



National Infrastructure Protection Center CyberNotes

Issue #2003-02

January 27, 2003

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

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

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

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between January 2 and January 22, 2003. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified.

Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text. Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Alpha Shield Inc. ¹	Multiple	Alpha Shield	A vulnerability exists due to insufficient connection tracking, which could let a remote malicious user spoof packets.	No workaround or patch available at time of publishing.	AlphaShield Connection Tracking	Medium	Bug discussed in newsgroups and websites.

¹ SecurityFocus, January 17, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Apache Software Foundation ²	Multiple	Apache 2.0.36-2.0.43	Several vulnerabilities exist: a vulnerability exists due to the way some HTTP requests that involve MS-DOS device names are handled, which could let a remote malicious user cause a Denial or Service or execute arbitrary code; a vulnerability exists due to the way some HTTP requests are handled if the request ends in illegal characters, which could let a remote malicious user obtain sensitive information; and a vulnerability exists when requests are made for files in directories with extensions, which could let a malicious user bypass existing default mappings when serving files.	Upgrade available at: http://www.apache.org/dist/httpd/	Apache Web Server Multiple Vulnerabilities CVE Names: CAN-2003-0016, CAN-2003-0017	Low/ Medium/ High (Low if a DoS, Medium is sensitive information is obtained, and High if arbitrary code is executed)	Bug discussed in newsgroups and websites. Exploits have been published.
Apache Software Foundation ³	Unix	Tomcat 4.0-4.0.5, 4.1, 4.1.3 beta, 4.1.9 beta, 4.1.10	An information disclosure vulnerability exists because the unprocessed source of a JSP page can be retrieved, which could let a remote malicious user obtain sensitive information.	Apache Software Foundation: http://jakarta.apache.org/builds/jakarta-tomcat-4.0/release/ Debian: http://security.debian.org/pool/updates/contrib/t/tomcat4/	Apache Tomcat Invoker Servlet File Disclosure CVE Name: CAN-2002-1394	Medium	Bug discussed in newsgroups and websites.
BEA Systems, Inc. ⁴	Windows NT 4.0/2000, Unix	WebLogic Server 6.1, 6.1 SP1-SP3, 7.0, 7.0 SP1, 7.0.0.1	A vulnerability exists because under some circumstances the system password will be disclosed, which could let a malicious user obtain sensitive information.	Upgrade available at: ftp://ftpna.beasys.com/pub/releases/security/CR093060_70sp1.jar	WebLogic System Password Disclosure	Medium	Bug discussed in newsgroups and websites.
BeanBug ⁵	Multiple	vSignup 2.1	An input validation vulnerability exists in the registration script, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	vSignup Remote SQL Injection	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
BeanBug ⁶	Multiple	vAuthenticate 2.8	An input validation vulnerability exists in various PHP scripts, which could let a remote malicious obtain administrative access.	No workaround or patch available at time of publishing.	vAuthenticate Input Validation	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

² SecurityFocus, January 22, 2003.

³ Debian Security Advisory, DSA 225-1, January 9, 2003.

⁴ BEA Security Advisory, BEA03-24.00, January 11, 2003.

⁵ Bugtraq, January 14, 2003.

⁶ Bugtraq, January 14, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
BitMover, Inc. ⁷	Unix	BitKeeper 3.0	Two vulnerabilities exist: a vulnerability exists in the source code management system due to improper filtering of user-supplied input, which could let a remote malicious user execute arbitrary code; and a vulnerability exists because unsafe temporary files are used when calling external programs, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	BitKeeper Daemon Mode Remote Command Execution & Insecure Temporary File	High	Bug discussed in newsgroups and websites. Exploit has been published.
Blackboard ⁸	Multiple	Blackboard 5.0, 5.0.2, 5.5, 5.5.1	A vulnerability exists due to improper filtering in the address book search feature, which could let a malicious user obtain sensitive information.	Upgrade to 5.5.1 and then apply the hotfix available at: http://behind.blackboard.com	Blackboard Learning System Address Book Search Feature	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
BRS ⁹	Windows	Web Weaver 1.01	Two vulnerabilities exist: a Directory Traversal vulnerability exists which could let a remote malicious user obtain sensitive information; and a vulnerability exists in the FTP server component, which could let a remote malicious user create arbitrary directories and obtain sensitive information.	No workaround or patch available at time of publishing.	BRS WebWeaver Information Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Business Objects ¹⁰	Windows NT 4.0/2000, Unix	Web Intelligence 2.7	A vulnerability exists due to an insecure session management implementation for authentication, which could let a remote malicious user obtain unauthorized access.	Contact the vendor for details on obtaining and applying fixes.	Web Intelligence Insecure Session Management	Medium	Bug discussed in newsgroups and websites.
Caldera ¹¹	Unix	OpenUnix 8.0, UnixWare 7.1.1	A buffer overflow vulnerability exists in the 'ps' command due to insufficient bounds checking, which could let a malicious user execute arbitrary code.	Upgrade available at: ftp://ftp.sco.com/pub/updates/OpenUNIX/CSSA-2003-SCO.1/erg712109.pkg.Z	UnixWare/ OpenUnix PS Buffer Overflow	High	Bug discussed in newsgroups and websites.

