Department of Homeland Security
Information Analysis and Infrastructure Protection Directorate
CyberNotes

Issue #2003-15 *July 28, 2003*

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

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

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

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between July 8 and July 26, 2003. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
3Com[1]	Multiple	Office Connect DSL Router 812 1.1.7, 1.1.9, 2.0	A Denial of Service vulnerability exists when a malicious user submits an excessively long HTTP request.	No workaround or patch available at time of publishing.	3Com DSL Route Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[1] Bugtraq, July 23, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Apache Software Founda-tion[2]	Windows, OS2, Unix	Apache 1.3.1, 1.3.3, 1.3.4, 1.3.6, 1.3.9, 1.3.11, 1.3.12, 1.3.14, 1.3.17-1.3.20, 1.3.22-1.3.27	Multiple vulnerabilities exist: a vulnerability exists in the 'rotatelogs' support program because special control characters received over the pipe are not ignored, which could let a malicious user cause the program to quit logging; a Denial of Service vulnerability exists because a malicious user can make the server enter infinite loops; and a vulnerability exists because several file descriptors can be leaked to child processes, such as CGI scripts, which could let a malicious user obtain sensitive information.	Upgrades available at: http://httpd.apache.org/download.cgi Conectiva: ftp://atualizacoes.conectiva.com.br/	Apache HTTP Server Multiple Vulnerabilities CVE Name: CAN-2003-0460	Low/ Medium (Medium is sensitive informa-tion can be obtained)	Bug discussed in newsgroups and websites.
Apache Software Founda-tion[3, 4] ***More updates issued[5, 6]***	**Windows, MacOS X 10.x, Unix**	**Apache 2.0, 2.0.28, 2.0.32, 2.0.35-2.0.46**	**A remote Denial of Service vulnerability exists in the FTP proxy component when a target server that has an IPV6 address format is specified.**	**Apache Software Foundation: http://httpd.apache.org/download.cgi Trustix: ftp://ftp.trustix.net/pub/Trustix/updates/2.0/RPMS/** ***Conectiva:*** **ftp://atualizacoes.conectiva.com.br** ***Mandrake:*** **http://www.mandrakesecure.net/en/ftp.php**	**Apache Web Server FTP Remote Denial of Service CVE Name: CAN-2003-0254**	**Low**	**Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.**
Apache Software Founda-tion[7, 8] ***More updates issued[9, 10]***	**Windows, MacOS X 10.x, Unix**	**Apache 2.0, 2.0.28, 2.0.32, 2.0.35-2.0.46**	**A remote vulnerability exists when the 'SSLCipherSuite' directive is used to upgrade a cipher suite, which could cause a weaker cipher suite being used.**	**Apache Software Foundation: http://httpd.apache.org/download.cgi Trustix: ftp://ftp.trustix.net/pub/Trustix/updates/2.0/RPMS/** ***Conectiva:*** **ftp://atualizacoes.conectiva.com.br** ***Mandrake:*** **http://www.mandrakesecure.net/en/ftp.php**	**Apache Web Server SSLCipher Suite Weak Cipher Suite CVE Name: CAN-2003-0192**	**Medium**	**Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.**

[2] SecurityFocus, July 24, 2003.
[3] Apache Security Announcement, July 9, 2003.
[4] Trustix Secure Linux Security Advisory, 2003-0025, July 11, 2003.
[5] Conectiva Linux Security Announcement, CLA-2003:698, July 21, 2003.
[6] Mandrake Linux Security Update Advisory, MDKSA-2003:075, July 21, 2003.
[7] Apache Security Announcement, July 9, 2003.
[8] Trustix Secure Linux Security Advisory, 2003-0025, July 11, 2003.
[9] Conectiva Linux Security Announcement, CLA-2003:698, July 21, 2003.
[10] Mandrake Linux Security Update Advisory, MDKSA-2003:075, July 21, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Apache Software Founda-tion[11, 12] ***More updates issued[13, 14]***	**Windows, MacOS X 10.x, Unix**	**Apache 2.0, 2.0.28, 2.0.32, 2.0.35-2.0.46**	**A remote Denial of Service vulnerability exists in the prefork Multi-Processing Module (MPM).**	**Apache Software Foundation:** **http://httpd.apache.org/download.cgi** **Trustix:** **ftp://ftp.trustix.net/pub/Trustix/updates/2.0/RPMS/** ***Conectiva:*** **ftp://atualizacoes.conectiva.com.br** ***Mandrake:*** **http://www.mandrakesecure.net/en/ftp.php**	**Apache Web Server Prefork MPM Remote Denial of Service** **CVE Name: CAN-2003-0253**	**Low**	**Bug discussed in newsgroups and websites.** **Vulnerability has appeared in the press and other public media.**
Apple[15]	Windows, MacOS X	Darwin Streaming Server 4.1.3, Quicktime Streaming Server 4.1.3	Multiple vulnerabilities exist: a remote Denial of Service vulnerability exists when a malicious user requests a DOS device name; a remote Denial of Service vulnerability exists in the '/view_broadcast.cgi' script when requested without the appropriate parameters; a vulnerability exists in the 'parse_xml.cgi' administrative script, which could let a remote malicious user obtain sensitive information; an information disclosure vulnerability exists when certain characters are appended to the script name when making HTTP requests, which could let a remote malicious user obtain sensitive information; a Directory Traversal vulnerability exists, which could let a remote malicious user obtain sensitive information; a vulnerability exists in the 'Setup Assistant' page because the administrator password can be set to an arbitrary value if not already set, which could let a remote malicious user obtain sensitive information; and a remote Denial of Service vulnerability exists when a DOS device name is requested via a URL containing '../' directory traversal characters.	A fixed version (4.1.3g or later) of the Darwin Streaming Server is available at: http://developer.apple.com/darwin/projects/streaming/ This version reportedly fixes all vulnerabilities except for the 'parse_xml.cgi' script vulnerability.	Multiple QuickTime/ Darwin Streaming Server Vulnerabilities CVE Names: CAN-2003-0421, CAN-2003-0422, CAN-2003-0423, CAN-2003-0424, CAN-2003-0425, CAN-2003-0426, CAN-2003-04502	Low/ Medium (Medium if sensitive informa-tion can be obtained)	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.

[11] Apache Security Announcement, July 9, 2003.
[12] Trustix Secure Linux Security Advisory, 2003-0025, July 11, 2003.
[13] Conectiva Linux Security Announcement, CLA-2003:698, July 21, 2003.
[14] Mandrake Linux Security Update Advisory, MDKSA-2003:075, July 21, 2003.
[15] Rapid7, Inc. Security Advisory, R7-0015, July 23, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Apple[16]	MacOS X	MacOS X Server 10.2-10.2.6	A vulnerability exists because accounts are created without a password, which could let a remote malicious user obtain unauthorized access or elevated privileges.	Patches available at: http://docs.info.apple.com/article.html?artnum=120235	Mac OS X Server Workgroup Manager Insecure Account Creation CVE Name: CAN-2003-0601	Medium	Bug discussed in newsgroups and websites.
Application Foundry[17]	Windows	Message Foundry 2.75 .0003	Multiple vulnerabilities exist: a vulnerability exists in the 'NAME' input field because a value can be submitted that contains HTML and script code, which cold let a remote malicious user execute arbitrary code; a vulnerability exists because the administrative password is stored in plaintext, which could let a remote information; and a vulnerability exists because a remote malicious user my change another user's password if they are in the same public or private area of an affected site.	No workaround or patch available at time of publishing.	Message Foundry Multiple Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required.
Ashweb-studio[18]	Windows, Unix	Ashnews 0.83	A vulnerability exists due to lack of input validation in the 'ashnews.php' and 'ashheadlines.php' scripts, which could let a remote malicious user execute arbitrary PHP scripts.	No workaround or patch available at time of publishing.	Ashnews Remote Code Execution	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
ASP-DEV[19]	Windows	Discussion Forum 2.0	A vulnerability exists in the '/forum/admin/' page due to insufficient restrictions, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	ASP-DEV Discussion Forum Admin Directory	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
ASUS-TeK Computer Inc.[20]	Multiple	AAM6000 EV, AAM6330 BI	Several vulnerabilities exist due to an access control error when the integrated web server is enabled, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Asus ADSL Router Information Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.

[16] Apple Security Update, 2003-07-23 v.1.0, July 24, 2003.
[17] SecurityFocus, July 19, 2003.
[18] Secunia Security Advisory, July 23, 2003.
[19] Zone-h Security Team Advisory, ZH2003-4SA, July 12, 2003.
[20] SecurityTracker Alert ID, 1007196, July 14, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Atomic Board[21]	Unix	Atomic Board 0.6.2	A Directory Traversal vulnerability exists in the 'index.php' file, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	AtomicBoard Directory Traversal	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Blaze Board[22]	Windows, Unix	BlazeBoard 1.0 BETA	An information disclosure vulnerability exists because the directory that contains the installation script is insufficiently protected, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	BlazeBoard Information Disclosure	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Bosch IT-Consult-ing [23]	Windows, Unix	SimpNews 2.0.1, 2.13	A vulnerability exists due to an input validation errors in 'eventcal2.php' and 'eventscroller.php,' which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	SimpNews Remote File Include	**High**	Bug discussed in newsgroups and websites. Exploits have been published.
Brooky[24]	Windows, Unix	eStore 1.0.1, 1.0.2b, 1.0.2	Two vulnerabilities exist: a vulnerability exists in the 'login.php' script due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary code; and a path disclosure vulnerability exists in the 'settings.inc.php' script, which could let a remote malicious user obtain sensitive information.	Patch available at: http://www.brooky.com/community/index.php?act=ST&f=9&t=934	eStore SQL Injection & Path Disclosure	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required for the SQL Injection vulnerability. Proof of Concept exploit has been published for the path disclosure vulnerability.
cftp[25]	Unix	cftp 0.12	A buffer overflow vulnerability exists when 'Welcome' banner messages are parsed from remote FTP servers, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	cftp 'Welcome' Banner Parsing Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Christoph Roeder[26]	Windows, Unix	phpForum 2.0 RC1	A vulnerability exists in the 'Mainfile.php' script, which could let a remote malicious user execute arbitrary code.	Patch available at: http://www.phpmyforum.de/download.php?id=21	PHPForum Mainfile.PHP Remote File Include	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[21] Securiteam, July 22, 2003.
[22] Databugs Team Advisory, July 12, 2003.
[23] Bugtraq, July 15, 2003.
[24] 1ndonesian Security Team (1st) Advisory, July 17, 2003.
[25] Secunia Security Advisory, July 14, 2003.
[26] Theblacksheep&erik Advisory, July 11, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Cisco Systems[27] ***Cisco updates advisory***[28]	**Multiple**	**Catalyst 4000 Series including models 2948G & 2980G/2980G-A, 5000 Series including models 2901, 2902 & 2926, Catalyst 6000**	**A remote Denial of Service vulnerability exists when handling a non-standard combination of TCP flags.**	**Patches available at: http://www.cisco.com/warp/public/707/cisco-sa-20030709-swtcp.shtml** ***More patches available at:*** **http://www.cisco.com/warp/public/707/cisco-sa-20030709-swtcp.shtml**	**Cisco Catalyst Non-Standard TCP Flags Remote Denial of Service**	**Low**	**Bug discussed in newsgroups and websites. Vulnerability can be exploited with one of several free, publicly available network testing utilities.** **Vulnerability has appeared in the press and other public media.**
Cisco Systems[29, 30]	Multiple	IOS 11.x, 12.x	A remote Denial of Service vulnerability exists when a malicious user submits a sequence of specifically crafted IPV4 packets.	Patches and workarounds available at: http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml	Cisco IOS Malicious IPV4 Packet Sequence Denial of Service CVE Name: CAN-2003-0567	**High** **(High because IOS is a very widely deployed network operating system and vulner-ability is currently being exploited in the wild)**	Bug discussed in newsgroups and websites. Vulnerability can be exploited with utilities such as hping, so specific exploit code is not required to exploit this issue, however, exploit scripts have been published. Vulnerability has appeared in the press and other public media.

[27] Cisco Security Advisory 43864 Rev. 1, July 10, 2003.
[28] Cisco Security Advisory 43864 Rev. 1.3, July 15. 2003.
[29] Cisco Security Advisory, 44020 Rev. 1.9, July 22, 2003.
[30] DHS/FedCIRC Advisory, FA-2003-15, July 17, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
citadel.org [31]	Windows, Unix	Citadel/UX 5.90, 6.0 7	Multiple vulnerabilities exist: a buffer overflow vulnerability exists when configuration data that is supplied by an IPGM authenticated user is imported, which could let a remote malicious user execute arbitrary code; a Denial of Service vulnerability exists because the amount of Biography data that clients can supply is not limited; and a vulnerability exists due to a weak internal program authentication key, which could let a remote malicious user obtain unauthorized access.	Upgrades available at: http://www.citadel.org/download.php	Citadel/UX Multiple Vulnerabilities	Low/ Medium **High** **(Low if a DoS; Medium if unauth-orized access can be obtained; and High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Exploit script has been published for the buffer overflow and authentication vulnerabilities. There is no exploit code required for the Denial of Service vulnerability.
Corporate Web Solutions Ltd. [32]	Windows	.netCART	An information disclosure vulnerability exists in the default configuration due to inadequate protection of directory contents, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	.netCART Information Disclosure	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Cyber Shop ASP[33]	Windows	CyberShop ASP 6.0 Fx	A vulnerability exists because debugging scripts are insufficiently protected, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	CyberShop ASP Debugging Scripts Information Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Dan Bernstein [34]	Unix	qmail-smtpd-auth 0.31	A vulnerability exists when malformed authentication requests are received, which could let a remote malicious user circumvent e-mail authentication.	No workaround or patch available at time of publishing.	QMail-SMTPD-Auth E-Mail Authentication	Medium	Bug discussed in newsgroups and websites.
Deutsche Telekom[35]	Multiple	Teledat 530	A remote Denial of Service vulnerability exists when handling portscans.	No workaround or patch available at time of publishing.	Teledat DSL Router Portscan Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Vulnerability may be exploited with one of several freely available utilities.

