written in Visual Basic, a high-level programming language, and compressed using UPX. It runs on Windows 95, 98, ME, NT, 2000, and XP.

Trojans

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

Trojan	Version	CyberNotes Issue #
A97M/AcceV	N/A	CyberNotes-2003-18
AdwareDropper-A	A	CyberNotes-2003-04
Adware-SubSearch.dr	dr	CyberNotes-2003-14
Afcore.q	N/A	CyberNotes-2003-20
AIM-Canbot	N/A	CyberNotes-2003-07
AprilNice	N/A	CyberNotes-2003-08
Backdoor.Acidoor	N/A	CyberNotes-2003-05
Backdoor.Amitis	N/A	CyberNotes-2003-01
Backdoor.Amitis.B	B	CyberNotes-2003-11
Backdoor.AntiLam.20.K	K	CyberNotes-2003-10
Backdoor.AntiLam.20.Q	20.Q	CyberNotes-2003-18
Backdoor.Apdoor	N/A	CyberNotes-2003-12
Backdoor.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

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

Trojan	Version	CyberNotes 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.Hazzer	N/A	CyberNotes-2003-20
Backdoor.Hethat	N/A	CyberNotes-2003-01
Backdoor.Hipo	N/A	CyberNotes-2003-04
Backdoor.Hitcap	N/A	CyberNotes-2003-04
Backdoor.Hornet	N/A	CyberNotes-2003-01
Backdoor.IRC.Aladinz	N/A	CyberNotes-2003-02
Backdoor.IRC.Aladinz.C	C	CyberNotes-2003-14
Backdoor.IRC.Bobbins	N/A	CyberNotes-2003-18
Backdoor.IRC.Cloner	N/A	CyberNotes-2003-04
Backdoor.IRC.Comiz	N/A	CyberNotes-2003-11
Backdoor.IRC.Flood.F	F	CyberNotes-2003-16
Backdoor.IRC.Hatter	N/A	CyberNotes-2003-18
Backdoor.IRC.Jemput	N/A	CyberNotes-2003-19
Backdoor.IRC.Lampsy	N/A	CyberNotes-2003-10
Backdoor.IRC.PSK	PSK	CyberNotes-2003-16
Backdoor.IRC.Ratsou	N/A	CyberNotes-2003-10
Backdoor.IRC.Ratsou.B	B	CyberNotes-2003-11
Backdoor.IRC.Ratsou.C	C	CyberNotes-2003-11
Backdoor.IRC.RPCBot.B:	B	CyberNotes-2003-18
Backdoor.IRC.RPCBot.C	C	CyberNotes-2003-18
Backdoor.IRC.RPCBot.D	D	CyberNotes-2003-18
Backdoor.IRC.RPCBot.F	F	CyberNotes-2003-19
Backdoor.IRC.Tastyred	N/A	CyberNotes-2003-20
Backdoor.IRC.Yoink	N/A	CyberNotes-2003-05
Backdoor.IRC.Zcrew	N/A	CyberNotes-2003-04
Backdoor.IRC.Zcrew.B	B	CyberNotes-2003-19
Backdoor.Jittar	N/A	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
Backdoor.Krei	N/A	CyberNotes-2003-03
Backdoor.Lala	N/A	CyberNotes-2003-01
Backdoor.Lala.B	B	CyberNotes-2003-16
Backdoor.Lala.C	C	CyberNotes-2003-16
Backdoor.Lanfilt.B	B	CyberNotes-2003-14
Backdoor.Lassrv	N/A	Current Issue
Backdoor.Lastras	N/A	CyberNotes-2003-17
Backdoor.LeGuardien.B	B	CyberNotes-2003-10
Backdoor.Litmus.203.c	c	CyberNotes-2003-09
Backdoor.LittleWitch.C	C	CyberNotes-2003-06
Backdoor.Lixy	N/A	Current Issue