⁷ SecurityTracker Alert ID, 1005913, January 11, 2003.

⁸ Securiteam, January 22, 2003.

⁹ Bugtraq, January 10, 2003.

¹⁰ Ubizen Security Intelligence Lab Security Advisory, SIL/03/001, January 9, 2003.

¹¹ SCO Security Advisory, CSSA-2003-SCO.1, January 10, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Canna ¹² <i>More patches released^{13, 14}</i>	Unix	Canna 3.5 b2	A buffer overflow vulnerability exists due to a lack of validation of requests, which could let a malicious user execute arbitrary code. <i>Note: Canna is typically installed only when Japanese language support is enabled.</i>	<u>RedHat:</u> ftp://updates.redhat.com/ <u>Debian:</u> http://security.debian.org/pool/updates/main/c/canna/canna <u>SCO:</u> ftp://ftp.sco.com/pub/updates/OpenLinux/3.1.1/	Canna Server Local Buffer Overflow CVE Names: CAN-2002-1158, CAN-2002-1159	High	Bug discussed in newsgroups and websites.
CSO Lanifex ¹⁵	Unix	Outreach Project Tool 0.946b	Multiple vulnerabilities exist: a vulnerability exists because values supplied by users in HTTP headers are accepted as the originating IP address, which could let a remote malicious user spoof e-mail messages; several Cross-Site Scripting vulnerabilities exist in most of the community functions due to insufficient filtering of user-supplied input, which could let a remote malicious user execute arbitrary code; and a vulnerability exists when the lockfile "lock01" in the setup_lock-directory is not removed, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	CSO Lanifex Outreach Project Tool Multiple Remote Vulnerabilities	Medium/High (High if arbitrary code is executed)	Bug discussed in newsgroups and websites. Exploits have been published.

¹² Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:246-18, December 4, 2002.

¹³ Debian Security Advisory, DSA 224-1, January 8, 2003.

¹⁴ SCO Security Advisory, CSSA-2003-005.0, January 21, 2003.

¹⁵ Bugtraq, January 16, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
CVS ^{16, 17, 18, 19, 20, 21}	Unix	CVS 1.10.7, 1.10.8, 1.11 1.11.1 p1, 1.11.1- 1.11.4	A double free vulnerability exists in Directory requests, which could let an unauthorized remote malicious user execute arbitrary code.	IBM: ftp://ftp.software.ibm.com/ai/x/freeSoftware/aixtoolbox/RPMS/ppc/cvs/cvs-1.11.1p1-3.aix4.3.ppc.rpm Debian: http://security.debian.org/pool/updates/main/c/cvs/ Mandrake: http://www.mandrakesecure.net/en/ftp.php Conectiva: ftp://atualizacoes.conectiva.com.br/ CVS: http://ccvs.cvshome.org/servlets/ProjectDownloadList RedHat: ftp://updates.redhat.com/ OpenBSD: OpenBSD ftp://ftp.openbsd.org/pub/OpenBSD/patches/ Slackware: ftp://ftp.slackware.com/pub/slackware/	CVS Directory Request Double Free Code Execution CVE Name: CAN-2003-0015	High	Bug discussed in newsgroups and websites.
D-Link ²²	Multiple	DWL-900AP+ 2.2, 2.3, 2.5	A vulnerability exists when the firmware is upgraded with Access Point Manager because configuration settings are reset to factory defaults, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	D-Link DWL-900AP+ Firmware Upgrade Configuration Reset	Medium	Bug discussed in newsgroups and websites.
Efficient Networks ²³	Multiple	5861 DSL Router	A remote Denial of Service vulnerability exists when the router is configured to block incoming TCP SYN flags and is subsequently portscanned.	Contact vendor for workaround.	DSL Router Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Vulnerability may be exploited with one of many available tools.