[31] Security Vulnerability Advisory, CLIVITT-2003-4, July 15, 2003.
[32] Zone-h Security Team Advisory, ZH2003-9SA, July 17, 2003.
[33] Securiteam, July 14, 2003.
[34] Bugtraq, July 15, 2003.
[35] SecurityTracker Alert ID, 1007211, July 16, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Digi-FX[36]	Windows, Unix	Digi-Ads 1.1, Digi-News 1.1	A vulnerability exists in the 'admin.php' page due to a programming error, which could let a remote malicious user obtain administrative access.	Upgrades available at: http://www.digi-fx.net/freebies/digi-ads1.2.zip http://www.digi-fx.net/freebies/digi-news1.2.zip	Digi-FX 'admin.php' Authentication Logic	**High**	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Drupal[37]	Windows, Unix	Drupal 4.1.0, 4.2.0 RC	A Cross-Site Scripting vulnerability exists through the main page and other sub-pages, which could let a remote malicious user execute arbitrary HTML and script code.	Patch available at: http://drupal.org/node/view/68	Drupal Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Exploits have been published.
Easy Software Products[38] ***Vendors release patches***[39, 40, 41, 42, 43, 44,] ***Conectiva issues patches***[45]	**Unix**	**CUPS 1.1.17, 1.1.18**	**A remote Denial of Service vulnerability exists due to an insufficient time-out process for malicious HTTP requests.**	**Patch available at: http://www.cups.org/strfiles/75/cups-1.1.18-str75.patchv2** ***Debian:*** **http://security.debian.org/pool/updates/main/c/cupsys/** ***Mandrake:*** **http://www.mandrakesecure.net/en/ftp.php** ***RedHat:*** **ftp://updates.redhat.com** ***Slackware:*** **ftp://ftp.slackware.com/pub/slackware/** ***SuSE:*** **ftp://ftp.suse.com/pub/suse/** ***YellowDog:*** **ftp://ftp.yellowdoglinux.com/pub/yellowdog/updates/yellowdog-3.0/** ***Conectiva:*** **ftp://atualizacoes.conectiva.com.br/**	**CUPS Time-out Remote Denial of Service**	**Low**	**Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.**

[36] SecurityTracker Alert ID, 1007219, July 16, 2003.
[37] Securiteam, July 23, 2003.
[38] Turbolinux Security Advisory, TLSA-2003-33, May 20, 2003.
[39] Red Hat Security Advisory, RHSA-2003:171-01, May 27, 2003.
[40] Mandrake Linux Security Update Advisory, MDKSA-2003:062:, May 29, 2003.
[41] Slackware Security Advisory, May 29, 2003.
[42] Yellow Dog Linux Security Announcement, YDU-20030602-3, June 2, 2003.
[43] SuSE Security Announcement, SuSE-SA:2003:028, June 6, 2003.
[44] Debian Security Advisor, DSA 317-1, June 11, 2003.
[45] Conectiva Linux Security Announcement, CLA-2003:702, July 22, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
EJ3[46]	Windows, Unix	BlackBook 1.0	Multiple vulnerabilities exist: Cross-Site Scripting vulnerabilities exist in the 'sign.php' script due to insufficient filtering of script code from input fields, which could let a remote malicious user execute arbitrary code; a vulnerability exists in the 'config.php' file due to insecure password storage, which could let a remote malicious user obtain sensitive information; an information disclosure vulnerability exists in the 'phpinfo.php,' which could let a remote malicious user obtain sensitive information; a vulnerability exists because a common default username and password are used, which could let a malicious user obtain unauthorized access; and a vulnerability exists because messages are stored in the in the '/blackbook/data/data.dat' file with insufficient protection, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	BlackBook Multiple Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Cross-Site Scripting, information disclosure, and message storage vulnerabilities can be exploited via a web browser. There is no exploit code required for the password storage vulnerability.
fdclone[47]	Unix	fdclone 2.0 0a	A vulnerability exists due to the way temporary directories are created, which could let a malicious user obtain sensitive information.	**Debian:** http://security.debian.org/pool/updates/main/f/fdclone/	FDClone Insecure Temporary Directory Creation CVE Name: CAN-2003-0596	Medium	Bug discussed in newsgroups and websites.
Firestorm Corpora-tion[48]	Windows, Unix	Elite News 1.0, 1.0.3 Beta, 1.0.3	An authentication vulnerability exists in 'stats.php' script, which could let a remote malicious user obtain administrative access.	No workaround or patch available at time of publishing.	Elite News Administrative Authentication Bypass	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.

[46] Exploitlabs.com, EXPL-A-2003-015, July 12, 2003.
[47] Debian Security Advisory DSA 352-1, July 22, 2003.
[48] Zone-h Security Team Advisory, ZH2003-11SA, July 16, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
GeeOS Team Software[49]	Windows NT 4.0/2000, XP	Gattaca Server 2003 1.0.8.1	Multiple vulnerabilities exist: a vulnerability exists when sending a GET command that contains two slashes ("//"), which could let a remote malicious user obtain sensitive information; a remote Denial of Service vulnerability exists when a LLIST command of excessive length is submitted; a Directory Traversal vulnerability exists which could let a remote malicious user obtain sensitive information; and a Cross-Site Scripting vulnerability exists in the 'view2.tmpl' file, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Multiple Gattaca Server 2003 Vulnerabilities	Low/ Medium/ **High** **(Low if a DoS; Medium is sensitive informa-tion can be obtained; and High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required.
GNU[50]	Unix	GNATS 3.113.1_6	A buffer overflow vulnerability exists in the 'queue-pr' utility due to insufficient checking on the arguments to the '-d' commandline option, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	GNATS 'Queue-PR' Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
GNU[51]	Unix	GNU Privacy Guard 1.2.2 -r1	A vulnerability exists because gnupg is installed setgid root, which could let a malicious user corrupt critical or sensitive files, or cause a Denial of Service and possibly obtain elevated privileges.	Gentoo has addressed this issue. Updates can be applied with the following commands: emerge sync emerge gnupg emerge clean	GnuPG Group Root File Corruption	Low/ Medium (Medium if files can be corrupted or elevated privileges can be obtained)	Bug discussed in newsgroups and websites. There is no exploit code required.

[49] Security Corporation Security Advisory, SCSA-019], July 10, 2003.
[50] SecurityFocus, July 21, 2003.
[51] Gentoo Linux Security Announcement, 200307-06, July 19, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Hewlett Packard Company [52] ***HP updates bulletin*** [53]	**Unix**	**HP-UX 10.10, 10.16, 10.20, 10.24, 10.26, 10.30, 10.34, 11.04, 11.0, 11.11, 11.20, 11.22**	**A buffer overflow vulnerability exists in 'rexec' due to a boundary error, which could let a malicious user execute arbitrary code with root privileges.**	**HP has released a fix for HP-UX 11.00 available at: http://itrc.hp.com/ Users of HP-UX 10.10 systems, as a temporary measure, are advised to download and install libc.1.10.20 on affected systems which is available at: ftp://rexec:rexec@hprc.external.hp.com/ ftp://rexec:rexec@192.170.19.51/** ***More patches available at:*** **http://itrc.hp.com/**	**HP-UX RExec Buffer Overflow**	**High**	**Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.**
Hewlett Packard Company [54]	Unix	HP-UX 11.0, 11.11, 11.20, 11.22, 11.23	Two vulnerabilities exist: a vulnerability exists in the Java(TM) Runtime Environment, which could let untrusted Java applets potentially access information in trusted applets; and a vulnerability exists in the Java Plugin, which could let a malicious user obtain sensitive information.	Upgrades available at: www.hp.com/go/java	HP Java Runtime Environment & Java Plugin	Medium	Bug discussed in newsgroups and websites.
htmlto nuke[55]	Multiple	HTMLTo Nuke	A Cross-Site Scripting vulnerability exists in 'htmltonuke,php' due to an input validation error, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	HTMLToNuke Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Hum-mingbird, Ltd.[56]	Multiple	Exceed 5.0, 6.0.1, 6.0.2, 6.1, 7.1, 7.1.1, 8.0	A buffer overflow vulnerability exists in the 'XLoadQueryFont()' request when excessive data is submitted as a font name or when a malicious font name is passed from the server to the client, which could let a malicious user cause a Denial of Service and a remote malicious user possibly execute arbitrary code.	No workaround or patch available at time of publishing.	Exceed Font Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.

[52] Davide Del Vecchio Adv#5, April 25, 2003.
[53] Hewlett-Packard Company Security Bulletin, HPSBUX0304-257, July 22, 2003.
[54] Hewlett-Packard Company Security Bulletin, HPSBUX0307-268, July 16, 2003.
[55] Bugtraq, July 12, 2003.
[56] Securiteam, July 17, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
IBM[57]	Unix	UniVerse 10.0, .0.9	A vulnerability exists in the 'cci_dir' utility due to insecure file links, which could let a malicious user obtain root privileges.	No workaround or patch available at time of publishing.	UniVerse cci_dir Root Access	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
IBM[58]	Unix	UniVerse 10.0, .0.9	A buffer overflow vulnerability exists in the 'uvrestore' utility when handling command line options, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	UniVerse uvrestore Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
IBM[59]	Unix	UniVerse 10.0, .0.9	A buffer overflow vulnerability exists in the 'uvadmsh; utility when processing command line arguments, which could let a malicious user obtain root privileges.	No workaround or patch available at time of publishing.	UniVerse 'UVADMSH' Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
IglooFTP [60]	Unix	IglooFTP 0.6.1	A buffer overflow vulnerability exists when 'Welcome' banner messages are parsed from remote FTP servers, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	IglooFTP 'Welcome' Banner Parsing Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
IglooFTP [61] ***Another exploit released[62]***	**Windows**	**IglooFTP PRO 3.8**	**Multiple buffer overflow vulnerabilities exist due to insufficient checking performed on data that is copied into a reserved internal memory buffer, which could let a remote malicious user execute arbitrary code.**	**Upgrade available at: http://www.iglooftp.com/windows/IFTPPro39.exe**	**IglooFTP PRO Multiple Buffer Overflows**	**High**	**Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.** ***Exploit script has been published.***
Image Magick[63]	Unix	Image Magick 5.4.3	A format string vulnerability exists when the program is invoked with a filename that includes malicious format specifiers, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	ImageMagick Format String	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[57] Secure Network Operations, Inc. Advisory, SRT2003-07-07-0831, July 16, 2003.
[58] Secure Network Operations, Inc. Advisory, SRT2003-07-07-0913, July 16, 2003.
[59] Secure Network Operations, Inc. Advisory, SRT2003-07-07-0833, July 16, 2003.
[60] SecurityFocus, July 10, 2003.
[61] SecurityTracker Alert, 1007114, July 7, 2003.
[62] SecurityFocus, July 18, 2003.
[63] Rosiello Security's Advisory, July 14, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Infopop[64]	Unix	Ultimate Bulletin Board 5.0.x Beta, 5.4.7e, 5.43, 6.0 Beta, 6.0-6.0.3, 6.0.4 f, 6.2.0 Beta Release 1.0, 6.2.0,	A vulnerability exists due to insufficient sanitization of cookie data, which could let a remote malicious user execute arbitrary HTML code.	No workaround or patch available at time of publishing.	Ultimate Bulletin Board Cookie HTML Injection	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Invision Power Services[65]	Windows, Unix	Invision Board 1.0-1.1.2	Multiple vulnerabilities exist: a vulnerability exists in the 'index.php' and 'edit.php' scripts due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary code; and Cross-Site Scripting vulnerabilities exist in the 'post.php' and 'ipchat.php' scripts due to insufficient validation of user-supplied input, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Invision Power Board Multiple Vulnerabilities	**High**	Bug discussed in newsgroups and websites. Vulnerabilities can be exploited via a web browser.
Look Smart, Ltd[66]	Windows	Grub 1.3.7	A vulnerability exists because passwords and user names are stored in cleartext, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Grub Clear Text Password Local Storage	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Mabry Software[67]	Windows	HTTP SERVER/ X 1.0 0.047	A Directory Traversal vulnerability exists due to insufficient validation of user-supplied input, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	HTTPServer/X File Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser, however exploits have been published.