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

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

Trojan	Version	CyberNotes Issue #
Backdoor.WinJank	N/A	CyberNotes-2003-15
Backdoor.Winker	N/A	CyberNotes-2003-15
Backdoor.WinShell.50	N/A	CyberNotes-2003-16
Backdoor.Wolf.16	16	CyberNotes-2003-18
Backdoor.Xenozbot	N/A	CyberNotes-2003-01
Backdoor.Xeory	N/A	CyberNotes-2003-03
Backdoor.XTS	N/A	CyberNotes-2003-08
Backdoor.Zdemon	N/A	CyberNotes-2003-02
Backdoor.Zdemon.126	126	CyberNotes-2003-10
Backdoor.Zdown	N/A	CyberNotes-2003-05
Backdoor.Zix	N/A	CyberNotes-2003-02
Backdoor.Zombam	N/A	CyberNotes-2003-08
Backdoor.Zombam.B	B	CyberNotes-2003-20
Backdoor.Zvrop	N/A	CyberNotes-2003-03
Backdoor-AFC	N/A	CyberNotes-2003-05
Backdoor-AOK	N/A	CyberNotes-2003-01
BackDoor-AQL	N/A	CyberNotes-2003-05
BackDoor-AQT	N/A	CyberNotes-2003-05
BackDoor-ARR	ARR	CyberNotes-2003-06
Backdoor-ARU	ARU	CyberNotes-2003-06
BackDoor-ARX	ARX	CyberNotes-2003-06
BackDoor-ARY	ARY	CyberNotes-2003-06
BackDoor-ASD	ASD	CyberNotes-2003-07
BackDoor-ASL	ASL	CyberNotes-2003-07
BackDoor-ASW	ASW	CyberNotes-2003-08
BackDoor-ATG	ATG	CyberNotes-2003-09
BackDoor-AUP	N/A	CyberNotes-2003-11
BackDoor-AVF	AVF	CyberNotes-2003-12
BackDoor-AVH	AVH	CyberNotes-2003-12
BackDoor-AVO	AVO	CyberNotes-2003-12
BackDoor-AXC	AXC	CyberNotes-2003-14
BackDoor-AXQ	AXQ	CyberNotes-2003-15
Backdoor-AXR	AXR	CyberNotes-2003-16
Backdoor-AZF	AZF	CyberNotes-2003-20
BackDoor-BAE	BAE	Current Issue
BDS/AntiPC	N/A	CyberNotes-2003-02
BDS/Backstab	N/A	CyberNotes-2003-02
BDS/CheckESP	N/A	CyberNotes-2003-12
BDS/Ciadoor.10	10	CyberNotes-2003-07
BDS/Evilbot.A	A	CyberNotes-2003-09
BDS/Evolut	N/A	CyberNotes-2003-03
BDS/GrayBird.G	G	CyberNotes-2003-17
BDS/PowerSpider.A	A	CyberNotes-2003-11
BDS/SdBot.76870	76870	Current Issue
BKDR_LITH.103.A	A	CyberNotes-2003-17
Cardown	N/A	CyberNotes-2003-19
CoolFool	N/A	CyberNotes-2003-17
Daysun	N/A	CyberNotes-2003-06

