Department of Homeland Security
Information Analysis and Infrastructure Protection Directorate
CyberNotes

Issue #2004-05 *March 15, 2004*

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

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the Department of Homeland Security US-CERT web site at http://www.us-cert.gov.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between February 18 and March 12, 2004. 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
1st Class Internet Solutions[1]	Windows	1st Class Mail Server 4.0	A buffer overflow vulnerability exists due to a boundary error in 'mailsrv.dll,' which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	1st Class Mail Server Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Adobe Systems Inc.[2]	Windows	Acrobat Reader 5.1	A buffer overflow vulnerability exists due to a boundary error within the debugging functionality when parsing documents in the XML forms data format ('.xfdf'), which could let a remote malicious user execute arbitrary code.	Latest versions of Adobe products can be found at the following location: http://www.adobe.com/support/downloads/main.html	Acrobat Reader XFDF File Handler Remote Buffer Overflow CVE Name: CAN-2004-0194	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.

[1] SecurityTracker Alert, 1009279, March 2, 2004.

[2] NGSSoftware Insight Security Research Advisory, March 3, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Alcatel[3]	Multiple	Omni Switch 7700, 7800	A Denial of Service vulnerability exists due to an unknown error while handling certain traffic. The problem is in the handling of scans by third-party security software.	No workaround or patch available at time of publishing.	OmniSwitch 7000 Series Security Scan Denial of Service	Low	Bug discussed in newsgroups and websites. Vulnerability can be exploited using Nessus 2.0.9.
AMAX Information Technologies Inc.[4]	Windows NT 4.0/2000, XP	Magic Winmail Server 3.6	A vulnerability exits in 'ldaplib.php' due to insufficient verification of the 'keywork' parameter, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Magic Winmail Server LDapLib.PHP Remote Information Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
America OnLine[5]	Windows 95/98/ME/ NT 4.0/2000	Instant Messenger 4.3, 4.3.2229, 4.4-4.7, 4.7.2480, 4.8 .2646, 4.8.2616, 4.8.2790, 5.0.2938, 5.1.3036, 5.2.3292, 5.5, 5.5.3415 Beta	A vulnerability exists because 'Buddy' icons are stored in a predictable location, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	AOL Instant Messenger Buddy Icon	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Apache Software Foundation[6]	Mac OS X 10.x, Unix	Apache 1.3, 1.3.1, 1.3.3, 1.3.4, 1.3.6, 1.3.7 – dev, 1.3.9, 1.3.11, 1.3.12, 1.3.14, 1.3.17 1.3.20, 1.3.22-1.3.29	A vulnerability exists in 'mod_access' due to a failure to properly enforce IP restrictions that are defined without a proper netmask, which could let remote malicious user bypass access controls.	Patch available at: http://cvs.apache.org/viewcvs.cgi/apache-1.3/src/modules/standard/mod_access.c?r1=1.46&r2=1.47	Mod_Access Access Control Rule Bypass CVE Name: CAN-2003-0993	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Apache Software Foundation[7]	Mac OS X 10.x, Unix	Apache 2.0.35-2.0.48	A remote Denial of Service vulnerability exists due to a handling error within the SSL engine when receiving normal HTTP requests on the SSL port of a SSL-enabled server.	Patch available at: http://cvs.apache.org/viewcvs.cgi/httpd-2.0/modules/ssl/ssl_engine_io.c?r1=1.117&r2=1.118	Apache Mod_SSL HTTP Request Remote Denial of Service CVE Name: CAN-2004-0113	Low	Bug discussed in newsgroups and websites. There is no exploit code required.

[3] Bugtraq, February 19, 2004.
[4] Secunia Advisory, SA11015, March 2, 2004.
[5] Secunia Advisory, SA10930, February 20, 2004.
[6] SecurityFocus, March 9, 2004.
[7] Secunia Advisory, SA11092, March 10, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Apache Software Foundation[8]	Windows, Unix, MacOS X 10.x	Apache 0.8.11, 0.8.14, 1.0, 1.0.2, 1.0.3, 1.0.5, 1.1, 1.1.1, 1.2, 1.2.5, 1.3, 1.3.1, 1.3.3, 1.3.4, 1.3.6, 1.3.7 -dev, 1.3.9, 1.3.11, 1.3.12, 1.3.14, 1.3.17-1.3.20, 1.3.22-1.3.29, 2.0 a9, 2.0, 2.0.28, Beta, 2.0.32, 2.0.35, 2.0.36-2.0.48	A Directory Traversal vulnerability exists in Apache that is running on 'Cygwin' platforms, which could let a remote malicious user obtain sensitive information.	Patch available at: http://nagoya.apache.org/bugzilla/showattachment.cgi?attach_id=10222	Apache Cygwin Directory Traversal	Medium	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
Apple[9]	MacOS X	Darwin Streaming Server 4.1.3, Darwin Streaming Server 4.1.3	A remote Denial of Service vulnerability exists when a malicious user submits a 'DESCRIBE' request that contains specially crafted User-Agent fields.	Upgrades available at: http://www.info.apple.com/kbnum/	QuickTime/ Darwin Streaming Server Remote Denial of Service CVE Name: CAN-2004-0169	Low	Bug discussed in newsgroups and websites.
Apple[10]	MacOS X	Safari Beta 2, 1.0, 1.1	A Denial of Service vulnerability exists due to a failure to handle the creation of very large arrays using JavaScript.	No workaround or patch available at time of publishing.	Safari Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[8] STG Security Advisory, SSA-20040217-06, February 24, 2004.
[9] iDEFENSE Security Advisory 02.23.04, February 23, 2004.
[10] Secunia Advisory, SA11056, March 8, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Apple[11]	MacOS X	MacOS X 10.1-10.1.5, 10.2-10.2.8, 10.3-10.3.2, MacOS X Server 10.1-10.1.5, 10.2-10.2.8, 10.3-10.3.2	Multiple vulnerabilities exist: a format string vulnerability exists in the 'option_error __V()' function, which could let a malicious user obtain PAP/CHAP authentication credentials; a vulnerability exists in the 'DiskArbitration' implementation due to insecure initialization of writeable removable media; and a vulnerability exists in 'CoreFoundation' due to insufficient notification logging.	Upgrades available at: http://www.info.apple.com/kbnum/n120322	Mac OS X PPPD Format String Memory Disclosure CVE Names: CAN-2004-0165, CAN-2004-0167, CAN-2004-0168	Medium	Bug discussed in newsgroups and websites.
Apple[12]	MacOS X 10.x	Mac OS X 10.0 3, 10.0-10.0.4, 10.1-10.1.5, 10.2-10.2.8, 10.3-10.3.2	Multiple vulnerabilities exist: a vulnerability exists because the AFP client does not issue a warning to a user if an SSH session cannot be established with a server, which could lead to a false sense of security; a vulnerability exists because the AFP client does not differentiate between various encrypted authentication mechanisms, which could let a malicious user carry out a man-in-the-middle attack; and a vulnerability exists in the AFP client due to insufficient verification of a server's host key before a secure connection is established, which could let a malicious user carry out a man-in-the-middle attacks.	No workaround or patch available at time of publishing.	Mac OS X Apple Filing Protocol Client Multiple Vulnerabilities	Medium	Bug discussed in newsgroups and websites. There is no exploit code required. Vulnerability has appeared in the press and other public media.
ArGoSoft[13]	Windows 95/98/ME/ NT 4.0/2000	FTP Server 1.0, 1.2.2 .2, 1.4.1 .1-1.4.1 .5	Multiple vulnerabilities exist: two buffer overflow vulnerabilities exist due to the way the 'SITE ZIP' command is used because parameters are not checked for their length, which could let a remote malicious user execute arbitrary code; a vulnerability exists in the 'SITE UNZIP' command, which could let a remote malicious user obtain sensitive information; and a remote Denial of Service vulnerability exists in the 'SITE PASS' command when a malicious user submits a long password.	Upgrades available at: http://www.argosoft.com/applications/ftpserver/download.asp	ArGoSoft FTP Server Multiple Remote Vulnerabilities	Low/ Medium/ **High** **(Low if a DoS; Medium is sensitive information can be obtained; and High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.

[11] Apple Security Advisory, APPLE-SA-2004-02-23, February 24, 2004.
[12] Bugtraq, February 27, 2004.
[13] Securiteam, March 2, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Bolin Tech[14] ***Another exploit script published[15]***	**Windows, Unix**	**Dream FTP Server 1.02**	**A format string vulnerability exists in 'Server Log' when log information is displayed, 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.**	**BolinTech Dream FTP Server User Name Format String**	**Low/High** **(High if arbitrary code can be executed)**	**Bug discussed in newsgroups and websites. Exploit script has been published.**
BolinTech[16]	Windows, Unix	Dream FTP Server 1.02	A format string vulnerability exists when processing a malicious request from a client, which could let a malicious user cause a Denial of Service and possibly execute arbitrary code.	No workaround or patch available at time of publishing.	Dream FTP Server Format String	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
CalaCode.com[17]	Windows NT 4.0/2000, XP	@mail Webmail System 3.64	Multiple vulnerabilities exist: a Cross-Site Scripting vulnerability exists in the 'util.pl' script due to insufficient sanitization of user-supplied data, which could let a remote malicious user execute arbitrary HTML or script code; a Cross-Site Scripting vulnerability exists in 'showmail.pl' due to insufficient validation of the 'folder' parameter, which could let a remote malicious user execute arbitrary HTML or script code; and a remote Denial of Service vulnerability exists when a malicious users establishes approximately 600 connections to the POP3 service.	No workaround or patch available at time of publishing.	@mail Webmail System Cross-Site Scripting & Denial of Service	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required.
Caolan Mc-Namara[18]	Unix	XIntercept Talk xitalk 1.1.11	A vulnerability exists due to the way privileges are handled, which could let a malicious user execute arbitrary code.	**Debian:** http://security.debian.org/pool/updates/main/x/xitalk/	XInterceptTalk XITalk Arbitrary Command Execution CVE Name: CAN-2004-0151	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[14] SP Research Labs Advisory x09, February 6, 2004.
[15] SecurityFocus, March 9, 2004.
[16] SecurityTracker Alert, 1009295, March 3, 2004.
[17] Secunia Advisory, SA10978, February 26, 2004.
[18] Debian Security Advisory, DSA 462-1, March 12, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Chaogic Systems[19]	Windows, Unix	vHost 3.05 r1-r6, 3.0 4r1, 3.0 3r1, 3.02r1 & r2, 3.01r1, 3.0 0r1-r6	A Cross-Site Scripting vulnerability exits in the graphical user interface due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML or script code.	Upgrades available at: ftp://ftp.chaogic.com/pub/vhost-3.10r1.tar.gz	VHost Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Cisco Systems[20]	Multiple	CSS11000 Content Services Switch, CSS11050 Content Services Switch, CSS11150 Content Services Switch, CSS11800 Content Services Switch	A Denial of Service vulnerability exists in the management port due to a failure to handle certain malformed packets to port 5002/UDP.	Upgrades available at; http://www.cisco.com	Cisco Content Service Switch Management Port UDP Denial of Service	Low	Bug discussed in newsgroups and websites.
Cisco Systems[21]	Multiple	ONS 15327 Edge Optical Transport Platform, ONS 15454 Optical Transport Platform, ONS 15454 SDH Multiplexer Platform, 15600 Multiservice Switching Platform	Multiple vulnerabilities exist: a vulnerability exists in the TFTP service (port 69/UDP) 'GET' and 'PUT' commands due to insufficient authentication, which could let a remote malicious user cause a Denial of Service or obtain sensitive information; a vulnerability exists due to the way the network management applications' connection is handled, which could let a remote malicious user cause a Denial of Service; and a vulnerability exists in the Telnet service because super users can by default obtain a VxWorks shell even though their account has been locked out, disabled, or suspended, which could let a remote malicious user obtain unauthorized access.	Upgrade procedures available at: http://www.cisco.com/warp/public/707/cisco-sa-20040219-ONS.shtml	Cisco ONS Platform Vulnerabilities	Low/ Medium (Medium if sensitive information can be obtained or unauthorized access is obtained)	Bug discussed in newsgroups and websites.

[19] Secunia Advisory, SA11113, March 12, 2004.
[20] Cisco Security Advisory, 49584, March 4, 2004.
[21] Cisco Security Advisory, 48800, February 19, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Computer Associates [22]	Multiple	Unicenter TNG 2.4, 2.4.2	Multiple buffer overflow vulnerabilities exist in the 'awservices.exe' and 'cam.exe' daemons when handling client requests, which could let a remote malicious user execute arbitrary code with SYSTEM privileges.	Contact the vendor regarding obtaining updates.	Unicenter TNG Utilities Multiple Remote Buffer Overflow Vulnerabilities	**High**	Bug discussed in newsgroups and websites.
cPanel, Inc. [23]	Unix	cPanel 5.0, 5.3, 6.0, 6.2, 6.4-6.4.2, 7.0, 8.0, 9.0, 9.1	A vulnerability exists due to insufficient verification of user input passed to the 'user' parameter in the 'resetpass' section, which could let a remote malicious user execute arbitrary code.	The vendor has outlined that affected customers should perform the following to update their product: Perform the following as root from the shell. # /scripts/upcp	cPanel 'Resetpass' Remote Command Execution	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
cPanel, Inc. [24]	Unix	cPanel 5.0, 5.3, 6.0, 6.2, 6.4-6.4.2, 7.0, 8.0, 9.0, 9.1	A Cross-Site Scripting vulnerability exists because the 'dohtaccess.html' page does not filter HTML code from user-supplied input in the 'dir' field, which could let a remote malicious user execute arbitrary HTML or script code.	No workaround or patch available at time of publishing.	cPanel 'dir' Field Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
cPanel, Inc. [25]	Unix	cPanel 5.0, 5.3, 6.0, 6.2, 6.4-6.4.2, 7.0, 8.0, 9.0, 9.1	A vulnerability exists in the login script due to insufficient sanitization, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	cPanel Login Script Remote Command Execution	**High**	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit script has been published.
Dan Bernstein [26]	Unix	QMail 1.0 3, 1.0 2	A buffer overflow vulnerability exists in 'qmail-qmtpd,' which could let a malicious user obtain elevated privileges.	No workaround or patch available at time of publishing.	QMail-QMTPD Buffer Overflow	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[22] Immunity, Inc. Advisory, March 12, 2004.
[23] cPanel Security Advisory - CPANEL-2004:01-01, March 11, 2004.
[24] SecurityTracker Alert, 1009402, March 12, 2004.
[25] Bugtraq, March 12, 2004.
[26] SecurityTracker Alert, 1009306, March 3, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
David Lechnyr[27]	Unix	Confirm 0.50-0.55, 0.60-0.62	A vulnerability exists in the 'Procmail' script due to a failure to filter user-supplied input in e-mail headers, which could let a remote malicious user execute arbitrary commands.	Upgrades available at: http://hr.uoregon.edu/davidrl/confirm/confirm-0.70.tgz	Confirm E-Mail Header Remote Command Execution	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
DAWKCo ™ Software[28]	Windows	POP3 Server Hosting Version w/t Web MAIL Extension. 6.1	A vulnerability exists due to a failure to properly handle timed out and logged out sessions, which could let a malicious user obtain unauthorized access.	No workaround or patch available at time of publishing.	POP3 with WebMAIL Extension Session Timeout Unauthorized Access	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Dell[29]	Multiple	Open Manage Web Server 3.4, 3.7	A buffer overflow vulnerability exists due to insufficient bounds checking performed on POST request data, which could let a remote malicious user execute arbitrary code.	Patches available at: Http://support.dell.com/filelib/	OpenManage Web Server POST Request Heap Overflow	**High**	Bug discussed in newsgroups and websites.
Dell[30]	Windows	True Mobile 1300 WLAN Mini-PCI Card Utility 3.10.39 .0	A vulnerability exists in the 'Help' command, which could let a malicious user obtain SYSTEM privileges.	No workaround or patch available at time of publishing.	TrueMobile 1300 WLAN Help Application	**High**	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published. Vulnerability has appeared in the press and other public media.
Digital Reality[31]	Windows	Haege-monia 1.0, 1.0.4, 1.0.5, 1.0.7	A remote Denial of Service vulnerability exists due to a failure to validate packet data size input supplied by a client.	No workaround or patch available at time of publishing.	Haegemonia Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.

[27] Lam3rZ Security Advisory #3/2004, February 23, 2004.
[28] SecurityFocus, March 4, 2004.
[29] SecurityFocus, March 4, 2004.
[30] Securiteam, February 26, 2004.
[31] Bugtraq, February 24, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Dogpatch Software[32]	Windows	CFWeb-store 5.0	Several vulnerabilities exist: a vulnerability exists in 'index.cfm' due to insufficient sanitization of the 'category_id,' 'product_id,' and 'feature_id'" parameters, which could let a remote malicious user execute arbitrary SQL commands; and a Cross-Site Scripting vulnerability exists due to insufficient sanitization of user-supplied input in an URL, which could let a remote malicious user execute arbitrary HTML or script code.	Update available at: http://www.cfwebstore.com/	CFWebstore Input Validation & Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
EMUMail Inc.[33]	Windows NT 4.0/2000, XP	EMU Webmail 5.2.7	Multiple vulnerabilities exist: a vulnerability exists in the 'emumail.fcgi' script due to insufficient filtering, which could let a remote malicious user execute arbitrary HTML or script code; a vulnerability exists because the username and password fields of the login page are not filtered, which could let a remote malicious user obtain sensitive information; and a vulnerability exists in the 'init.emu' file because it contains the installation path, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	EMU Webmail Multiple Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[32] S-Quadra Advisory #2004-03-12, March 12, 2004.
[33] SecurityTracker Alert, 1009397, March 11, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Epic Games[34]	Windows, MacOS, Unix	Unreal Engine 436, 433, 226f, Unreal Tournament 2003 2199 win32, 2003 2199 linux, 2003 Demo Version 2206 win32, 2003 Demo Version 2206 linux, Unreal Tournament Server 436.0	A format string vulnerability exists in the Unreal Tournament server engine due to insufficient sanitization of user-supplied network data, which could let a remote malicious user cause a Denial of Service and potentially execute arbitrary code.	No workaround or patch available at time of publishing.	Epic Games Unreal Tournament Server Engine Remote Format String	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
extremail.com[35]	Unix	eXtremail 1.0-1.0.3, 1.1-1.1.10, 1.5 –8, 1.5 –5, 1.5, 1.5.9	A vulnerability exists due to insufficient verification of authentication requests when passwords start with a digit, which could let a malicious user bypass authentication to obtain unauthorized access.	No workaround or patch available at time of publishing.	eXtremail Authentication Bypass	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
EZBoard, Inc.[36]	Multiple	EZBoard 7.3 u	A Cross-Site Scripting vulnerability exists due to a failure to filter illegal characters in [font] tags, which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	EZBoard Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Frank Pilhofer[37]	Windows, Unix	UU-Deview 0.5.18, 0.5.19	A vulnerability exists due to the insecure creation of temporary files, which could let a remote malicious user cause a Denial or Service or a loss of data.	**OpenPKG:** ftp://ftp.openpkg.org/release/	UUDeview Insecure Temporary File Creation	Low/ Medium (Medium if data is lost)	Bug discussed in newsgroups and websites.

[34] Bugtraq, March 10, 2004.
[35] Bugtraq, February 26, 2004.
[36] Bugtraq, February 23, 2004.
[37] OpenPKG Security Advisory, OpenPKG-SA-2004.006, March 12, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
FreeBSD [38]	Unix	FreeBSD 5.1 – Release, 5.1, 5.2 – Release, 5.2	A vulnerability exists due to an error in the 'jail_attach()' system call when verifying the privilege level of a calling process, which could let a malicious user obtain unauthorized access to other jails.	Patches available at: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-04:03/jail.patch	FreeBSD Unauthorized Jailed Process Attaching CVE Name: CAN-2004-0126	Medium	Bug discussed in newsgroups and websites.
FreeBSD/ OpenBSD [39]	Unix	FreeBSD 4.6.2, 4.7-4.9, 5.0-5.2; OpenBSD 3.3, 3.4	A remote Denial of Service vulnerability exists due to the way out-of-sequence packets are handled.	**FreeBSD:** ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-04:04/tcp47.patch **OpenBSD:** ftp://ftp.openbsd.org/pub/OpenBSD/patches/	BSD Out-of-Sequence Packets Remote Denial of Service CVE Name: CAN-2004-0171	Low	Bug discussed in newsgroups and websites.
F-Secure[40]	Unix	Anti-Virus For Linux 4.52	An unspecified vulnerability exists which could let malicious code bypass scanning. *Note: This issue is reportedly related to detections of W32.Sober.D@mm.*	Hotfix available at: ftp://ftp.f-secure.com/support/hotfix/fsav/fsav-4.52-hotfix3.tgz	Anti-Virus For Linux Unspecified Scanner Bypass	Medium	Bug discussed in newsgroups and websites.
F-Secure[41]	Unix	SSH Server 3.0.0-3.0.9, 3.1 .0	A vulnerability exists due to a design error, which could let a remote malicious user bypass virus detection.	Hotfix available at: ftp://ftp.f-secure.com/support/hotfix/fsav/fsav-4.52-hotfix3.tgz	F-Secure SSH Server Policy Evasion	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
GameSpy [42]	Windows, MacOS, Unix	GameSpy Software Development Kit	A remote Denial of Service vulnerability exists due to a failure to handle exceptional conditions during network communications.	Fixes available at: http://www.gamespy.com/	Gamespy Software Development Kit Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Giga-Byte Technology [43]	Multiple	Gigabyte Gn-B46B	An authentication vulnerability exists because a malicious user can host a copy of the router's HTML menu locally on their system.	No workaround or patch available at time of publishing.	Gn-B46B Wireless Router Authentication Bypass	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
GNU[44]	Unix	Automake 1.7-1.7.9, 1.8.1, 1.8.2	A vulnerability because the '/lib/am/distdir.am' component creates a temporary directory in an unsafe manner (using 'mkdir_p'), which could let a malicious user modify data or obtain elevated privileges.	Upgrades available at: http://ftp.gnu.org/gnu/automake/automake-1.8.tar.gz	GNU Automake Insecure Temporary Directory Creation	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[38] FreeBSD Security Advisory, FreeBSD-SA-04:03.jail, February 27, 2004.
[39] FreeBSD Security Advisory, FreeBSD-SA-04:04.tcp, March 2, 2004.
[40] SecurityFocus, March 10, 2004.
[41] SecurityFocus, March 9, 2004.
[42] SecurityFocus, February 24, 2004.
[43] Bugtraq, February 24, 2004.
[44] SecurityTracker Alert, 1009345, March 8, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
GNU[45]	Unix	Anubis 3.6.2, 3.9.93	Several vulnerabilities exist: format string vulnerabilities exist in 'ssl.c,' 'errs.c,' and 'log.c,' which could let a malicious user execute arbitrary code; and a vulnerability exists due to the way the IDENT protocol is processed, which could let a malicious user execute arbitrary code.	Patches available at: http://savannah.gnu.org/patch/	Anubis Multiple Vulnerabilities	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published.
GNU[46]	Unix	Coreutils 4.5.1-4.5.12, 5.0, 5.0.1, 5.0.90, 5.0.91, 5.1-5.1.3, fileutils 4.0, 4.0.33, 4.0.36, 4.1, 4.1.1, 4.1.5-4.1.7, 4.1.9, 4.1.11	A vulnerability exists in the coreutils 'dir' command, which could let a malicious user cause a Denial of Service and possibly execute arbitrary code.	Upgrade available at: http://ftp.gnu.org/pub/gnu/coreutils/coreutils-5.2.0.tar.gz	Coreutils 'DIR' Command	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
GNU[47]	Windows, Unix	MyProxy 20030629	A Cross-Site Scripting vulnerability exists due to insufficient sanitization of user-supplied input in URLs, which could let a remote malicious user execute arbitrary HTML or script code.	No workaround or patch available at time of publishing.	MyProxy Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.