[64] Bugtraq, July 16, 2003.
[65] Bugtraq, July 11, 2003.
[66] Exploitlabs.com, EXPL-A-2003-016, July 13, 2003.
[67] SecurityFocus, July 11, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Mail System[68]	Multiple	Mail System 0.9 Beta	Two vulnerabilities exist: a vulnerability exists in the 'message.mdb' database file due to an access control error, which could let a remote malicious user obtain sensitive information; and an input validation vulnerability exists during the login process, which could let a remote malicious user bypass authentication.	No workaround or patch available at time of publishing.	Mail System Database Access & Input Validation	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Marc Druilhe[69]	Windows, Unix	W-Agora 4.1.5	Multiple vulnerabilities exist: a vulnerability exists in the 'index.php' script, which could let a remote malicious user obtain sensitive information; a vulnerability exists in the 'modules.php' script, which could let a remote malicious user obtain sensitive information; a vulnerability exists in the 'insert.php' script if the administrator has not protected the upload directory, which could let a remote malicious user execute arbitrary code; a vulnerability exists in the 'index.php' script, which could let a remote malicious user execute arbitrary code; and an input validation vulnerability exists in the 'profile.php' script, which could let a remote malicious user execute arbitrary code.	Patches available at: http://cvs.sourceforge.net/cgi-bin/viewcvs.cgi/*checkout*/w-agora/w-agora4/	W-Agora Multiple Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Vulnerabilities can be exploited via a web browser.
Microsoft [70]	Windows 2000	Exchange Server 2000, SP1&SP2, Windows 2000 Server SP2&SP3	A remote Denial of Service vulnerability exists on the SMTP Service when a malicious user submits an e-mail message with a corrupt time stamp.	Upgrade available at: http://www.microsoft.com/windows2000/downloads/servicepacks/sp4/default.asp	Microsoft SMTP Service Remote Denial of Service	Low	Bug discussed in newsgroups and websites.
Microsoft [71]	Windows 2000	Internet Security and Accelera-tion (ISA) Server 2000, FP1, SP1	A Cross-Site Scripting vulnerability exists because some of the error pages returned by the ISA Server display the requested URL in HTML text without proper encoding, which could let a malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-028.asp	ISA Server Cross-Site Scripting CVE Name: CAN-2003-0526	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[68] Zone-h Security Team Advisory, ZH2003-10SA, July 16, 2003.
[69] Bugtraq, July 11, 2003.
[70] Microsoft Knowledge Base Article 330716, July 15, 2003.
[71] Microsoft Security Bulletin, MS03-028 V1.1, July 16, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [72]	Windows XP	Windows XP 64-bit Edition, SP1, XP Home, SP1, XP Profes-sional, SP1	A buffer overflow vulnerability exists in the 'Desktop.ini' file due to insufficient bounds checking in the code that reads and applies folder attributes, which could let a malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-027.asp	Windows XP Desktop.ini Buffer Overflow CVE Name: CAN-2003-0351	**High**	Bug discussed in newsgroups and websites.
Microsoft [73]	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.	No workaround or patch available at time of publishing.	Media Player IE Zone Access Control Bypass	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[72] Microsoft Security Bulletin, MS03-027 V1.1, July 17, 2003.
[73] SecurityTracker Alert ID, 1007287, July 24, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [74] ***Exploit script released*** [75]	**Windows NT 4.0/2000, XP**	**Windows 2000 Advanced Server, SP1-SP3, 2000 Datacenter Server, SP1-SP3, 2000 Profes-sional, SP1-SP3, 2000 Server, SP1-SP3, 2000 Terminal Services, SP1-SP3**	**A vulnerability exists because named pipes are not properly handled through the 'CreateFile' API, which could let a malicious user obtain elevated privileges.**	**Upgrade available at: http://www.microsoft.com/windows2000/downloads/servicepacks/sp4/default.asp**	**Windows CreateFile API Named Pipe Privilege Escalation** **CVE Name: CAN-2003-0496**	**Medium**	**Bug discussed in newsgroups and websites. Exploit has been published.** ***Exploit script has been published.***
Microsoft [76]	Windows 2000	Windows 2000 Advanced Server, SP1-SP4, 2000 Datacenter Server, SP1-SP4, 2000 Profes-sional, SP1-SP4, 2000 Server, SP1-SP4,	A remote Denial of Service vulnerability exists in the RPC service when a malicious user submits a malformed packet to TCP port 135.	No workaround or patch available at time of publishing.	Windows 2000 RPC Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
Microsoft [77] ***Exploit script has been published*** [78] ***Another exploit published*** [79]	**Windows 2000**	**Windows 2000 Advanced Server, SP1-SP4, 2000 Datacenter Server, SP1- SP4, 2000 Server, SP1- SP4**	**A buffer overflow vulnerability exists in the way 'nsiislog.dll' processes incoming client requests, 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/MS03-022.asp**	**Windows Media Services NSIISlog.DLL Remote Buffer Overflow** **CVE Name: CAN-2003-0349**	**High**	**Bug discussed in newsgroups and websites.** ***Exploit script has been published.*** ***Another exploit script published.***

[74] @stake, Inc. Security Advisory, July 8, 2003.
[75] Bugtraq, July 14, 2003.
[76] Bugtraq, July 20, 2003.
[77] Microsoft Security Bulletin, MS03-022, June 25, 2003.
[78] SecurityFocus, July 9, 2003.
[79] SecurityFocus, July 18, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [80, 81]	Windows NT 4.0/2000, 2003, XP	Windows 2000 Advanced Server, SP1-SP4, 2000 Datacenter Server, SP1-SP4, 2000 Profes-sional, 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 Work-station 4.0, SP1-SP6a, Server 2003 Datacenter Edition, 64-bit, 2003 Enterprise Edition, 64-bit, Server 2003 Standard Edition, Server 2003 Web Edition, Windows XP 64-bit Edition, SP1, XP Home, SP1, XP Profes-sional, SP1	A buffer overflow vulnerability exists in the RPC interface that implements the Distributed Component Object Model services (DCOM) due to insufficient bounds checking of client DCOM object activation requests, which could let a malicious user install programs, view, change or delete data, create new accounts with full privileges or execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-026.asp	Windows DCOM RPC Buffer Overflow CVE Name: CAN-2003-0352	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.

[80] Microsoft Security Bulletin, MS03-026 V1.2, July 21, 2003.
[81] Department of Homeland Security Advisory, July 24, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [82]	Windows 98/ME/NT 4.0/2000, XP, 2003	DirectX 5.2, 6.1, 7.0a, 7.0, 8.1, 9.0 a	Two buffer overflow vulnerabilities exists in the function used by DirectShow to check parameters in a Musical Instrument Digital Interface (MIDI) file, which could let a malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-030.asp	DirectShow MIDI Filetype Buffer Overflows CVE Name: CAN-2003-0346	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Microsoft [83]	Windows 95/98/ME/ NT 4.0/2000, 2003	Internet Explorer 5.5, SP1&SP2, 6.0, SP1	A vulnerability exists in the 'window.createPopup()' function due to the use of 'chromeless' windows, which could let a remote malicious user create fake or modified user interfaces on the target user's system.	No workaround or patch available at time of publishing.	Internet Explorer window.create Popup 'chromeless' Window	Medium	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.
Microsoft [84]	Windows XP	MySQL AB ODBC Driver 3.51	A vulnerability exists in the ODBC (Open Data Base Connectivity) driver implementation because credentials are stored in plaintext, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	MySQL AB ODBC Driver Plain Text Password	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Microsoft [85]	Windows NT	Windows NT Enterprise Server 4.0, SP1-SP6a, NT Server 4.0, SP1-SP6a, NT Terminal Server 4.0, SP1-SP6	A remote Denial of Service vulnerability exists in the 'GetCanonicalPath()' function because memory that the function does not own can be freed when a specially crafted request is submitted, which could let a malicious user cause a Denial of Service and possibly 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/MS03-029.asp	Windows NT File Management Function Remote Denial of Service CVE Name: CAN-2003-0525	Low	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Microsoft [86]	Windows 98/ME/ NT 4.0/2000, 2003	Internet Explorer 6.0, SP1,	A vulnerability exists due to the way the AutoScan method is implemented, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Internet Explorer AutoScan Method	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Microsoft [87]	Windows NT	MSN Messenger Service 6.0	A remote Denial of Service vulnerability exists when a malicious user submits several malformed image files through a file transfer.	No workaround or patch available at time of publishing.	MSN Messenger Denial of Service	Low	Bug discussed in newsgroups and websites.

[82] Microsoft Security Bulletin, MS03-030, July 23, 2003.
[83] Bugtraq, July 13, 2003.
[84] Bugtraq, July 22, 2003.
[85] Microsoft Security Bulletin, 03-029, July 23, 2003.
[86] Bugtraq, July 12, 2003.
[87] Securiteam, July 20, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [88]	Windows 2003	IIS 6.0	Multiple vulnerabilities exist in the web admin interface; Cross-Site Scripting vulnerabilities exist in the 'ReturnURL' parameter due to insufficient filtering, which could let a remote malicious user execute arbitrary code; a vulnerability exists because valid session IDs can be exposed, which could let a remote malicious user obtain sensitive information or obtain unauthorized access; and a vulnerability exists in the 'users/user_set password.asp' script because it is possible to change the password of the currently logged user.	No workaround or patch available at time of publishing.	Multiple IIS 6.0 Web Admin	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required.
Microsoft [89]	Windows NT 4.0/2000, XP, 2003	Data Engine 1.0, SQL Server 7.0, SP1-SP4, SQL Server 2000, SP1-SP3a, SQL Server 2000 Desktop Engine	Multiple vulnerabilities exist: a vulnerability exists due to a flaw in the method used to check for named pipes, which could let a malicious user hijack a named pipe to obtain elevated privileges; a local/remote Denial of Service vulnerability exists when a malicious user submits a specially crafted large packet to a specific named pipe; and a buffer overflow vulnerability exists in the listening local procedure call (LPC) port of the system, 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/MS03-031.asp	SQL Server / MSDE Multiple Vulnerabilities CVE Names: CAN-2003-0230, CAN-2003-0231, CAN-2003-0232	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Mobydisk [90]	Windows NT	Moby Netsuite 1.0, 1.2	A Directory Traversal vulnerability exists in the HTTP component due to an input validation error, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	NetSuite HTTP Server Directory Traversal	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
more groupware [91]	Windows, Unix	moregroup ware 0.6.8	A vulnerability exists in 'WEBMAIL2_INC_DIR' because the include path for several configuration scripts may be influenced, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	MoreGroup Ware Remote File Include	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[88] Bugtraq, July 22, 2003.
[89] Microsoft Security Bulletin, MS03-031 V1.1, July 24, 203.
[90] Securiteam, July 17, 2003.
[91] SecurityFocus, July 23, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[92]	Unix	Linux kernel 2.4.0-test1-2.4.0-test12, 2.4-2.4.17, 2.4.18, 2.4.18 x86, 2.4.18 pre-1-2.4.18 pre-8, 2.4.19, 2.4.19 - pre1-2.4.19 – pre6, 2.4.20, 2.4.21, 2.4.21 pre1, 2.4.21 pre4	Multiple vulnerabilities exist: an information disclosure vulnerability exists due to a flaw in '/proc/tty/driver/serial,' which could let a malicious user obtain sensitive information; a Denial of Service vulnerability exists due to a race condition in the execve() system call; an access control vulnerability exists because a malicious user can bind services to UDP ports that have already been allocated; an access control vulnerability exists in the 'execve()' because the file descriptor of an executable process is recorded in the calling process's file table, which could let a malicious user obtain sensitive information; a vulnerability exists in the '/proc' filesystem, which could let a malicious user obtain sensitive information; a remote Denial of Service vulnerability exists in the Spanning Tree Protocol (STP) implementation due to insufficient validation of user-supplied input; a vulnerability exists because the bridge topology can be modified due to the inherent insecurity of the STP protocol, which could let a remote malicious user modify information; and a vulnerability exists in the forwarding table, which could let a remote malicious user spoof packets.	**RedHat:** ftp://updates.redhat.com/	Multiple Linux 2.4 Kernel Vulnerabilities CVE Names: CAN-2003-0461, CAN-2003-0462, CAN-2003-0464, CAN-2003-0476, CAN-2003-0501, CAN-2003-0550, CAN-2003-0551, CAN-2003-0552	Low/ Medium (Medium if sensitive informa-tion can be obtained or elevated privileges are obtained)	Bug discussed in newsgroups and websites.

[92] Red Hat Security Advisory, RHSA-2003:238-01, July 21, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [93, 94, 95] ***More updates issued*** [96, 97, 98, 99] ***More updates issued*** [100, 101] ***Conectiva issues patches*** [102]	**MacOS X 10.2, Unix**	**Apple MacOS X 10.2 (Jaguar), 10.2.2; Easy Software Products CUPS 1.0.4, 1.0.4–8, 1.1.1, 1.1.4-5, 1.1.4-3, 1.1.4-2, 1.1.4, 1.1.6, 1.1.7, 1.1.10, 1.1.12-1.1.15, 1.1.17**	**Several vulnerabilities exist: vulnerability exists in the HTTP server component of the Common UNIX Printing System (CUPS), which could let a local/remote malicious user obtain root privileges; a race condition exists in the creation of /etc/cups/certs/<pid>, which could let a malicious user create or overwrite any file as root; a vulnerability exists because printers can remotely be added to CUPS by sending a specially crafted UDP packet; a remote Denial of Service vulnerability exits due to negative length memcpy() calls; an integer overflow vulnerability exists in the image handling code, which could let a malicious user obtain elevated privileges; a buffer overflow vulnerability exists in the strncat function call in the setup of the 'options' string, which could let a malicious user obtain root access; a vulnerability exists because CUPS improperly checks for zero width images in filters/image-gif.c, which could let a malicious user execute arbitrary code; and a vulnerability exists because the return values of many file and socket operations are not checked, which could let a malicious user cause a Denial of Service.** ***Debian issues update that corrects a library dependency for the libcupsys2 package.***	**Apple:** **http://www.info.apple.cpm/kbnum/** **Easy Software:** **http://www.cups.org/software.html** **SuSE:** **ftp://ftp.suse.com/pub/suse** ***SCO:*** **ftp://ftp.sco.com/pub/updates/OpenLinux/** ***Debian:*** **http://security.debian.org/pool/updates/main/c/cupsys/** ***Mandrake:*** **http://www.mandrakesecure.net/en/ftp.php** ***RedHat:*** **ftp://updates.redhat.com** ***Debian:*** **http://security.debian.org/pool/updates/main/c/cupsys** ***Information regarding Apple updates available at:*** http://docs.info.apple.com/article.html?artnum=61798 ***Conectiva:*** **ftp://atualizacoes.conectiva.com.br/**	**CUPS HTTP Multiple Vulnerabil-ities** **CVE Names: CAN-2002-1366, CAN-2002-1367, CAN-2002-1368, CAN-2002-1369, CAN-2002-1371, CAN-2002-1372, CAN-2002-1383, CAN-2002-1384**	**Low/High** **(High if root access can be obtained or arbitrary code can be executed)**	**Bug discussed in newsgroups and websites. Exploits have been published.**