Trojan	Version	CyberNotes Issue #
DDoS-Stinkbot	N/A	CyberNotes-2003-08
Delude	N/A	CyberNotes-2003-19
Desex	N/A	CyberNotes-2003-20
DoS-iFrameNet	N/A	CyberNotes-2003-04
Download.Aduent.Trojan	N/A	CyberNotes-2003-18
Download.Trojan.B	B	CyberNotes-2003-13
Downloader.BO.B	B	CyberNotes-2003-10
Downloader.BO.B.dr	B.dr	CyberNotes-2003-10
Downloader.Dluca	N/A	CyberNotes-2003-17
Downloader.Dluca.B	B	CyberNotes-2003-19
Downloader.Dluca.C	C	CyberNotes-2003-20
Downloader.Mimail	N/A	CyberNotes-2003-16
Downloader.Slime	N/A	Current Issue
Downloader-BN.b	BN.b	CyberNotes-2003-13
Downloader-BO.dr.b	N/A	CyberNotes-2003-02
Downloader-BS	N/A	CyberNotes-2003-02
Downloader-BW	N/A	CyberNotes-2003-05
Downloader-BW.b	BW.b	CyberNotes-2003-06
Downloader-BW.c	BW.c	CyberNotes-2003-07
Downloader-CY	CY	CyberNotes-2003-16
Downloader-DM	DM	CyberNotes-2003-16
Downloader-DN.b	DN.b	CyberNotes-2003-17
Downloader-EB	EB	CyberNotes-2003-18
DownLoader-EG	EG	CyberNotes-2003-20
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	CyberNotes-2003-19
Hacktool.PWS.QQPass	N/A	CyberNotes-2003-06
ICQPager-J	N/A	CyberNotes-2003-05
IgetNet.dr	dr	Current Issue
IRC/Backdoor.e	E	CyberNotes-2003-01
IRC/Backdoor.f	f	CyberNotes-2003-02
IRC/Backdoor.g	g	CyberNotes-2003-03
IRC/Flood.ap	N/A	CyberNotes-2003-05
IRC/Flood.bi	N/A	CyberNotes-2003-03
IRC/Flood.br	br	CyberNotes-2003-06
IRC/Flood.bu	bu	CyberNotes-2003-08
IRC/Flood.cd	cd	CyberNotes-2003-11
IRC/Flood.cm	cm	CyberNotes-2003-13
IRC/Fyle	N/A	CyberNotes-2003-16
IRC-BBot	N/A	CyberNotes-2003-16
IRC-Emoz	N/A	CyberNotes-2003-03
IRC-OhShootBot	N/A	CyberNotes-2003-01
IRC-Vup	N/A	CyberNotes-2003-09
JS.Fortnight.B	B	CyberNotes-2003-06
JS.Seeker.J	J	CyberNotes-2003-01
JS.Seeker.K	K	CyberNotes-2003-20

Trojan	Version	CyberNotes Issue #
JS/Fortnight.c@M	c	CyberNotes-2003-11
JS/Seeker-C	C	CyberNotes-2003-04
JS/StartPage.dr	dr	CyberNotes-2003-11
JS_WEBLOG.A	A	CyberNotes-2003-05
Keylogger.Cone.Trojan	N/A	CyberNotes-2003-14
KeyLog-Kerlib	N/A	CyberNotes-2003-05
Keylog-Keylf	N/A	CyberNotes-2003-17
Keylog-Kjie	N/A	CyberNotes-2003-12
Keylog-Mico	N/A	CyberNotes-2003-20
Keylog-Perfect.dr	dr	CyberNotes-2003-09
Keylog-Razytimer	N/A	CyberNotes-2003-03
KeyLog-TweakPan	N/A	CyberNotes-2003-02
Keylog-Yeehah	N/A	CyberNotes-2003-12
Linux/DDoS-Ferlect	N/A	CyberNotes-2003-17
Linux/Exploit-SendMail	N/A	CyberNotes-2003-05
Lockme	N/A	CyberNotes-2003-15
MultiDropper-FD	N/A	CyberNotes-2003-01
OF97/ExeDrop-B	N/A	CyberNotes-2003-19
Pac	N/A	CyberNotes-2003-04
Petala	N/A	CyberNotes-2003-20
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-Bugmaf	N/A	Current Issue
PWS-Moneykeeper	N/A	CyberNotes-2003-18
PWS-Sincom.dr	dr	CyberNotes-2003-17
PWSteal.ABCHlp	N/A	CyberNotes-2003-12
PWSteal.ALlight	N/A	CyberNotes-2003-01
PWSteal.Bancos	N/A	CyberNotes-2003-15
PWSteal.Bancos.B	B	CyberNotes-2003-16
PWSteal.Banpaes	N/A	Current Issue
PWSteal.Finero	N/A	Current Issue
PWSteal.Hukle	N/A	CyberNotes-2003-08
PWSteal.Kipper	N/A	CyberNotes-2003-10
PWSteal.Lemir.105	105	CyberNotes-2003-10
PWSteal.Lemir.C	C	CyberNotes-2003-17
PWSteal.Lemir.D	D	CyberNotes-2003-18
PWSteal.Lemir.E	E	CyberNotes-2003-20
PWSteal.Lemir.F	F	CyberNotes-2003-20
PWSteal.Nikana	N/A	Current Issue
PWSteal.Reanet	N/A	Current Issue
PWSteal.Rimd	N/A	CyberNotes-2003-01
PWSteal.Rimd.B	B	CyberNotes-2003-10
PWSteal.Salira	N/A	Current Issue