[45] SecurityTracker Alert, 1009272, March 1, 2004.
[46] Bugtraq, March 2, 2004.
[47] Bugtraq, March 11, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
GNU[48, 49, 50, 51] ***SGI issues another advisory***[52]	**Unix**	**Mailman 1.0, 1.1, 2.0 beta3 - beta5, 2.0-2.0.13, 2.1, 2.3**	**A remote Denial of Service vulnerability exists in 'MailCommandHandler.py' when a malicious user submits a specially crafted e-mail message.**	**Upgrade available at:** **http://ftp.gnu.org/gnu/mailman/** **Debian:** **http://security.debian.org/pool/updates/main/m/mailman/** **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** **RedHat:** **http://rhn.redhat.com/errata/RHSA-2004-019.html** **SGI:** **ftp://patches.sgi.com/support/free/security/patches/ProPack/2.3/patch10050.tar.gz**	**GNU Mailman Remote Denial of Service** **CVE Name: CAN-2003-0991**	**Low**	**Bug discussed in newsgroups and websites.**
Hewlett Packard Company[53]	Unix	Compaq Tru64 5.1 b, 5.1 b PK2 (BL22), 5.1 a PK6 (BL24)	A vulnerability exists when IPSec and Internet Key Exchange (IKE) is used with digital certificates, which could let a remote malicious user obtain elevated privileges.	ERP Kit available at: http://www.itrc.hp.com/service/patch/patchDetail.do?patchid=T64KIT0021591-V51BB24-ES-20040216	Tru64 UNIX Unspecified IPsec/IKE Remote Privilege Escalation	Medium	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Hewlett Packard Company[54]	Windows NT 4.0/2000, 2003, Unix	HTTP Server 5.0, 5.92	A vulnerability exists if HP HTTP has been configured to accept 'Anonymous Access' because it is possible to upload a client certificate that will be accepted as a valid certificate for authorization, which could let a malicious user obtain access to administrative functions.	Patches available at: http://h18023.www1.hp.com/support/files/Server/us/download/20197.html	HP HTTP Server Trusted Certificates	**High**	Bug discussed in newsgroups and websites.
Hot Open Tickets[55]	Windows, Unix	Hot Open Tickets 2.0 c	A vulnerability exists due to an unspecified error, which can be exploited by malicious authenticated users to manipulate their own security level to obtain administrative privileges.	Upgrade available at: http://sourceforge.net/project/showfiles.php?group_id=89508	Hot Open Tickets Unspecified Elevated Privileges	**High**	Bug discussed in newsgroups and websites.
IBM[56]	Unix	AIX 4.3.3	A vulnerability exists in the 'rexecd' implementation, which could let a remote malicious user obtain ROOT privileges.	Patches available at: http://www-912.ibm.com/eserver/support/fixes/fcgui.jsp	AIX 'Rexecd' ROOT Privileges	**High**	Bug discussed in newsgroups and websites.

[48] Debian Security Advisories, DSA 436-1 & DSA 436-2, February 8 & 21, 2004.
[49] RedHat Security Advisory, RHSA-2004:019-04, February 9, 2004.
[50] SGI Security Advisory, 20040201-01-U, February 11, 2004.
[51] Mandrake Linux Security Update Advisory, MDKSA-2004:013, February 13, 2004.
[52] SGI Security Advisory, 20040202-01-U:, February 26, 2004.
[53] Hewlett Packard Security Bulletin, HPSBTU00030, March 3, 2004.
[54] HP Software Security Response Team Security Advisory, SSRT4679, March 12, 2004.
[55] Secunia Advisory, SA11018, March 2, 2004.
[56] IBM Global Services Managed Security Services, MSS-OAR-E01-2004:0303.1, March 9, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
IBM[57]	Windows	DB2 Universal Database for Windows 8.1	A vulnerability exists in 'DB2RCMD.EXE,' which could let a remote malicious user obtain administrative access.	Patch available at: http://www-306.ibm.com/cgi-bin/db2www/data/db2/udb/winos2unix/support/v8fphist.d2w/report	DB2 Remote Command Server Administrative Access	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
iGeneric[58]	Windows, Unix	Free Shopping Cart 1.4	A Cross-Site Scripting vulnerability exists in 'page.php' due to insufficient validation of user-supplied input in the 'type_id' field, which could let a remote malicious user execute arbitrary HTML or script code.	No workaround or patch available at time of publishing.	IGeneric Free Shopping Cart Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
Inari, Inc. [59]	Windows	Avirt SOHO 4.3	A buffer overflow vulnerability exists in the embedded server component when handling HTTP GET requests, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.	No workaround or patch available at time of publishing.	Avirt Soho Server HTTP GET Remote Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
Inari, Inc. [60]	Windows	Avirt Voice 4.0	A buffer overflow vulnerability exists in the embedded server component when handling HTTP GET requests, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.	No workaround or patch available at time of publishing.	Avirt Voice HTTP GET Remote Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
Infopulse Electronic Commerce B.V.[61]	Windows	Proxy-Pro Professional Gate Keeper 4.7	A buffer overflow vulnerability exists in 'GKHttp.dll' due to a boundary error, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Proxy-Pro Professional GateKeeper Web Proxy Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published.

[57] NGSSoftware Insight Security Research Advisory, #NISR09032004, March 9, 2004.
[58] Secunia Advisory, SA11009, March 1, 2004.
[59] Bugtraq, February 23, 2004.
[60] Bugtraq, February 23, 2004.
[61] Corompuer Security Advisory, February 23, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Internet Security Systems[62]	Multiple	Real Secure Network 7.0, XPU 20.15-22.9, Server Sensor 7.0 XPU 20.16-22.9, Proventia A Series XPU 20.15-22.9, G Series XPU 22.3-22.9, M Series XPU 1.3-1.7, Real Secure Desktop 7.0 eba-ebh, 3.6 ebr-ecb, Real Secure Guard 3.6 ebr-ecb, Real Secure Sentry 3.6 ebr-ecb, BlackICE PC Protection 3.6 cbr-ccb, Server Protection 3.6 cbr-ccb	A vulnerability exists in the SMB (Server Message Block) protocol parsing routines of the ISS Protocol Analysis Module (PAM) component found in some ISS products due to insufficient bounds checking of protocol fields, which could let a malicious user execute arbitrary code.	Upgrades available at: http://www.iss.net/download	Internet Security Systems Protocol Analysis Module SMB Parsing Heap Overflow	**High**	Bug discussed in newsgroups and websites.
iNvicta[63]	Windows	wMCam Server 2.1.348	A remote Denial of Service vulnerability exists due to a failure to handle malformed requests.	No workaround or patch available at time of publishing.	WMCam Server Remote Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.

[62] Internet Security Systems Security Alert, February 26, 2004
[63] Bugtraq, March 10, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Invision Power Services[64]	Windows, Unix	Invision Board 1.0, 1.0.1, 1.1.1, 1.1.2, 1.2, 1.3, 2.0, 2.0 Alpha 3	An input validation vulnerability exists in ‘search.php’ due to insufficient sanitization of the ‘st’ parameter, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Invision Power Board Input Validation	**High**	Bug discussed in newsgroups and websites.
Invision Power Services[65]	Windows, Unix	Invision Board 1.3	A vulnerability exists when an invalid request is submitted for uploading an image file, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Invision Power Board Information Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Invision Power Services[66]	Windows, Unix	Invision Board 1.3 Final	Multiple Cross-Site Scripting vulnerabilities exist due to insufficient sanitization of input supplied via the 'c,' 'f,’’ 'showuser,' and 'username' URI parameters, which could let a remote malicious user execute arbitrary HTML or script code.	No workaround or patch available at time of publishing.	Invision Power Board Multiple Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Invision Power Services[67]	Windows, Unix	Invision Board 1.3 Final	A Cross-Site Scripting vulnerability exists in the ‘pop; URL parameter due to insufficient sanitization, which could let a remote malicious user execute arbitrary HTML or script code.	No workaround or patch available at time of publishing.	Invision Power Board Pop Parameter Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
IP3 Networks[68]	Multiple	IP3 NetAccess Campus and MDUs, Hospitality, Wireless HotSpots, Wireless HotZones & Small Hotels, Wireless ISPs & MDUs	A vulnerability exists due to a failure to sanitize user input, which could let a remote malicious user execute arbitrary SQL.	No workaround or patch available at time of publishing.	IP3 NetAccess Appliance SQL Injection	**High**	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.

[64] Secunia Advisory, SA11008, March 1, 2004.
[65] Bugtraq, March 5, 2004.
[66] SecurityFocus, February 28, 2004.
[67] SecurityFocus, March 9, 2004.
[68] SecurityFocus, March 12, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
IpSwitch[69] ***Another exploit script published***[70]	**Windows NT 4.0/2000, XP, 2003**	**IMail 8.0.3, 8.0.5**	**A buffer overflow vulnerability exists in 'iLDAP.exe' due to a boundary error when handling tags in LDAP messages, which could let a remote malicious user execute arbitrary code.**	**Hotfix available at:** **ftp://ftp.ipswitch.com/Ipswitch/Product_Support/IMail/im805HF2.exe**	**IMail Server Remote LDAP Daemon Buffer Overflow**	**High**	**Bug discussed in newsgroups and websites. Exploit script has been published.**
Jabber Studio[71]	Unix	Jabber Gadu-Gadu Transport 2.0-2.0.7	Multiple remote Denial of Service vulnerabilities exist due to various errors when importing rosters.	Upgrades available at: http://www.jabberstudio.org/projects/jabber-gg-transport/releases/download.php&file=jabber-gg-transport-2.0.8.tar.gz	Jabber Gadu-Gadu Transport Multiple Remote Denials of Service	Low	Bug discussed in newsgroups and websites.
Justin C. Kibell[72]	Unix	xboing 2.4	Multiple buffer overflow vulnerabilities exists due to insufficient validation of user-supplied environment variables, which could let a malicious user execute arbitrary code.	**Debian:** http://security.debian.org/pool/updates/main/x/xboing/	xboing Buffer Overflows CVE Name: CAN-2004-0149	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
LionMax Software[73]	Windows	Chat Anywhere 2.72	A vulnerability exists when handling nicknames due to an input validation error, which could let a malicious user circumvent certain administrative user management features.	Upgrade available at: http://www.lionmax.com/download.htm#ca	Chat Anywhere Input Validation	Medium	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
Live Journal[74]	Unix	Live Journal 1.0, 1.1	A Cross-Site Scripting vulnerability exists due to a failure to filter parentheses and semicolons from URLs to background images and from stylesheets, which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	LiveJournal Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Macro-media[75]	MacOS X	Contribute 2.0, Studio MX 2004	A vulnerability exists due to a design error that causes the creation of a setuid binary that is globally writable, which could let a malicious user obtain elevated privileges.	Patch available at: http://download.macromedia.com/pub/updates/licensing/hotfix/osx_upgrades_1_039en.dmg	Studio MX 2004 /Contribute 2 Local Privilege Escalation	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[69] iDEFENSE Security Advisory, February 17, 2004.
[70] SecurityFocus, February 19, 2004.
[71] Secunia Advisory, SA10974, February 25, 2004.
[72] Debian Security Advisory, DSA 451-1, February 27, 2004.
[73] Bugtraq, March 9, 2004.
[74] Bugtraq, February 19, 2004.
[75] Macromedia Security Bulletin, March 12, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Michael Speck[76]	Unix	Lgames LBreakout 2 2.0, 2.0.1, 2.1-2.1.2, 2.2-2.2.2	A buffer overflow vulnerability exists due to a boundary error when handling certain environment variables, which could let a malicious user execute arbitrary code.	**Debian:** http://security.debian.org/pool/updates/main/l/lbreakout2/	LBreakout2 Remote Buffer Overflow CVE Name: CAN-2004-0158	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Microsoft[77]	Windows 95/98/ME/ NT 4.0/2000, XP, 2003	Internet Explorer 5.5, SP1&SP2, 6.0, SP1	A vulnerability exists due to an access validation error within the event handling routines, which could let a malicious user capture keystrokes from a foreign domain.	Microsoft has reportedly not categorized this as a vulnerability, but will address it in a future service pack. Microsoft advises users to follow best practices when browsing: http://www.microsoft.com/security/incident/spoof.asp	Internet Explorer Cross-Domain Event Leakage	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Microsoft[78]	Widows	MSN Mes-senger Service 6.0, 6.1	A vulnerability exists due to the way file requests are handled, which could let a remote malicious user obtain sensitive information.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/ms04-010.mspx	MSN Messenger Information Disclosure CVE Name: CAN-2004-0122	Medium	Bug discussed in newsgroups and websites.
Microsoft[79]	Windows 98/ME/NT 4.0,/2000, XP	Office XP, SP1& SP2, Outlook 2002, SP1 & SP2	A vulnerability exists due to the way 'mailto' URLs are handled, 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/security/bulletin/ms04-009.mspx	Outlook 'Mailto' Parameter Arbitrary Code Execution CVE Name: CAN-2004-0121	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
Microsoft[80]	Windows 2000	Windows Media Services 4.1	A remote Denial of Service vulnerability exists due to the way TCP/IP connections are handled.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/ms04-008.mspx	Windows Media Services Remote Denial of Service CVE Name: CAN-2003-0905	Low	Bug discussed in newsgroups and websites.

[76] Debian Security Advisory, DSA 445-1, February 22, 2004.
[77] iDEFENSE Security Advisory, February 27, 2004.
[78] Microsoft Security Bulletin MS04-010, March 9, 2004
[79] Microsoft Security Bulletin MS04-009 1.0, 2.0, 2.1, March 9 & 10, 2004.
[80] Microsoft Security Bulletin MS04-008, March 9, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [81]	Windows 98/NT 4.0/2000, XP, 2003	2000 Advanced Server, SP1-SP3, Data-center Server, SP1-SP3, Profes-sional, SP1-SP3, Server, SP1-SP3, Windows 98, 98SE, NT Enterprise Server 4.0, SP1-SP6a, Server 4.0, SP1-SP6a, Terminal Server 4.0, SP1-SP6, Work-station 4.0, SP1-SP6a, Server 2003 Data center Edition, 64-bit, 2003 Enterprise Edition, 64-bit, Standard Edition, Web Edition, XP 64-bit Edition, SP1, 64-bit Edition Version 2003, SP1, Home, SP1, Media Center Edition, Profes-sional SP1	Multiple buffer overflow vulnerabilities exist in the ASN.1 library in the 'ASN1BERDecDouble' and 'ASN1PERDecDouble' functions, which could let a malicious user execute arbitrary code.	The first issue described concerning the ASN1BERDecDouble function is reportedly fixed in Microsoft Windows 2000 SP4. The issue in the ASN1PERDecDouble function has allegedly been fixed with the updates provided in MS04-007.	Microsoft ASN.1 Library Multiple Stack-Based Buffer Overflows	**High**	Bug discussed in newsgroups and websites.

[81] SecurityFocus, February 25, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [82]	Windows 95/98/ME/ NT 4.0/2000, XP	Outlook 2000, SP1-SP3, 2002, SP1&SP2, 2003, Outlook Express 4.0, 4.0 1 SP2, 4.27.3110, 4.72.2106, 4.72.3120, 4.72.3612, 5.0 1, 5.0, 5.5, 6.0	A vulnerability exists because various files are stored in predictable locations, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Multiple Outlook/ Outlook Express Predictable File Location Vulnerabilities	**High**	Bug discussed in newsgroups and websites.
Microsoft [83]	Windows XP	Windows XP Home, SP1, XP Media Center Edition, XP Profes-sional, SP1	Vulnerabilities exist due to boundary errors when processing Enhanced Metafiles, 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.	Windows XP explorer.exe Multiple Memory Corruption Vulnerabilities	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Exploit has been published.
Motorola [84]	Multiple	Motorola T720	A remote Denial of Service vulnerability exists when a malicious user submits an excessive amount of IP traffic.	No workaround or patch available at time of publishing.	Motorola T720 Phone Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Mozilla. org [85]	Windows 95/98/ME/ NT 4.0/2000, MacOS, MacOS X, Unix	Mozilla Browser 0.8, 0.9.2.1, 0.9.2-0.9.9, 0.9.35, 0.9.48, 1.0, RC1& RC2, 1.0.1, 1.0.2, 1.1-1.5	A Cross-Site Scripting vulnerability exists in 'nsDOMClassInfo.cpp' and occurs when a large number of event handlers are used within HTML tags, which could let a remote malicious user execute arbitrary code.	The vulnerability has been fixed in versions 1.6b and 1.4.2 available at: http://www.mozilla.org/	Mozilla Browser Zombie Document Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites.
mtools. linux.lu [86]	Unix	MTools 3.9.1-3.9.9	A vulnerability exists in the 'mformat' program, which could let a malicious user obtain root privileges.	**Mandrake:** http://www.mandrakesecure.net/en/ftp.php	MTools MFormat Root Privileges	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.

[82] Bugtraq, February 12, 2004.
[83] Secunia Advisory, SA10968, February 25, 2004.
[84] Bugtraq, March 1, 2004.
[85] Public Security Advisory, Sandblad #13, February 25, 2004.
[86] Mandrake Linux Security Update Advisory, MDKSA-2004:016, February 25, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[87]	Multiple	Double Precision Incorporated Courier MTA 0.43, 0.43.1, 0.43.2, 0.44, 0.44.2, SqWebMail 3.5.2, 3.5.3, 3.6.0-3.6.2; Inter7 Courier-IMAP 1.6, 1.7, 2.0 .0, 2.1-2.1.2, 2.2 .0, 2.2.1	Multiple buffer overflow vulnerabilities exist in the 'SHIFT_JIS' converter in 'shiftjis.c' and 'ISO2022JP' converter in 'so2022jp.c' due to boundary errors, which could let a remote malicious user execute arbitrary code.	**Double Precision Inc.:** http://www.courier-mta.org/download.php **Inter7:** http://www.courier-mta.org/download.php	Courier Multiple Remote Buffer Overflows	**High**	Bug discussed in newsgroups and websites.
Multiple Vendors [88, 89, 90] ***More advisories issued***[91, 92]	**Windows, Unix**	**Metamail 2.7 & prior; RedHat Advanced Workstation for the Itanium Processor 2.1, Enterprise Linux WS 2.1, ES 2.1, AS 2.1**	**Multiple vulnerabilities exist: a format string vulnerability exists in the 'SaveSquirrelFile()' function, which could let a remote malicious user execute arbitrary code; a format string vulnerability exists in the 'PrintHeader()' function, which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability exists in the 'PrintHeader()' function, which could let a remote malicious user execute arbitrary code; and a buffer overflow vulnerability exists in the 'splitmail' application in the 'ShareThisHeader()' function, which could let a remote malicious user execute arbitrary code.**	**Mandrake:** **http://www.mandrakesecure.net/en/advisories/** **RedHat:** **http://rhn.redhat.com/errata/RHSA-2004-073.html** **Slackware:** **ftp://ftp.slackware.com/pub/slackware/slackware-8.1/patches/packages/metamail-2.7-i386-2.tgz** ***Debian:*** **http://security.debian.org/pool/updates/main/m/metamail/** ***SGI:*** **ftp://patches.sgi.com/support/free/security/patches/**	**Metamail Multiple Buffer Overflow & Format String Vulnerabilities** **CVE Names: CAN-2004-0104, CAN-2004-0105**	**High**	**Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.**

[87] Secunia Advisory, SA11087, March 11, 2004.
[88] Slackware Security Advisory, SSA:2004-049-02, February 18, 2004.
[89] RedHat Security Advisory, RHSA-2004:073-07, February 18, 2004.
[90] Mandrake Linux Security Update Advisory, MDKSA-2004:014, February 19, 2004.
[91] Debian Security Advisory DSA 449-1, February 24, 2004.
[92] SGI Security Advisory, 20040203-01-U, February 26, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [93, 94, 95, 96, 97, 98, 99, 100] ***More vendor advisories issues & another exploit script published*** [101, 102, 103, 104, 105, 106]	**Unix**	**Linux kernel 2.2-2.2.24, 2.4.0, test1-test12, 2.4-2.4.24, 2.6. text1-test10, 2.6.1-2.6.2; Netwosix Netwosix Linux 1.0; RedHat kernel-2.4.20-8, athlon. rpm, i386.rpm, i686.rpm, kernel-bigmem-2.4.20-8.i686. rpm, kernel-BOOT-2.4.20-8.i386. rpm, kernel-doc-2.4.20-8.i386. rpm, kernel-smp-2.4.20-8, athlon. rpm, i686.rpm, kernel-source-2.4.20-8.i386. rpm**	**A vulnerability exists in the 'do_mremap' system function due to insufficient checking of return values, which could let a malicious user execute arbitrary code with ROOT privileges.**	**Patches available at:** **http://www.kernel.org/pub/linux/kernel/v2.6/linux-2.6.3.tar.bz2** **http://www.kernel.org/pub/linux/kernel/v2.6/patch-2.6.3.bz2** **Conectiva:** **ftp://atualizacoes.conectiva.com.br/8/RPMS/** **Debian:** **http://security.debian.org/pool/updates/main/k/kernel-source-2.4.18/** **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/** **RedHat:** **ftp://updates.redhat.com/** **Slackware:** **ftp://ftp.slackware.com/pub/slackware/slackware-current/slackware/** **SuSE:** **ftp://ftp.suse.com/pub/suse/i386/update/8.2/rp** **Trustix:** **ftp://ftp.trustix.org/pub/trustix/updates/2.0/rpms/** ***Immunix:*** **http://download.immunix.org/ImmunixOS/7+/Updates/RPMS/** ***Mandrake:*** *http://www.mandrakesecure.net/en/advisories/* ***SGI:*** **ftp://patches.sgi.com/support/free/security/** ***SmoothWall:*** http://smoothwall.net/u/ ***TurboLinux:*** **ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/**	**Linux Kernel do_mremap Function** **CVE Name: CAN-2004-0077**	**High**	**Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.**