¹⁶ Conectiva Linux Security Announcement, 2003-01-23, January 23, 2003.

¹⁷ Gentoo Linux Security Announcement, 0301-12, January 23, 2003.

¹⁸ CERT Advisory, CA-2003-02, January 23, 2003.

¹⁹ Debian Security Advisory, DSA 233-1, January 21, 2003.

²⁰ Mandrake Linux Security Update Advisory, MDKSA-2003:009, January 20, 2003.

²¹ Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:012-07, January 20, 2003.

²² Bugtraq, January 15, 2003.

²³ Securiteam, January 12, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Ethereal Group ²⁴	Windows 95/98/ME/NT 4.0/2000, XP, Unix	Ethereal 0.8, 0.8.18, 0.9.0-0.9.7	Several vulnerabilities exist: Multiple integer signed errors exists in the BGP dissector, which could let a remote malicious user cause a Denial of Service; and memory corruption vulnerabilities exists in the PPP, LMP, and TDS dissectors, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code.	Ethereal Group: http://www.ethereal.com/download.html RedHat: ftp://updates.redhat.com/	Ethereal Multiple Vulnerabilities CVE Names: CAN-2002-1355, CAN-2002-1356	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites.
Evolvable Corporation ²⁵	Windows 98/98/NT 4.0/2000	Shambala Server 4.5	A Denial of Service vulnerability exists when a malicious FTP user attempts to 'CWD' to the root directory.	No workaround or patch available at time of publishing.	Shambala Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Follett Software Company ²⁶	Windows	Web Collection Plus 5.0	An information disclosure vulnerability exists due to improper filtering of user-supplied input, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	WebCollection Information Disclosure	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
GameSpy ²⁷	Multiple	GameSpy 3D 2.62	A Denial of Service vulnerability exists when a malicious user submits a query that may result in a game server responding with overly large responses.	No workaround or patch available at time of publishing.	GameSpy 3D Denial of Service	Low	Bug discussed in newsgroups and websites.
Geeklog ²⁸	Unix	Geeklog 1.3.7	Multiple Cross-Site Scripting vulnerabilities exist in the 'profiles.php,' 'users.php,' and 'comment.php,' scripts, and the 'Homepage' field due to insufficient sanitization of URI parameters input, which could let a remote malicious user execute arbitrary HTML or script code.	Upgrade available at: http://www.geeklog.net/filemgmt/visit.php?lid=101	Geeklog Multiple Cross-Site Scripting	High	Bug discussed in newsgroups and websites.
global SCAPE, Inc. ²⁹	Windows	CuteFTP 5.0	A buffer overflow vulnerability exists due to insufficient bounds checking on FTP command responses, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	CuteFTP Buffer Overflow	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

²⁴ Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:290-07, January 9, 2003.

²⁵ SecurityTracker Alert ID, 1005943, January 18, 2003.

²⁶ Bugtraq, January 14, 2003.

²⁷ Securiteam, January 23, 2003.

²⁸ Bugtraq, January 14, 2003.