Trojan	Version	CyberNotes Issue #
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
Startpage-N	N	CyberNotes-2003-13
StartPage-U	U	CyberNotes-2003-20
Stealther	N/A	CyberNotes-2003-16
Stoplete	N/A	CyberNotes-2003-06
Swizzor	N/A	CyberNotes-2003-07
Tellafriend.Trojan	N/A	CyberNotes-2003-04
Tr/Decept.21	21	CyberNotes-2003-07
Tr/Delf.r	r	CyberNotes-2003-16
Tr/DelWinbootdir	N/A	CyberNotes-2003-07
TR/Fake.YaHoMe.1	N/A	CyberNotes-2003-02
TR/Gaslide.C	C	CyberNotes-2003-17
Tr/SpBit.A	A	CyberNotes-2003-04
Tr/VB.t	T	CyberNotes-2003-11
TR/WinMx	N/A	CyberNotes-2003-02
Troj/Apdoor-A	A	CyberNotes-2003-19
Troj/Ataka-E	E	CyberNotes-2003-15
Troj/Autoroot-A	A	CyberNotes-2003-16
Troj/Backsm-A	A	CyberNotes-2003-19
Troj/Bdoor-AAG	AAG	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	CyberNotes-2003-19
Troj/Golon-A	A	CyberNotes-2003-15

Trojan	Version	CyberNotes Issue #
Troj/Hackarmy-A	A	CyberNotes-2003-20
Troj/Hacline-B	B	CyberNotes-2003-13
Troj/IRCBot-C	C	CyberNotes-2003-11
Troj/Ircbot-M	M	Current Issue
Troj/Manifest-A	N/A	CyberNotes-2003-03
Troj/Migmaf-A	A	CyberNotes-2003-15
Troj/Mystri-A	A	CyberNotes-2003-13
Troj/PcGhost-A	A	CyberNotes-2003-13
Troj/Peido-B	B	CyberNotes-2003-10
Troj/Qhosts-1	N/A	CyberNotes-2003-20
Troj/QQPass-A	A	CyberNotes-2003-16
Troj/Qzap-248	N/A	CyberNotes-2003-01
Troj/SadHound-A	N/A	CyberNotes-2003-03
Troj/Sandesa-A	A	CyberNotes-2003-14
Troj/Slacker-A	A	CyberNotes-2003-05
Troj/Slanret-A	N/A	CyberNotes-2003-03
Troj/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.Abaxo	N/A	CyberNotes-2003-20
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.Bootconf	N/A	Current Issue
Trojan.Boxer	N/A	CyberNotes-2003-19
Trojan.Cuydoc	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.Downloader.Inor	N/A	CyberNotes-2003-02
Trojan.Fwin	N/A	CyberNotes-2003-18
Trojan.Gaslide.Intd	N/A	CyberNotes-2003-20
Trojan.Grepape	N/A	CyberNotes-2003-05
Trojan.Guapeton	N/A	CyberNotes-2003-08
Trojan.Idly	N/A	CyberNotes-2003-04
Trojan.Ivanet	N/A	CyberNotes-2003-02
Trojan.Kaht	N/A	CyberNotes-2003-10
Trojan.Kalshi	N/A	Current Issue
Trojan.KillAV.B	B	CyberNotes-2003-19
Trojan.KKiller	N/A	CyberNotes-2003-01
Trojan.Lear	N/A	CyberNotes-2003-10
Trojan.Mumuboy	N/A	CyberNotes-2003-13
Trojan.Mumuboy.B	B	CyberNotes-2003-20
Trojan.Myet	N/A	CyberNotes-2003-12