[93] Debian Security Advisories DSA 438-1-DSA 442-1, DSA 444-1, February 18-20, 2004.
[94] Fedora Security Update Notifications, FEDORA-2004-079 & 080, February 18 & 19, 2004.
[95] Red Hat Security Advisory, RHSA-2004:065-01, February 18, 2004.
[96] Slackware Security Advisory, SSA:2004-049-01, February 18, 2004.
[97] SUSE Security Announcement, SuSE-SA:2004:005, February 18, 2004.
[98] Trustix Secure Linux Security Advisory, TSLSA-2004-0007, February 18, 2004.
[99] Netwosix Linux Security Advisory, February 20, 2004
[100] Conectiva Linux Security Announcement, CLA-2004:820, February 20, 2004.
[101] Turbolinux Security Advisory, TLSA-2004-7, February 23, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [107, 108]	Unix	GNOME Gdk Pixbuf 0.18, 0.20; RedHat Advanced Workstation for the Itanium Processor 2.1, Enterprise Linux WS 3, 2.1, ES 3, 2.1, AS 3, AS 2.1, gdk-pixbuf-0.18.0-7.i386.rpm, gdk-pixbuf-devel-0.18.0-7.i386.rpm, gdk-pixbuf-gnome-0.18.0-7.i386.rpm	A Denial of Service vulnerability exists in the GdkPixbuf library due to a handling error when displaying BMP images.	**Mandrake:** http://www.mandrakesecure.net/en/advisories/ **RedHat:** ftp://updates.redhat.com/9/en/os/i386	GdkPixbuf Denial of Service CVE Name: CAN-2004-0111	Low	Bug discussed in newsgroups and websites.
Multiple Vendors [109, 110] ***More advisories issued***[111, 112,]	**Unix**	**Linux kernel 2.4.0, test1-test12, 2.4-2.4.24**	**A vulnerability exists because the Vicam USB driver does not use the copy_from_user() function to access userspace, which could let a local process cross security boundaries..**	**Upgrade available at:** **http://www.kernel.org/pub/linux/kernel/v2.4/linux-2.4.25.tar.bz2** **RedHat:** **ftp://updates.redhat.com/9/en/os/** **SuSE:** **ftp://ftp.suse.com/pub/suse** ***Fedora:*** **http://download.fedoralegacy.org/redhat/7.2/updates/** ***Mandrake:*** **http://www.mandrakesecure.net/en/mlist.php**	**Linux Kernel Vicam USB Driver** **CVE Name: CAN-2004-0075**	**Medium**	**Bug discussed in newsgroups and websites.**

[102] SecurityFocus, March 3, 2004.
[103] Immunix Secured OS Security Advisory, IMNX-2004-7+-001-01, February 26, 2004.
[104] Mandrakelinux Security Update Advisory, MDKSA-2004:015-1, February 26, 2004.
[105] SGI Security Advisory, 20040204-01-U, February 28, 2004.
[106] SmoothWall Limited Product Advisory, SWL-2004:002, March 3, 2004.
[107] Mandrakelinux Security Update Advisory, MDKSA-2004:020, March 10, 2004.
[108] Red Hat Security Advisories, RHSA-2004:102-0 & RHSA-2004:103-05, March 10, 2004.
[109] SUSE Security Announcement, SuSE-SA:2004:005, February 18, 2004.
[110] Red Hat Security Advisory, RHSA-2004:065-01, February 18, 2004.
[111] Mandrake Linux Security Update Advisory, MDKSA-2004:015-1, February 26, 2004.
[112] Fedora Legacy Update Advisory, FLSA:1284, March 2, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [113, 114]	Unix	RedHat sysstat-4.0.7-3.i386.rpm; SGI ProPack 2.3, 2.4; Sysstat Sysstat 4.0.7, 4.1.1-4.1.7, 5.0.1	Two vulnerabilities exist: a vulnerability exists in the monitoring utility due to insecure creation of temporary files, which could let a malicious user corrupt system files, cause a loss of data, or a Denial of Service; and a vulnerability exists in the 'isag' utility because temporary files are created with predictable names, which could let a malicious user cause a Denial of Service or obtain elevated privileges.	**RedHat:** ftp://updates.redhat.com/9/en/os/i386/sysstat-4.0.7-4.rhl9.1.i386.rpm **SGI:** ftp://patches.sgi.com/support/free/security/patches/ProPack/ **Sysstat:** http://perso.wanadoo.fr/sebastien.godard/download_en.html	Sysstat Insecure Temporary File Creation & Names CVE Names: CAN-2004-0107, CAN-2004-0108	Low/ Medium (Medium if data is corrupted or lost)	Bug discussed in newsgroups and websites. There is no exploit code required.
Multiple Vendors [115, 116, 117, 118] ***Vendors issue advisories*** [119, 120]	**Unix**	**Linux kernel 2.4.0, test1-test12, 2.4-2.4.24**	**A vulnerability exists in the 'ncp_lookup()' function due to insufficient validation of name component lengths, which could let a malicious user execute arbitrary code.**	**Conectiva:** **ftp://atualizacoes.conectiva.com.br/8/RPMS/** **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/** **RedHat:** **ftp://updates.redhat.com/9/en/os/** **SuSE:** **ftp://ftp.suse.com/pub/suse/i** ***Mandrake:*** **http://www.mandrakesecure.net/en/advisories/** ***SGI:*** **ftp://patches.sgi.com/support/free/security/patches/ProPack/2.4/**	**Linux Kernel NCPFS ncp_lookup() Arbitrary Code Execution** **CVE Name: CAN-2004-0010**	**High**	**Bug discussed in newsgroups and websites.**
Multiple Vendors. [121]	Windows	UUDeview 0.5.19; WinZip WinZip 7.0, 8.0, 8.1 SR-1, 8.1	A buffer overflow vulnerability exists due to a boundary error in the MIME parsing routines, which could let a malicious user execute arbitrary code.	**UUDeview:** Windows http://www.fpx.de/fp/Software/UUDeview/download/uudeview-win32.zip Unix http://www.fpx.de/fp/Software/UUDeview/download/uudeview-0.5.20.tar.gz **WinZip:** http://www.winzip.com/downwzeval.htm	UUDeview MIME Archive Buffer Overrun	High	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.

[113] Red Hat Security Advisory, RHSA-2004:093-01, March 10, 2004.
[114] SGI Security Advisory, 20040302-01-U, March 12, 2004.
[115] Red Hat Security Advisory, RHSA-2004:065-01, February 18, 2004.
[116] Fedora Security Update Notification, FEDORA-2004-079, February 18, 2004.
[117] SUSE Security Announcement, SuSE-SA:2004:005, February 18, 2004.
[118] Conectiva Linux Security Announcement, CLA-2004:820, February 20, 2004.
[119] Mandrakelinux Security Update Advisory, MDKSA-2004:015-1, February 26, 2004.
[120] SGI Security Advisory, 20040204-01-U, February 26, 2004.
[121] iDEFENSE Security Advisory, February 27, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts

Multiple Vendors [122, 123, 124, 125]	Windows 95/98/NT 4.0/2000, MacOS X, BeOS, Unix	Apple Safari 1.0, 1.1;
		KDE Konqueror 2.x, 3.x, Embedded 0.1;
		Microsoft Internet Explorer 5.0.1, SP1-SP4, 5.5 SP1&SP2, 6.0, SP1;
		Opera Software Opera Web Browser 5.x, 6.x, 7.x;
		RedHat Advanced Work-station for the Itanium Processor 2.1, Enterprise Linux WS 2.1, ES 2.1, AS 2.1, RedHat kdelibs-3.1-10.i386. rpm, kdelibs-devel-3.1-10.i386. rpm
			A vulnerability exists because it possibly to bypass the path restrictions specified by the cookie's originator due to validation errors in multiple browsers, which could let a malicious user obtain sensitive information.	**Debian:**
				http://security.debian.org/pool/updates/main/k/kdelibs/
				RedHat:
				ftp://updates.redhat.com/9/en/os/i386
				Mandrake:
				http://www.mandrakesecure.net/en/advisories/
					Multiple Vendor Internet Browser Cookie Path Argument Restriction Bypass	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[122] Corsaire Security Advisory, March 10, 2004.
[123] Debian Security Advisory, DSA 459-1, March 10, 2004.
[124] Mandrakelinux Security Update Advisory, MDKSA-2004:022, March 10, 2004.
[125] Red Hat Security Advisories, RHSA-2004:074-06 & RHSA-2004:075-0, March 10, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[126, 127, 128, 129, 130, 131, 132] *More advisories issued*[133, 134, 135, 136]	Unix	OpenBSD 3.3, 3.4; XFree86 X11R6 4.1 .0, 4.1–12, 4.1–11, 4.2 .0, 4.2 1, 4.2.1 Errata, 4.3	A buffer overflow vulnerability exists in the 'font.alias' file due to insufficient validation of user-supplied data, which could let a malicious user obtain ROOT privileges.	Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/ Immunix: http://download.immunix.org/ImmunixOS/7.3/Updates/RPMS/ Mandrake: http://www.mandrakesecure.net/en/advisories/ OpenBSD: ftp://ftp.openbsd.org/pub/OpenBSD/patches/ RedHat: ftp://updates.redhat.com/9/en/os/ Slackware: ftp://ftp.slackware.com/pub/slackware/ TurboLinux: ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/Desktop/10/updates/ Xfree86: ftp://ftp.xfree86.org/pub/XFree86/4.3.0/fixes/fontfile.diff *Conectiva:* ftp://atualizacoes.conectiva.com.br/ *Debian:* http://security.debian.org/pool/updates/main/x/xfree86/ *SGI:* ftp://patches.sgi.com/support/free/security/patches/ProPack/ *SuSE:* ftp://ftp.suse.com/pub/suse/i386/update/	XFree86 Font Information File Buffer Overflow CVE Name: CAN-2004-0083	High	Bug discussed in newsgroups and websites. Exploit scripts have been published.

[126] iDEFENSE Security Advisory, February 10, 2004.
[127] Slackware Security Advisory, SSA:2004-043-02, February 12, 2004.
[128] Fedora Update Notification, FEDORA-2004-069, February 13, 2004.
[129] Immunix Secured OS Security Advisory, IMNX-2004-73-002-01, February 13, 2004.
[130] Mandrake Linux Security Update Advisory, MDKSA-2004:012, February 13, 2004.
[131] Red Hat Security Advisories, RHSA-2004:059-01& RHSA-2004:060-16, February 13, 2004.
[132] TurboLinux Security Advisory, TLSA-2004-5, February 17, 2004.
[133] Debian Security Advisory, DSA 443-1, February 19, 2004.
[134] Conectiva Linux Security Announcement, CLA-2004:821, February 20, 2004.
[135] SUSE Security Announcement, SuSE-SA:2004:006, February 23, 2004.
[136] SGI Security Advisory, 20040203-01-U, February 26, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[137, 138, 139, 140, 141, 142, 143] More advisories issued[144, 145, 146, 147]	Unix	OpenBSD 3.3, 3.4; XFree86 X11R6 4.1 .0, 4.1–12, 4.1–11, 4.2 .0, 4.2 1, 4.2.1 Errata, 4.3	A buffer overflow vulnerability exists due to insufficient bounds checking when parsing the 'font.alias' file, which could let a remote malicious user execute arbitrary code with ROOT privileges.	Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/ Immunix: http://download.immunix.org/ImmunixOS/7.3/Updates/RPMS/ Mandrake: http://www.mandrakesecure.net/en/advisories/ OpenBSD: ftp://ftp.openbsd.org/pub/OpenBSD/patches/ RedHat: ftp://updates.redhat.com/9/en/os/ Slackware: ftp://ftp.slackware.com/pub/slackware/ TurboLinux: ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/Desktop/10/updates/ Xfree86: ftp://ftp.xfree86.org/pub/XFree86/4.3.0/fixes/fontfile.diff Conectiva: ftp://atualizacoes.conectiva.com.br/ Debian: http://security.debian.org/pool/updates/main/x/xfree86/ SGI: ftp://patches.sgi.com/support/free/security/patches/ProPack/ SuSE: ftp://ftp.suse.com/pub/suse/i386/update/	Xfree86 Font_Name Buffer Overflow CAN-2004-0084	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[137] iDEFENSE Security Advisory, February 12, 2004.
[138] Slackware Security Advisory, SSA:2004-043-02, February 12, 2004.
[139] Fedora Update Notification, FEDORA-2004-069, February 13, 2004.
[140] Immunix Secured OS Security Advisory, IMNX-2004-73-002-01, February 13, 2004.
[141] Mandrake Linux Security Update Advisory, MDKSA-2004:012, February 13, 2004.
[142] Red Hat Security Advisories, RHSA-2004:059-01& RHSA-2004:060-16, February 13, 2004.
[143] TurboLinux Security Advisory, TLSA-2004-5, February 17, 2004.
[144] Debian Security Advisory, DSA 443-1, February 19, 2004.
[145] Conectiva Linux Security Announcement, CLA-2004:821, February 20, 2004.
[146] SUSE Security Announcement, SuSE-SA:2004:006, February 23, 2004.
[147] SGI Security Advisory, 20040203-01-U, February 26, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[148, 149, 150, 151, 152, 153, 154] **More advisories issued**[155, 156, 157, 158]	**Unix**	**OpenBSD 3.3, 3.4; XFree86 X11R6 4.1 .0, 4.1–12, 4.1–11, 4.2 .0, 4.2 1, 4.2.1 Errata, 4.3**	**A buffer overflow vulnerability exists in 'encparse.c' and 'fontfile.c' due to the way font file paths are processed, which could let a malicious user obtain ROOT privileges.**	**Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/** **Immunix:** **http://download.immunix.org/ImmunixOS/7.3/Updates/RPMS/** **Mandrake:** **http://www.mandrakesecure.net/en/advisories/** **OpenBSD:** **ftp://ftp.openbsd.org/pub/OpenBSD/patches/** **RedHat:** **ftp://updates.redhat.com/9/en/os/** **Slackware:** **ftp://ftp.slackware.com/pub/slackware/** **TurboLinux:** **ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/Desktop/10/updates/** **Xfree86:** **ftp://ftp.xfree86.org/pub/XFree86/4.3.0/fixes/fontfile.diff** **Conectiva:** **ftp://atualizacoes.conectiva.com.br/** **Debian:** **http://security.debian.org/pool/updates/main/x/xfree86/** **SGI:** **ftp://patches.sgi.com/support/free/security/patches/ProPack/** **SuSE:** **ftp://ftp.suse.com/pub/suse/i386/update/**	**XFree86 Buffer Overflow** **CVE Name: CAN-2004-0106**	**High**	**Bug discussed in newsgroups and websites.**

[148] iDEFENSE Security Advisory, February 12, 2004.
[149] Slackware Security Advisory, SSA:2004-043-02, February 12, 2004.
[150] Fedora Update Notification, FEDORA-2004-069, February 13, 2004.
[151] Immunix Secured OS Security Advisory, IMNX-2004-73-002-01, February 13, 2004.
[152] Mandrake Linux Security Update Advisory, MDKSA-2004:012, February 13, 2004.
[153] Red Hat Security Advisories, RHSA-2004:059-01& RHSA-2004:060-16, February 13, 2004.
[154] TurboLinux Security Advisory, TLSA-2004-5, February 17, 2004.
[155] Debian Security Advisory, DSA 443-1, February 19, 2004.
[156] Conectiva Linux Security Announcement, CLA-2004:821, February 20, 2004.
[157] SUSE Security Announcement, SuSE-SA:2004:006, February 23, 2004.
[158] SGI Security Advisory, 20040203-01-U, February 26, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[159, 160, 161, 162, 163, 164, 165, 166] *More vendors issue advisories*[167, 168, 169, 170, 171]	Unix	Linux kernel 2.2-2.2.24, 2.4.0, test1-test 12, 2.4-2.4.24, 2.6. text1-test10, 2.6.1-2.6.2; Netwosix Netwosix Linux 1.0; RedHat kernel-2.4.20-8, athlon. rpm, i386.rpm, i686.rpm, kernel-bigmem-2.4.20-8.i686. rpm, kernel-BOOT-2.4.20-8.i386. rpm, kernel-doc-2.4.20-8.i386. rpm, kernel-smp-2.4.20-8, athlon. rpm, i686.rpm, kernel-source-2.4.20-8.i386. rpm	A vulnerability exists in the 'do_mremap' system function due to insufficient checking of return values, which could let a malicious user execute arbitrary code with ROOT privileges.	Patches available at: http://www.kernel.org/pub/linux/kernel/v2.6/linux-2.6.3.tar.bz2 http://www.kernel.org/pub/linux/kernel/v2.6/patch-2.6.3.bz2 **Conectiva:** ftp://atualizacoes.conectiva.com.br/8/RPMS/ **Debian:** http://security.debian.org/pool/updates/main/k/kernel-source-2.4.18/ **Fedora:** http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/ **RedHat:** ftp://updates.redhat.com/ **Slackware:** ftp://ftp.slackware.com/pub/slackware/slackware-current/slackware/ **SuSE:** ftp://ftp.suse.com/pub/suse/i386/update/8.2/rp **Trustix:** ftp://ftp.trustix.org/pub/trustix/updates/2.0/rpms/ ***Immunix:*** http://download.immunix.org/ImmunixOS/7+/Updates/RPMS/ ***Mandrake:*** http://www.mandrakesecure.net/en/advisories/ ***SGI:*** ftp://oss.sgi.com/projects/sgi_propack/download/2.4/updates/ ***SmoothWall:*** http://smoothwall.org/p/2.0-fixes2.html ***TurboLinux:*** ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/	Linux Kernel do_mremap Function CVE Name: CAN-2004-0077	High	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.

[159] Debian Security Advisories DSA 438-1-DSA 442-1, DSA 444-1, February 18-20, 2004.
[160] Fedora Security Update Notifications, FEDORA-2004-079 & 080, February 18 & 19, 2004.
[161] Red Hat Security Advisory, RHSA-2004:065-01, February 18, 2004.
[162] Slackware Security Advisory, SSA:2004-049-01, February 18, 2004.
[163] SUSE Security Announcement, SuSE-SA:2004:005, February 18, 2004.
[164] Trustix Secure Linux Security Advisory, TSLSA-2004-0007, February 18, 2004.
[165] Netwosix Linux Security Advisory, February 20, 2004
[166] Conectiva Linux Security Announcement, CLA-2004:820, February 20, 2004.
[167] Turbolinux Security Advisory, TLSA-2004-7, February 23, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Nathaniel S.Boren-stein[172]	Unix	Metamail 2.7	A vulnerability exists in 'extcompose' because files are created without first verifying the existence of the specified file, which could let a malicious user cause a Denial of Service or potentially obtain elevated privileges.	No workaround or patch available at time of publishing.	Metamail Extcompose Program Symlink	Low/ Medium (Medium if elevated privileges can be obtained)	Bug discussed in newsgroups and websites. There is no exploit code required.
nCipher[173]	Multiple	nShield 1.71.11, 1.71.15, 1.71.90, 1.75.15, 1.77.9, 1.77.93, 1.77.97, 1.79.12, 1.79.80, 1.79.81, 2.0, 2.0.4, 2.12, 2.12.2	A vulnerability exists inside the Hardware Security Module (HSM) firmware, which could let a malicious user access secret data stored in the module, including encryption keys.	Update available at: support@ncipher.com.	nCipher HSM Firmware Secret Data Disclosure	Medium	Bug discussed in newsgroups and websites.
NetScreen[174]	Multiple	NetScreen -SA 5000 Series	A Cross-Site Scripting vulnerability exists in the 'delhomepage.cgi' CGI binary due to insufficient verification of the 'row' parameter, which could let a remote malicious user execute arbitrary HTML or script code.	Patches available at: https://support.neoteris.com.	NetScreen SA 5000 Series Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
nfs[175]	Unix	nfs-utils 1.0, 1.0.1, 1.0.3, 1.0.4, 1.0.6	A Denial of Service vulnerability exists in the 'get_reliable_hostbyaddr()' function in 'support/export/hostname.c' when a client has certain incorrect DNS settings.	**RedHat:** http://rhn.redhat.com/ **Trustix:** ftp://ftp.trustix.org/pub/trustix/updates/2.0/rpms/nfs-utils-1.0.6-1tr.i586.rpm	NFS-Utils rpc.mountd Denial of Service CVE Name: CAN-2004-0154	Low	Bug discussed in newsgroups and websites.
Nortel Networks[176]	Multiple	WLAN Access Point 2225, 2221, 2220	A remote Denial of Service vulnerability exists due to a failure to handle large amounts of data sent to an administrative port (23/TCP and 80/TCP).	No workaround or patch available at time of publishing.	Nortel Wireless LAN Access Point 2200 Series Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.

[168] Mandrake Linux Security Update Advisory, MDKSA-2004:015-1, February 26, 2004.
[169] SGI Security Advisory, 20040204-01-U, February 26, 2004.
[170] Immunix Secured OS Security Advisory, IMNX-2004-7+-001-01, February 26, 2004.
[171] SmoothWall Project Security Advisory, SWP-2004:002, February 26, 2004.
[172] SecurityFocus, March 12, 2004.
[173] nCipher Security Advisory No. 9, February 23, 2004.
[174] NetScreen Advisory 58412, March 2, 2004.
[175] Trustix Secure Linux Security Advisory, TSLSA-2004-0009, March 6, 2004.
[176] SecurityTracker Alert, 1009294, March 2, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
NTP[177]	Unix	NTPd 3.0	An integer overflow vulnerability exists if a request is submitted that contains a date that is more than 34 years of the server's date, which could cause an incorrect date/time offset.	Upgrade available at: http://www.ntp.org/downloads.html	Network Time Protocol Daemon Integer Overflow	Low	Bug discussed in newsgroups and websites. Vulnerability does not require active exploitation.
Ollivier Robert[178]	Unix	Calife 2.8.4 c, 2.8.5	A vulnerability exists due to a boundary error when processing a supplied password, which could let a malicious user execute arbitrary code with ROOT privileges.	Upgrade available at: ftp://ftp.frmug.org/pub/calife/latest.tar.gz	Calife Password Arbitrary Code Execution	**High**	Bug discussed in newsgroups and websites.
Ollivier Robert[179, 180]	Unix	Calife 2.8.4 c, 2.8.5, 2.8.6	A vulnerability exists in the '/etc/calife.auth' file due to insufficient sanity checking, which could let a malicious user execute arbitrary code.	**Debian:** http://security.debian.org/pool/updates/main/c/calife/	Calife Arbitrary Code Execution	**High**	Bug discussed in newsgroups and websites.
Oracle Corporation[181]	Windows NT 4.0/2000, XP, Unix, OpenVMS	Oracle9i Application Server 1.0.2 .2, 9.0.3 .1, 9.0.3, Enterprise Edition 9.0.1 .4, 9.2 .0.2, Personal Edition 9.0.1 .4, 9.2 .0.2, Standard Edition 9.0.1 .4, 9.2 .0.2	A remote Denial of Service vulnerability exists when a malicious user passes malformed DTDs (Data Type Definitions) via XML inside of a SOAP (Simple Object Access Protocol) message.	Patches available via Metalink Document ID 259556.1 located at: http://metalink.oracle.com/	Oracle 9i Application/ Database Server Remote Denial of Service	Low	Bug discussed in newsgroups and websites.
Oracle Corporation[182]	Windows NT 4.0/2000, XP, Unix, OpenVMS	Oracle9i Enterprise Edition 9.0.1 .4, 9.2 .0.4, 9.2 .0.3, Personal Edition 9.0.1 .4, 9.2 .0.4, 9.2 .0.3, Standard Edition 9.0.1 .4, 9.2 .0.4, 9.2 .0.3	Vulnerabilities exist that could let a remote malicious user cause a Denial of Service to obtain unauthorized access to a user session.	Patches available via Metalink Document ID 258254.1 located at: http://metalink.oracle.com	Oracle9i Database Server Unspecified Security Vulnerabilities	Low	Bug discussed in newsgroups and websites.