[93] iDEFENSE Security Advisory, December 19, 2002.
[94] Gentoo Linux Security Announcement, 200212-13, December 29, 2002.
[95] SuSE Security Announcement, SuSE-SA:2003:002, January 2, 2003.
[96] SCO Security Advisory, CSSA-2003-004.0, January 21, 2003.
[97] Debian Security Advisory, DSA 232-1, January 20, 2003.
[98] Mandrake Linux Security Update Advisory, MDKSA-2003:001, January 10, 2003.
[99] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:295-07, January 13, 2003.
[100] Debian Security Advisory, DSA 232-2, February 20, 2003.
[101] Apple Security Updates, 61798, February 14, 2003.
[102] Conectiva Linux Security Announcement, CLA-2003:702, July 22, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[103, 104] ***More vendors release upgrades***[105] ***More vendors release upgrades***[106, 107] ***HP updates bulletin***[108]	**Unix**	**Cray UNICOS 6.0, 6.0 E, 6.1, 7.0, 8.0, 8.3, 9.0, 9.0.2.5, 9.2, 9.2.4; FreeBSD 4.0- 4.6, 4.7, 5.0, 4.1.1–4.7 Stable & Release; GNU glibc 2.1-2.1.3, 2.2-2.2.5, 2.3-2.3.2; HP HP-UX 10.20 Series 700 & 800, 10.20, 10.24, 11.04, 11.0, 11.11, 11.20, 11.22; IBM AIX 4.3.3, 5.1, 5.2; MIT Kerberos 5 1.2-1.2.7; OpenAFS 1.0-1.3.2; OpenBSD 2.0-3.2; SGI IRIX 6.5-6.5.20, 6.5m-6.5.20m, 6.5f-6.5.20f; Sun Solaris 2.5.1, 2.5.1_x86, 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86,, 9.0, 9.0_x86**	**An integer overflow vulnerability exists in the xdrmem_getbytes() function that is distributed as part of the Sun Microsystems XDR library, which could let a remote malicious user execute arbitrary code.**	**FreeBSD:** **ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-03:05/xdr-4.patch** **SCO:** **ftp://ftp.sco.com/pub/updates/OpenLinux/** **MIT:** **http://web.mit.edu/kerberos/www/advisories/2003-003-xdr_patch.txt** **RedHat:** **ftp://updates.redhat.com/** **IBM:** **http://techsupport.services.ibm.com/r** **FreeBSD:** **ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-03:05/xdr-4.patch** ***Debian:*** **http://security.debian.org/pool/updates/main/o/openssh-krb5/** ***Mandrake:*** **http://www.mandrakesecure.net/en/ftp.php** ***NetBSD:*** **ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2003-008.txt.asc** ***Trustix:*** **http://www.trustix.net/pub/Trustix/updates/** ***Immunix:*** **http://download.immunix.org/ImmunixOS/7+/Updates/RPMS/** ***Conectiva:*** **ftp://atualizacoes.conectiva.com.br/** ***Hewlett Packard:*** **http://itrc.hp.com/**	**Sun XDR Library xdrmem_getbytes() Integer Overflow** **CVE Name: CAN-2003-0028**	**High**	**Bug discussed in newsgroups and websites.**

[103] eEye Security Advisory, AD20030318, March 19, 2003.
[104] CERT® Advisory, CA-2003-10, March 19, 2003.
[105] SecurityFocus, April 2, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [109, 110, 111, 112] ***More patches released*** [113]	**Unix**	**Mandrake Soft Corporate Server 2.1, Linux Mandrake 8.2, ppc, 9.0; Terra Soft Solutions Yellow Dog Linux 2.3, 3.0; ypserv ypserv 1.3.11, 1.3.12, 2.2, 2.5-2.7**	**A Denial of Service vulnerability exists in the Network Information Service (NIS) server when a malicious user queries ypserv via TCP and subsequently ignores the server's response.**	**Ypserv:** **ftp://ftp.kernel.org/pub/linux/utils/net/NIS/ypserv-2.8.tar.gz** **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** **RedHat:** **ftp://updates.redhat.com/** **Sun:** **http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F55600** **YellowDog:** **ftp://ftp.yellowdoglinux.com/pub/yellowdog/updates/** ***Sun:*** **http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F55600**	**Multiple Vendor YPSERV Denial of Service** **CVE Name: CAN-2003-0251**	**Low**	**Bug discussed in newsgroups and websites.**
Neo-modus[114]	Windows NT 4.0	Direct Connect 1.0	A remote Denial of Service vulnerability exists due to an error when handling multiple requests from the same client.	No workaround or patch available at time of publishing.	Direct Connect Remote Denial of Service	Low	Bug discussed in newsgroups and websites.
Net Screen Technolo-gies[115]	Multiple	ScreenOS 3.x, 4.x	A vulnerability exists when operating in Bridge Mode because any non-IP or ARP traffic will bypass the firewall without being logged, which could let a remote malicious user bypass security restrictions.	The vendor plans to issue maintenance releases to ScreenOS 4.0.1 and 4.0.3 the week of July 14.	NetScreen Non-IP Traffic Firewall Bypass	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Netscape [116]	Windows	Navigator 7.0 2	A buffer overflow vulnerability exists in the Client Detection Tool plug-in due to a boundary error, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Netscape Client Detection Tool Plug-In Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[106] Immunix Secured OS Security Advisory, IMNX-2003-7+-009-01, April 15, 2003.
[107] Conectiva Linux Security Announcement, CLA-2003:633, April 30, 2003.
[108] Hewlett-Packard Company Security Bulletin, HPSBUX0303-252, July 22, 2003.
[109] Red Hat Security Advisory RHSA-2003:173-01, June 25, 2003.
[110] Mandrake Linux Security Update Advisory, MDKSA-2003:072, June 27, 2003.
[111] Yellow Dog Linux Security Announcement, YDU-20030627-1, June 27, 2003.
[112] Sun(sm) Alert Notification, 55600, July 2, 2003.
[113] Sun(sm) Alert Notification, 55600, July 25, 2003.
[114] Sec-labs Team Advisory, July 14, 2003.
[115] SecurityTracker Alert ID, 1007148, July 9, 2003.
[116] Bugtraq, July 14, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
nfs[117, 118, 119, 120, 121, 122, 123, 124]	Unix	nfs-utils 0.2, 0.2.1, 0.3.1, 0.3.3, 1.0, 1.0.1, 1.0.3	A buffer overflow vulnerability exists due to a boundary error (off-by-one) in the "xlog()" function when adding missing trailing newlines to a logged string, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code.	Upgrade available at: http://sourceforge.net/project/showfiles.php?group_id=14&release_id=171379 **Conectiva:** ftp://atualizacoes.conectiva.com.br/ **Debian:** http://security.debian.org/pool/updates/main/n/nfs-utils/ **Immunix:** http://download.immunix.org/ImmunixOS/7+/Updates/RPMS/nfs-utils-0.3.1-7_imnx_3.i386.rpm **Mandrake:** http://www.mandrakesecure.net/en/ftp.php **RedHat:** ftp://updates.redhat.com/ **Slackware:** ftp://ftp.slackware.com/pub/slackware/ **SuSE:** ftp://ftp.suse.com/pub/suse/ **Trustix:** ftp://ftp.trustix.net/pub/Trustix/updates/	NFS-Utils Xlog Remote Buffer Overflow CVE Name: CAN-2003-0252	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
Novell, Inc.[125]	Multiple	Netware 5.1, SP4&SP6, 6.0, SP1&SP2	A buffer overflow vulnerability exists in the 'cgi2perl.nlm' module due to insufficient bounds checking, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code.	Patches available at: http://support.novell.com/cgi-bin/search/searchtid.cgi?/2966549.htm	Netware Enterprise Web Server Remote Buffer Overflow CVE Name: CAN-2003-0562	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Opera Software[126]	Multiple	Opera Web Browser 7.20 Beta 1 build 2981	A vulnerability exists in the in the M2 mail client because it is possible to circumvent the option that suppresses viewing of external embeds, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Opera Client Policy Circumvention	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[117] Debian Security Advisory, DSA 349-1, July 14, 2003.
[118] Red Hat Security Advisory, RHSA-2003:206-01, July 14, 2003.
[119] Slackware Security Advisory, SSA:2003-195-01, July 15, 2003.
[120] Immunix Secured OS Security Advisory, IMNX-2003-7+-018-01, July 15, 2003.
[121] Trustix Secure Linux Security Advisory, TSLSA-2003-0027, July 18, 2003.
[122] SuSE Security Announcement, SuSE-SA:2003:031, July 16, 2003.
[123] Mandrake Linux Security Update Advisory, MDKSA-2003:076, July 21, 2003.
[124] Conectiva Linux Security Announcement, CLA-2003:700, July 22, 2003.
[125] Novell Security Alert, NOVL-2003-2966549, July 23, 2003.
[126] Bugtraq, July 23, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Oracle Corporation[127]	Windows NT 4.0/2000, XP, Unix, OpenVMS	Oracle9i Release 2; Oracle9i Release 1 Oracle8i (8.1.x all releases)	Several buffer overflow vulnerabilities exist in the 'EXTPROC' application, which could let a remote malicious user execute arbitrary code.	Patches available at: http://metalink.oracle.com.	Oracle Database Server EXTPROC Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Oracle Corporation[128]	Windows NT 4.0/2000, XP, Unix, OpenVMS	Applications 10.7, 11.0, E-Business Suite 11i 11.1-11.8	An information disclosure vulnerability exists because certain JSP scripts can be accessed, which could let a remote malicious user obtain sensitive information.	Patches available at: http://metalink.oracle.com patch number 2939083	AOL/J Setup Test Suite Information Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Oracle Corporation[129]	Windows NT 4.0/2000, XP, Unix, OpenVMS	Applications 10.7, 11.0, E-Business Suite 11i 11.1-11.8	A buffer overflow vulnerability exists in the 'FNDWRR.CGI' program, which could let a remote malicious user execute arbitrary code.	Patches available at: http://metalink.oracle.com.	Oracle Applications 'FNDWRR CGI' Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
PHP[130]	Unix	PHP 4.3, 4.3.1, 4.3.2	A vulnerability exists when the 'safe_mode"include_dir' PHP directive is not defined, which could let a remote malicious user obtain unauthorized access or bypass safemode.	No workaround or patch available at time of publishing.	PHP Safe_Mode_ Include_Dir Bypass	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
PHP Group Ware[131] ***Patches now available*** [132, 133]	**Windows, Unix**	**PHPGroupWare 0.9.14 .003**	**Multiple Cross-Site Scripting vulnerabilities exist in the form fields due to insufficient input validation, which could let a remote malicious user execute arbitrary HTML and script code.**	***Patches available at:*** **http://www.phpgroupware.org/downloads/** ***Conectiva:*** **ftp://atualizacoes.conectiva.com.br** ***Mandrake:*** **http://www.mandrakesecure.net/en/ftp.php**	**Multiple PHPGroup Ware HTML Injection**	**High**	**Bug discussed in newsgroups and websites. There is no exploit code required.**

[127] NGSSoftware Insight Security Research Advisory, #NISR25072003, July 25, 2003.
[128] Oracle Security Alert 55, July 23, 2003.
[129] Oracle Security Alert 56, July 23, 2003.
[130] Bugtraq, July 16, 2003.
[131] Kereval Security Advisory, KSA-003, July 2, 2003.
[132] Conectiva Linux Security Announcement, CLA-2003:697, July 16, 2003.
[133] Mandrake Linux Security Update Advisory, MDKSA-2003:077, July 23, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
PHP Group Ware[134, 135]	Unix	PHPGroup Ware 0.9.12, 0.9.13, 0.9.14 .005, 0.9.14 .003	A vulnerability exists because a parameter used to include files isn't verified before it is used, which could let a remote malicious user execute arbitrary code.	**PHPGroupWare:** http://www.phpgroupware.org/downloads/ **Conectiva:** ftp://atualizacoes.conectiva.com.br/ **Mandrake:** http://www.mandrakesecure.net/en/ftp.php	PHPGroupWare Unspecified Remote File Include	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Polycom[136]	Multiple	MGC-100, MGC-25 5.51.21, 5.51.211, MGC-50	A remote Denial of Service vulnerability exists in the administrative interface when multiple packets are submitted to the service (port 5003/tcp).	No workaround or patch available at time of publishing.	Polycom MGC Systems Remote Administration Denial Of Service	Low	Bug discussed in newsgroups and websites. Vulnerability may be exploited with one of several freely available utilities.
RAV[137]	Windows	RAV AntiVirus Online Virus Scan	A buffer overflow vulnerability exists in the 'ravonline.dll' file, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	RAV AntiVirus Online Virus Scan Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Savant[138]	Windows	Savant Webserver 3.1	Multiple vulnerabilities exist: a Cross-Site Scripting vulnerability exists in the 'cgitest.html' script due to insufficient sanitization of user-supplied data, which could let a remote malicious user execute arbitrary HTML and script code; a remote Denial of Service vulnerability exists when a malicious user creates numerous connections from the same originating host to; and a remote Denial of Service vulnerability exists when a malicious user submits a HTTP request of excessive length.	No workaround or patch available at time of publishing.	Savant Web Server Multiple Vulnerabilities	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proof of Concept exploits have been published for the Cross-Site Scripting & Denial of Service vulnerabilities.
SCO[139]	Unix	Open Server 5.0.6, 5.0.7	A vulnerability exists in the display program, which could let a malicious user obtain elevated privileges.	Patches available at: http://www.sco.com/download	OpenServer Elevated Privileges	Medium	Bug discussed in newsgroups and websites.