Trojan	Version	CyberNotes Issue #
Trojan.Myss.B	B	Current Issue
Trojan.Norio	N/A	CyberNotes-2003-19
Trojan.OptixKiller	N/A	CyberNotes-2003-16
Trojan.Poetas	N/A	CyberNotes-2003-14
Trojan.Poldo.B	B	CyberNotes-2003-02
Trojan.Poot	N/A	CyberNotes-2003-05
Trojan.PopSpy	N/A	CyberNotes-2003-11
Trojan.Progent	N/A	CyberNotes-2003-16
Trojan.ProteBoy	N/A	CyberNotes-2003-04
Trojan.PSW.Gip	N/A	CyberNotes-2003-06
Trojan.PSW.Platan.5.A	N/A	CyberNotes-2003-01
Trojan.PWS.QQPass.D	N/A	CyberNotes-2003-02
Trojan.PWS.QQPass.E	E	CyberNotes-2003-20
Trojan.Qforager	N/A	CyberNotes-2003-02
Trojan.Qforager.Dr	N/A	CyberNotes-2003-02
Trojan.Qwe	N/A	CyberNotes-2003-02
Trojan.Sarka	N/A	CyberNotes-2003-14
Trojan.Sidea	N/A	CyberNotes-2003-12
Trojan.Sinkin	N/A	Current Issue
Trojan.Snag	N/A	CyberNotes-2003-02
Trojan.Unblockee	N/A	CyberNotes-2003-01
Trojan.Vardo	N/A	CyberNotes-2003-20
Trojan.Visages	N/A	CyberNotes-2003-15
Trojan.Windelete	N/A	CyberNotes-2003-14
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.Adelicker.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.Laorenshe.Trojan	N/A	CyberNotes-2003-14
W32.Noops.Trojan	N/A	CyberNotes-2003-09
W32.Socay.Worm	N/A	CyberNotes-2003-02
W32.Spybot.dr	dr	CyberNotes-2003-15
W32.Systentry.Trojan	N/A	CyberNotes-2003-03
W32.Trabajo	N/A	CyberNotes-2003-14
W32.Xilon.Trojan	N/A	CyberNotes-2003-01
W32.Yinker.Trojan	N/A	CyberNotes-2003-04
W32/Igloo-15	N/A	CyberNotes-2003-04

Trojan	Version	CyberNotes Issue #
W97M.Tabi.Trojan	N/A	CyberNotes-2003-20
Woodcot	N/A	CyberNotes-2003-16
Xin	N/A	CyberNotes-2003-03

BackDoor-BAE (Alias: Portless Backdoor v1.1): This is a remote access Trojan that is written in Visual C++ and works only on W2k/XP/2003 Operating Systems. It consists of the following two files:

- portlessinst.exe (3800 bytes) – installer
- svchostdll.dll (22,016 bytes) - contains backdoor functions

Upon execution, the Trojan installs the dll component into svchost.exe, which is a system process. After installing, the Trojan needs to be manually connected to target machine. The following key is created on a compromised machine:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\PortLess

The Trojan also hooks the registry at the following places:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\IPRIP\Parameters
"ServiceDll" =%SYSDIR%\svchostdll.dll
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\IPRIP\Parameters
"ServiceDll" = %SYSDIR%\svchostdll.dll

Once running on the victim machine, the server component is able to accept commands sent from the client component.

Backdoor.Daemonize (Alias: TrojanProxy.Win32.Daemonize): This is a Trojan Horse that runs as a proxy server. It is packed with UPX. Backdoor.Daemonize is a command line tool. It can be configured to connect to any external IP on any port.

Backdoor.Jittar: This is a Backdoor Trojan Horse that gives its creator remote access to and complete control over a compromised system. By default it uses ports 1309 and 2699 to listen for commands from the Trojan's creator. The existence of the file dm_mgr.exe or linuxp.exe is an indication of a possible infection. It is written in Microsoft Visual C++ and is packed with UPX.

Backdoor.Lassrv: This is a Backdoor Trojan Horse that gives its creator remote access and complete control over a compromised system. It is packed with ASPack. Backdoor.Lassrv consists of one .dll file and one .exe file. The file names are usually the following:

- lsasrv32.exe. This file injects lsasrv32.dll into the Windows file Lsass.exe
- lsarv32.dll. This file contains the main routine of the backdoor.