[177] Vulnerability Note VU#584606, March 8, 2004.
[178] Bugtraq, February 27, 2004.
[179] SecurityFocus, March 1, 2004.
[180] Debian Security Advisory, DSA 461-1, March 11, 2004.
[181] Oracle Security Alert 65, February 18, 2004.
[182] Oracle Security Alert 64, February 18, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Oracle Corporation[183]	Windows 95/98/CE/ NT 4.0, PalmOS	Oracle9i Lite 5.0.2.9.0, 5.0 .2.0.0, 5.0 .1.0.0, 5.0 .0.0.0	Vulnerabilities exist that could let a remote malicious user obtain unauthorized access to a connected Oracle database server by executing SQL commands.	Patches available via Metalink Document ID 261992.1 located at: http://metalink.oracle.com	Oracle9i Lite Multiple Unspecified Vulnerabilities	Medium	Bug discussed in newsgroups and websites.
Paul Francis Harrison[184]	Unix	Synaesthesia 2.1.0-2.1.2, 2.2	A vulnerability exists because a configuration file is created with root privileges and is writable by the users group, which could let a malicious user obtain root privileges.	Upgrades available at: http://security.debian.org/pool/updates/main/s/synaesthesia/synae	Synaesthesia Insecure File Creation CVE Name: CAN-2004-0160	**High**	Bug discussed in newsgroups and websites.
pbdb. Source forge.net[185]	Windows	Punk Buster Database 1.0 alpha-6.0 alpha	A vulnerability exists due to insufficient validation of user-supplied input in the username and password variables, which could let a remote malicious user obtain sensitive information, modify user information, or execute arbitrary code.	No workaround or patch available at time of publishing.	PunkBuster Database Remote Input Validation	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
Pegasi Web Server[186]	Windows Unix	Pegasi Web Server 0.2.2	Multiple vulnerabilities exist: a Directory Traversal vulnerability exists due to insufficient sanitization of HTTP requests, which could let a remote malicious user obtain sensitive information; and a Cross-Site Scripting vulnerability exists due to insufficient sanitization of HTML code from user-supplied requests before displaying error messages, which could let a remote malicious user execute arbitrary HTML or script code.	Upgrade available at: http://prdownloads.sourceforge.net/pws/pws-0.2.3.tar.gz?download	Pegasi Web Server Multiple Input Validation	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required; however, Proofs of Concepts have been published.
Perfect Nav[187]	Windows	Perfect Nav	A remote Denial of Service vulnerability exists in the search plug-in when a malformed URI is processed.	No workaround or patch available at time of publishing.	PerfectNav Malformed URI Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.

[183] Oracle Security Alert 63, February 18, 2004.

[184] Debian Security Advisory, DSA 446-1, February 21, 2004.

[185]Timberlake Advisory, 200402181e-03, February 19, 2004.

[186] SecurityTracker Alert. 1009396, March 11, 2004.

[187] Secure Target Network Security Advisory, February 25, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
phpBB Group[188]	Windows, Unix	phpBB 2.0 .0, 2.0 RC4, 2.0.1-2.0.7	A Cross-Site Scripting vulnerability exists in 'viewtopic.php' due to insufficient verification of the 'postorder' parameter, which could let a remote malicious user execute arbitrary HTML or script code.	No workaround or patch available at time of publishing.	PHPBB ViewTopic. PHP Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
Platform Comput-ing Inc. [189]	Windows NT 4.0/2000, Unix	Load Sharing Facility (LSF) 4.0, 4.2, 5.0, 5.1, 6.0	A buffer overflow vulnerability exists in the 'eauth' component due to insufficient bounds checking, which could let a local/remote malicious user execute arbitrary code.	Patch available at: FTP: ftp.platform.com Path: patches/<version>/os/<os>/eauth*	Load Sharing Facility 'Eauth' Local/Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Platform Comput-ing Inc. [190]	Windows NT 4.0/2000, Unix	Load Sharing Facility (LSF) 4.0, 4.2, 5.0, 5.1, 6.0	Several vulnerabilities exist: a vulnerability exists because it is possible to communicate with LSF while impersonating another user due to an authentication error in the 'eauth' component, which could let a remote malicious user obtain elevated privileges; and a buffer overflow vulnerability exists when 'eauth' runs in '-s' mode, which could let a remote malicious user execute arbitrary code with administrative privileges.	Patch available at: FTP: ftp.platform.com Path: patches/<version>/os/<os>/eauth*	Load Sharing Facility 'Eauth' Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Exploit has been published.
ProFTPD Project[191]	Unix	ProFTPD 1.2.7, 1.2.8, 1.2.9 rc1& rc2	A buffer overflow vulnerability exists due to two off-by-one errors in the '_xlate_ascii_write()' function, which could let a remote malicious user execute arbitrary code.	Upgrades available at: http://proftpd.linux.co.uk/download.html	ProFTPD '_xlate_ascii_write()' Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
PSOProxy [192]	Windows XP, Unix	PSOProxy Server 0.91	A buffer overflow vulnerability exists due to a boundary error when handling received data, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	PSOProxy Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.

[188] Bugtraq, February 28, 2004.
[189] Lam3rZ Security Advisory #1/2004, February 23, 2004.
[190] Lam3rZ Security Advisory #2/2004, February 23, 2004.
[191] Bugtraq, March 2, 2004.
[192] Bugtraq, February 25, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Pweb Server[193]	Windows, Unix	PWeb Server 0.3.0, 0.3.2, 0.3.3	A Directory Traversal vulnerability exists due to a failure to properly filter user supplied URI requests, which could let a remote malicious user obtain sensitive information.	Upgrades available at: http://prdownloads.sourceforge.net/pwebserver/pwebserver-0.3.4.tgz	PWebServer Remote Directory Traversal	Medium	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
Python Software Foundation[194, 195]	Windows, Unix	Python 2.2, 2.2.1	A buffer overflow vulnerability exists in the 'getaddrinfo()' function due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.python.org/2.2.2/ **Debian:** http://security.debian.org/pool/updates/main/p/python2.2 **Mandrake:** http://www.mandrakesecure.net/en/advisories/	Python 'getaddrinfo ' Function Remote Buffer Overflow CVE Name: CAN-2004-0150	**High**	Bug discussed in newsgroups and websites.
Rainer Wichmann[196]	Unix	Samhain Labs hsftp 1.4-1.7, 1.9-1.11, 1.13, 1.14	A vulnerability exists due to a format string error when processing file names, which could let a remote malicious user execute arbitrary code.	Update available at: http://la-samhna.de/hsftp/hsftp-1.14.tar.gz **Debian:** http://security.debian.org/pool/updates/main/h/hsftp	Samhain Labs HSFTP Remote Format String CVE Name: CAN-2004-0159	**High**	Bug discussed in newsgroups and websites.
RedStorm[197]	Windows NT 4.0	Ghost Recon Game Engine	A remote Denial of Service vulnerability exists when handling text strings.	No workaround or patch available at time of publishing.	Ghost Recon Game Engine Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
Rhino Soft[198] ***Exploit scripts published[199]***	**Windows**	**Serv-U 4.1 .0.11, 4.1**	**A buffer overflow vulnerability exists in the 'SITE CHMOD' command when a malicious user file name is submitted, 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.**	**Serv-U FTP Server SITE CHMOD Buffer Overflow**	**Low/High** **(High if arbitrary code can be executed)**	**Bug discussed in newsgroups and websites. Proof of Concept Denial of Service exploit script has been published.**

[193] Securiteam, March 10, 2004.
[194] Debian Security Advisory, DSA 458-1, March 10, 2004.
[195] Mandrakelinux Security Update Advisory, MDKSA-2004:019, March 10, 2004.
[196] Debian Security Advisory, DSA 447-1, February 23, 2004.
[197] Securiteam, February 26, 2004.
[198] Vuln-Dev, February 16, 2004.
[199] SecurityFocus, February 27, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
RhinoSoft[200]	Windows	Serv-U 3.0, 3.1, 4.0 .0.4, 4.1 .0.11, 4.1, 4.2	A buffer overflow vulnerability exists in the 'MDTM' command when handling time zone arguments, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Serv-U FTP Server 'MDTM' Command Buffer Overflow	High	Bug discussed in newsgroups and websites. Proofs of Concepts exploit scripts have been published.
robotftp. com[201] ***Another exploit published***[202]	**Windows**	**RobotFTP Server 1.0, 2.0 Beta 1**	**A vulnerability exists when processing 'USER' command arguments of excessive length due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code.**	**No workaround or patch available at time of publishing.**	**RobotFTP Server Remote Buffer Overflow**	**High**	**Bug discussed in newsgroups and websites. Proof of Concept Denial of Service exploit script has been published.** ***Exploit script has been published.***
Sand Surfer[203]	Unix	Sand Surfer 1.6.5, 1.7.0	Several Cross-Site Scripting vulnerabilities exist due to input validation errors, which could let a remote malicious user execute arbitrary HTML or script code.	Upgrades available at: http://prdownloads.sourceforge.net/sandsurfer/SandSurfer-1.7.1.tar.gz?download	SandSurfer Multiple Cross-Site Scripting Vulnerabilities	High	Bug discussed in newsgroups and websites.
Seattle Lab Software[204]	Windows 2000	SLMail Pro 2.0-2.0.9	A buffer overflow vulnerability exists when a specially crafted HTTP request is submitted to the Supervisor Report Center on TCP port 801, which could let a remote malicious user execute arbitrary code.	Patches available at: http://216.26.170.92/Download/webfiles/Patches/SLMailPro_Patch_2.0.14.exe	SLMail Pro Remote Buffer Overflow	High	Bug discussed in newsgroups and websites.
Seattle Lab Software[205]	Windows 2000	SLWeb Mail	Multiple buffer overflow vulnerabilities exist in 'user.dll,' loadpageadmin.dll,' and 'loadpageuser.dll,' which could let a remote malicious user execute arbitrary code.	Patch available at: http://216.26.170.92/Download/webfiles/Patches/SLMailPro_Patch_2.0.14.exe	SLWebMail Multiple Remote Buffer Overflow	High	Bug discussed in newsgroups and websites.
Seyeon Tech Co.[206]	Multiple	Flex WATCH Network Video Server 2.2	A Cross-Site Scripting vulnerability exists due to insufficient filtering of HTML code from user-supplied input, which could let a remote malicious user execute arbitrary HTML or script code.	No workaround or patch available at time of publishing.	FlexWATCH Server Network Video Server Cross-Site Scripting	High	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.

[200] Bugtraq, February 27, 2004.
[201] Securiteam, February 17, 2004.
[202] SecurityFocus, February 20, 2004.
[203] SecurityFocus, March 3, 2004.
[204] NGSSoftware Insight Security Research Advisory, #NISR05022004a, March 5, 2004.
[205] NGSSoftware Insight Security Research Advisory #NISR05022004b, March 5, 2004.
[206] Bugtraq, February 24, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Shawn Keaney[207]	Windows, Unix	GWeb HTTP Server 0.5, 0.6	A Directory Traversal vulnerability exists due to a failure to properly validate user-supplied HTTP requests, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	GWeb HTTP Server Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Singularity Software[208]	Windows, Unix	Team Factor 1.25, 1.25m	A remote Denial of Service vulnerability exists when a malicious user submits a negative value for the data block size.	No workaround or patch available at time of publishing.	Team Factor Integer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
SkinTech[209]	Windows, Unix	phpNews Manager 1.36	A Directory Traversal vulnerability exists in the 'functions.php' script due to insufficient sanitization of the 'clang' parameter, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	PhpNews Manager Directory Traversal	Medium	Bug discussed in newsgroups and websites. Vulnerability may be exploited via a web browser.
Software 602[210]	Windows 98/ME/NT 4.0/2000	602Pro LAN SUITE 2002, 2003	A vulnerability exists because the login form ('http://<host>/mail/') contains a hidden variable that discloses the LAN SUITE installation path, which could let a malicious user obtain sensitive information,	Upgrades available at: http://www.software602.com/download/	602Pro LAN Suite Web Mail Information Disclosure	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.

[207] SecurityFocus, March 3, 2004.
[208] Securiteam, February 25, 2004.
[209] Zone-h Security Team Advisory, ZH2004-09SA, February 23, 2004.
[210] SecurityFocus, March 10, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
SonicWall[211]	Multiple	Sonic WALL Sonic OS 6.2 .0.0, 6.3.1.4, 6.3.1 .0, 6.4 .0.2, 6.4 .0.1, 6.5 .0.4, 6.5 .0.3	Multiple vulnerabilities exist that could let a remote malicious user on the WAN-side local network determine IP addresses located behind the firewall: a vulnerability exists because the device will respond to ARP requests made from the WAN interface via Ethernet if the ARP cache contains an entry for the requested IP address on the LAN interface; a vulnerability exists because the device will proxy ARP requests through the firewall for IP addresses that are on the LAN subnetwork but are not found in the device's ARP cache; a vulnerability exists because ARP requests are not logged, except when the requested IP address is not in the ARP cache and the IP address on the LAN side is not responding; and a vulnerability exists because ARP requests are not passed back from the LAN to the WAN interface when the device is in 'NAT Mode' (the default mode).	No workaround or patch available at time of publishing.	SonicWall Firewall/VPN Appliance Multiple ARP Request Handling	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Spider Sales[212]	Windows	Spider Sales 2.0	Multiple vulnerabilities exist: a vulnerability exists due to an insecure implementation of the RSA Cryptosystem used to encrypt sensitive information in the database, which could let a remote malicious user obtain sensitive information; a vulnerability exists because the private key is stored in the database in the same table as the public key, which could let a remote malicious user obtain sensitive information; and a vulnerability exits in 'viewCart.asp' due to insufficient verification of the 'userId' parameter, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	SpiderSales Shopping Cart Multiple Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[211] SecurityTracker Alert, 1009288, March 4, 2004.
[212] S-Quadra Advisory #2004-03-03, March 3, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Squid-cache.org [213]	Unix	Squid Web Proxy Cache 2.0 PATCH2, 2.1 PATCH2, 2.3 STABLE 5, 2.4 STABLE 7, 2.4, 2.5 STABLE 4, 2.5 STABLE3	A vulnerability exists in the '%xx' URL decoding function, which could let a remote malicious user bypass access controls.	Upgrades available at: http://www.squid-cache.org/Versions/v2/2.5/squid-2.5.STABLE5.tar.gz	Squid Proxy Access Control Bypass	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Sun Micro-systems, Inc.[214]	Unix	Solaris 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86, 9.0, 9.0_x86	Multiple buffer overflow vulnerabilities exists due to boundary errors in 'UUCP,' which could let a malicious user execute arbitrary code with ROOT privileges.	Patches available at: http://sunsolve.sun.com/pub-cgi/	Solaris Multiple 'UUCP' Buffer Overflows	**High**	Bug discussed in newsgroups and websites.
Sun Micro-systems, Inc.[215]	Unix	Solaris 7.0, 7.0_96, 8.0, 8.0_x86, 9.0, 9.0_x86	A vulnerability exists due to an unspecified error in the '/usr/lib/print/conv_fix' command, which is invoked by the 'conv_lpd' script, which could let a malicious user obtain ROOT privileges.	Patches available at: http://sunsolve.sun.com/pub-cgi/	Solaris conv_fix Root Access	**High**	Bug discussed in newsgroups and websites.
Sun Micro-systems, Inc.[216]	Unix	Solaris 8.0, 8.0_x86, 9.0, 9.0_x86	A vulnerability exists due to an unspecified error related to the 'passwd' command, which could let a malicious user obtain unauthorized ROOT privileges.	Patches available at: http://sunsolve.sun.com/pub-cgi/	Sun Solaris Passwd Local Root Compromise	**High**	Bug discussed in newsgroups and websites.
SureCom Technol-ogy Corp.[217]	Multiple	SureCom EP-4504AX, EP-9510AX	A remote Denial of Service vulnerability exists when a malicious user submits a specially crafted HTTP request to the web configuration interface.	No workaround or patch available at time of publishing.	SureCom Network Device Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Proofs of Concepts exploits have been published.

[213] Squid Proxy Cache Security Update Advisory, SQUID-2004:1, February 1, 2004.
[214] Sun(sm) Alert Notification, 57508, March 4, 2004.
[215] Sun Alert ID: 57509, February 27, 2004.
[216] Sun Alert ID 57454, February 27, 2004.
[217] SecurityTracker Alert, 1009334, March 5, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
SWSoft[218]	Multiple	Confixx Pro 2	Two vulnerabilities exist: an input validation vulnerability exists in the 'db_mysql_loeschen2.php' script, which could let a remote malicious user execute arbitrary SQL code; and a vulnerability exists in the debugging utility functionality, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Confixx DB Input Validation & Debugging Utility	**High**	Bug discussed in newsgroups and websites. Proofs of Concepts exploits have been published.
Symantec [219]	Windows	Symantec Firewall/ VPN Appliance 100, 200, 200R	A vulnerability exists because the administration password credential may be stored in the browser\proxy cache in plaintext format depending on browser settings, which could let a malicious user obtain sensitive information.	Patches available at: ftp://ftp.symantec.com/public/english_us_canada/products/symantec_firewall_vpn_appliance/updates/vpn100_161_app.zip ftp://ftp.symantec.com/public/english_us_canada/products/symantec_firewall_vpn_appliance/updates/vpn100_161_all.zip	Symantec Firewall/VPN Appliance Cached Plaintext Password	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Symantec [220]	Windows	Symantec Gateway Security 2.0	A Cross-Site Scripting vulnerability exists because invalid requests for objects in the '/sgmi/' folder aren't properly sanitized before the URI is returned in an error page, which could let a remote malicious user execute arbitrary HTML or script code.	Symantec Hotfix bundle-sgs20.exe ftp://ftp.symantec.com/public/updates/bundle-sgs20.exe	Symantec Gateway Security Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Targem Games[221]	Multiple	Battle Mages 1.0	A remote Denial of Service vulnerability exists when the server receives incomplete client data.	No workaround or patch available at time of publishing.	Targem Games Battle Mages Remote Denial of Service	Kiw	Bug discussed in newsgroups and websites. Proofs of Concepts exploits have been published.

[218] Secunia Advisory, SA11101, March 11, 2004.
[219] Symantec Security Response, SYM04-004, March 2, 2004.
[220] SecurityTracker Alert, 1009231, February 26, 2004.
[221] SecurityFocus, March 11, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Texas Imperial Software[222]	Windows 95/98/ME/ NT 3.5/4.0/2000	WFTPD 3.0, Pro, 0R5 Pro, 0R5, 0R4 Pro, 0R4, 0R3, 3.10 R1, 3.20, Pro 3.10 R1, 3.20, 3.21	Multiple vulnerabilities exist: a buffer overflow vulnerability exists within a routine for handling arguments supplied to the 'LIST,' 'NLST,' and 'STAT' FTP commands, which could let a remote malicious user execute arbitrary code; a vulnerability exists due to various errors within the routines for handling FTP commands, which could let a remote malicious user cause a Denial of Service; and an off-by-one vulnerability exists when the option 'XeroxDocutech' is set to '1,' which could let a remote malicious user cause a Denial of Service.	Upgrades available at: http://www.wftpd.com/downloads/protr321.zip	Multiple WFTPD Remote Vulnerabilities	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Exploit scripts have been published.
The Ignition Project[223]	Windows, Unix	Ignition Server 0.1.2, Release 2	A vulnerability exists because an unofficial command allows operators to manipulate their Mode, which could let a malicious user obtain elevated privileges.	Upgrade available at: http://sourceforge.net/project/showfiles.php?group_id=96071	IgnitionServer Global IRC Operator Privilege Escalation	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
The Opt-x Project[224]	Unix	Opt-X 0.7.2	A vulnerability exists in '/includes/header.php' because user-supplied input that is passed to the 'systempath' parameter is not properly verified before being used to include files, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Opt-X header.php Remote File Include	**High**	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.

[222] Secunia Advisory, SA11001, March 1, 2004.
[223] Secunia Advisory, SA11017, March 2, 2004.
[224] Zone-H Security Team Advisory, ZH2004-10SA, February 24, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
The XMB Group[225]	Multiple	XMB Forum 1.8, SP1&SP2	Multiple vulnerabilities exist: Cross-Site Scripting vulnerabilities exist in the 'forumdisplay.php,' 'member.php,' 'u2uadmin.php,' and 'editprofile.php' scripts due to insufficient sanitization of user-supplied data, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability exists in '[align=xxx][/align]' and '[img=1x1][/img]' because arbitrary script code can be injected by including parameters with script code; and SQL injection vulnerabilities exist due to lack of input validation in 'viewthread.php,' 'misc.php,' 'forumdisplay.php,' and 'stats.php,' which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.xmbforum.com/download/1.8/?type=zip	XMB Forum Multiple Input Validation Vulnerabilities	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
TYPSoft[226]	Windows	TYPSoft FTP Server 1.1	A remote Denial of Service vulnerability exists due to a failure to handle certain queries that contain invalid paths.	No workaround or patch available at time of publishing.	TYPSoft FTP Server Remote Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploits have been published.
vbfreechat .source forge.net[227]	Windows	FreeChat 0.1.1 a, 1.1.1 a	A remote Denial of Service vulnerability exists due to an inability to handle unexpected strings.	No workaround or patch available at time of publishing.	FreeChat Remote Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
Virtua Systems[228]	Windows, Unix	Virtua News Pro 1.0-1.0.3	Multiple Cross-Site Scripting vulnerabilities exist in the 'admin.php' and 'search.php' scripts due to insufficient validation, which could let a remote malicious user execute arbitrary HTML or script code.	No workaround or patch available at time of publishing.	VirtuaNews Multiple Module Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proofs of Concepts exploits have been published.