[134] Mandrake Linux Security Update Advisory, MDKSA-2003:077, July 23, 2003.
[135] Conectiva Linux Security Announcement, CLA-2003:703, July 23, 2003.
[136] Exploitlabs.com Advisory, EXPL-A-2003-014, July 12, 2003.
[137] Securiteam, July 20, 2003.
[138] SecurityTracker Alert ID, 1007232, July 21, 2003.
[139] SCO Security Advisory, CSSA-2003-SCO.11, July 22, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
SGI[140]	Unix	IRIX 6.5-6.5.20	A vulnerability exists due to an error in '/usr/lib/iaf/scheme' when a user logs in and certain environment variables are set, which could let a malicious user execute arbitrary code with root privileges.	Upgrade available at: ftp://patches.sgi.com/support/free/security/patches/	IRIX Scheme Login Privilege Escalation CVE Name: CAN-2003-0574	**High**	Bug discussed in newsgroups and websites.
SGI[141]	Unix	IRIX 6.5-6.5.20	Multiple vulnerabilities exist: a remote Denial of Service vulnerability exists on the nsd service by performing a UDP portscanning on a NIS master; a vulnerability exists because group entries in "/etc/group" are not ignored, which could let a malicious user obtain sensitive information; a Denial of Service vulnerability exists when a malicious user submits a specially crafted dynamic table; and a vulnerability exists because DNS callbacks are not sanitized properly, which could let a remote malicious user cause a Denial of Service.	Upgrade available at: ftp://patches.sgi.com/support/free/security/patches/	IRIX Multiple Name Service Daemon CVE Names: CAN-2003-0176, CAN-2003-0177, CAN-2003-0572, CAN-2003-0573	Low/ Medium (Medium if sensitive informa-tion can be obtained)	Bug discussed in newsgroups and websites.
Sierra Entertain-ment, Inc.[142]	Windows	StarSeige Tribes	A remote Denial of Service vulnerability exists when malformed UDP datagrams are received and processed.	No workaround or patch available at time of publishing.	StarSiege Tribes Server Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Proofs of Concept exploit scripts have been published.
Splatt.it [143]	Windows, Unix	Splatt Forum 3.0-3.2, 4.0, 4.1.1	A Cross-Site Scripting vulnerability exists due to insufficient filtering of icon images, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Splatt Forum Post Icon Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
Sun Micro-systems, Inc.[144]	Unix	Solaris 8.0	A remote Denial of Service vulnerability exists due to a failure to handle certain IPv6 packets.	Patch and workaround information available at: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F55301	Solaris Pv6 Packet Remote Denial of Service	Low	Bug discussed in newsgroups and websites.

[140] SGI Security Advisory, 20030702-01-P, July 16, 2003.
[141] SGI Security Advisory, 20030701-01-P, July 16, 2003.
[142] Bugtraq, July 14, 2003.
[143] Bugtraq, July 15, 2003.
[144] Sun(sm) Alert Notification, 55301, July 21, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Sun Micro-systems, Inc.[145]	Unix	Solaris 8.0	A Denial of Service vulnerability exists in 'automountd' due to errors in patches 108993-14 through 108993-19 and 108994-14 through 108994-19.	Patch and workaround information available at: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F55340	Solaris 'automountd' Denial of Service	Low	Bug discussed in newsgroups and websites.
Surf Control[146]	Multiple	E-Mail Filter for SMTP 4.6	A vulnerability exists because the rules engine contains a flaw if an attachment is a .zip file and it contains more than 15 zip files, the 16th zip file will not be scanned by the filter, which could let a remote malicious user bypass security restrictions.	No workaround or patch available at time of publishing.	E-Mail Filter Nested Zip File Filter Bypass	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Tolis Group[147]	Unix	BRU 17.0	A vulnerability exists due to a failure to properly parse commandline arguments, which could let a malicious user obtain root access.	No workaround or patch available at time of publishing.	BRU Improper Command-line Parsing	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Trend Micro[148]	Multiple	Damage Cleanup Server 1.0, HouseCall 5.5, 5.7	Multiple buffer overflow vulnerabilities exist due to a boundary error in the ActiveX control, which could let a remote malicious user, cause a Denial of Service or execute arbitrary code.	Upgrades available at: http://housecall.trendmicro.com	Multiple Trend Micro HouseCall ActiveX Control Remote Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
Turbo Soft, Inc.[149]	Windows 95/98/ME/ NT 4.0/2000, XP	TurboFTP 3.85 Build 304	A buffer overflow vulnerability exists due to a boundary error when handling server responses, which could let a remote malicious user cause a Denial or Service and possibly execute arbitrary code.	No workaround or patch available at time of publishing.	TurboFTP Receive Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
Twilight Utilities[150]	Windows	WebServer 1.3.3 .0	A buffer overflow vulnerability exists due to an error in the handling of long GET requests, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code.	Update available at: http://www.twilightutilities.com/WebServer.html	Twilight WebServer GET Request Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.

[145] Sun(sm) Alert Notification, 55340, July 21, 2003.
[146] Securiteam, July 20, 2003.
[147] SecurityFocus, July 16, 2003.
[148] Secunia Security Advisory, July 12, 2003.
[149] Securiteam, July 14, 2003.
[150] Tripbit Security Advisory, TA-2003-07, July 13, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
University of Minnesota [151]	Unix	gopherd 1.12, 2.0.3, 2.0.4, 2.3, 2.3.1, 3.0.0-3.0.5	Two vulnerabilities exist: a buffer overflow vulnerability exists in the 'GopherFile()' function, which could let a remote malicious user execute arbitrary code; and a buffer overflow vulnerability exists in the 'GSisText()' function, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	GopherD Buffer Overflows	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Virtual Program-ming[152]	Windows	VP-ASP 5.0	A vulnerability exists in the 'shopexd.asp' script due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	Virtual Programming VP-ASP shopexd.asp SQL Injection	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published.
VMWare, Inc.[153]	Unix	GSX Server 2.5.1, VMWare Work-station 4.0	A vulnerability exists because environment variables may be manipulated, which could let a malicious user execute arbitrary code and obtain root access.	Patch available at: http://www.vmware.com/vmwarestore/newstore/download.jsp?ProductCode=GSX-LX-ESD	VMware GSX Server/ Workstation Host Operating System Compromise	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Watch Guard[154]	Windows 2000	ServerLock 2.0, 2.0.1, 2.0.2	Two vulnerabilities exist: a vulnerability exists in the 'ZwSetSystemInformation()' function, which could let a malicious user execute arbitrary code; and a vulnerability exists in "\Device\PhysicalMemory' because symlinks are not properly processed, which could let a malicious user bypassing the ServerLock access restrictions and take full control of the system.	Upgrade available at: https://www.watchguard.com/archive/softwarecenter.asp	ServerLock Access Control	**High**	Bug discussed in newsgroups and websites. There is no exploit code required for the symlink vulnerability.
Web Calendar [155]	Unix	Web Calendar 0.9.8, 0.9.11, 0.9.15, 0.9.16, 0.9.19-0.9.41	A Directory Traversal vulnerability exists due to an input validation error in 'login.php' and 'week_ssi.php,' which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	WebCalendar Directory Traversal	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[151] Bugtraq, July 12, 2003.
[152] Securiteam, July 8, 2003.
[153] Bugtraq, July 26, 2003.
[154] Bugtraq, July 17, 2003.
[155] Securiteam, July 21, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
William LeFebvre [156]	Unix	top 1.0, 1.2-1.8, 2.0 pre, 2.0, 2.0.11	A buffer overflow vulnerability exists when handling environment variables of excessive length, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Top Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
With Enterprise Pty Ltd.[157]	Windows	Witango Tango Server 2000, Witango Server 5.0.1.061	A buffer overflow vulnerability exists because 'Witango_UserReference' cookies are not handled correctly, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.witango.com	Witango Server Remote Cookie Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Xavi[158]	Multiple	X7028r DSL Router	A Denial of Service vulnerability exists due to a failure to handle HTTP requests longer than 1008 characters.	No workaround or patch available at time of publishing.	Xavi DSL Router Denial of Service	Low	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
XBlock Out[159] ***Vendor issues upgrade*** [160]	**Unix**	**xbl 1.0k, 1.0i**	**A buffer overflow vulnerability exists in the '-display' commandline option due to a boundary error, which could let a malicious user execute arbitrary code.**	**Upgrades available at: http://security.debian.org/pool/updates/main/x/xbl/** ***Upgrade available at:*** **ftp://ftp710.univ-lyon1.fr/pub/xbl/xbl-1.1.1.tar.gz**	**XBlockOut Buffer Overflow** **CVE name: CAN-2003-0535**	**High**	**Bug discussed in newsgroups and websites.**
xfstt[161]	Unix	xfstt 1.4	A buffer overflow vulnerability exists in the TrueType Font Server for X11 (xfstt) due to a boundary error in the "working()" function, 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.	xfstt Remote Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
xfstt[162]	Unix	xfstt 1.4	A memory corruption vulnerability exists 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.	xfstt Memory Corruption	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[156] SecurityFocus, July 22, 2003.
[157] NGSSoftware Insight Security Research Advisory, #NISR18072003, July 18, 2003.
[158] Secunia Security Advisory, July 23, 2003.
[159] Debian Security Advisory, DSA 345-1, July 8, 2003.
[160] SecurityFocus, July 19, 2003.
[161] ERA IT Solutions Security Advisory, July 14, 2003.
[162] SecurityFocus, July 23, 2003.

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

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

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

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

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between July 8 and July 24, 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, 36 scripts, programs, and net-news messages containing holes or exploits were identified. *Note: At times, scripts/techniques may contain names or content that may be considered offensive.*

Date of Script (Reverse Chronological Order)	Script name	Script Description
July 24, 2003	msqlex.c	Remote exploit for miniSQL Elevated Privileges vulnerability.
July 22, 2003	amap-4.0.tar.gz	A next-generation scanning tool that allows you to identify the applications that are running on a specific port. It does this by connecting to the port(s) and sending trigger packets.
July 22, 2003	insider.zip	A utility to set up a reverse backdoor for Win32 platforms that simply connects out to a server over HTTP and has the server tunnel commands back over the inbound connection.
July 22, 2003	**UHAGr.c**	**Exploit for the Top Buffer Overflow vulnerability.**
July 21, 2003	**0x333bru-fmtx.c**	**Script that exploits the BRU Improper Command-line Parsing vulnerability.**
July 21, 2003	cisco-bug-44020.tar.gz	Script that exploits the Cisco IOS Malicious IPV4 Packet Sequence Denial of Service vulnerability.
July 21, 2003	ciscodos.sh	Script that exploits the Cisco IOS Malicious IPV4 Packet Sequence Denial of Service vulnerability.
July 20, 2003	ettercap-0.6.b.tar.gz	A network sniffer/interceptor/logger for switched LANs that uses ARP poisoning and the man-in-the-middle technique to sniff all the connections between two hosts.
July 20, 2003	**rpc_dos_poc.c**	**Exploit for the Windows 2000 RPC Remote Denial of Service vulnerability.**
July 19, 2003	**DSR-gnats.pl**	**Perl script that exploits the GNATS 'Queue-PR' Buffer Overflow vulnerability.**
July 18, 2003	CA-2003-17.ciscoexp.txt	Exploit for the Cisco IOS Malicious IPV4 Packet Sequence Denial of Service vulnerability.

Date of Script (Reverse Chronological Order)	Script name	Script Description
July 18, 2003	**ex_bru.c**	**Script that exploits the BRU Improper Command-line Parsing vulnerability.**
July 18, 2003	firew0rker.c	Exploit for the Windows Media Services NSIISlog.DLL Remote Buffer Overflow vulnerability.
July 18, 2003	IglooExloit.c	Exploit for the IglooFTP PRO Multiple Buffer Overflows vulnerability.
July 18, 2003	shadowchode.tar.gz	Exploit for the Cisco IOS Malicious IPV4 Packet Sequence Denial of Service vulnerability.
July 18, 2003	shagg-0.2.0.tar.gz	An application that bruteforces check digit algorithms. It analyzes a given list of serial numbers and tries to find a matching algorithm and its setup.
July 17, 2003	CLIVITT-2003-4-Citadel-exploit.c	Script that exploits the Citadel/UX Buffer Overflow vulnerability.
July 17, 2003	mine.c	Script that exploits the Cisco IOS Malicious IPV4 Packet Sequence Denial of Service vulnerability.
July 17, 2003	nmap-3.30.tgz	A utility for port scanning large networks, although it works fine for single hosts.
July 15, 2003	**splatt.html**	**Exploit for the Splatt Forum Post Icon Cross-Site Scripting vulnerability.**
July 14, 2003	0x333openssh-3.6.1p2.tar.gz	Backdoored version of OpenSSH 3.6.1p2 that has a magic password, logs logins and passwords to a specified file, and disables use of the default configuration file.
July 14, 2003	**byebye_tribes.phps**	**Exploit for the StarSiege Tribes Server Remote Denial of Service vulnerability.**
July 14, 2003	**byebye_tribes.zip**	**Exploit for the StarSiege Tribes Server Remote Denial of Service vulnerability.**
July 14, 2003	**DSR-ftp_clients.pl**	**Perl script that exploits the cftp 'Welcome' Banner Parsing Buffer Overflow vulnerability and the IglooFTP 'Welcome' Banner Parsing Buffer Overflow vulnerability.**
July 14, 2003	DSR-upclient.pl	Perl script that exploits the Upclient 5.0.b5 vulnerability.
July 14, 2003	**exceed.c**	**Script that exploits the Exceed Font Buffer Overflow vulnerability.**
July 14, 2003	openssh-3.6.1p2-backdoor.patch.gz	A backdoor patch that has a magic password allowing access to all accounts, does not log any connections, logs passwords and logins, and bypasses configuration file options.
July 14, 2003	shatterSEH.txt	Paper that discusses shatter attacks that are possible using SEH memory locations to escalate privileges in Windows.
July 14, 2003	tac0tac0.c	Script that exploits the Windows CreateFile API Named Pipe Privilege Escalation vulnerability.
July 14, 2003	YahPoo.c	Script that exploits the Yahoo Messenger Remote Command vulnerability.
July 13, 2003	twilight.c	Script that exploits the Twilight WebServer GET Request Buffer Overflow vulnerability.
July 12, 2003	**xgopherd2k3-ftp.c**	**Script that exploits the GopherD Buffer Overflows vulnerabilities.**
July 12, 2003	**xgopherd2k3-jesustext.c**	**Script that exploits the GopherD Buffer Overflows vulnerabilities.**
July 12, 2003	**xgopherd2k3-view.c**	**Script that exploits the GopherD Buffer Overflows vulnerabilities.**
July 8, 2003	**tioeuy.pl**	**Perl script that exploits the Virtual Programming VP-ASP shopexd.asp SQL Injection vulnerability.**
July 8, 2003	**tio-fux.pl**	**Perl script that exploits the Virtual Programming VP-ASP shopexd.asp SQL Injection vulnerability.**