If the .exe file is executed, it injects lsasrv32.dll as a thread into Lsass.exe. The thread connects to ports 1988 and 1989 of a specific IP address in the backdoor and waits for the commands from the Trojan's author.

Backdoor.Lixy: This is a Backdoor Trojan Horse that opens a proxy server on TCP port 1080. It consists of one .dll file and two .exe files. The file names are usually the following:

- Rlid.exe: For setting up and running other Trojan files
- Lid.exe: Contains the main routine of the backdoor
- Lid.dll: A malicious Browser Helper Object that runs Lid.exe.

When Backdoor.Lixy is executed, it adds the value, "Key1"="<path to the Rlid.exe>," to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
- so that the Trojan starts when you start Windows. It also adds the following keys in the registry:
- HKEY_CLASSES_ROOT\CLSID\{1E1B2879-88FF-11D2-8D96-D7ACAC95951A}
 - HKEY_CLASSES_ROOT\HTMLEdit.SSocks5
 - HKEY_CLASSES_ROOT\HTMLEdit.SSocks5.1
 - HKEY_LOCAL_MACHINE\Software\CLASSES\CLSID\{1E1B2879-88FF-11D2-8D96-D7ACAC95951A}\HKEY_LOCAL_MACHINE\Software\CLASSES\HTMLEdit.SSocks5
 - HKEY_LOCAL_MACHINE\Software\CLASSES\HTMLEdit.SSocks5.1

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\explorer\Browser Helper Objects\{1E1B2879-88FF-11D2-8D96-D7ACAC95951A}

which adds Lid.dll as a Browser Helper Object.

Backdoor.MeteorShell (Aliases: Backdoor.MeteorShell.58, BackDoor-AWI): This is a Trojan Horse that allows unauthorized access to an infected computer. This Trojan opens TCP port 7441, by default. It is written in Microsoft Visual C++. When Backdoor.MeteorShell is executed, it adds the value, "Services" = "<path to trojan>," to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\CurrentVersion\Run

so that the Trojan runs when Windows starts.

Backdoor.Mxsender (Aliases: Trojan Horse, TrojanSpy.Win32.Mxsender, Mxsender): This is a Backdoor Trojan Horse that gives a malicious user unauthorized access to a compromised computer. It connects to port 8311 of the predetermined servers and waits for commands from its author.

Backdoor.SDBot.Q: This is a Backdoor Trojan Horse that can be controlled through an IRC server. It has been packed using the run-time compression utility, Petite. When Backdoor.SDBot.Q is executed, it creates a copy of itself as %SYSTEM%\winz32.exe and adds the value, "INTERNET_SERVICES" = "winz32.exe," to the registry key:

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

It connects to the IRC server, greenz.dyn.nu, joins a predefined channel, and waits for commands from the malicious user.

Backdoor.Sdbot.R (Alias: Backdoor.Sdbot): This is a Backdoor Trojan Horse that is a variant of Backdoor.Sdbot. It allows the Trojan's creator to use Internet Relay Chat (IRC) to gain access to an infected computer.

Backdoor.Sincom (Alias: TrojanSpy.Win32.Sincom.ab): This is a Backdoor Trojan Horse that gives the Trojan's author unauthorized access to an infected computer. It allows the author to control the system through a TCP connection, through an FTP server, or have the backdoor program reconnect to the malicious user's computer. When Backdoor.Sincom runs, it moves itself to %Windir%. The Trojan drops a configuration file to %Windir%\Rb.ini. It uses this file to store all the configurable options for the backdoor server. It also drops a file of the malicious user's choice. Backdoor.Sincom stops all the processes that have certain file names. The file name list is configurable. The following value is created, "<filename>""=%windir%\<filename>.exe Run:Auto," in the registry key:

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

so that the Trojan starts when you start Windows.