[225] waraxe-2004-SA#004, February 23, 2004.
[226] Securiteam, February 25, 2004.
[227] SecurityTracker Alert, 1009227, February 26, 2004.
[228] Secunia Advisory, SA11054, March 8, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Volition [229]	Windows 95/98/ME, MacOS X, Unix	Red Faction 1.0, 1.1, 1.20	A buffer overflow vulnerability exists when a specially crafted server name string that is 260 characters or more is submitted, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Red Faction Game Client Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Volition, Inc. [230]	Windows	Freespace 2 1.2	A buffer overflow vulnerability exists when the client receives information replies from servers, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Freespace 2 Game Client Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
W3C[231]	Windows, Unix	Jigsaw 2.0-2.0.5, 2.1-2.1.2, 2.2-2.2.3	A vulnerability exists due to a flaw in the parsing of user-supplied URLs, which could let a remote malicious user execute arbitrary code.	Upgrades available at: http://jigsaw.ws.org/Distrib/jigsaw_2.2.4.zip	Jigsaw Input Validation	**High**	Bug discussed in newsgroups and websites.
Washington University [232, 233]	Unix	wu-ftpd 2.4.1, 2.4.2 academ [BETA1-15], academ [BETA-18], 2.4.2 VR16 & VR17, 2.4.2 (beta 18) VR4-VR15, 2.5.0, 2.6.0-2.6.2	A vulnerability exists because directory access restrictions imposed by the 'restricted-gid' option can be bypassed, which could let a remote malicious user bypass access restrictions.	**Debian:** http://security.debian.org/pool/updates/main/w/wu-ftpd/ **RedHat:** http://rhn.redhat.com/errata/RHSA-2004-096.html	WU-FTPD restricted-gid Access Control CVE Name: CAN-2004-0148	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Working Resources Inc.[234]	Multiple	BadBlue 2.4	A vulnerability exists in the 'phptest.php' script because the installation path is revealed in HTML output, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	BadBlue Server 'phptest.php' Path Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.

[229] Bugtraq, March 1, 2004.
[230] SecurityFocus, March 2, 2004.
[231] SecurityTracker Alert ID: 1009169, February 23, 2004.
[232] RedHat Security Advisory, RHSA-2004:096-09, March 8, 2004.
[233] Debian Security Advisory, DSA 457-1, March 9, 2004.
[234] Secunia Advisory, SA10984, February 26, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
XFree86 Project [235]	Unix	XFree86 X11R6 4.1 .0, 4.1–12, 4.1–11, 4.2 .0, 4.2.1 Errata, 4.2.1, 4.3	A remote Denial of Service vulnerability exists in the GLX extension and Direct Rendering Infrastructure components due to insufficient bounds checking.	**Debian:** http://security.debian.org/pool/updates/main/x/xfree86/	XFree86 GLX Extension & Direct Rendering Infrastructure Denial of Service CVE Names: CAN-2004-0093, CAN-2004-0094	Low	Bug discussed in newsgroups and websites.
XMLSoft [236, 237, 238, 239, 240, 241, 242, 243]	Unix	Libxml2 2.6.0-2.6.5	A buffer overflow vulnerability exists in 'nanoftp.c' and 'nanohttp.c' when parsing overly long URIs, which could let a remote malicious user execute arbitrary code.	Upgrade available at: ftp://xmlsoft.org/ **Debian:** http://security.debian.org/pool/updates/main/libx/libxml/ **Fedora:** http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/ **Mandrake:** http://www.mandrakesecure.net/en/advisories/ **Netwosix:** http://download.netwosix.org/0004/nepote **OpenPKG:** ftp://ftp.openpkg.org/release **RedHat:** ftp://updates.redhat.com/9/en/os/ **SGI:** ftp://oss.sgi.com/projects/sgi_propack/download/ **Trustix:** http://www.trustix.org/errata/misc/2004/TSL-2004-0010-libxml2.asc.txt	Libxml2 Remote URI Parsing Remote Buffer Overflow CVE Name: CAN-2004-0110	**High**	Bug discussed in newsgroups and websites.

[235] Debian Security Advisory, DSA 443-1, February 19, 2004.
[236] Fedora Update Notification, FEDORA-2004-087, February 26, 2004.
[237] Red Hat Security Advisory, RHSA-2004:091-01, February 26, 2004.
[238] SGI Security Advisory, 20040301-01-U, March 3, 2004.
[239] Debian Security Advisory, DSA 455-1, March 4, 2004.
[240] Netwosix Linux Security Advisory, March 4, 2004.
[241] Mandrakelinux Security Update Advisory, MDKSA-2004:018, March 4, 2004.
[242] OpenPKG Security Advisory, OpenPKG-SA-2004.003, March 5, 2004.
[243] Trustix Secure Linux Security Advisory, TSLSA-2004-0010, March 6, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
YaBB SE[244]	Windows, Unix	YaBB SE 1.5.4, 1.5.5 b, SE 1.5.5	Multiple vulnerabilities exists in the 'ModifyMessage.php' file: a vulnerability exists in the '$msg' parameter due to insufficient validation, which could let a remote malicious user obtain sensitive information; a vulnerability exists in the '$postid' parameter due to insufficient validation, which could let a remote malicious user execute arbitrary commands; and a Directory Traversal vulnerability exists in the '$attachOld' parameter due to insufficient validation, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	YABB SE Multiple Input Validation Vulnerabilities	**High**	Bug discussed in newsgroups and websites. There is no exploit code required; however, Proofs of Concepts have been published.
Zone Labs[245]	Windows	Labs Integrity Client 4.0, Zone Alarm 4.0, Plus 4.0, Pro 4.0, 4.5	A buffer overflow vulnerability exists due to a boundary error in the Simple Mail Transfer Protocol (SMTP) processing system, which could let a local/remote malicious user execute arbitrary code.	Update instructions available at: http://download.zonelabs.com/bin/free/securityAlert/8.html	ZoneAlarm SMTP Local/Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

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

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

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

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

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between February19 and March 11, 2004, 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,

[244] SecurityTracker Alert, 1009275, March 1, 2004.

[245] Zone Labs Security Advisory, ZL04-008, February 18, 2004.

or which represent scripts that malicious users are utilizing. During this period 60 scripts, programs, and net-news messages containing holes or exploits were identified by US-CERT. *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**
March 11, 2004	adore-ng-0.41.tgz	A Linux LKM based rootkit that features smart PROMISC flag hiding, persistent file and directory hiding (still hidden after reboot), process-hiding, netstat hiding, rootshell-backdoor, and an uninstall routine.
March 11, 2004	**battlemages-adv.txt**	**Exploit for the Targem Games Battle Mages Remote Denial of Service vulnerability.**
March 11, 2004	**battlemagx.rar**	**Exploit for the Targem Games Battle Mages Remote Denial of Service vulnerability.**
March 11, 2004	**battlemagx.rar**	**Exploit for the Targem Games Battle Mages Remote Denial of Service vulnerability.**
March 11, 2004	**battlemagy.zip**	**Exploit for the Targem Games Battle Mages Remote Denial of Service vulnerability.**
March 11, 2004	**cpanelroot.txt**	**Exploit for the user password in cPanel User Password Root Commands vulnerability.**
March 11, 2004	eckbox-v0.9b2.tar.bz2	Eckbox is van Eck phreaking software that interprets a radio signal emanating from a computer's monitor to recreate the image (in black and white) that is displayed on it.
March 11, 2004	prismstumbler-0.7.1.tar.bz2	Software that finds 802.11 (W-LAN) networks. It comes with an easy to use GTK2 frontend and is small enough to fit on a small portable system. It is designed to be a flexible tool to find as much information about wireless LAN installations as possible.
March 10, 2004	anubis.pl	Script that exploits the Anubis Multiple Vulnerabilities.
March 10, 2004	anubisexp.c	Script that exploits the Anubis Remote Root vulnerability.
March 10, 2004	anubisRootExploit.c	Script that exploits the Anubis Multiple Vulnerabilities.
March 10, 2004	outlooksploit.html	Exploit for the Outlook 'Mailto' Parameter Arbitrary Code Execution vulnerability.
March 10, 2004	**unrealEngine.txt**	**Exploit for the Epic Games Unreal Tournament Server Engine Remote Format String vulnerability.**
March 10, 2004	**unrfs-poc.zip**	**Proof of Concept exploit for the Epic Games Unreal Tournament Server Engine Remote Format String vulnerability.**
March 9, 2004	**dreamftp-DoS.c**	**Script that exploits the BolinTech Dream FTP Server User Name Format String vulnerability.**
March 9, 2004	**servu-mdtm.pl**	**Script that exploits the Serv-U FTP Server 'MDTM' Command Buffer Overflow vulnerability.**
March 5, 2004	**hgmcrash.zip**	**Exploit for the Haegemonia Remote Denial of Service vulnerability.**
March 5, 2004	mimedefang-2.40.tar.gz	A flexible MIME e-mail scanner.
March 4, 2004	anubisAdv.txt	Script that exploits the Anubis Buffer Overflow Vulnerabilities
March 4, 2004	oseen_shoutcast.c	SHOUTcast version 1.9.2 remote exploit with connect back code
March 4, 2004	prismstumbler-0.7.0.tar.gz	Software that finds 802.11 (W-LAN) networks. It comes with an easy to use GTK2 frontend and is small enough to fit on a small portable system and is designed to be a flexible tool to find as much information about wireless LAN installations as possible
March 4, 2004	whitepaper_httpresponse.pdf	A whitepaper that discusses new application attack techniques: Divide and Conquer, HTTP Response Splitting, Web Cache Poisoning Attacks, and Related Topics.

Date of Script (Reverse Chronological Order)	Script name	Script Description
March 3, 2004	**gshinfo.zip**	**Exploit for the GWeb HTTP Server Directory Traversal vulnerability.**
March 3, 2004	wftpd.c	Exploit for the Multiple WFTPD Remote Vulnerabilities.
March 2, 2004	argosoft-poc.pl	Exploit for the ArGoSoft FTP Server Multiple Remote Vulnerabilities.
March 2, 2004	**fs2cbof.zip**	**Exploit for the Freespace 2 Game Client Remote Buffer Overflow vulnerability.**
March 2, 2004	**surecomkill.c**	**Proof of Concept exploit for the SureCom Network Device Malformed Web Authorization Request Denial of Service vulnerability.**
March 2, 2004	**surecom-tester.pl**	**Proof of Concept exploit script for the SureCom Network Device Remote Denial of Service vulnerability.**
March 2, 2004	**WLAN-DoS.c**	**Proof of Concept exploit script for the SureCom Network Device Remote Denial of Service vulnerability.**
March 1, 2004	isec-0014-mremap-unmap.v2.txt	Exploit for the Linux Kernel do_mremap Function vulnerability.
March 1, 2004	**motorolakill.c**	**Script that exploits the Motorola T720 Phone Remote Denial of Service vulnerability.**
March 1, 2004	**rfcbof.zip**	**Exploit for the Volition Red Faction Game Client Remote Buffer Overflow vulnerability.**
February 28, 2004	tcpick-0.1.21.tar.gz	A textmode sniffer that can track TCP streams and saves the data captured in files or displays them in the terminal.
February 27, 2004	**ex_servu.c**	**Script that exploits the Serv-U FTP Server 'MDTM' Command Buffer Overflow vulnerability.**
February 27, 2004	**exp_servu_site_chmod.c**	**Script that exploits the Serv-U FTP Server SITE CHMOD Buffer Overflow vulnerability.**
February 27, 2004	**servu_ftpd_mdtm.c**	**Script that exploits the Serv-U FTP Server 'MDTM' Command Buffer Overflow vulnerability.**
February 27, 2004	**Servu2.c**	**Script that exploits the Serv-U FTP Server 'MDTM' Command Buffer Overflow vulnerability.**
February 27, 2004	**serv-u-mdtm-expl.c**	**Script that exploits the Serv-U FTP Server 'MDTM' Command Buffer Overflow vulnerability.**
February 27, 2004	**thcservu.c**	**Script that exploits the Serv-U FTP Server SITE CHMOD Buffer Overflow vulnerability.**
February 27, 2004	wftpd_exp.c	Exploit for the Multiple WFTPD Remote Vulnerabilities.
February 27, 2004	wftpd_STAT_exp.py	Exploit for the Multiple WFTPD Remote Vulnerabilities.
February 27, 2004	xp_wftpd.zip	Exploit for the Multiple WFTPD Remote Vulnerabilities.
February 26, 2004	mtools-exp.pl	Proof of Concept exploit for the MTools MFormat Root Privileges vulnerability.
February 25, 2004	**GateKeeper.c**	**Script that exploits the Proxy-Pro Professional GateKeeper Web Proxy Remote Buffer Overflow vulnerability.**
February 25, 2004	**pso-exploit.c**	**Script that exploits the PSOProxy Remote Buffer Overflow vulnerability.**
February 25, 2004	**PSOProxy-exp.c**	**Script that exploits the PSOProxy Remote Buffer Overflow vulnerability.**
February 25, 2004	**PSOproxyExploit.c**	**Script that exploits the PSOProxy Remote Buffer Overflow vulnerability.**
February 25, 2004	**psoproxy-exploit.c**	**Script that exploits the PSOProxy Remote Buffer Overflow vulnerability.**
February 24, 2004	**grboom.rar**	**Exploit for the Ghost Recon Game Engine Remote Denial of Service vulnerability.**
February 24, 2004	gshboom.zip	Exploit for the Gamespy Software Development Kit Remote Denial of Service vulnerability.
February 24, 2004	**hgmcrash.c**	**Script that exploits the Haegemonia Remote Denial of Service vulnerability.**

Date of Script (Reverse Chronological Order)	Script name	Script Description
February 23, 2004	**gatekeeper_exploit.c**	**Script that exploits the Proxy-Pro Professional GateKeeper Web Proxy Remote Buffer Overflow vulnerability.**
February 23, 2004	**gatekeeper_exploit_linux.c**	**Script that exploits the Proxy-Pro Professional GateKeeper Web Proxy Remote Buffer Overflow vulnerability.**
February 22, 2004	3com-DoS.c	Proof of concept DoS exploit for 3Com Office Connect DSL Routers vulnerability.
February 22, 2004	breakout2-exp.c	Script that exploits the LBreakout2 Buffer Overflow vulnerability.
February 20, 2004	**Ftboom.c**	**Proof of Concept exploit for the Team Factor Integer Overflow vulnerability.**
February 20, 2004	**PSOProxy.c**	**Script that exploits the PSOProxy Remote Buffer Overflow vulnerability.**
February 20, 2004	**PSOProxy091.txt**	**Exploit for the PSOProxy Remote Buffer Overflow vulnerability.**
February 20, 2004	**robotFtpDoSExploit.c**	**Script that exploits the RobotFTP Server Remote Buffer Overflow vulnerability.**
February 19, 2004	ldaped.c	Script that exploits the IMail Server Remote LDAP Daemon Buffer Overflow vulnerability.

Trends

- **US-CERT has become aware of publicly available exploit code for the ASN.1 vulnerability. For more information see Microsoft ASN.1 Library Buffer Overflow and Multiple Vendors ASN.1 Library Integer Handling entries in "Bugs, Holes & Patches" Table above.**
- **US-CERT has received reports of a new mass-mailing virus, referred to as "W32/Netsky.B," "WORM_NETSKY.B," or "Moodown.B." It can spread via e-mail, or network file shares. For more information, see W32/Netsky-B entry (item is boldfaced/red) in the Virus Section below and US-CERT entry located at: http://www.us-cert.gov/current/.**
- **US-CERT has received reports of a new mass-emailing virus, referred to as "W32/Baegle.B," "W32/Bagle.B," or "W32.Alua." For more information, see Win32/Bagle.B entry (item is boldfaced/red) in the Virus Section below and US-CERT entry located at: http://www.us-cert.gov/current/.**
- **On February 9, 2004, the CERT/CC began receiving reports of a new variant of the Mydoom virus known as W32/Mydoom.C or W32.HLLW.Doomjuice. Systems previously infected with Mydoom.A have a backdoor listening on port 3127/tcp. For more information, see CERT/CC entry located at: http://www.cert.org/current.**
- **A new variant of the previously discovered MyDoom virus, MyDoom.B, has been identified. In addition to the common traits of email-borne viruses, this virus may prevent your computer from updating anti-virus and other software. For more information, see Cyber Security Alert, SA04-028A, located at: http://www.us-cert.gov/cas/alerts/SA04-028A.html.**
- A Trojan horse program that appears to be a Microsoft Corp. security update can download malicious code from a remote Web site and install a back door on the compromised computer, leaving it vulnerable to remote control.

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.

The Virus and Trojan sections are derived from compiling information from the following anti-virus vendors and security related web sites: Sophos, Trend Micro, Symantec, McAfee, Network Associates, Central Command, F-Secure, Kaspersky Labs, MessageLabs, and The WildList Organization International.

W32/Agobot-DQ (Aliases: Backdoor.Agobot.3.gen, W32/Gaobot.worm.gen.d) (Win32 Worm): This is a network worm that also allows unauthorized remote access to the computer via IRC channels. It tries to copy itself to network shares that have weak passwords. W32/Agobot-DQ copies itself to the Windows system folder as FILENAME.EXE and creates entries in the registry at the following locations to run itself on system restart:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Configuration Loader
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\Configuration Loader

The worm disables the shares C$, D$, ADMIN$, and IPC$. W32/Agobot-DP attempts to terminate the various virus, anti-virus and security processes. It listens on a particular port and supplies a copy of the worm in response to incoming connections.

W32/Agobot-FE (Aliases: Backdoor.Agobot.3.gen, Win32/Agobot.3.HF, W32.HLLW.Gaobot.AF) (Win32 Worm): This is a network worm that also allows unauthorized remote access to the computer via IRC channels. It attempts to copy itself to network shares that have weak passwords and spread to computers using the DCOM RPC and the RPC locator vulnerabilities. These vulnerabilities allow the worm to execute its code on target computers with System level privileges. For further information on these vulnerabilities and for details on how to protect/patch the computer against such attacks please see Microsoft security bulletins MS03-001 and MS03-026. MS03-026 has been superseded by Microsoft security bulletin MS03-039. W32/Agobot-FE moves itself to the Windows system folder as WINSEC16.EXE and creates entries in the registry at the following locations to run itself on system restart:

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

W32/Agobot-FE attempts to connect to a remote IRC server and join a specific channel. It attempts to terminate the following security or virus related.

W32/Bagle-C (Aliases: W32.Beagle.C@mm, WORM_Bagle.C, Win32.Bagle.C, W32/Bagle.c@MM, W32.Beagle.A@mm, I-Worm.Bagle.c) (Win32 Worm): This worm has been reported in the wild. It is an e-mail worm that sends itself via its own SMTP engine to addresses harvested from your hard disk. The worm appears with a Microsoft Office 2000 Excel icon. When run, the worm opens NOTEPAD.EXE, copies itself to the Windows system folder as README.EXE, and creates the following files in the same folder:

- DOC.EXE - a DLL plugin used to load ONDE.EXE
- ONDE.EXE - the main DLL component of the worm
- README.EXEOPEN - a copy of the worm in ZIP format

W32/Bagle-C adds the value, “gouday.exe = <SYSTEM>\readme.exe,” to the registry key:

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

This means that W32/Bagle-C runs every time you logon to your computer: W32/Bagle-C also creates the following registry entries:

- HKCU\Software\DateTime2\frun=1
- HKCU\Software\DateTime2\port=2745
- HKCU\Software\DateTime2\uid=<number>

E-mails have various subject lines, no message text and the attachment is a randomly named ZIP archive. W32/Bagle-C opens up a backdoor on port 2745 and listens for connections. If it receives the appropriate command, it attempts to download and execute a file. W32/Bagle-C also makes a web connection to a remote URL and reports the location and open port of infected computers. If the date is after 14 March 2004, W32/Bagle-C terminates itself and deletes all the registry entries it created when it first ran.

W32/Bagle-D (Win32 Worm): This worm has been reported in the wild. It is an e-mail worm that sends itself via its own SMTP engine to addresses harvested from your hard disk. When run, the worm opens

NOTEPAD.EXE, copies itself to the Windows system folder as README.EXE and creates the following files in the same folder:

- DOC.EXE - a DLL plugin used to load ONDE.EXE
- ONDE.EXE - the main DLL component of the worm
- README.EXEOPEN - a copy of the worm in ZIP format

W32/Bagle-D adds the value, “gouday.exe = <SYSTEM>\readme.exe,” to the registry key:

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

This means that W32/Bagle-D runs every time you logon to your computer. W32/Bagle-D also creates the following registry entries:

- HKCU\Software\DateTime3\frun=1
- HKCU\Software\DateTime3\port=2745
- HKCU\Software\DateTime3\uid=<number>

E-mails have various subject lines, no message text, and a randomly named ZIP archive. It opens up a backdoor on port 2745 and listens for connections. If it receives the appropriate command, it attempts to download and execute a file. W32/Bagle-D also makes a web connection to a remote URL and reports the location and open port of infected computers. If the date is after 14 March 2004, W32/Bagle-D terminates itself and deletes all the registry entries it created when it first ran.

W32/Bagle.E (Aliases: WORM_BAGLE.E, Worm/Bagle.E.GODO, Win32:Beagle-C [Unp], W32/Bagle.gen@MM, I-Worm.Bagle.e, W32/Bagle.E.worm, W32.Beagle.E@mm, Bagle.E, Win32.Bagle.E) (Win32 Worm): This worm arrives as a randomly-named zipped e-mail attachment. It uses a text file icon in order to entice users into running it. The worm drops several files and injects one of its components (GODO.EXE) into EXPLORER.EXE to stay resident in memory. Using its own SMTP (Simple Mail Transfer Protocol) engine, it then sends its e-mail messages using a spoofed return address to several gathered recipients. The worm then adds a copy of itself as an attachment. The e-mail has various subject lines, message text, and attachments. W32/Bagle.E opens port 2745, which enables it to download and execute an updated copy of itself. It terminates some active processes if they are detected. The worm runs on Windows 95, 98, ME, 2000 and XP.

W32/Bagle-F (Aliases: I-Worm.Bagle.f, W32/Bagle.f@MM**, WORM_BAGLE.F, W32.Beagle.F@mm, Win32.Bagle.F) (Win32 Worm):** This worm has been reported in the wild. It is an e-mail worm that sends itself via its own SMTP engine to addresses harvested from your hard disk. W32/Bagle-F also spreads via peer-to-peer shared folders. The worm copies itself to the Windows system folder as I1RU54N.EXE and creates the following files in the same folder:

- II5NJ4.EXE - a DLL plugin used to load GO54O.EXE
- GO54O.EXE - the main DLL component of the worm
- I1RU54N4.EXEOPEN - an exact copy of the worm or a copy of the worm in ZIP format (the ZIP may be password protected)

W32/Bagle-F adds the value, “rate.exe = <SYSTEM>\i1ru54n4.exe,” to the registry key:

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

This means that W32/Bagle-F runs every time you logon to your computer. W32/Bagle-F also creates the following registry entry:

- HKCU\Software\winword\frun=1

E-mails have various subject lines, message text, and attachment files (extension EXE, SCR or ZIP). W32/Bagle-F copies itself to folders containing the text 'shar.' The worm opens up a backdoor on port 2745 and listens for connections. If it receives the appropriate command, it attempts to download and execute a file. The worm also makes a web connection to a remote URL and reports the location and open port of infected computers. If the date is after 25 March 2005, W32/Bagle-F terminates itself and deletes all the registry entries it created when it first ran.