Trends

- **The Department of Homeland Security (DHS) / Information Analysis and Infrastructure Protection (IAIP) National Cyber Security Division (NCSD) has issued an advisory in consultation with the Microsoft Corporation to heighten awareness of potential Internet disruptions resulting from the possible spread of malicious software exploiting a vulnerability in popular Microsoft Windows operating systems. DHS expects that exploits are being developed for malicious use. For more information see, "Bugs, Holes & Patches" Table "Windows DCOM RPC Buffer Overflow" and DHS/IAIP Advisory located: http://www.nipc.gov/warnings/advisories/2003/Potential72403.htm. Additional information on the Microsoft vulnerability may also be found at: http://microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-026.asp.**
- **The Department of Homeland Security (DHS) / Information Analysis and Infrastructure Protection (IAIP) National Cyber SecurityDivision (NCSD) has issued an advisory to heighten awareness of a remotely exploitable vulnerability in Cisco IOS 10.3 or later. The recently announced vulnerability in devices running Cisco IOS 10.3 or later may be exploited to cause a Denial of Service state. Because routers and switches are an essential part of all network infrastructures, and because Cisco devices comprise a significant portion of those infrastructures, widespread exploitation of vulnerable Cisco devices could disrupt portions of the Internet. For more information see "Bugs, Holes & Patches" Table and DHS/FedCIRC Advisory FA-2003-15 located at: http://www2.fedcirc.gov/advisories/FA-2003-15.html.**
- **Recent reports to the CERT/CC have highlighted two chronic problems:**
  - **The speed at which viruses are spreading is increasing. This echoes the trend toward faster propagation rates seen in the past few years in self-propagating malicious code (i.e., worms). A similar trend from weeks to hours has emerged in the virus (i.e., non-self-propagating malicious code) arena.**
  - **In a number of the reports, users who were compromised may have been under the incorrect impression that merely having antivirus software installed was enough to protect them from all malicious code attacks. This is simply a mistaken assumption, and users must always exercise caution when handling e-mail attachments or other code or data from untrustworthy sources. For more information see, CERT® Incident Note IN-2003-01, located at: http://www.cert.org/incident_notes/IN-2003-01.html.**
- **The Fortnight Internet worm takes advantage of a the Microsoft VM ActiveX security vulnerability for which Microsoft released a security patch three years ago. When this security breach is left unpatched the worm's code is allowed to be executed on victim computers.**
- **A growing trend sees spammers targeting home computers with Trojan programs to remotely send out spam. Spammers are less likely to crack corporate boxes and are now increasingly turning toward using large quantities of home computers.**

Viruses

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

BAT.Wimpey.dr (Batch File Virus): This is a dropper for the VBS.Wimpey@mm virus. It disables the mouse and keyboard and attempts to delete all the .jpg, .bmp, .avi, .mov, .sys, .txt, .dll, and .pwd files, but fails due to a bug in the code. It also attempts to create randomly named copies of itself in C:\Windows, if the folder exists.

Haver.1309 (DOS Virus): This is a DOS memory-resident virus that infects the .exe files. It contains a destructive payload that will be triggered on April 6th. When a file that is infected with Haver.1309 is

executed, it hooks interrupt 21h and 24h. After this occurs, the virus will infect any uninfected .exe files, which were loaded and executed.

Kamadina (Alias: P2P. Kamadina) (P2P Worm): This is one of the smallest P2P (peer-to-peer) worms. Its size is only 1.5 kilobytes. When the worm is run, it copies itself to shared folders of several file sharing clients: KaZaA, Limewire, Grokster, Bearshare, Edonkey, Morpheus, and a few others. The worm also copies itself to ICQ share files folder. It does this only on the Spanish installation of Windows. Additionally the worm copies itself to 'My Music,' 'My Downloads,' and 'My Documents\My Music' subfolders if they are located in '\Archivos de programa' folder. The worm copies itself with the same name as the name of the file it was started from. So far we received reports that the worm's file name is: "MySQL-checker.exe." It doesn't stay in Windows memory and exits as soon as it copies itself to all the above mentioned folders.

VBS.Dasbud.int (Alias: VBS/Dasbud.intd) (Visual Basic Script Virus): This is a Visual Basic Script (VBS) virus that infects HTML files and displays the message "PopUp Buddy was here..." VBS.Dasbud.int appends itself to any files with "hta," "html," or "htm" extensions in the current folder and the following folders:

- C:\InetPub\wwwroot
- C:\Program Files\Microsoft FrontPage\bin

VBS.Renegy (Aliases: VBS.Renegy, VBS.Renergy, VBS.Renegy) (Visual Basic Script Virus): This is a Visual Basic Script (VBS) virus that infects HTML files, changing the title field in original file to "HTML.Replace Was Here." VBS.Renegy appends itself to any files with "hta," "html," or "htm" extensions in the current folder and the following folders:

- C:\InetPub\wwwroot
- C:\Program Files\Microsoft FrontPage\bin

VBS.Wimpey@mm (Visual Basic Script Worm): This is a mass-mailing worm that sends itself to all the addresses in the Microsoft Outlook Address Book. It does not have a malicious payload; its only action is to send itself through Microsoft Outlook using MAPI calls. The worm spreads with the following message:

- Subject: Warning
- Attachment: Outlook.vbs

JS/Fortnight-H (Alias: JS/IEStart.M) (JavaScript Virus): This is a virus that is combination of JavaScripts and Java Applets. When an e-mail infected with JS/Fortnight-H is read by an HTML-aware mail client, the virus attempts to open a website. The website runs a Java Applet that makes use of Troj/ByteVeri-B to run itself locally. It then attempts to drop a file, D.HTM, in WINDOWS that it will set as the signature for Outlook Express 5.0. The following registry entries are edited:

- HKCU\Software\Microsoft\Internet Explorer\Main\Search Page
- HKCU\Software\Microsoft\Internet Explorer\Main\Search Bar
- HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\URL\DefaultPrefix

The following files will be dropped in the Favorites Folder:

- Nude Nurses.url
- Search You Trust.url
- Your Favorite Porn Links.url

JS/Fortnight-H exploits a vulnerability in the Microsoft VM ActiveX component. If an affected web page is opened, a JScript embedded on the page attempts to use the vulnerability in order to drop files on a local drive, change registry keys without the user's knowledge, or perform any other malicious action on the local computer. *(Note: For more details about the Microsoft VM ActiveX component exception vulnerability please see Microsoft Security Bulletin MS00-075 located at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms00-075.asp).*

W32.Babybear@mm (Win32 Worm): This worm is written in Visual Basic. It spreads using e-mail. Once activated, this worm damages the installations of Symantec antivirus products and may prevent them from running. It copies itself all over the system and creates many empty folders.

W32/Coconut-A (Alias: W32/Conut@MM) (Win32 Virus): This is a prepending virus (written in C#) and a mass mailing worm. It places a dropper copy of itself as C:\coconut.exe and temporarily drops VBS/Coconut-A as C:\mail.vbs. The virus then uses the VBScript to mail the dropper to all entries in the Windows address book using an e-mail with the following characteristics:

- Subject line: The Coconut Game
- Attached File: coconut.exe

W32/Coconut-A will then display a 'Coconut Shy' game, in which the user has 3 chances at hitting a picture of either Frans Devaere (for 1 point) or Graham Cluley (for 2 points) by pressing a button. The virus then infects 6-<score> files on the system. Finally, the virus displays a message box telling the user how many points they scored, and how many files are infected. Frans Devaere is an alleged malicious user from Belgium. Graham Cluley is senior technology consultant and head of corporate communications for Sophos Anti-Virus.

W32.Enegg@mm (Win32 Worm): This is a mass-mailing worm that attempts to delete security software and system files. It is written in Visual Basic and mails itself to contacts in the Microsoft Outlook Address Book, using a variety of Spanish subject lines and message bodies. The attachment will be named, "Cynthia.exe. "

W32/Gruel-A (Win32 Worm): This is a mass mailing worm that arrives in an e-mail with the following characteristics:

- Subject line: Symantec: New serious virus found
- Attached File: Rundll32.exe

On execution, the worm displays a Windows XP style messagebox with two buttons: "Send Error" and "Send and Close." Clicking on "Send Error" displays a bogus technical-looking error message, similar to the above, with "<< Back" and "Close" buttons. "Close" does nothing and "<< Back" takes you back to the previous screen. Clicking on "Send and Close" will cause the worm to run many control panel applets, eject the CD-Rom drive, remove the taskbar, and display a rant about Windows that cannot be closed. W32/Gruel-A disables many Windows features, such as task manager, logoff, shutdown, lock computer, change password, etc. The worm also changes the default association for EXE files and deletes many files in the Windows system folder and its sub-folders. The worm also copies itself as Norton 2003 Pro.exe into the default KaZaA shared folder.

W32/Gruel-B (Win32 Worm): This is a mass mailing worm very similar to W32/Gruel-A. But this variant arrives in an e-mail with different characteristics:

- Subject: Microsoft Windows Critical Update
- Attached File: Rundll32.exe
  (Safety tip: remember that Microsoft never sends out security updates as e-mail attachments.)

W32/Gruel-C (Win32 Worm): This is a mass mailing worm very similar to W32/Gruel-A. It uses the same subject line and message text as the -A variant.

W32/Gruel-D (Alias: I-Worm.Kiguat) (Win32 Worm): This is a mass mailing worm very similar to W32/Gruel-A that arrives in an e-mail with the following characteristics:

- Subject line: Microsoft Windows Critical Update
- Attached File: Rundll32.exe

On execution, the worm displays a Windows XP style message with two buttons, "Send Error" and "Send and Close." Clicking on "Send Error" displays a bogus technical-looking error message, similar to the above, with "<< Back" and "Close" buttons. "Close" does nothing and "<< Back" takes you back to the previous screen. Clicking on "Send and Close" will cause the worm to run many control panel applets, eject the CD-Rom drive, remove the taskbar, and display a rant about Windows that cannot be closed. W32/Gruel-D disables many Windows features, such as task manager, logoff, shutdown, lock computer, change password, etc. The worm also changes the default association for EXE files and deletes many files in the Windows system folder and its sub-folders. The worm also copies itself to the Desktop as kIlLeRgUaTe1.03.

W32/Gruel-E (Aliases I-Worm.Gruel.e, I-Worm.Gruel.f, I-Worm.Gruel.g, I-Worm.Gruel.h, I-Worm.Gruel.i) (Win32 Worm): This is a mass mailing worm very similar to the other variants in this family.

W32.HLLW.Symten@mm (Aliases: Bloodhound.W32.VBWORM, I-Worm.Symten.b) (Win32 Worm): This is a mass-mailing worm that distributes itself by a randomly generated e-mail. It is written in Visual Basic.

W32.Jantic.F@mm (Win32 Worm): This is a mass-mailing worm that uses Microsoft Outlook to spread. In an attempt to disguise itself, it uses the same icon as Norton AntiVirus. It is written in Microsoft Visual Basic.

W32.Lohack.B.Worm (Win32 Worm): This is a worm that attempts to spread itself through file-sharing networks. It also attempts to mass mail itself to all the contacts in the Windows Address Book. The e-mail will have a variable subject and attachment name. The attachment will have a .exe or .scr file extension. The worm uses an internal SMTP client engine. In addition, W32.Lohack.B.Worm is a network-aware worm. It is a Visual Basic application that is compiled to native code and is packed with UPX v1.23.

W32.Lohack.C.Worm (Alias: I-Worm.Lohack.c) (Win32 Worm): This is a variant of W32.Lohack.Worm that infects peer-to-peer file-sharing applications, in addition to sending itself to e-mail addresses found on the system. The e-mail will have the following characteristics:

- Subject: Windows update
- Attachment: windows_update.txt.exe

W32.Nogrov@mm (Win32 Worm): This is a mass-mailing e-mail worm. The worm sends itself to the contacts it finds in the Windows Address Book and copies itself to the C:\My downloads folder. The e-mail will have a variable subject line and attachment name. The attachment will have a .exe file extension.

W97M.Acus.A (Aliases: WM97/Vmpck1-DV, W97M/VMPCK.gen, Macro.Word97.VMPC-based) IWord 97 Macro Virus): This is a simple macro virus that infects Microsoft Word documents and the Normal.dot template. This virus also has a payload that has a one-in-one hundred chance of replacing a specific word with new text.

W97M.Bench.G (Aliases: Macro.Word97.Skyline, W97M/Skyline.A, W97M/Bench.C, W97M_BENCH.F, W97M/Bencg.gen) (Word 97 Macro Virus): This is a simple macro virus that infects the currently active document and Normal.dot template when an infected document is opened. Once Normal.dot is infected, clean documents will be infected when they are opened. The virus sets the animation property of the font of the active document to SparkleText or Shimmer, depending on the current time.