²⁹ Bugtraq, January 18, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
GNU ^{30, 31, 32} <i>SCO releases patch³³</i>	Unix	wget 1.5.3, 1.6, 1.7, 1.7.1, 1.8, 1.8.1, 1.8.2	A vulnerability exists due to inadequate input checks when a NLST response is received from an FTP server, which could let a remote malicious user overwrite files on the client system.	Debian: http://security.debian.org/pool/updates/main/w/wget RedHat: ftp://updates.redhat.com/ Mandrake: http://www.mandrakesecure.net/en/ftp.php SCO: ftp://ftp.sco.com/pub/updates/OpenLinux/	WGet NLST Client Side File Overwriting CVE Name: CAN-2002-1344	Medium	Bug discussed in newsgroups and websites.
Hewlett Packard Company ³⁴	Unix	HP-UX 10.0 1, 10.10, 10.20, 11.04, 11.0, 11.11	A vulnerability exists in the sort utility, which could let a malicious user cause a Denial of Service or obtain unauthorized access.	Upgrades available at: http://itrc.hp.com Patch PHCO_28142, Patch PHCO_27940, Patch PHCO_27564, Patch PHCO_27565, Patch PHCO_25918	HP-UX sort Unspecified File Handling	Low/Medium (Medium if unauthorized access is obtained)	Bug discussed in newsgroups and websites.
Hewlett Packard Company ³⁵	Unix	HP-UX 11.22	A vulnerability exists because the Xserver was built incorrectly, which could let a malicious user obtain elevated privileges.	Patch available at: http://itrc.hp.com Patch PHSS_25291	HP-UX 11.22 Xserver Privilege Escalation	Medium	Bug discussed in newsgroups and websites.
Horde ³⁶	Unix	IMP 2.2-2.2.8	Multiple SQL injection vulnerabilities exist due to insufficient sanitization of user-supplied input in SQL queries, which could let a remote malicious user corrupt the database.	Upgrade available at: http://www.horde.org/imp/3.1/ Debian: http://security.debian.org/pool/updates/main/i/imp/	Horde IMP Database Files SQL Injection CVE Name: CAN-2003-0025	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
libpng ^{37, 38, 39, 40, 41}	Unix	libpng 1.0, 1.0.5-1.0.14, 1.2.0-1.2.5	A buffer overflow vulnerability exists because the libpng graphics library may incorrectly calculate some offsets when creating or modifying PNG files, which could let a malicious user cause a Denial of Service or possibly execute arbitrary code.	SuSE: ftp://ftp.suse.com/pub/suse/ Debian: http://security.debian.org/pool/updates/main/libp/libpng/ Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: ftp://updates.redhat.com/	LibPNG Incorrect Offset Calculation Buffer Overflow CVE Name: CAN-2002-1363	Low/High (High if arbitrary code is executed)	Bug discussed in newsgroups and websites.

³⁰ Debian Security Advisory, DSA-209-1, December 13, 2002.

³¹ Mandrake Security Advisory, MDKSA-2002:086, December 11, 2002.

³² Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:229-10, December 10, 2002.

³³ SCO Security Advisory, CSSA-2003-003.0, January 16, 2003.

³⁴ Hewlett-Packard Company Security Bulletin, HPSBUX0301-237, January 17, 2003.

³⁵ Hewlett-Packard Company Security Bulletin, HPSBUX0301-238, January 17, 2003.

³⁶ Debian Security Advisory, DSA 229-2, January 15, 2003.

³⁷ Gentoo Linux Security Announcement, 200301-7, January 8, 2003.

³⁸ OpenPKG Security Advisory, OpenPKG-SA-2003.001, January 15, 2003.

³⁹ SuSE Security Announcement, SuSE-SA:2003:0004, January 14, 2003.

⁴⁰ Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:006-06, January 13, 2003.

⁴¹ Mandrake Linux Security Update Advisory, MDKSA-2003:008, January 20, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Imatix ⁴²	Multiple	Xitami 2.4 d3, 2.4 c3	A Denial of Service vulnerability exists when a malicious user submits overly long input to the administrative port.	Upgrade available at: http://www.imatix.com/html/xitami/index2.htm#download	Xitami Webserver Administrative Port Buffer Overflow	Low	Bug discussed in newsgroups and websites.
ISC ⁴³	Unix	DHCPD 3.0.1 rc1-rc10	A remote Denial of Service vulnerability exists in 'dchrelay' when a malicious bootp packet is submitted.	No workaround or patch available at time of publishing.	DHCPD dchrelay Extraneous Network Packets Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
ISC ^{44, 45, 46, 47, 48, 49, 50, 51}	Unix	DHCPD 3.0, 3.0 rc4, rc12, pl1, b2pl9, b2pl23, 3.0.1 rc1-rc10	Multiple buffer overflow vulnerabilities exist in the library that is used by NSUPDATE to resolve hostnames when the Dynamic Host Configuration Protocol (DHCP) server is configured to dynamically update records, which could let a remote malicious user execute arbitrary code.	ISC: ftp://ftp.isc.org/isc/dhcp/dhcp-3.0pl2.tar.gz SuSE: ftp://ftp.suse.com/pub/suse/ RedHat: ftp://updates.redhat.com/ Mandrake: http://www.mandrakesecure.net/en/ftp.php Debian: http://security.debian.org/pool/updates/main/d/dhcp3/ Conectiva: ftp://atualizacoes.conectiva.com.br/	ISC DHCPD NSUPDATE Remote Buffer Overflow CVE Name: CAN-2003-0026	High	Bug discussed in newsgroups and websites. Exploit script has been published.