W32/Bagle-G (Aliases: W32/Bagle.g@MM**, WORM_BAGLE.G, W32.Beagle.G@mm) (Win32 Worm):** This worm has been reported in the wild. It is an e-mail worm that sends itself via its own SMTP engine to addresses harvested from your hard disk. W32/Bagle-G also spreads via peer-to-peer shared folders. The worm copies itself to the Windows system folder as I1RU54N.EXE and creates the following files in the same folder:

- II5NJ4.EXE - a DLL plugin used to load GO54O.EXE
- GO54O.EXE - the main DLL component of the worm
- I1RU54N4.EXEOPEN - an exact copy of the worm or a copy of the worm in ZIP format (the ZIP may be password protected)

W32/Bagle-G adds the value, 'rate.exe = <SYSTEM>\i1ru54n4.exe,' to the registry key:

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

This means that W32/Bagle-G runs every time you logon to your computer. W32/Bagle-G also creates the following registry entry:

- HKCU\Software\winword\frun=1

E-mails have various subject lines, message text, and various attachments (extension EXE, SCR or ZIP). W32/Bagle-G copies itself to folders containing the text 'shar.' The worm opens up a backdoor on port 2745 and listens for connections. If it receives the appropriate command, it attempts to download and execute a file. The worm also makes a web connection to a remote URL and reports the location and open port of infected computers. If the date is after 25 March 2005, W32/Bagle-G terminates itself and deletes all the registry entries it created when it first ran.

W32/Bagle-H (Aliases: W32/Bagle-H@mm, I-Worm.Bagle.h, W32/Bagle.h@MM, Bagle.H, WORM_BAGLE.H, I-Worm.Bagle.Gen, Win32.Bagle.H) (Win32 Worm): This worm has been reported in the wild. It 32/Bagle-H is an e-mail worm that sends itself via its own SMTP engine to addresses harvested from your hard disk. The worm searches for files with the extensions WAB, TXT, HTM, XML, DBX, MDX, EML, NCH, MMF, ODS, CFG, ASP, PHP, PL, ADB, TBB, and SHT and uses the files to extract the recipient and the sender e-mail addresses (therefore the sender e-mail address is spoofed) . When run, the worm copies itself to the Windows system folder as i11r54n4.exe and creates the following files in the same folder:

- i1i5n1j4.exe - a DLL plugin used to load go154o.exe
- go154o.exe - the main DLL component of the worm
- i11r54n4.EXEOPEN - a copy of the worm in a password protected ZIP format

W32/Bagle-H adds the value, "rate.exe = <SYSTEM>\i11r54n4.exe," to the registry key:

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

This means that W32/Bagle-H runs every time you logon to your computer. E-mails have various subject lines, randomly chosen message text, and various attachments (extension ZIP). W32/Bagle-H opens up a backdoor on port 2745 and listens for connections. If an appropriate command is received, the worm attempts to download and execute a file. The worm makes a web connection to a remote URL and reports the location and open port of infected computers. W32/Bagle-H searches the mapped drives for the folders containing the string "shar" in the folder name. If such a folder is found, the worm copies itself to the folder using the various filenames. If the date is after 25 March 2005, W32/Bagle-H terminates itself and deletes all the registry entries it created when it first ran.

W32/Bagle-I (Aliases: I-Worm.Bagle.h, W32.BEAGLE.I@MM, WORM_BAGLE.I, W32.Beagle.I@mm, Win32.Bagle.I, W32/Bagle.i@MM) (Win32 Worm): This worm has been reported in the wild. It is an e-mail worm that sends itself via its own SMTP engine to addresses harvested from your hard disk. The worm searches for files with the extensions WAB, TXT, HTM, XML, DBX, MDX, EML, NCH, MMF, ODS, CFG, ASP, PHP, PL, ADB, TBB, and SHT. When run, the worm opens copies itself to the Windows system folder as i11r54n4.exe and creates the following files in the same folder:

- go154o.exe - the main DLL component of the worm
- i1i5n1j4.exe - a DLL plugin used to load go154o.exe
- i11r54n4.EXEOPEN - a copy of the worm in a password protected ZIP format

W32/Bagle-I adds the value rate.exe = <SYSTEM>\i11r54n4.exe to the registry key:

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

This means that W32/Bagle-I runs every time you logon to your computer. E-mails have various subject lines, randomly chosen message text, and various attachments. W32/Bagle-I opens up a backdoor on port 2745 and listens for connections. If it receives the appropriate command, it attempts to download and execute a file. The worm also makes a web connection to a remote URL and reports the location and open port of infected computers. W32/Bagle-I attempts to terminate several anti-virus and security-related processes. It searches mapped drives for folders containing the string 'shar' in the folder name.

If the date is after 25 March 2005, W32/Bagle-I terminates itself and deletes all the registry entries it created.

W32/Bagle-J (Aliases: W32/Bagle.j@MM, WORM_BAGLE.J, W32/Bagle.j@mm, Win32.Bagle.J) (Win32 Worm): This worm has been reported in the wild. It is an e-mail worm that sends itself via its own SMTP engine to addresses harvested from your hard disk. The worm searches for files with the extensions WAB, TXT, MSG, HTM, XML, DBX, MDX, EML, NCH, MMF, ODS, CFG, ASP, PHP, PL, ADB, TBB, SHT, UIN, and CGI. The worm copies itself to the Windows system folder as IRUN4.EXE and creates the file IRUN4.EXEOPEN (a copy of the worm in a password protected ZIP format) in the same folder. W32/Bagle-J adds the value, 'ssate.exe = <SYSTEM>\irun4.exe,' to the registry key:

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

This means that W32/Bagle-J runs every time you logon to your computer. E-mails have various subject lines, message texts, and attachments. W32/Bagle-J opens up a backdoor on port 2745 and listens for connections. If it receives the appropriate command, it attempts to download and execute a file. The worm also makes a web connection to a remote URL and reports the location and open port of infected computers. W32/Bagle-J attempts to terminate several Anti-Virus and security related Processes. W32/Bagle-J searches the mapped drives for folders containing the string "shar" in the folder name. If the date is after 25 April 2005, W32/Bagle-J terminates itself and deletes all the registry entries it created when it first ran. W32/Bagle-J contains text hidden inside its code, which is not displayed.

W32/Bagle-K (Aliases: I-Worm.Bagle.j, W32.Beagle.A@mm, WORM_BAGLE.GEN, WORM_BAGLE.K, Worm.Bagle.j, Win32.HLLM.Beagle.based, W32/Bagle.K.worm, Win32:Beagle-C [Unp]., Worm/Bagle.H.GODO, I-Worm/Bagle.K, W32/Bagle.k@MM, Win32.Bagle.K, Bagle.K,) (Win32 Worm): This worm has been reported in the wild. It is an e-mail worm that sends itself via its own SMTP engine to addresses harvested from your hard disk. The worm searches for files with the extensions WAB, TXT, HTM, XML, DBX, MDX, EML, NCH, MMF, ODS, CFG, ASP, PHP, PL, ADB, TBB, and SHT. When run, the worm opens copies itself to the Windows system folder as winsys.exe and creates the following files in the same folder:

- W32/Bagle-K adds the value ssate.exe = <SYSTEM>\winsys.exe to the registry entry HKCU\Software\Microsoft\Windows\CurrentVersion\Run.

This means that W32/Bagle-K runs every time you logon to your computer. E-mails have various sender lines, subject lines, message text, and attachment files chosen from a randomly named ZIP archive. W32/Bagle-K opens up a backdoor on port 2745 and listens for connections. If it receives the appropriate command, it attempts to download and execute a file. The worm also makes a web connection to a remote URL and reports the location and open port of infected computers. W32/Bagle-K attempts to terminate several anti-virus and security-related processes. W32/Bagle-K searches the mapped drives for the folders containing the string "shar" in the folder name. If such folder is found, the worm copies itself to the folder using various names. If the date is after 25 April 2005, W32/Bagle-K terminates itself and deletes all the registry entries it created. W32/Bagle-K contains text hidden inside its code, which is not displayed.

W32/Bagle.L@mm (Aliases: WORM_BAGLE.L, I-Worm.Bagle.l,) (Win32 Worm): This worm drops a copy of itself in the Windows system folder and modifies the registry so that its copy runs at every Windows startup. It also drops the following files, which are actually the DLL components of this malware:

- IINJ4.EXE - a file loader for the SYSTEM.EXE file.
- SYSTEM.EXE - a malicious file that is detected by Trend Micro as TROJ_MITGLIEDR.C.

This malware connects to the several Web sites to report the user's IP address and proxy port. It also has the ability to terminate certain processes, which are usually related to antivirus and firewall applications. It runs on Windows 95, 98, ME, NT, 2000 and XP.

W32/Bagle-N (Aliases: W32/Bagle.n@MM, PE_BAGLE.N, W32.Beagle.M@mm, Bagle.N, Win32.Bagle.N) (Win32 Worm): This worm has been reported in the wild. It is an e-mail worm that sends itself via its own SMTP engine to addresses harvested from your hard disk. The worm searches for files with the extensions WAB, TXT, HTM, XML, DBX, MDX, EML, NCH, MMF, ODS, CFG, ASP, PHP, PL, ADB, TBB, and SHT. When run, the worm copies itself to the Windows system folder using the name winupd.exe. W32/Bagle-N adds the value, "winupd.exe = [SYSTEM]\winupd.exe," to the registry entry:

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

This means that W32/Bagle-N runs every time you logon to your computer. E-mails have various subject line, message text, and attachments. Attached files arrive either as programs (with a .PIF extension) or as password-protected archives (with a .ZIP or .RAR extension). The password is included in the e-mail. W32/Bagle-N opens up a backdoor and listens for connections. If it receives the appropriate command, it attempts to download and execute a file. The worm also makes a web connection to a remote URL and reports the location and open port of infected computers. W32/Bagle-N attempts to terminate several anti-virus and security-related processes. W32/Bagle-N searches the mapped drives for the folders containing the string "shar" in the folder name. The worm copies itself to these folders using various names. The author of the worm has hidden an ASCII text representation of a butterfly inside the viral code, alongside the words:

The White Rabbit Presents
The first and the single
Anti-NetSky AntiVirus

W32/Bagle-O (Win32 Worm): This worm has been reported in the wild. It is an e-mail worm that sends itself via its own SMTP engine to addresses harvested from your hard disk. The worm searches for files with the following extensions: WAB, TXT, MSG, HTM, SHTM, STM, XML, DBX, MBX, MDX, EML, NCH, MMF, ODS, CFG, ASP, PHP, PL, ADB, TBB, SHT, XLS, OFT, UIN, CGI, MHT, DHTM, and JSP. When run, the worm copies itself to the Windows system folder using the name winupd.exe. W32/Bagle-O adds the value, "winupd.exe = <SYSTEM>\winupd.exe," to the registry entry:

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

This means that W32/Bagle-O runs every time you logon to your computer. E-mails have various subject lines, subject text, and attachments. W32/Bagle-O opens port 2556 and listens for remote commands. If it receives the appropriate command, it attempts to download and execute a file. The worm also makes a web connection to a remote URL and reports the location and open port of infected computers. W32/Bagle-O attempts to terminate a wide range of anti-virus and security related processes. W32/Bagle-O searches the mapped drives for the folders containing the string "shar" in the folder name. If run after 31 December 2005, the worm deletes the registry entries it created when first run. The author of the worm has hidden an ASCII text representation of a butterfly inside the virus code, alongside the words:

The White Rabbit Presents
The first and the single
Anti-NetSky AntiVirus

W32/Bereb-B (Aliases: Worm.P2P.Astaber, Win32/Bereb.C, W32.HLLW.Bereb, WORM_BEREB.B) (Win32 Worm): This is a peer-to-peer worm that copies itself to the shared folder startrwin in the Windows folder using a variety of names. The following registry entry is added to make startrwin a shared folder:

- HKCU\Software\Kazaa\LocalContent\Dir0 = <path to startrwin folder>

The worm will also copy itself to the Windows folder as svckernell.com and set the following registry entry that points to this copy to ensure it is run at system logon:

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

W32/Bereb-B is an IRC backdoor Trojan that listens for commands on specific IRC channels. It creates the file library.dat in the subfolder WinMx in the Program Files folder. This file is not malicious and can be deleted.

W32/Bizex-A (Aliases: W32/Bizex.worm, Worm.Win32.Bizex, Worm.Bizex, Worm/Bizex.3, WORM_BIZEX.A) (Win32 Worm): W32/Bizex-A is a worm that propagates over ICQ. The worm appears as an ICQ message prompting the user to visit a website hosted on www.jokeworld.com. The web page downloads a file to the user's computer as startup.wav and runs the file. Startup.wav contains a script that creates the file WinUpdate.exe in the startup folder. When Windows is next started, WinUpdate.exe attempts to download a file named updater.exe to the Windows temp folder as aptgetupd.exe. Aptgetupd.exe is the main component of W32/Bizex-A. The worm copies itself to the sysmon subfolder of the Windows system folder as a file named sysmon.exe and adds the following registry entry to ensure that the worm is run each time Windows starts up:

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

W32/Bizex-A also drops the following DLL files in the Windows system folder icw_socket.dll, ICQ2003Decrypt.dll, java32.dll, and javaext.dll. The DLL files are used to send ICQ messages to people on the infected user's contact list and to monitor user activity. Logged information is sent via FTP to a remote server.

W32/Cissi-B (Aliases: Worm.Win32.Pinom.c, W32/Imbiat.worm, Win32/Pinom.C, W32/Pinom.worm!backdoor, Win32.HLLW.Imbiat, Backdoor:Win32/Rirc.B, W32.Cissi.A@mm, WORM_CISSI.B) (Win32 Worm): This is a worm that attempts to spread by e-mailing itself via SMTP and by copying itself to network shares with weak passwords. The worm allows unauthorized remote access to the computer via IRC channels. It copies itself to the Windows system folder as PENIS.EXE and changes the [boot] field within SYSTEM.INI (or WIN.INI under MS Win NT/2000/XP) to run itself on system restart. Under Windows NT-based systems, the worm may change the following entry in the registry to run the worm on system restart:

- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell

W32/Cissi-B may attempt to e-mail itself to e-mail addresses gleaned from files on the user's hard disk. The worm attempts to copy itself to the Startup folder on remote shared computers as !IMPORTANT!.EXE or SETUP.EXE.

W32.Cone@mm (Alias: W32.Cone.B@mm) (Win32 Worm): This is a mass-mailing worm that sends itself to e-mail addresses it gathers from the files on an infected computer.

W32.Cone.E@mm (Win32 Worm): This is a minor variant of W32.Cone@mm. The worm sends itself to the e-mail addresses it gathers from the files on an infected computer. It also modifies the local hosts file to prevent access to various Web sites. The attachment will have a .exe, .scr, or .zip file extension.

W32.Cone.F@mm (Win32 Worm): This is a mass-mailing worm that uses its own SMTP engine to send itself to the e-mail addresses it gathers from the files on an infected computer. The e-mail attachment will have a .exe or .zip file extension. It is written in Microsoft Visual C++ and is compressed with Petite.

W32/Hiton-A (Aliases: I-Worm.Hiton, W32/Hiton.a@MM**, WORM_HITON.A, W32.Hiton@mm, Win32.Hiton.A) (Win32 Worm):** This is a mass mailing worm that e-mails itself, using its own SMTP engine, to addresses harvested from address books and files on the hard disk. When first run, W32/Hiton-A displays a fake error message. The worm copies itself to the Windows system folder as SVCHOST.EXE and creates the following files in the same folder:

- MSSVC.DLL - a component of the worm
- WSUCK32.DLL - a list of filenames
- WSICK32.DLL - a file containing sent e-mail addresses

W32/Hiton-A creates registry entries in the following locations to run itself every time the user logs on to the computer:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run
- HKCU\Software\Microsoft\Command Processor\AutoRun
- HKCR\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\InProcServer32

E-mails sent by the worm have various subject lines, message text, and attachments (extension EXE, BAT, PIF, SCR or ZIP). The worm also terminates various processes.

W32.HLLW.Annil@mm (Win32 Worm): This is a mass-mailing worm that uses its own SMTP engine to spread. The e-mail subject, message, and attachment vary. This threat also attempts to spread through the KaZaA file-sharing network.

W32.HLLW.Citor (Win32 Worm): This is a worm that attempts to spread through IRC by sending a URL link to other people in the channel. The URL link is the worm executable.

W32.HLLW.Cult.P@mm (Win32 Worm): This is a mass-mailing worm that uses its own SMTP engine to send itself to randomly generated e-mail addresses. The worm also has IRC Trojan functionality that allows a malicious user to control your computer by using Internet Relay Chat (IRC). The e-mail message has the following characteristics:

- Subject: Hello , I sent you a beautiful Love Card ^_*
- Attachment: BeautyLove.pif

It is compressed with FSG.

W32.HLLW.Evianc (Win32 Worm): This is a worm that attempts to spread through the KaZaA file-sharing network. It is written in the Microsoft Visual Basic (VB) programming language and is compressed with UPX.

W32.HLLW.Heycheck (Win32 Worm): This is a worm that attempts to spread using Microsoft Instant Messenger and peer-to-peer file sharing networks. It acts as a web server on an infected computer, accepting connections on port 80 and sending a link to the worm in response to HTTP requests. The existence of the file C:\Card.exe is an indication of possible infection.

W32.HLLW.Moega.AP (Win32 Worm): This is a minor variant of W32.HLLW.Moega.AG. The W32.HLLW.Moega.AP executable icon looks similar to that of the Windows XP Windows Update executable, Wupdated.exe. See the "Technical Details" section for an illustration.

W32/Maddis-A (Aliases: W32/Maddis.worm, W32/Aveng.A, TrojanProxy.Win32.TexLock, Win32.Maddis.A, WORM_MADDIS.A) (Win32 Worm): This is a worm which spreads via networks shares. The worm uses stealth techniques in an attempt to hide its presence on an infected computer. When first run, W32/Maddis-A creates a copy of itself named usrinit.exe in the Windows system folder and a file named helper.dll in the Windows or Temp folder. On Windows98 based operating systems, the worm adds the registry entry:

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

On Windows NT based operating systems, usrinit.exe is registered as a service. Helper.dll hides the worm by intercepting system functions and masking any values which contain various strings. W32/Maddis-A sends an HTTP packet containing various system and password information to the following URLs:

- http://www.proxylist.ru/control/21/
- http://www.proxylist.com.ua/control/21/
- http://www.proxylist.com.ru/control/21/
- http://www.proxylist.biz/control/21/
- http://66.98.173.166/control/21/

W32/Maddis-A opens several ports and runs proxy servers for Telnet, HTTP and Socks.

W32.Mockbot.A.Worm (Win32 Worm): This is a worm that spreads using computers infected with the W32.Mydoom.A@mm, W32.Blaster.Worm, and Backdoor.Optix worms. To spread itself, the worm can also exploit the DCOM RPC vulnerability (described in Microsoft Security Bulletin MS03-026), as well as a vulnerability in the DameWare Mini Remote Control program. It is written in C and is packed with UPX.

W32/MyDoom-G (Aliases: W32.Mydoom.G@mm, W32/Mydoom.g@MM, WORM_MYDOOM.G, Win32.Mydoom.G) (Win32 Worm): This is a worm that spreads by e-mail. When the infected attachment is launched, the worm harvests e-mail addresses from address books and from files on the hard disk. When first run, W32/MyDoom-G creates the file MESSAGE containing random characters in the temp folder, opens the file in Notepad, and then deletes it. E-mails have spoofed ‘To:’ and ‘From:’ fields, various subject lines, various message texts (can be absent, same as the subject line, or random characters), and random attachment filenames (can have one of the following extensions EXE, SCR, COM, PIF, BAT, CMD, or ZIP). The worm will not send itself to e-mail addresses belonging to domains containing the following strings: bsd, mit.edu, gnu., fsf., urlon, ibm.com, google., kernel., rfc-edit, sendmail., isi.edu, isc.org, secur, packetstorm, stanford.edu, berkeley, rutgers.edu, ucsd.edu, uci.edu, mozilla., sourceforge, sf.net, slashdot., ymante, example.com, sopho, nai.co, trend.c, trendmic, ruslis, avp, norma, icrosoft., msn.c, hotmail.com, panda, ssagelab, support, .gov, gov., .mil, iana., arin., ripe., or ietf. W32/MyDoom-G creates a randomly named file in the Windows system or temp folder and adds a randomly named registry entry to:

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

to run this file every time the user logs on to the computer. The worm also drops a randomly named DLL file in the Windows system or temp folder. The DLL is a backdoor program loaded by the worm that allows remote malicious users to connect to TCP port 1080 and upload files for the infected computer to run. The DLL creates the following registry entry to load itself on system restart:

- HKCR\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\InProcServer32\Default= <location of dll>

The DLL also terminates several processes, for example avpupd, start.exe, and cmd32.exe. W32/MyDoom-G overwrites PIF files and creates several copies of itself with filenames matching existing filenames found on the computer but having double extensions, for example <filename>.doc.exe. It attempts a Denial of Service attack on www.symantec.com by sending numerous HTTP GET requests to this URL. Hidden inside the W32/MyDoom-G worm's code is text that never is displayed.

W32/Netsky-C (Aliases: I-Worm.Moodown.c, Win32/Netsky.C, W32.Netsky.C@mm, WORM_NETSKY.C, Win32.HLLM.Foo.41984, Worm/NetSky.C, I-Worm/Netsky.C, W32/Netsky.c@MM, Win32/Netsky.C@mm, I-Worm.NetSky.c, W32/Netsky.C@mm!petite) (Win32 Worm): This worm has been reported in the wild. It is a worm that spreads via shared networks and by e-mailing itself to addresses found within files located on drives C: to Z:. The e-mail subject line, message text, and attachment filename are randomly chosen from lists within the worm. The attachment extension will be ZIP, COM, EXE, PIF, or SCR and may be preceded by .DOC, .HTM, .RTF, or .TEXT. (e.g. visa.htm.scr) When first run ,W32/Netsky-C copies itself to the Windows folder as winlogon.exe and creates the following registry entry so that winlogon.exe is run automatically each time Windows is started:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\ICQNet = <WINDOWS>\winlogon.exe -stealth

W32/Netsky-C spreads via file sharing networks by copying itself to folders on drives C: to Z: whose name contains the sub-string 'Shar,' using a filename randomly chosen. When the worm is run on the 26th of February 2004 between 06:00 and 09:00, it may cause the computer to beep sporadically. The Netsky-C worm contains text that is embedded in its code.