W97M.Kazoy (Aliases: Macro.Word97.Yozak.b, WM97/Yozak-B, W97M/Yozak.B) (Word 97 Macro Virus): This is a macro virus that infects documents created in Microsoft Word 97 and later. The virus infects documents when they are opened. W97M.Kazoy checks to see whether the Normal.dot template is infected each time the AutoOpen macro opens an infected document. If Normal.dot is not infected, the virus adds the viral THISDOCUMENT module to the Normal.dot template. It adds the viral module to the document and disables the macro virus warning of Microsoft Word. The virus performs a randomization, and if the month equals the generated random number, the macro will do the following:

- Display a message box containing a political statement
- Attempt to ping an IP address with a random number of packets
- Display greetings to the virus writers.

In addition, if you access the Word Basic editor, the macro will run the AutoOpen module.

W97M.Tooth (Aliases: Macro.Word97.Intended.Toothpaste, W97M/Tooth.A, W97M_TOOTHPASTE, W97M/Tooth.A, WM97/Toothpaste) (Word 97 Macro Virus): This is a macro virus that attempts to infect Microsoft Word documents and the Normal.dot template. If the system

date is the 12th of the month, it will display a graphic titled "Toothpaste!" *Note: Due to a bug in the code, the virus may not work properly.*

Win16.HLLP.Hiro.10240 (Parasitic Virus): This virus is not dangerous. It is a non-memory resident parasitic virus written in Pascal. It is a 16 bit NE EXE file that also works under Windows 3.xx. The virus contains the text string: "Hiroshima end 000 v1.2000:0000."

Win32.Seppuku.2764 (Alias: Win32.Seppuku.2764) (Win32 Virus): Seppuku is not a dangerous parasitic Win32 virus. The Win32.Seppuku.2764 virus searches for PE EXE files in the current and Windows directories. It contains the following text string:

- Win32/Seppuku v1.1
- (c) 2001 Tokugawa Ieyasu

Win32.SanKey (Win32 Virus): This is a very dangerous parasitic Win32 virus. It searches for PE EXE files in the current directory and corrupts files while infecting them. When infecting a PE EXE file the virus creates a section named "kaze/FAT."

WORM_AINJO.E (Aliases: Aliases: W32.HLLW.Indor.E@mm, W32/Pkasa, Win32/Indowing.A, I-Worm.Ainjo.e, Win32.HLLM.Generic.132) (Internet Worm): This worm propagates via Internet Relay Chat (IRC), peer-to-peer file-sharing networks such as KaZaA, and through e-mail using Microsoft Outlook. It sends itself to all contacts listed in the Microsoft Outlook address book using an e-mail with the various subject lines, message bodies and attachments. The attachment is a compressed ZIP file containing a single copy of this worm.

Trojans

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

Trojan	Version	CyberNotes Issue #
AdwareDropper-A	A	CyberNotes-2003-04
Adware-SubSearch.dr	dr	CyberNotes-2003-14
AIM-Canbot	N/A	CyberNotes-2003-07
AprilNice	N/A	CyberNotes-2003-08
Backdoor.Acidoor	N/A	CyberNotes-2003-05
Backdoor.Amitis	N/A	CyberNotes-2003-01
Backdoor.Amitis.B	B	CyberNotes-2003-11
Backdoor.AntiLam.20.K	K	CyberNotes-2003-10
Backdoor.Apdoor	N/A	CyberNotes-2003-12
Backdoor.Assasin.D	D	CyberNotes-2003-01
Backdoor.Assasin.E	E	CyberNotes-2003-04
Backdoor.Assasin.F	F	CyberNotes-2003-09
Backdoor.Badcodor	N/A	CyberNotes-2003-12
Backdoor.Beasty	N/A	CyberNotes-2003-02
Backdoor.Beasty.B	B	CyberNotes-2003-03
Backdoor.Beasty.C	C	CyberNotes-2003-05

Trojan	Version	CyberNotes Issue #
Backdoor.Beasty.Cli	Cli	CyberNotes-2003-10
Backdoor.Beasty.D	D	CyberNotes-2003-06
Backdoor.Beasty.E	E	CyberNotes-2003-06
Backdoor.Bigfoot	N/A	CyberNotes-2003-09
Backdoor.Bmbot	N/A	CyberNotes-2003-04
Backdoor.Bridco	N/A	CyberNotes-2003-06
Backdoor.CamKing	N/A	CyberNotes-2003-10
Backdoor.CHCP	N/A	CyberNotes-2003-03
Backdoor.Cmjspy	N/A	CyberNotes-2003-10
Backdoor.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.Cow	N/A	CyberNotes-2003-01
Backdoor.Cybspy	N/A	CyberNotes-2003-01
Backdoor.Dani	N/A	CyberNotes-2003-04
Backdoor.Darmenu	N/A	CyberNotes-2003-05
Backdoor.Death.Cli	Cli	CyberNotes-2003-10
Backdoor.Deftcode	N/A	CyberNotes-2003-01
Backdoor.Delf.Cli	Cli	CyberNotes-2003-10
Backdoor.Delf.F	F	CyberNotes-2003-07
Backdoor.Drator	N/A	CyberNotes-2003-01
Backdoor.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.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.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.Grobodor	N/A	CyberNotes-2003-12
Backdoor.Guzu.B	B	CyberNotes-2003-14
Backdoor.HackDefender	N/A	CyberNotes-2003-06
Backdoor.Hethat	N/A	CyberNotes-2003-01
Backdoor.Hipo	N/A	CyberNotes-2003-04
Backdoor.Hitcap	N/A	CyberNotes-2003-04
Backdoor.Hornet	N/A	CyberNotes-2003-01
Backdoor.IRC.Aladinz	N/A	CyberNotes-2003-02
Backdoor.IRC.Aladinz.C	C	CyberNotes-2003-14
Backdoor.IRC.Cloner	N/A	CyberNotes-2003-04
Backdoor.IRC.Comiz	N/A	CyberNotes-2003-11

Trojan	Version	CyberNotes Issue #
Backdoor.IRC.Lampsy	N/A	CyberNotes-2003-10
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.Yoink	N/A	CyberNotes-2003-05
Backdoor.IRC.Zcrew	N/A	CyberNotes-2003-04
Backdoor.Kaitex.D	D	CyberNotes-2003-09
Backdoor.Kalasbot	N/A	CyberNotes-2003-09
Backdoor.Khaos	N/A	CyberNotes-2003-04
Backdoor.Kilo	N/A	CyberNotes-2003-04
Backdoor.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.Lanfilt.B	B	CyberNotes-2003-14
Backdoor.LeGuardien.B	B	CyberNotes-2003-10
Backdoor.Litmus.203.c	c	CyberNotes-2003-09
Backdoor.LittleWitch.C	C	CyberNotes-2003-06
Backdoor.Longnu	N/A	CyberNotes-2003-06
Backdoor.Marotob	N/A	CyberNotes-2003-06
Backdoor.Massaker	N/A	CyberNotes-2003-02
Backdoor.MindControl	N/A	CyberNotes-2003-14
Backdoor.Monator	N/A	CyberNotes-2003-08
Backdoor.Mots	N/A	CyberNotes-2003-11
Backdoor.MSNCorrupt	N/A	CyberNotes-2003-06
Backdoor.Netdevil.15	**15**	**Current Issue**
Backdoor.NetDevil.B	B	CyberNotes-2003-01
Backdoor.NetTrojan	N/A	CyberNotes-2003-01
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.Optix.04.d	04.d	CyberNotes-2003-04
Backdoor.OptixDDoS	N/A	CyberNotes-2003-07
Backdoor.OptixPro.10.c	10.c	CyberNotes-2003-01
Backdoor.OptixPro.12.b	12.b	CyberNotes-2003-07
Backdoor.OptixPro.13	13	CyberNotes-2003-09
Backdoor.Peers	N/A	CyberNotes-2003-10
Backdoor.Plux	N/A	CyberNotes-2003-05
Backdoor.Pointex	N/A	CyberNotes-2003-09
Backdoor.Pointex.B	B	CyberNotes-2003-09
Backdoor.Private	N/A	CyberNotes-2003-11
Backdoor.Prorat	N/A	CyberNotes-2003-13
Backdoor.PSpider.310	310	CyberNotes-2003-05
Backdoor.Queen	N/A	CyberNotes-2003-06
Backdoor.Ratega	N/A	CyberNotes-2003-09
Backdoor.Recerv	N/A	CyberNotes-2003-09
Backdoor.Redkod	N/A	CyberNotes-2003-05

Trojan	Version	CyberNotes Issue #
Backdoor.Remohak.16	16	CyberNotes-2003-01
Backdoor.RemoteSOB	N/A	CyberNotes-2003-01
Backdoor.Rephlex	N/A	CyberNotes-2003-01
Backdoor.Rsbot	N/A	CyberNotes-2003-07
Backdoor.SchoolBus.B	B	CyberNotes-2003-04
Backdoor.Sdbot.C	C	CyberNotes-2003-02
Backdoor.Sdbot.D	D	CyberNotes-2003-03
Backdoor.Sdbot.E	E	CyberNotes-2003-06
Backdoor.Sdbot.F	F	CyberNotes-2003-07
Backdoor.Sdbot.G	G	CyberNotes-2003-08
Backdoor.Sdbot.H	H	CyberNotes-2003-09
Backdoor.Sdbot.L	L	CyberNotes-2003-11
Backdoor.Sdbot.M	M	CyberNotes-2003-13
Backdoor.Serpa	N/A	CyberNotes-2003-03
Backdoor.Servsax	N/A	CyberNotes-2003-01
Backdoor.SilverFTP	N/A	CyberNotes-2003-04
Backdoor.Simali	N/A	CyberNotes-2003-09
Backdoor.Sixca	N/A	CyberNotes-2003-01
Backdoor.Slao	N/A	CyberNotes-2003-11
Backdoor.Snami	N/A	CyberNotes-2003-10
Backdoor.Snowdoor	N/A	CyberNotes-2003-04
Backdoor.Socksbot	N/A	CyberNotes-2003-06
Backdoor.Softshell	N/A	CyberNotes-2003-10
Backdoor.Stealer	N/A	CyberNotes-2003-14
Backdoor.SubSari.15	15	CyberNotes-2003-05
Backdoor.SubSeven.2.15	2.15	CyberNotes-2003-05
Backdoor.Syskbot	N/A	CyberNotes-2003-08
Backdoor.SysXXX	N/A	CyberNotes-2003-06
Backdoor.Talex	N/A	CyberNotes-2003-02
Backdoor.Tankedoor	N/A	CyberNotes-2003-07
Backdoor.Trynoma	N/A	CyberNotes-2003-08
Backdoor.Turkojan	N/A	CyberNotes-2003-07
Backdoor.Udps.10	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.Uzbet	**N/A**	**Current Issue**
Backdoor.VagrNocker	N/A	CyberNotes-2003-01
Backdoor.Vmz	N/A	CyberNotes-2003-01
Backdoor.Winet	N/A	CyberNotes-2003-11
Backdoor.WinJank	**N/A**	**Current Issue**
Backdoor.Winker	**N/A**	**Current Issue**
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

Trojan	Version	CyberNotes Issue #
Backdoor.Zombam	N/A	CyberNotes-2003-08
Backdoor.Zvrop	N/A	CyberNotes-2003-03
Backdoor-AFC	N/A	CyberNotes-2003-05
Backdoor-AOK	N/A	CyberNotes-2003-01
BackDoor-AQL	N/A	CyberNotes-2003-05
BackDoor-AQT	N/A	CyberNotes-2003-05
BackDoor-ARR	ARR	CyberNotes-2003-06
Backdoor-ARU	ARU	CyberNotes-2003-06
BackDoor-ARX	ARX	CyberNotes-2003-06
BackDoor-ARY	ARY	CyberNotes-2003-06
BackDoor-ASD	ASD	CyberNotes-2003-07
BackDoor-ASL	ASL	CyberNotes-2003-07
BackDoor-ASW	ASW	CyberNotes-2003-08
BackDoor-ATG	ATG	CyberNotes-2003-09
BackDoor-AUP	N/A	CyberNotes-2003-11
BackDoor-AVF	AVF	CyberNotes-2003-12
BackDoor-AVH	AVH	CyberNotes-2003-12
BackDoor-AVO	AVO	CyberNotes-2003-12
BackDoor-AXC	AXC	CyberNotes-2003-14
BackDoor-AXQ	**AXQ**	**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/PowerSpider.A	A	CyberNotes-2003-11
Daysun	N/A	CyberNotes-2003-06
DDoS-Stinkbot	N/A	CyberNotes-2003-08
DoS-iFrameNet	N/A	CyberNotes-2003-04
Download.Trojan.B	B	CyberNotes-2003-13
Downloader.BO.B	B	CyberNotes-2003-10
Downloader.BO.B.dr	B.dr	CyberNotes-2003-10
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
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.PWS.QQPass	N/A	CyberNotes-2003-06
ICQPager-J	N/A	CyberNotes-2003-05
IRC/Backdoor.e	E	CyberNotes-2003-01
IRC/Backdoor.f	f	CyberNotes-2003-02
IRC/Backdoor.g	g	CyberNotes-2003-03