⁴² SecurityFocus, January 13, 2003.

⁴³ Bugtraq, January 15, 2003.

⁴⁴ CERT® Advisory, CA-2003-01, January 20, 2003.

⁴⁵ OpenPKG Security Advisory, OpenPKG-SA-2003.002, January 16, 2003.

⁴⁶ Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:011-07, January 16, 2003.

⁴⁷ Debian Security Advisory, DSA 231-1, January 17, 2003.

⁴⁸ Gentoo Linux Security Announcement, 200301-10, January 17, 2003.

⁴⁹ Mandrake Linux Security Update Advisory, MDKSA-2003:007, January 17, 2003.

⁵⁰ SuSE Security Announcement, SuSE-SA:2003:0006, January 20, 2003.

⁵¹ Conectiva Linux Security Announcement, CLA-2003:562, January 23, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
iTop10 ⁵²	Multiple	PHP TopSites Free 2.0 b, Pro 2.2	Multiple vulnerabilities exist: a vulnerability exists in the 'help.php' script due to insufficient sanitization of user-supplied data, which could let a remote malicious user execute arbitrary code; a vulnerability exists because user's passwords are stored in plaintext, which could let a remote malicious user obtain unauthorized access; a vulnerability exists in the 'edit.php' script due to insufficient sanitization of user-supplied data, which could let a remote malicious user execute arbitrary code; and a vulnerability exists in the 'add.php' script due to insufficient sanitization of user-supplied data, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	PHP TopSites Multiple Vulnerabilities	Medium/ High (High if arbitrary code is executed)	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.
Jason Smith ⁵³	Multiple	Cyboards PHP Lite 1.21, 1.25	Several vulnerabilities exist; multiple Cross-Site Scripting vulnerabilities exist due to insufficient validation of user-supplied input, which could let a remote malicious user execute arbitrary code; and a vulnerability exists because it is possible to specify a location to include a PHP script, which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	Cyboards PHP Lite Multiple Vulnerabilities	High	Bug discussed in newsgroups and websites.
Jean-Jacques Sarton ^{54, 55}	Unix	mtink 0.9.32, 0.9.33, 0.9.52	A buffer overflow vulnerability exists in the mtink binary HOME environment variable due to insufficient bounds checking, which could let a malicious user execute arbitrary code with elevated privileges.	Mandrake: http://www.mandrakesecure.net/en/ftp.php	MTink Printer Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit has been published.

⁵² Bugtraq, January 15, 2003.

⁵³ SecurityTracker Alert ID, 1005932, January 16, 2003.

⁵⁴ iDEFENSE Security Advisory, 01.21.03, January 21, 2003.