Backdoor.Smokodoor (Aliases: Backdoor:Win32/Smokodoor, BackDoor-APO, BackDoor-APO.dll): This is a Backdoor Trojan Horse that gives a remote malicious user complete control over a compromised system. By default the Trojan listens on port 4300 for incoming connections. When Backdoor.Smokodoor is executed, it copies the following files onto the computer:

- %System%\Server.exe
- %System%\Server.dll

and adds the value, "server.exe" = "server.exe," to the registry key:

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

so that the Trojan will be executed each time Windows starts. The Trojan also injects %System%\Server.dll into the Explorer process, which will then launch the backdoor functionality.

Backdoor.Sinit (Aliases: BackDoor.Iterator, Trojan.Win32.DirectPlugin.a, BackDoor-BAM): This is a Backdoor Trojan Horse that gives a malicious user unauthorized access to a compromised computer, by opening a random UDP port. It is written in the Microsoft Visual C++ programming language and is compressed with UPX. When Backdoor.Sinit is executed, it copies itself as %System%\Svcinit.exe, which runs in the background and deletes the original file and adds the value, "SVC Service" = "%System%\svcinit.exe," to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices so that the Trojan runs when you start Windows. The Trojan modifies the value, "Userinit" = "%System%\userinit.exe," in the registry key:

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

so that the Trojan runs when a user logs on. The following registry key is created:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DirectPlugin

Backdoor.Usirf: This is a general class of Trojan Horses that uses an FTP server as a backdoor into your system.

Downloader.Slime (Alias: PE_Slime): This is a Trojan Horse that downloads updates from a Web site. It also sets itself to run whenever a .exe file is executed. When Downloader.Slime runs, it creates a file named %System%\Rundll.exe and adds itself to the default value of the registry key:

- HKEY_CLASSES_ROOT\exefile\shell\open\command

so that the Trojan runs before any .exe command is executed. The Trojan attempts to connect to an external Web site to download and run the files without a user's knowledge or consent. The location and content of the downloaded files are configurable for each instance of the downloader.

BDS/SdBot.76870: This is a memory resident backdoor program that connects to an IRC server. The established connection could potentially allow someone, at the other end, with malicious intent backdoor access to your computer. If executed, the backdoor adds the following files to the \windows%\system% directory, "wnetlib.exe" and "cool.exe." So that it gets run each time a user restart their computer the following registry keys get added:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
"Microsoft System Checkup"="wnetlib.exe"
"NT Logging Service"="syslog32.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
"Microsoft System Checkup"="wnetlib.exe"

IGetNet.dr: This file may come bundled with another program, which discloses the fact that it is ad-supported. Users agree to have this program installed in the license agreement, although they may not realize at first that this particular file was packaged with the product they installed. When executed, two files called WINSTART001.EXE and rules.dat are dropped into C:\Windows\System. This Trojan installs the IGetNet application (WINSTART001.EXE is already detected as IGetNet application). The following change is made to the registry to run the executable at startup:

- HKEY_LOCAL_MACHINE\Software\Windows\CurrentVersion\Run
"WINSTART001.EXE"

The Trojan contains a counter stored in:

- HKEY_CURRENT_USER\Software\VB and VBA Program Settings\ Ie Rsp\System "pid"
- HKEY_CURRENT_USER\Software\VB and VBA Program Settings\ Ie Rsp\System "rules"

These registry keys are intended to monitor the number of times that the Trojan has run. Lastly, this Trojan will delete all *.EX* files from Temp folders.

PWSteal.Banpaes: This is a Trojan Horse that attempts to steal online banking information. It is written in the Delphi language and is packed with UPX.

PWS-Bugmaf : This is a password stealing Trojan that captures information from the local file systems such as the username and password and sends this information to the author via e-mail in Romania. Online e-mail and bank account information (username/password), if locally cached, and local access credentials are particularly vulnerable to this threat. When run, the Trojan copies itself to %system% directory. It uses the name "winrarshell32.exe." The Trojan was distributed in a malformed archive file (ZIP with RAR extension) that seems to suggest that it has 2 files:

- README.TXT - 50 bytes
- SUBTITLES.RAR - 35072 bytes

In reality when TXT file is clicked a Trojan program will be unpacked and executed.