W32/Netsky-D (Aliases: W32/Netsky.c@MM, I-Worm.NetSky.d, Win32/Netsky.D, WORM_NETSKY.D, W32.Netsky.D@mm, W32/Netsky.d@MM, W32/Netsky.D.worm, I-Worm.Netsky.d) (Win32 Worm): This worm has been reported in the wild. It is a worm that spreads via e-mail and by copying itself to the root folders of available network drives. When sending itself via e-mail the worm can forge the sender's e-mail address. W32/Netsky-D may arrive in an e-mail various subject lines, message text, and attachments. When first run, W32/Netsky-D copies itself to the Windows folder as winlogon.exe and creates the following registry entry so that winlogon.exe is run automatically each time Windows is started:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\ICQ Net = <WINDOWS>\winlogon.exe -stealth

W32/Netsky-D searches all mapped drives for files with the following extensions in order to find e-mail addresses: MSG, OFT, SHT, DBX, TBB, ADB, DOC, WAB, ASP, UIN, RTF, VBS, HTML, HTM, PL, PHP, TXT, and EML. It also attempts to delete various registry entries. The worm queries for various IP addresses and it programmed to not forward itself via e-mail if the recipient e-mail address contains certain strings. W32/Netsky-D attempts to delete some registry entries including ones related to the W32/MyDoom-A and W32/MyDoom-B worms in a similar way to previous variants. When the worm is run on 2 March 2004 between 06:00 and 08:59, it may cause the computer to beep sporadically.

W32/Netsky-E (Aliases: W32/Netsky.c@MM, W32.Netsky.E@mm, WORM_NETSKY.E, W32.Netsky.E@mm, Win32.Netsky.E, W32/Netsky.e@MM, I-Worm.Netsky.e) (Win32 Worm): This is a worm that spreads by e-mailing itself to addresses found within files located on drives C: to Z:. The e-mail subject line, message text, and attachment filename are randomly chosen from internal lists. The attachment extension will be ZIP, COM, EXE, PIF, SCR, BAT, or CMD and may be preceded by an extension of TXT, RTF, DOC, HTM, JPG, or GIF. When first run, the worm copies itself to the Windows folder as winlogon.exe and creates the following registry entry, so that winlogon.exe is run automatically each time Windows is started:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\ICQ Net =<Windows folder>\winlogon.exe -stealth

When the worm is run on the 2nd of March 2004 between 06:00 and 09:00, it may cause the computer to beep sporadically. W32/Netsky-E contains hidden text inside its code that is not displayed.

W32.NETSKY.F@mm (Aliases: WORM_NETSKY.F, W32/NETSKY.F@MM, NetSky.F, Win32.Netsky.F) (Win32 Worm): This memory-resident worm drops a copy of itself as the file SVCHOST.EXE in the Windows folder. It creates threads for its mass-mailing routine, gathering of e-mail addresses, and its payload. The worm uses its own SMTP engine to propagate via e-mail and has a spoofed 'From' line, various subject lines, message text, and attachments. It connects to a local or several external DNS servers, which it uses as its SMTP server, to search for a mail exchanger that matches the domain name of the target recipient's address. This malware modifies the Windows registry, and in the process deactivates several other malware files. If the current system date is March 2, 2004 and the time is between 6 and 9 AM, this malware generates beeping sounds. This activity lasts until 8:59 AM. It runs on Windows 95, 98, ME, NT, 2000 and XP.

W32/Netsky-G (Aliases: I-Worm.NetSky.g, W32/Netsky.c@MM, NetSky.G, W32.Netsky.G@mm, Win32.Netsky.G, WORM_NETSKY.G, NetSky.G) (Win32 Worm): This is a worm that spreads via e-mail. In order to run automatically when Windows starts up the worm copies itself to the file avguard.exe in the Windows folder and creates the registry entry:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Special Firewall Service = "C:\WINDOWS\avguard.exe -av service"

The worm attempts to disable various anti-virus and security related applications as well as other worms by deleting registry entries used by them. Some of the registry entries removed by W32/Netsky-G are produced by variants of the W32/Bagle family of worms. W32/Netsky-G scans all local drives for files with various extensions and attempts to extract e-mail addresses from them. In order to spread, the worm creates 16 threads that send e-mails to the harvested addresses containing the worm as an attachment. W32/Netsky-G uses its own SMTP engine to send the mail. The subject lines, message texts, and attached filenames are randomly chosen. In some cases W32/Netsky-G creates a zip archive of the attachment before sending the e-mail. On 10 March 2004, W32/Netsky-G plays random sounds between 6 a.m. and 8 a.m.

W32/Netsky-H (Aliases: W32.NETSKY.H@mm, W32/NETSKY.H@MM, NetSky.H, WORM_NETSKY.H) (Win32 Worm): This is a worm that spreads via e-mail. In order to run automatically when the user logs on to the computer the worm copies itself to the file maja.exe in the Windows folder and creates the following registry entry:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Antivirus = "<Windows>\maja.exe -antivirus service"

The worm attempts to disable various anti-virus and security related applications as well as other worm processes by deleting registry entries used by them. In particular it attempts to delete the following values: Taskmon, Explorer, KasperskyAv, system., msgsvr32, DELETE ME, service, Sentry, Windows Service Host below the registry key:

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

The worm deletes the following values: Taskmon, Explorer, KasperskyAv, d3dupdate.exe, au.exe, OLE, Windows Service Host, gouday.exe, rate.exe, sate.exe, ssate.exe, srate.exe, sysmon.exe below the registry key:

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

W32/Netsky-H also deletes the following registry entries:

- HKCR\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\InProcServer32
- HKCU\System\CurrentControlSet\Services\WksPatch
- HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\PINF

These entries are partly produced by the different variants of the W32/Bagle and W32/MyDoom families of worms. It harvests e-mail addresses from files on all local drives which have one of the following extensions: DHTM, CGI, SHTM, MSG, OFT, SHT, DBX, TBB, ADB, DOC, WAB, ASP, UIN, RTF, VBS, HTML, HTM, PL, PHP, TXT, or EML. The worm avoids e-mail addresses containing various strings. In order to spread, the worm creates several threads that send e-mails containing the worm as an attachment to the harvested addresses. W32/Netsky-H uses its own SMTP engine to send the mail. E-mails have various subject lines, message texts, and attachments. On 8 March 2004 at 11:00 AM, W32/Netsky-H plays random sounds for one hour.

W32.Netsky.I@mm (Aliases: WORM_NETSKY.I, NetSky.I, Win32/Netsky.gen!, I-Worm.Netsky.gen, W32/Netsky.i@MM, Win32.Netsky.I, W32/Netsky-I) (Win32 Worm): This memory-resident worm drops a copy of itself as the file FOODING.EXE in the Windows folder. It uses its own SMTP engine to propagate via e-mail, that has various subject lines, message text, and attachments. The worm connects to a local or several external DNS servers, which it uses as its SMTP server, to search for a mail exchanger that matches the domain name of the target recipient's address. This malware modifies the Windows registry, and in the process deactivates several other malware files. If the current system date is March 8, 2004 and the time is 11 AM, this malware generates beeping sounds. It runs on Windows 95, 98, ME, NT, 2000 and XP.

W32/Netsky-J (Aliases: W32/Netsky.j@MM, W32.Netsky.J@mm, NetSky.J, WORM_NETSKY.J, W32/Netsky-K, Win32.Netsky.K) (Win32 Worm): This worm has been reported in the wild. It is a mass mailing worm that uses its own SMTP engine to e-mail itself to addresses harvested from files on local drives. In order to run automatically when the user logs on to the computer, the worm copies itself to the file winlogon.exe in the Windows folder and creates the following registry entry:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\ICQ Net =<Windows folder>\winlogon.exe -stealth

It attempts to disable various anti-virus and security related applications as well as other worm processes by deleting registry entries used by them. In particular it attempts to delete the following values: Taskmon, Explorer, KasperskyAv, system., msgsvr32, DELETE ME, service, Sentry, Windows Services Host below the registry key:

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

The worm deletes the following values: Explorer, KasperkyAv, d3dupdate.exe, au.exe, OLE, Windows Services Host below the registry key:

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

W32/Netsky-J also deletes the following registry entries:

- HKCR\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\InProcServer32
- HKLM\System\CurrentControlSet\Services\WksPatch
- HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\PINF

Some of the above entries are created by the different variants of the W32/Bagle and W32/MyDoom families of worms. W32/Netsky-J harvests e-mail addresses from files on all local drives which have one of the following extensions: DHTM, CGI, SHTM, MSG, OFT, SHT, DBX, TBB, ADB, DOC, WAB, ASP, UIN, RTF, VBS, HTML, HTM, PL, PHP, TXT, and EML. The worm avoids e-mail addresses containing various strings. The e-mail message has various subject lines, message text, and attachments. On 2 March 2004 at 6:00 AM, W32/Netsky-I plays random sounds for three hours.

W32/Netsky-K (Aliases: W32.Netsky.K@mm, W32/Netsky@MM, NetSky.K, WORM_NETSKY.K) (Win32 Worm): This worm has been reported in the wild. It is a mass mailing worm that uses its own SMTP engine to e-mail itself to addresses harvested from files on local drives. In order to run automatically when the user logs on to the computer the worm copies itself to the file avpguard.exe in the Windows folder and creates the following registry entry:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\My AV = <Windows folder>\avpguard.exe -av serv

The worm attempts to disable various anti-virus and security related applications as well as other worm processes by deleting registry entries used by them. In particular it attempts to delete the following values: Taskmon, Explorer, system., msgsvr32, DELETE ME, service, Sentry, Windows Services Host below the registry key:

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

The worm deletes the following values: Explorer, d3dupdate.exe, au.exe, OLE, Windows Services Host, gouday.exe, rate.exe, sate.exe, ssate.exe, srate.exe, sysmon.exe below the registry key:

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

W32/Netsky-K also deletes the following registry entries:

- HKCR\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\InProcServer32
- HKLM\System\CurrentControlSet\Services\WksPatch
- HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\PINF

Some of the above entries are created by variants of the W32/Bagle and W32/MyDoom families of worms. W32/Netsky-K harvests e-mail addresses from files on all local drives which have one of the following extensions: XML, WSH, JSP, DHTM, CGI, SHTM, MSG, OFT, SHT, DBX, TBB, ADB, DOC, WAB, ASP, UIN, RTF, VBS, HTML, HTM, PL, PHP, TXT, and EML. The e-mails have various subject lines, message text, and attachments. On 10 March 2004, W32/Netsky-K plays random sounds between 10 a.m. and 11 a.m.

W32/Netsky-L (Aliases: W32.Netsky.Gen@MM, NetSky.L, WORM_NETSKY.L,) (Win32 Worm): This worm has been reported in the wild. It is a worm that arrives in an e-mail with various subject lines, message text, and attachments. When W32/Netsky-L is run, a copy will be created in the Windows folder with the filename AVprotect.exe and the following registry entry will be created so that the worm is run when the victim logs on to Windows:

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

W32/Netsky.m@MM (Aliases: WORM_NETSKY.M, I-Worm.NetSky.m, W32/Netsky-M, Win32.Netsky.M) (Win32 Worm): This a mass-mailing worm. The worm may be received in an e-mail message with a spoofed ‘From’ line, various subject lines, message text, and attachments. The mailing component harvests address from the local system. Files with various extensions are also targeted. It sends itself via SMTP, constructing messages using its own SMTP engine. W32/Netsky.m@MM queries the DNS server for the MX record and connects directly to the MTA of the targeted domain and sends the message

W32/Randex-AA (Aliases: Backdoor.SdBot.gen, W32/Randbot.worm, Win32/Randex.AL, W32.Randex.R) (Win32 Worm): This is a network worm with backdoor capabilities which allows a remote intruder to access and control the computer via IRC channels. W32/Randex-AA spreads over a network by copying itself to the Windows system32 folder of C$ and Admin$ shares that contain weak passwords. Each time the worm is run it tries to connect to a remote IRC server and join a specific channel. The worm then runs in the background as a server process listening for commands to execute. When first run the worm copies itself to Windows system folder and creates the following registry entries so that the worm is run when Windows starts up:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Microsoft Mouse Driver Ver 3.0
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce\Microsoft Mouse Driver Ver 3.0
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\Microsoft Mouse Driver Ver 3.0
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Microsoft Mouse Driver Ver 3.0
- HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce\Microsoft Mouse Driver Ver 3.0

W32/Randex-AA collects CD keys of popular games that are installed on the computer.

W32/Roca-A (Aliases: Sober.D, W32/Sober.D@mm, I-Worm.Sober.D, I-Worm.Sober.D, W32/Sober.d@MM, WORM_SOBER.D, Win32.Sober.D) (Win32 Worm): This worm has been reported in the wild. It is a worm that arrives in an e-mail with various subject lines, message text, and attachments. W32/Roca-A copies itself to the Windows system folder using a combination of the following words with an EXE extension: sys, host, dir, explorer, win, run, log, 32, disc, crypt, data, diag, spool, service, smss32 and sets the following registry entries to ensure it is run at system logon:

- HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce\<random name> = <SYSTEM>\<random file> %1
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\<random name>\<random name> = <SYSTEM>\<random file>

where <random file> is the name of the copy of the worm and <random name> is generated using the same word list. W32/Roca-A will also create various files in the Windows system folder. The files mslogs32.dll, zmndpgwf.kxx, yfjq.yqwm and Humgly.lkur are not malicious and can be deleted. When first run W32/Roca-A will display a message box stating "This patch has been successfully installed." If the worm is executed again it will display a message box stating "This patch does not need to be installed on this system. Status: OK"

W97M.Ortant@mm (Aliases: WM97/Ortant-A, W97M/Ortant, W97M_ORTANT.A) (Worm 97 Macro Virus): W97M.Ortant@mm is a macro virus that has worm and Trojan properties. It attempts to delete system files and antivirus program files.

W97M.Trug.B (Word 97 Macro Virus): This is a macro virus that infects Microsoft Word documents when they are opened or closed. W97M.Trug.B attempts to hide its malicious actions and it may delete several files from the system.

WORM_AGOBOT.DE (Internet Worm): This worm exploits certain vulnerabilities to propagate across networks. Like the earlier AGOBOT variants, it takes advantage of the following Windows vulnerabilities:

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

It attempts to log into systems using a list of user names and passwords and then drops a copy. It also terminates antivirus-related processes and steals CD keys of certain game applications. It also has backdoor capabilities and may execute remote commands in the host machine. It runs on Windows NT, 2000 and XP.

WORM_AGOBOT.DU (Alias: W32/Gaobot.worm.mb) (Internet Worm): This new AGOBOT worm exploits certain vulnerabilities to propagate across networks, just like its older variants. It takes advantage of the following Windows vulnerabilities:

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

It attempts to log into systems using a list of user names and passwords. This worm then drops a copy of itself in accessed machines. It also terminates antivirus-related processes and dropped files by other malware. This worm steals CD keys of certain game applications, then sends gathered data to a remote user via mIRC, a chat application. It also has backdoor capabilities and may execute remote commands in the host machine. It runs on Windows NT, 2000 and XP.

WORM_AGOBOT.GA (Aliases: Backdoor.Agobot.gen, W32/Gaobot.worm.gen.d) (Internet Worm): This worm takes advantage of the following Windows vulnerabilities to propagate:

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

It also attempts to log on to systems using a list of user names and passwords. It drops a copy of itself into accessible machines. This worm has backdoor capabilities. It executes commands sent in via Internet Relay Chat (IRC) and can be used to launch as denial of service attack against specified target sites. It terminates certain antivirus processes and files dropped by other malware. It steals the CD keys of popular game applications. This worm runs on Windows NT, 2000, and XP.

WORM_AGOBOT.JP (Alias: W32.HLLW.Gaobot.BF) (Internet Worm): This Agobot worm propagates through network shares by taking advantage of the following Windows vulnerabilities:

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

It attempts to log into systems using a list of user names and passwords. This worm then drops a copy of itself in accessed machines. It also terminates antivirus-related processes and dropped files by other malware. This worm steals CD keys of certain game applications, then sends gathered data to a remote user via mIRC, a chat application. It also has backdoor capabilities and may execute remote commands in the host machine. It runs on Windows NT, 2000 and XP.

WORM_AGOBOT.PY (Internet Worm): This worm exploits certain vulnerabilities to propagate across networks. It takes advantage of the following Windows vulnerabilities:

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

It attempts to log into systems using a list of user names and passwords. This worm then drops a copy of itself in accessed machines. It also terminates antivirus-related processes and dropped files by other malware. This worm steals CD keys of certain game applications, then sends gathered data to a remote user via mIRC, a chat application. It also has backdoor capabilities and may execute remote commands in the host machine. It runs on Windows NT, 2000 and XP.

WORM_AGOBOT.VP (Internet Worm): This polymorphic, memory-resident malware has both worm and backdoor capabilities. Like the earlier AGOBOT variants, it takes advantage of the following Windows vulnerabilities to propagate across networks:

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

It drops itself as the file WINCRT32.EXE in the Windows system folder and attempts to log into systems using a list of user names and passwords. It connects to an Internet Relay Chat (IRC) server and joins an IRC channel to receive malicious commands, which it processes on the system. It also terminates antivirus-related programs and steals CD keys of certain game applications. This UPX-compressed malware runs on Windows NT, 2000, and XP.

WORM_AGOBOT.ZF (Internet Worm): This memory-resident malware has both worm and backdoor capabilities. Like the earlier AGOBOT variants, it takes advantage of the following Windows vulnerabilities to propagate across networks:

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

It attempts to log into systems using a list of user names and passwords. It drops a copy of itself as the file WINSEC16.EXE in the Windows system. It also terminates antivirus-related processes and steals CD keys of certain game applications. It also has backdoor capabilities and may execute remote commands on the host machine. This UPX-compressed malware runs on Windows NT, 2000 and XP.

WORM_CASPID.B (Internet Worm): This memory-resident worm propagates via peer-to-peer (P2P) applications and e-mail. It then drops the following copies of itself in the Windows folder:

- EDISPAC.EXE
- CAPGEDZAC.PIF
- CAPCodB.HTM
- CAPBPlan.HTM

It also drops a copy of itself using a random file name with an SCR extension in the Windows system folder. It takes advantage of the following vulnerabilities:

- A known vulnerability that affects Microsoft Outlook Express 5.5 and 6.0
- Object Tag Code Base Exploit, which affects Microsoft Internet Explorer 5.01, 5.5, and 6.0

This UPX-compressed malware runs on Windows 95, 98, ME, NT, 2000, and XP.

WORM_CONE.C (Alias: W32.Cone.C@MM) (Internet Worm): This worm arrives as a ZIP attachment to an e-mail message with varying subjects. It also propagates via KaZaA, a popular peer-to-peer file-sharing program, by dropping a copy of itself in the shared directory of KaZaA. The dropped copies use any of the following file names:

- Strip Girls-part%d.scr
- Sky lopez - Screensaver.scr
- Playboy Screensaver Dec 2003.scr
  (Note: %d is a generated number.)

It has a payload of overwriting the HOSTS file of the infected system. As a result, this prevents the infected system from accessing certain Web sites, which are usually related to security and antivirus pages. This malware runs on Windows NT and 2000.

WORM_CONE.D (Alias: W32.Cone.D@mm) (Internet Worm): This worm arrives as a ZIP attachment to an e-mail message with varying subjects. It sends out the e-mail message using Simple Mail Transfer Protocol (SMTP). This malware runs on Windows 95, 98, ME, NT, 2000 and XP.

WORM_DARBY.D (Alias: WORM/Darby.D) (Internet Worm): This memory-resident worm propagates through peer-to-peer applications, e-mail, or floppy disk. To propagate through peer-to-peer networks, it drops copies of itself using enticing file names in default shared folders. It sends copies of itself via e-mail using its own Simple Mail Transfer Protocol (SMTP) engine to all e-mail addresses found on the infected machine. It overwrites .HTM files. and exploits known vulnerabilities in Windows as follows:

- Object Tag Code Base Exploit (MS02-015)
- MHTML Exploit (MS03-014)

It also terminates certain processes, which are usually associated with antivirus programs. It uses an icon usually associated with Folders. This UPX-compressed malware is written and compiled using Visual Basic, a high-level programming language. The worm runs on Windows 95, 98, ME, NT, 2000 and XP.

WORM_KECO.A (Aliases: W32.Keco@mm, W32/Keco.worm, Win32.Keco.A, I-Worm.Keco) (Internet Worm): This memory-resident worm uses its own SMTP engine to propagate via e-mail with varying subjects, message bodies, and attachment file names. It gathers target e-mail addresses from certain files found in the hard drive. The worm also connects to a particular Internet Relay Chat (IRC) server on port 6667. It uses random nicknames and e-mail addresses, which have the suffix @foo.bar and performs the following tasks:

- Drop a copy of itself as the file WINSHELLB.EXE in the Windows system folder
- Create the mutex COKE_DESTROYS_YOUR_BRAIN_5 to ensure that only one instance of itself exists in memory
- Display a message box, which allows it to proceed to its malicious routines
- Query the local DNS server using port 53, and other external DNS servers for a mail exchange that matches the domain of the recipient's e-mail address

This UPX-compressed malware runs on Windows 95, 98, ME, NT, 2000, and XP.

WORM_MYDOOM.H (Aliases: W32.Mydoom.H@mm, W32/Mydoom.h@MM, Win32.Mydoom.H) (Internet Worm): This memory-resident worm uses its own SMTP (Simple Mail Transfer Protocol) engine to send copies of itself via e-mail. It drops a copy of itself using a random file name, and modifies the Windows registry. It also terminates certain running processes. It runs on Windows 95, 98, ME, NT, 2000, and XP.

WORM_NACHI.D (Aliases: W32.Welchia.D.Worm, W32/Nachi.worm.d) (Internet Worm): This memory-resident worm exploits certain vulnerabilities to propagate across networks. It takes advantage of the following vulnerabilities:

- Remote Procedure Call (RPC) Distributed Component Object Model (DCOM) Vulnerability
- IIS5/WEBDAV Buffer Overrun Vulnerability

- MS Workstation Service Vulnerability
- Locator Service Vulnerability

It patches the system against the RPC DCOM Buffer Overflow vulnerability by checking the operating system version and locale information, and connecting to specific sites. It attempts to delete several files, which it assumes to be related to the malware WORM_MYDOOM.A and WORM_MYDOOM.B. This UPX-compressed malware runs on Windows 2000 and XP.