Trojan	Version	CyberNotes Issue #
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-Emoz	N/A	CyberNotes-2003-03
IRC-OhShootBot	N/A	CyberNotes-2003-01
IRC-Vup	N/A	CyberNotes-2003-09
JS.Fortnight.B	B	CyberNotes-2003-06
JS.Seeker.J	J	CyberNotes-2003-01
JS/Fortnight.c@M	c	CyberNotes-2003-11
JS/Seeker-C	C	CyberNotes-2003-04
JS/StartPage.dr	dr	CyberNotes-2003-11
JS_WEBLOG.A	A	CyberNotes-2003-05
Keylogger.Cone.Trojan	N/A	CyberNotes-2003-14
KeyLog-Kerlib	N/A	CyberNotes-2003-05
Keylog-Kjie	N/A	CyberNotes-2003-12
Keylog-Perfect.dr	dr	CyberNotes-2003-09
Keylog-Razytimer	N/A	CyberNotes-2003-03
KeyLog-TweakPan	N/A	CyberNotes-2003-02
Keylog-Yeehah	N/A	CyberNotes-2003-12
Linux/Exploit-SendMail	N/A	CyberNotes-2003-05
Lockme	**N/A**	**Current Issue**
MultiDropper-FD	N/A	CyberNotes-2003-01
Pac	N/A	CyberNotes-2003-04
ProcKill-AE	N/A	CyberNotes-2003-05
ProcKill-AF	N/A	CyberNotes-2003-05
ProcKill-AH	AH	CyberNotes-2003-08
ProcKill-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
PWSteal.ABCHlp	N/A	CyberNotes-2003-12
PWSteal.AlLight	N/A	CyberNotes-2003-01
PWSteal.Bancos	**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.Rimd	N/A	CyberNotes-2003-01
PWSteal.Rimd.B	B	CyberNotes-2003-10
PWSteal.Senhas	N/A	CyberNotes-2003-03
PWSteal.Snatch	N/A	CyberNotes-2003-10
PWSteal.Sysrater	N/A	CyberNotes-2003-12
PWS-Tenbot	N/A	CyberNotes-2003-01
PWS-Truebf	N/A	CyberNotes-2003-13
PWS-Watsn	N/A	CyberNotes-2003-10
PWS-Wexd	N/A	CyberNotes-2003-14

Trojan	Version	CyberNotes Issue #
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
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/DelWinbootdir	N/A	CyberNotes-2003-07
TR/Fake.YaHoMe.1	N/A	CyberNotes-2003-02
Tr/SpBit.A	A	CyberNotes-2003-04
Tr/VB.t	T	CyberNotes-2003-11
TR/WinMx	N/A	CyberNotes-2003-02
Troj/Ataka-E	**E**	**Current Issue**
Troj/Dloader-BO	BO	CyberNotes-2003-02
Troj/DownLdr-DI	**DI**	**Current Issue**
Troj/Golon-A	**A**	**Current Issue**
Troj/Hacline-B	B	CyberNotes-2003-13
Troj/IRCBot-C	C	CyberNotes-2003-11
Troj/Manifest-A	N/A	CyberNotes-2003-03
Troj/Migmaf-A	**A**	**Current Issue**
Troj/Mystri-A	A	CyberNotes-2003-13
Troj/PcGhost-A	A	CyberNotes-2003-13
Troj/Peido-B	B	CyberNotes-2003-10
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**	**Current Issue**
TROJ_JBELLZ.A	A	CyberNotes-2003-02
TROJ_KILLBOOT.B	B	CyberNotes-2003-01
TROJ_RACKUM.A	A	CyberNotes-2003-05

Trojan	Version	CyberNotes Issue #
Trojan.Ailati	**N/A**	**Current Issue**
Trojan.AprilFool	N/A	CyberNotes-2003-08
Trojan.Barjac	N/A	CyberNotes-2003-05
Trojan.Dasmin	N/A	CyberNotes-2003-01
Trojan.Dasmin.B	B	CyberNotes-2003-03
Trojan.Downloader.Aphe	N/A	CyberNotes-2003-06
Trojan.Downloader.Inor	N/A	CyberNotes-2003-02
Trojan.Grepage	N/A	CyberNotes-2003-05
Trojan.Guapeton	N/A	CyberNotes-2003-08
Trojan.Idly	N/A	CyberNotes-2003-04
Trojan.Ivanet	N/A	CyberNotes-2003-02
Trojan.Kaht	N/A	CyberNotes-2003-10
Trojan.KKiller	N/A	CyberNotes-2003-01
Trojan.Lear	N/A	CyberNotes-2003-10
Trojan.Mumuboy	N/A	CyberNotes-2003-13
Trojan.Myet	N/A	CyberNotes-2003-12
Trojan.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.ProteBoy	N/A	CyberNotes-2003-04
Trojan.PSW.Gip	N/A	CyberNotes-2003-06
Trojan.PSW.Platan.5.A	N/A	CyberNotes-2003-01
Trojan.PWS.QQPass.D	N/A	CyberNotes-2003-02
Trojan.Qforager	N/A	CyberNotes-2003-02
Trojan.Qforager.Dr	N/A	CyberNotes-2003-02
Trojan.Qwe	N/A	CyberNotes-2003-02
Trojan.Sarka	N/A	CyberNotes-2003-14
Trojan.Sidea	N/A	CyberNotes-2003-12
Trojan.Snag	N/A	CyberNotes-2003-02
Trojan.Unblockee	N/A	CyberNotes-2003-01
Trojan.Visages	**N/A**	**Current Issue**
Trojan.Windelete	N/A	CyberNotes-2003-14
Uploader-D	D	CyberNotes-2003-06
Uploader-D.b	D.b	CyberNotes-2003-07
VBS.ExitWin	N/A	CyberNotes-2003-12
VBS.Kasnar	N/A	CyberNotes-2003-06
VBS.Moon.B	B	CyberNotes-2003-02
VBS.StartPage	N/A	CyberNotes-2003-02
VBS.Trojan.Lovcx	N/A	CyberNotes-2003-05
VBS.Zizarn	N/A	CyberNotes-2003-09
VBS/Fourcourse	N/A	CyberNotes-2003-06
W32.Adclicker.C.Trojan	C	CyberNotes-2003-09
W32.Bambo	N/A	CyberNotes-2003-14
W32.Benpao.Trojan	N/A	CyberNotes-2003-04
W32.CVIH.Trojan	N/A	CyberNotes-2003-06
W32.Laorenshen.Trojan	N/A	CyberNotes-2003-14
W32.Noops.Trojan	N/A	CyberNotes-2003-09

Trojan	Version	CyberNotes Issue #
W32.Socay.Worm	N/A	CyberNotes-2003-02
W32.Spybot.dr	**dr**	**Current Issue**
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
Xin	N/A	CyberNotes-2003-03

BackDoor-AXQ (Alias: Backdoor.WinRC): This is a remote access Trojan. It is spread manually and may arrive with the file name winrcLoader.exe, however is not limited to this file name or extension. It opens a TCP port (1976) to allow a remote malicious user to perform various tasks on an infected system. When run, the Trojan installs 3 components to the WINDOWS (%WinDir%) directory:

- winrc.htm (130 bytes)
- winrc.dll (28,672 bytes)
- winrcobj.dll (126,976 bytes)

It also copies itself to this directory and creates an HTML file, winrc.htm. Several registry keys are created:

- HKEY_CLASSES_ROOT\NoLook.Spy
- HKEY_CLASSES_ROOT\CLSID\{65863AB3-8D15-4953-8B66-281B2BCEC937}
- HKEY_CLASSES_ROOT\TypeLib\{1FC9D71A-6B65-41AB-BE9D-13A7DFA70DAD}
- HKEY_CLASSES_ROOT\Interface\{561E2361-8484-4EED-9E67-D9F7B19D54D2}
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "winrcLoader.exe" = winrcLoader.exe

A remote malicious user may connect to port 1976, provide the correct password, and perform various tasks.

Backdoor.Netdevil.15: This Trojan horse is a variant of Backdoor.Netdevil. It is usually packed and allows unauthorized access to an infected computer. When Backdoor.Netdevil.15 is run, it copies itself as %System%\Kernel32.dli and adds the value, “Kernel32"="%sysdir%\Kernel32.dli,” to the registry key:

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

The Trojan adds the registry keys:

- HKEY_CLASSES_ROOT\.dli
- HKEY_LOCAL_MACHINE\software\classes\.dli

so that the files of the .dli file type can be executed. It opens port 190 to listen for commands from the Trojan's author.

Backdoor.Uzbet (Alias: TrojanProxy.Win32.Uzbet): This is a Trojan that runs as a proxy server under Windows 2000/XP. When the Trojan is executed with the -install option, it adds the service "USB2Eh" and sets it to run itself. The Trojan also opens port 829. When it is executed with the -remove option, it deletes the service.

Backdoor.WinJank: This is a Trojan Horse that gives its creator unobstructed access to your computer. When Backdoor.WinJank runs, it adds a value that refers to the Trojan file in the registry keys:

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

so that the Trojan runs when you restart Windows. The Trojan opens a TCP port and listens for commands from its creator. The TCP port may vary; by default, it is 5277. The commands allow the Trojan's creator to perform various actions.

Backdoor.Winker (Alias: Backdoor.Winker.f): This is a Trojan Horse that attempts to download files from the Internet and send e-mail to its creator. It is packed with UPX. Backdoor.Winker. When the Trojan

is executed, it copies itself as %System%\Hello.exe and adds the value, "systhread"="%System%\Hello.exe," to the registry key:

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

The Trojan horse receives e-mails from a specific POP mail server.

Lockme: This is a Trojan package comprised of several different batch files, command-line utilities, applications, and an NT Rootkit. A compromised system provides several ways for a remote malicious user to take complete control of the computer.

PWSteal.Bancos: This is a Trojan Horse that mimics the online interfaces of certain Brazilian banks in an attempt to steal account information. This Trojan may arrive as the e-mail attachment, Book com amor.exe. When the e-mail attachment is executed, the dropper displays a message box, titled "BOOK COM AMOR." If you click Continue, the Trojan will install the following files in the %System% folder:

- Msvbvm60.dll: A legitimate .dll file, 1,388,544 bytes in length
- Winmaxy.exe: The Trojan, 258,048 bytes long

After the files are dropped, the Trojan is launched. When the Trojan executes, it sets itself to run on startup by modifying the registry and adding the value, "WinMenssage = %System%\winmaxy.exe," to the registry key:

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

If the file, C:\BancoBrasil\officeIE\officeIE.CAB, exists, the Trojan will move it to C:\officeIE.CAB. The Trojan monitors active Internet Explorer windows, waiting for you to open a Web page that matches the characteristics of certain banking sites. When such a site is opened, the Trojan displays one of several login screens, selected according to the title of the bank's Web page. The information entered on these screens may then be uploaded to an FTP site, which the Trojan's author controls.

Troj/Ataka-E: This is a multicomponent IRC backdoor Trojan. The main installer component (sx.exe) is typically downloded from the Internet by a downloader. The installer drops the numerous files into the folder Program Files\NetMeeting\conf\. Some of these files are clean and are not detected. It sets the following registry entry:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\NTsocket = C:\Program Files\NetMeeting\conf\NoeWinnt.exe

Troj/DownLdr-DI: This Trojan has been reported in the wild. It is a malicious program that downloads and deploys additional components from URLs stored (in encrypted form) inside the program. Because these components are fetched only when you run the Trojan, their contents may change at any time. There have been several reports of this Trojan from users who appear to have received it in an orchestrated e-mail blast, presumably by the Trojan's author.

Troj/Golon-A: This is a backdoor Trojan. It copies itself to the Windows system folder as logon.exe and sets the following registry entry:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\logon.exe =<Windows system>\logon.exe

Troj/Golon-A also creates several registry entries under:

- HKLM\Software\Microsoft\Kernel

Troj/Migmaf-A: This is a backdoor Trojan that allows unauthorized remote access to the computer over a network. It adds an entry to the registry at:

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

to run itself on system restart. Troj/Migmaf-A may act as reverse proxy web server on the victim's computer. This would allow a remote user to host undesirable websites via the victim's computer without being traced and shutdown.

Troj/Webber-A (Aliases: TrojanProxy.Win32.Webber.10, Backdoor.Berbew, BackDoor-AXJ, Downloader-DI): This Trojan has been reported in the wild. It is a backdoor Trojan with two components. The loader component downloads the main part from a web address into the system folder and executes it. The downloaded component is a password-stealing Trojan that attempts to extract sensitive information

from several locations on the system and sends them to CGI scripts at another web address. The downloaded component copies itself with a random name into the Windows system folder and drops and executes a DLL file (also with a random name) that runs the copy of the Trojan. In order to be started automatically the Trojan creates the following registry entries:

- HTLM\Software\Classes\CLSID\79FA9088-19CE-715D-D85A-216290C5B738\InProcServer32\
- HKLM\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad\Web Event Logger

The Trojan also functions as a web proxy.

Trojan.Ailati: This Trojan is written in Microsoft Visual Basic. It removes critical system folders from an infected computer. The Trojan has an icon that depicts the Italian flag. It creates 13 files to C:\ named Italy1.exe, through Italy13.exe. The files are 9 and 10 byte text files and are not executable. It searches for the C:\Windows folder. If the folder exists, the Trojan deletes it. Because C:\Windows is the default installation location on Windows 95/98/ME/XP, if Windows was installed to this location, this deletes the operating system. The Trojan also searches for C:\Program Files\Outlook Express. If the folder exists, the Trojan deletes it. This is the default location of Outlook Express application files. It displays the message: GOOD LUCK!!! This Trojan does not have mailing capabilities and does not set registry keys.

Trojan.Visages: This is a Trojan Horse that does not copy itself, drop files, or have a malicious payload. It is written in Microsoft Visual Basic. When Trojan.Visages is run, it displays the message, "Welcome to W32.2faced," when first run and makes continuous calls to the A: drive, so the drive is always spinning. The Trojan adds the value, “Microsoft Corporation"="<Trojan path/file name>,” to the registry key:

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

It loads at startup as a System Tray icon that looks like the Norton AntiVirus Auto-Protect icon. If the icon is double-clicked, it will display the message, "Are you Ready for when Jesus comes?" Clicking OK displays the message, "I Am."

W32.Spybot.dr: This is an installer that drops and executes W32.Spybot.Worm. It also installs a Backdoor Trojan that is detected as Backdoor.IRC.Cloner.