PWSteal.Finero: This is a Trojan Horse that mimics the online interfaces of certain Brazilian banks to steal account information. This Trojan may arrive as the e-mail attachment "BBsetup.exe."

PWSteal.Nikana: This is a Visual Basic Script (VBScript) Trojan Horse that gathers user data, passwords, and registration information for various online services and sends it to the Trojan's author. The downloader and the Trojan are both written in Borland Delphi, and all the files are UPX-packed.

PWSteal.Reanet: This is a Trojan Horse that attempts to steal information from Real Internet Banking. It is written in the Microsoft Visual Basic (VB) programming language. The VB run-time libraries are required for the Trojan to execute. When PWSteal.Reanet is executed, it resides in memory and searches for the window "Real Internet Banking - Microsoft Internet Explorer." If the window is found open, the Trojan will close it and display a fake window that will prompt the user to enter information into fields such as the username, and password to log into the banking site. The fake window looks very similar to that of the true login screen. The information that the Trojan collects from this form is saved in the file, C:\Realcomp.bsp

PWSteal.Salira: This is a Trojan Horse that attempts to steal user names and passwords, and masquerades as an rar archive, when it is in fact a normal Win32 PE executable. The file may be hidden inside a compressed zip file in which the file header information is forged to disguise the Trojan. Usually, the Trojan has a .rar extension and an rar self-extracting file icon. This Trojan is written in Visual C++.

Troj/Bdoor-AAG (Alias: Backdoor.G_Spot.20, Backdoor.Spigot.C): This is a configurable IRC backdoor Trojan that allows unauthorized access to the user's computer. It drops itself into the Windows system folder using a configured name and creates a registry entry under:

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

to run itself automatically when Windows starts up.

Troj/Ircbot-M (Aliases: W32.IRCBot.B, Win32.Sdbot.18976, Backdoor.IRCBot.gen, W32/Sdbot.worm.gen, BKDR_SDBOT.441B1): This Trojan has been reported in the wild. It is a backdoor Trojan that allows a malicious user remote access to the system. In order to run automatically when Windows boots up the Trojan copies itself as RPCX1sq23.exe to the Windows system folder and creates the following registry entries that point to this file:

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

The Trojan attempts to connect to a remote IRC server and join a specific channel and can be controlled via this connection.

Trojan.Bootconf (Aliases: Trojan.Qhosts.A, Trojan.Qhosts.B, TrojanClicker.Win32.Qhost.a): This is a Trojan Horse that modifies the TCP/IP settings to point to a different DNS server. It will also change your home page and search page in Internet Explorer to connect to out.true-counter.com. It is written in Microsoft Visual C++.

Trojan.Cuydoc (Alias: W32/Cuydoc): This is a Trojan Horse that infects Spanish versions of Windows. It copies itself to the A drive, and deletes all the .doc files from the C:\Mis documentos folder. It is written in Visual Basic and is packed with UPX. When Trojan.Cuydoc runs, it deletes all the files that have the .doc extension from the c:\Mis documentos folder and prevents you from running Regedit.exe or

Msconfig.exe. This Trojan copies itself to C:\Archiv~1\Win.com and A:\Cupido.exe and adds one of the following the values, "c"="c:\archiv~1\win.com," to these registry keys:

- HKEY_Current_User\Software\Microsoft\Windows\CurrentVersion\Run

so that the worm runs when you start Windows.

Trojan.Kalshi (Alias: W32.Kalshi.A@mm): This is a Trojan Horse that spammers use to anonymously send spam messages. It may arrive in an install package that includes Backdoor.HackDefender, a rootkit used to hide its malicious activities.

Trojan.Myss.B (Aliases: Backdoor.Avstral, Backdoor.Avstral, BackDoor-AWW, MultiDropper-GP Trojan, Win32.Myss): This is a Trojan Horse that can capture keystrokes and periodically send them to a predefined e-mail address. It is compressed with UPX.

Trojan.Sinkin (Aliases: VBS/Sinkin, Win32.Realphx, W32/Alphx.worm): This is a Trojan Horse that changes the Internet Explorer start and search pages, and sends AOL Instant Messenger information to a remote host. It may also display advertisements when the user is browsing the Web.