WORM_NACHI.E (Aliases: Worm.Win32.Welchia.e, Win32:Nachi-E, Worm/Welchia.E) (Internet Worm): This memory-resident worm exploits certain vulnerabilities to propagate across networks. It takes advantage of the following vulnerabilities:

- Remote Procedure Call (RPC) Distributed Component Object Model (DCOM) Vulnerability
- IIS5/WEBDAV Buffer Overrun Vulnerability
- MS Workstation Service Vulnerability
- Locator Service Vulnerability

It patches the system against the RPC DCOM Buffer Overflow vulnerability by checking the operating system version and locale information, and connecting to specific sites. It attempts to delete several files, which it assumes to be related to the malware WORM_MYDOOM.A and WORM_MYDOOM.B. This worm has backdoor capabilities, modifies the Windows registry and overwrites certain files if the system language is Japanese. It runs on Windows 2000 and XP.

WORM_NACHI.F (Alias: Nachi.F) (Internet Worm): This memory-resident worm drops a copy of itself as SVCHOST.EXE in the %System32%\drivers folder. It attempts to delete certain files and registry entries associated with the following MYDOOM variants:

- WORM_MYDOOM.A
- WORM_MYDOOM.B

To propagate, this worm takes advantage of the following vulnerabilities:

- Remote Procedure Call (RPC) Distributed Component Object Model (DCOM) Vulnerability
- IIS5/WEBDAV Buffer Overrun Vulnerability
- MS Workstation Service Vulnerability
- Locator Service Vulnerability

It patches the system against the RPC DCOM Buffer Overflow vulnerability by checking the operating system version and locale information, and connecting to specific sites. WORM_NACHI.F overwrites files located in certain folders with an HTML code. This UPX-compressed malware runs on Windows 2000 and XP.

X97M.Kbase (Alias: X97M/Generic) (Excel 97 Macro Virus): This is a macro virus that replicates under Microsoft Excel 98 and later. When X97M.Kbase is executed, it creates a viral ThisWorkbook module. Then, it spreads using the file, 0Killbase.xls, which is dropped in the Xlstart folder. When an infected worksheet is opened, the macro creates 0Killbase.exe. When subsequent worksheets are saved either by Save or Save As, the macro inserts the viral module. There is no malicious payload other than replication.

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.*

The Virus and Trojan sections are derived from compiling information from the following anti-virus vendors and security related web sites: Sophos, Trend Micro, Symantec, McAfee, Network Associates, Central Command, F-Secure, Kaspersky Labs, MessageLabs and The WildList Organization International.

Trojan	Version	CyberNotes Issue #
Backdoor.Aphexdoor	N/A	CyberNotes-2004-03
Backdoor.Domwis	N/A	CyberNotes-2004-04
Backdoor.Gaster	N/A	CyberNotes-2004-01
Backdoor.Graybird.H	H	CyberNotes-2004-01
Backdoor.IRC.Aladinz.F	F	CyberNotes-2004-01
Backdoor.IRC.Aladinz.G	G	CyberNotes-2004-02
Backdoor.IRC.Aladinz.H	H	CyberNotes-2004-02
Backdoor.IRC.Aladinz.J	J	CyberNotes-2004-04
Backdoor.IRC.Aladinz.L	**L**	**Current Issue**
Backdoor.IRC.Aladinz.M	**M**	**Current Issue**
Backdoor.IRC.Loonbot	**N/A**	**Current Issue**
Backdoor.Kaitex.E	**E**	**Current Issue**
Backdoor.OptixPro.13.C	13.C	CyberNotes-2004-04
Backdoor.OptixPro.13b	13b	CyberNotes-2004-02
Backdoor.Portless	N/A	CyberNotes-2004-01
Backdoor.Sdbot.S	S	CyberNotes-2004-01
Backdoor.Threadsys	N/A	CyberNotes-2004-02
Backdoor.Trodal	N/A	CyberNotes-2004-01
Backdoor.Tuxder	N/A	CyberNotes-2004-02
BackDoor-AWQ.b	B	CyberNotes-2004-01
BackDoor-CBH	N/A	CyberNotes-2004-01
BDS/Purisca	N/A	CyberNotes-2004-01
BKDR_UPROOTKIT.A	A	CyberNotes-2004-01
Dial/ExDial-A	A	CyberNotes-2004-01
DOS_MASSMSG.A	A	CyberNotes-2004-01
Download.Berbew.dam	N/A	CyberNotes-2004-01
Downloader.Botten	**N/A**	**Current Issue**
Downloader.Mimail.B	B	CyberNotes-2004-02
Downloader-GD	GD	CyberNotes-2004-01
Downloader-GH	GH	CyberNotes-2004-02
Downloader-GN	GN	CyberNotes-2004-02
Dyfuca	N/A	CyberNotes-2004-01
Exploit-URLSpoof	N/A	CyberNotes-2004-01
Hacktool.Sagic	N/A	CyberNotes-2004-01
IRC-Bun	N/A	CyberNotes-2004-01
Java.StartPage	**N/A**	**Current Issue**
JS/AdClicker-AB	AB	CyberNotes-2004-01
Keylogger.Stawin	N/A	CyberNotes-2004-03
MultiDropper-GP.dr	GP.dr	CyberNotes-2004-04
Needy.C	C	CyberNotes-2004-03
Ouch	N/A	CyberNotes-2004-02
Perl/Exploit-Sqlinject	N/A	CyberNotes-2004-01
Phish-Potpor	N/A	CyberNotes-2004-04
Proxy-Agent	N/A	CyberNotes-2004-03
Proxy-Cidra	N/A	CyberNotes-2004-01
PWS-Datei	N/A	CyberNotes-2004-01
PWSteal.Bancos.D	D	CyberNotes-2004-01
PWSteal.Bancos.E	**E**	**Current Issue**
PWSteal.Banpaes.C	**C**	**Current Issue**
PWSteal.Freemega	N/A	CyberNotes-2004-02
PWSteal.Irftp	**N/A**	**Current Issue**
PWSteal.Leox	N/A	CyberNotes-2004-02
PWSteal.Olbaid	N/A	CyberNotes-2004-03
PWSteal.Sagic	N/A	CyberNotes-2004-01
PWSteal.Tarno.B	**B**	**Current Issue**
QReg-9	9	CyberNotes-2004-04

Trojan	Version	CyberNotes Issue #
Startpage-AI	AI	CyberNotes-2004-01
StartPage-AU	AU	CyberNotes-2004-02
StartPage-AX	AX	CyberNotes-2004-02
TR/DL906e	N/A	CyberNotes-2004-01
TR/Psyme.B	B	CyberNotes-2004-01
Troj/AdClick-Y	Y	CyberNotes-2004-03
Troj/Agent-C	C	CyberNotes-2004-01
Troj/Antikl-Dam	N/A	CyberNotes-2004-01
Troj/Apher-L	L	CyberNotes-2004-02
Troj/Bdoor-CCK	**CCK**	**Current Issue**
Troj/BeastDo-M	M	CyberNotes-2004-01
Troj/BeastDo-N	N	CyberNotes-2004-01
Troj/ByteVeri-E	E	CyberNotes-2004-03
Troj/Chapter-A	A	CyberNotes-2004-03
Troj/Cidra-A	A	CyberNotes-2004-01
Troj/Cidra-D	**D**	**Current Issue**
Troj/Control-E	E	CyberNotes-2004-03
Troj/CoreFloo-D	D	CyberNotes-2004-01
Troj/Daemoni-B	B	CyberNotes-2004-03
Troj/Daemoni-C	C	CyberNotes-2004-03
Troj/Darium-A	A	CyberNotes-2004-01
Troj/DDosSmal-B	B	CyberNotes-2004-04
Troj/Delf-JV	JV	CyberNotes-2004-02
Troj/Delf-NJ	NJ	CyberNotes-2004-01
Troj/DelShare-G	G	CyberNotes-2004-01
Troj/Digits-B	B	CyberNotes-2004-03
Troj/Divix-A	A	CyberNotes-2004-02
Troj/Dloader-K	K	CyberNotes-2004-01
Troj/Domwis-A	**A**	**Current Issue**
Troj/Eyeveg-C	**C**	**Current Issue**
Troj/Femad-B	B	CyberNotes-2004-03
Troj/Femad-D	D	CyberNotes-2004-01
Troj/Flator-A	A	CyberNotes-2004-01
Troj/Flood-CR	CR	CyberNotes-2004-02
Troj/Flood-DZ	DZ	CyberNotes-2004-03
Troj/Getdial-A	A	CyberNotes-2004-01
Troj/HacDef-100	**100**	**Current Issue**
Troj/Hackarmy-A	A	CyberNotes-2004-02
Troj/Hidemirc-A	A	CyberNotes-2004-03
Troj/Hosts-A	A	CyberNotes-2004-01
Troj/Hosts-B	B	CyberNotes-2004-02
Troj/IEStart-G	G	CyberNotes-2004-02
Troj/Inor-B	B	CyberNotes-2004-02
Troj/Ipons-A	A	CyberNotes-2004-01
Troj/Ircbot-S	S	CyberNotes-2004-02
Troj/IRCBot-U	U	CyberNotes-2004-03
Troj/Ircfloo-A	A	CyberNotes-2004-03
Troj/Ketch-A	A	CyberNotes-2004-01
Troj/Kuzey-A	A	CyberNotes-2004-02
Troj/Lalus-A	A	CyberNotes-2004-01
Troj/Ldpinch-C	C	CyberNotes-2004-02
Troj/LDPinch-G	**G**	**Current Issue**
Troj/LDPinch-H	**H**	**Current Issue**
Troj/Legmir-E	E	CyberNotes-2004-01
Troj/Lindoor-A	A	CyberNotes-2004-02
Troj/Linploit-A	A	CyberNotes-2004-02
Troj/Mahru-A	A	CyberNotes-2004-03
Troj/Mircsend-A	A	CyberNotes-2004-02

Trojan	Version	CyberNotes Issue #
Troj/Mmdload-A	A	CyberNotes-2004-02
Troj/MsnCrash-B	B	CyberNotes-2004-01
Troj/Mssvc-A	A	CyberNotes-2004-01
Troj/Myss-C	C	CyberNotes-2004-04
Troj/Narhem-A	**A**	**Current Issue**
Troj/NoCheat-B	B	CyberNotes-2004-03
Troj/Noshare-K	K	CyberNotes-2004-02
Troj/Pinbol-A	A	CyberNotes-2004-04
Troj/Proxin-A	A	CyberNotes-2004-02
Troj/Ranck-K	**K**	**Current Issue**
Troj/Saye-A	A	CyberNotes-2004-02
Troj/Sdbot-AP	AP	CyberNotes-2004-03
Troj/SdBot-BB	BB	CyberNotes-2004-02
Troj/Sdbot-CY	CY	CyberNotes-2004-01
Troj/Sdbot-EF	EF	CyberNotes-2004-01
Troj/SdBot-EG	EG	CyberNotes-2004-01
Troj/SdBot-EI	EI	CyberNotes-2004-01
Troj/Sdbot-EJ	EJ	CyberNotes-2004-02
Troj/Sdbot-EK	EK	CyberNotes-2004-02
Troj/Sdbot-EL	EL	CyberNotes-2004-02
Troj/Sdbot-FM	FM	CyberNotes-2004-04
Troj/Search-A	A	CyberNotes-2004-02
Troj/Sect-A	A	CyberNotes-2004-02
Troj/Seeker-F	F	CyberNotes-2004-01
Troj/Small-AW	AW	CyberNotes-2004-03
Troj/Spooner-C	C	CyberNotes-2004-02
Troj/SpyBot-AA	AA	CyberNotes-2004-01
Troj/Spybot-AM	AM	CyberNotes-2004-01
Troj/Spybot-C	C	CyberNotes-2004-01
Troj/StartPag-C	C	CyberNotes-2004-01
Troj/StartPag-E	E	CyberNotes-2004-02
Troj/StartPg-AU	AU	CyberNotes-2004-01
Troj/StartPg-AY	AY	CyberNotes-2004-01
Troj/StartPg-BG	BG	CyberNotes-2004-01
Troj/StartPg-U	U	CyberNotes-2004-01
Troj/Stawin-A	A	CyberNotes-2004-03
Troj/TCXMedi-E	E	CyberNotes-2004-01
Troj/Tofger-F	F	CyberNotes-2004-01
Troj/Tofger-L	L	CyberNotes-2004-01
Troj/Troll-A	A	CyberNotes-2004-02
Troj/Uproot-A	A	CyberNotes-2004-01
Troj/Volver-A	A	CyberNotes-2004-03
Troj/Weasyw-A	A	CyberNotes-2004-02
Troj/Webber-D	D	CyberNotes-2004-01
Troj/Winpup-C	C	CyberNotes-2004-03
Trojan.Anymail	N/A	CyberNotes-2004-01
Trojan.Bansap	N/A	CyberNotes-2004-04
Trojan.Bookmarker	N/A	CyberNotes-2004-01
Trojan.Bookmarker.B	B	CyberNotes-2004-02
Trojan.Bookmarker.C	C	CyberNotes-2004-02
Trojan.Bookmarker.D	C	CyberNotes-2004-03
Trojan.Bookmarker.E	E	CyberNotes-2004-03
Trojan.Bookmarker.F	**F**	**Current Issue**
Trojan.Download.Revir	N/A	CyberNotes-2004-01
Trojan.Etsur	**N/A**	**Current Issue**
Trojan.Gema	N/A	CyberNotes-2004-01
Trojan.Gipma	**N/A**	**Current Issue**
Trojan.Gutta	N/A	CyberNotes-2004-04

Trojan	Version	CyberNotes Issue #
Trojan.Httpdos	N/A	CyberNotes-2004-02
Trojan.Mitglieder.C	C	CyberNotes-2004-02
Trojan.Mitglieder.D	**D**	**Current Issue**
Trojan.Mitglieder.E	**E**	**Current Issue**
Trojan.Noupdate	**N/A**	**Current Issue**
Trojan.PWS.Qphook	N/A	CyberNotes-2004-01
Trojan.PWS.QQPass.F	F	CyberNotes-2004-04
Trojan.Simcss.B	**B**	**Current Issue**
Trojan.Tilser	**N/A**	**Current Issue**
Unix/Exploit-SSHIDEN	N/A	CyberNotes-2004-02
UrlSpoof.E	E	CyberNotes-2004-03
VBS.Bootconf.B	B	CyberNotes-2004-04
VBS.Shania	N/A	CyberNotes-2004-03
VBS/Inor-C	C	CyberNotes-2004-03
VBS/Suzer-B	B	CyberNotes-2004-01
VBS/Wisis-A	A	CyberNotes-2004-02
W32.Bizten	N/A	CyberNotes-2004-01
W32.Hostidel.Trojan.B	B	CyberNotes-2004-03
W32.Kifer	N/A	CyberNotes-2004-04
W32.Kifer.B	B	CyberNotes-2004-04
Xombe	N/A	CyberNotes-2004-01

Backdoor.IRC.Aladinz.L: This is a backdoor Trojan horse that uses malicious scripts in the mIRC client software, allowing unauthorized remote access.

Backdoor.IRC.Aladinz.M: This is a backdoor Trojan horse that uses malicious scripts in the mIRC client software, allowing unauthorized remote access.

Backdoor.IRC.Loonbot: This is a Trojan horse that has backdoor capabilities. It can allow a malicious user to remotely control your computer using Internet Relay Chat (IRC). This Trojan can also download and execute files. This threat is written in C and is packed with AsPack v2.12.

Backdoor.Kaitex.E: Backdoor.Kaitex.E connects to a remote computer and allows a malicious user to control your computer. It is a minor variant of Backdoor.Kaitex.D. When Backdoor.Kaitex.E is executed, it adds the value, "Service"="<the Trojan file path and name>," to the registry key:

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

so that the Trojan runs each time you start Windows. It connects to a computer at devestator.dirdy30.com on port 1863 and waits for commands from the malicious user.

Downloader.Botten: This is a Trojan horse that takes advantage of a vulnerability in Microsoft Internet Explorer to download and execute arbitrary code on the system. When Downloader.Botten is executed, it creates the Mutex "BotNetd" so that only one copy of the Trojan runs on the system at any one time and attempts to download a file from one of the following servers:

- http:/ /66.98.190.39/
- http:/ /sonyasys.com/

and save the file as one of the following:

- %Windir%\Notepad.exe
- %System%\Notepad.exe
- %Temp%\<random file name>.tmp

It also adds the value, "qbotd"="<filename of Trojan>," to the registry key:

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

so that the Trojan runs when you start Windows.

Java.StartPage (Aliases: Trojan.Java.StartPage, Exploit-ByteVerify): Java.StartPage is a Java-based Trojan horse program that modifies the default home page of Microsoft Internet Explorer. When Java.StartPage is executed, it modifies one or more of the following values:

- "Start Page"
- "Search Page"
- "Search Bar"

in the registry key:

- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Main

PWSteal.Bancos.E: This is a Trojan horse that mimics the online interfaces of certain Brazilian banks to try to steal account information. It is a minor variant of PWSteal.Bancos.D.

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

PWSteal.Irftp: This is a Trojan horse that mimics the online interfaces of Brazilian banks to try to steal account information. This Trojan is typically found inside a self-extracting archive with a deceptive file name (for example, "cartao.exe"). When it is executed, the archive installs the Trojan, which is usually named Ir_Ftp.exe.

PWSteal.Tarno.B: This is a Trojan Horse that attempts to intercept user names and passwords, and other computer information. It sends the user names and passwords to a certain e-mail address using its own SMTP engine.

Troj/Bdoor-CCK (Alias: BackDoor-CCK): This is a backdoor Trojan. This program may drop the file WMER.HTM into the Windows Help folder and also drop the file Trojan.INI into the Windows folder. Troj/Bdoor-CCK will also set the following registry entries so that it runs on system restart:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\ blss = <full file path>
- HKLM\Software\blss\installdate = <number>

Troj/Cidra-D: This Trojan has been reported in the wild. It is a backdoor proxy Trojan that allows a remote intruder to relay TCP traffic through the compromised computer. The Trojan normally runs as the file usb_d.exe. In order to be executed automatically when the user logs on to the computer Troj/Cidra-D adds a registry entry at the following location:

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

The Trojan opens a random listening port and periodically attempts to connect to a remote website to register itself. It also has the ability to download and execute a file from a remote website. Troj/Cidra-D appears to have been spammed out. The e-mail has the following characteristics:

- Subject: "This your photo?," possibly interspersed with non-Roman characters.
- Message text is "Is this your photo? I can't belive it made it onto the internet!"
- Attachment: p_usb.zip.

Troj/Domwis-A (Aliases: BackDoor-AOZ, BKDR_DOMWIS.A): This is an IRC backdoor Trojan that allows a malicious user remote access to an infected computer. When first run, the Trojan copies itself to the Windows folder as RUNDLL16.EXE and creates the following registry entry to ensure it is run on system logon:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Windows DLL Loader = <WINDOWS>\RUNDLL16.EXE

Troj/Domwis-A will steal system information and log keystrokes. It can download and execute remote files on the infected computer. The Trojan can also be instructed to retrieve file listings and delete files and terminate processes. Troj/Domwis-A will create the file temp.bat in the Windows folder. This file is not malicious on its own, however it should be deleted.

Troj/Eyeveg-C (Alias: TrojanDropper.JS.Mimail.b): This is a password stealing Trojan for the Windows platform. In order to run automatically when Windows starts, up Troj/Eyeveg-C copies itself to a file with a random name in the Windows system folder and adds a registry entry pointing to this file. The Trojan also attempts to copy itself to the Windows startup folder. Troj/Eyeveg-C collects system information and account passwords and sends them to a remote web site.

Troj/HacDef-100 (Aliases: Backdoor.HacDef.084, Win32/HacDef.084, Backdoor.HackDefender): This is backdoor Trojan that is targeted at NT/2000/XP operating systems. As well as allowing unauthorized remote access to the victim's computer, this Trojan is also able to hide information about the victim's system including files, folders, processes, services, and registry entries.

Troj/LDPinch-G (Aliases: Trojan.PSW.LdPinch.ca, PWS-LDPinch): This Trojan sends passwords and confidential information to a remote location and provides backdoor access to the computer. When first run, the Trojan moves itself to the Windows folder and adds its pathname to the following registry entry, to run itself on startup:

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

The Trojan periodically attempts to send confidential information to a remote location. The Trojan then runs continuously in the background providing backdoor access to the computer on port 2050. A remote intruder will be able to connect to this port and receive a remote command shell. The Trojan also drops the file isfpr.dll into the Windows folder.

Troj/LDPinch-H (Aliases: Trojan.PSW.LdPinch.o, PWS-LDPinch trojan, PWSteal.Trojan): This Trojan sends passwords and confidential information to a remote location and provides backdoor access to the computer. When first run, the Trojan moves itself to the Windows folder and adds its pathname to the following registry entry, to run itself on startup:

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

The Trojan periodically attempts to send confidential information to a remote location. The Trojan then runs continuously in the background providing backdoor access to the computer. The Trojan may also drop the file isfpr.dll to the Windows folder.

Troj/Narhem-A (Alias: Backdoor.VB.gen): Troj/Narhem-A: This is a keylogging Trojan. It copies itself to the following locations:

- <Windows>\Reader.exe
- <Windows>\Help\Mehran.exe
- <Windows>\System\Mehran.exe
- <Windows>\System32\Acrobat.exe

Troj/Narhem-A creates the following registry entries in order to run on system startup:

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

Troj/Narhem-A logs keystrokes into C:\Syslog.dat and periodically e-mails this file to a predefined e-mail address.

Troj/Ranck-K (Aliases: TrojanProxy.Win32.Ranky.a, Proxy-FBSR.gen): This is an HTTP proxy Trojan that allows a remote intruder to route HTTP traffic through the computer. Troj/Ranck-K sets the following registry entry so as to run itself on system startup:

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

Troj/Ranck-K runs continuously in the background listening on a port.

Trojan.Bookmarker.F: This is a variant of Trojan.Bookmarker.E that modifies the Internet Explorer home page and adds bookmarks to the Favorites folder.

Trojan.Etsur: This Trojan monitors and records certain user activity and sends information to its creator. In particular, it may record online banking user names and passwords.

Trojan.Gipma: This is a Trojan horse program that displays obscene messages and makes the desktop and task bar invisible. Trojan.Gipma is written in Microsoft Visual Basic.

Trojan.Mitglieder.D: This is a variant of Trojan.Mitglieder. The Trojan opens a proxy on the system, attempts to stop security software, and is able to update itself.

Trojan.Mitglieder.E: This is a variant of Trojan.Mitglieder. The Trojan opens a proxy on the system, attempts to stop security software, and is able to update itself.

Trojan.Noupdate: This is a Trojan horse that attempts to prevent users from updating their computer with the latest Microsoft Windows patches.

Trojan.Simcss.B: Trojan.Simcss.B is a variant of Trojan.Simcss that terminates processes and downloads and executes files from the Internet. The Trojan is packed using UPX.

Trojan.Tilser: This Trojan gives a malicious user complete access to your computer. By default, the Trojan listens on port 6187.