⁵⁵ Mandrake Linux Security Update Advisory, MDKSA-2003:010, January 21, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Leafnode ⁵⁶ <i>Mandrake issues advisory</i> ⁵⁷	Unix	Leafnode 1.9.20-1.9.27, 1.9.29	A Denial of Service vulnerability exists when certain news postings are retrieved.	Upgrade available at: http://prdownloads.sourceforge.net/leafnode/leafnode-1.9.31.rel.tar.bz2?download <i>Mandrake:</i> http://www.mandrakesecure.net/en/ftp.php	Leafnode Denial of Service	Low	Bug discussed in newsgroups and websites.
Macromedia ⁵⁸	Windows NT 4.0/2000, XP, Unix	ColdFusion Server MX Enterprise	A vulnerability exists in the 'cfinclude' and 'fmodule' tags because the Sandbox Security Files/Dirs permissions are not properly checked before including files, which could let a remote malicious user obtain sensitive information.	For patch information, see advisory located at: http://www.macromedia.com/v1/handlers/index.cfm?ID=23638	ColdFusion MX CFInclude & CFModule Tags Input Validation	Medium	Bug discussed in newsgroups and websites.
Mambo ⁵⁹	Unix	Mambo Site Server 4.0.11, 4.0.12 BETA	A Cross-Site Scripting vulnerability exists due to improper filtering of HTML code, which could let a remote malicious user execute arbitrary HTML code.	No workaround or patch available at time of publishing.	Mambo Site Server Multiple Cross Site Scripting	High	Bug discussed in newsgroups and websites. Exploit has been published.
Mambo ⁶⁰	Unix	Mambo Site Server 4.0.10, 4.0.11, 4.0.12 BETA	A vulnerability exists due to inadequate security checks, which could let a remote malicious user upload arbitrary files to the system.	Patch available at: http://www.mamboserver.com/Security_Patch_307.tar.gz Upgrade available at: http://freshmeat.net/redirect/mambo/15020/url_tgz/MamboV4012-BETA-2.tar.gz	Mambo Site Server Arbitrary File Upload	Medium	Bug discussed in newsgroups and websites.
Manuel Lemos ⁶¹	Unix	HTML Forms Generation And Validation	A vulnerability exists in the 'forms.php' component due to insufficient checking of user-supplied input, which could let a malicious user execute arbitrary HTML code.	Upgrade available at: http://www.phpclasses.org/goto/browse.html/file/1.html	HTML Forms Generation And Validation Forms.PHP HTML Injection	High	Bug discussed in newsgroups and websites.
Marc Druilhe ⁶²	Unix	W-Agora 4.1.5	A file disclosure vulnerability exists in the 'index.php' and 'modules.php' scripts due to insufficient sanitization of user-supplied input, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	W-Agora Remote File Disclosure	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

⁵⁶ Leafnode Security Advisory, SA-2002:01, December 29, 2002.

⁵⁷ Mandrake Linux Security Update Advisory, MDKSA-2003:005, January 15, 2003.

⁵⁸ Macromedia Security Advisory, MPSB03-01, January 9, 2003.

⁵⁹ Bugtraq, January 11, 2003.

⁶⁰ Bugtraq, January 11, 2003.

⁶¹ SecurityFocus, January 15, 2003.

⁶² Shell Security Team Advisory, January 12, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Matt Wright ⁶³	Multiple	FormMail 1.92	A Cross-Site Scripting vulnerability exists due to insufficient sanitization of HTML tags and script code, which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	FormMail Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Mcrypt ^{64, 65} <i>More vendors release advisories</i> <i>66, 67</i>	Unix	libmccrypt 2.5.1 -r4, 2.5.2, 2.5.3	Multiple buffer overflow vulnerabilities exist in various functions that are used to process user-supplied input due to insufficient bounds checking, which could let a malicious user execute arbitrary code.	Upgrade available at: http://mcrypt.hellug.gr/lib/index.html <i>Debian:</i> http://security.debian.org/pool/updates/main/libm/libmccrypt/ <i>SuSE:</i> ftp://ftp.suse.com/pub/suse	Libmccrypt Multiple Buffer Overflow Vulnerabilities CVE Name: CAN-2002-1363	High	Bug discussed in newsgroups and websites.
Microsoft ⁶⁸ <i>Microsoft updates bulletin</i> ⁶⁹	Windows 2000, XP	Windows 2000 Advanced Server, SP1-SP3, 2000 Datacenter Server, SP1-SP3, 2000 Professional, SP1-SP3, 2000 Server, SP1-SP3, 2000 Terminal Services, SP1-SP3, XP 64-bit Edition, XP Home, XP Professional	A vulnerability exists in the negotiation process because it is possible to cause the signing of Server Message Block (SMB) packets to be disabled, even when it is required by the host, which could let a malicious user obtain sensitive information. <i>Subsequent to the release of this bulletin, it was determined that the patch was not included in XP Service Pack 1. The bulletin and patch have been updated so that it installs on Windows XP Service Pack 1 systems.</i>	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-070.asp	Windows SMB Signing CVE Name: CAN-2002-1256	Medium	Bug discussed in newsgroups and websites.

⁶³ SecurityTracker Alert ID, 1005916, January 13, 2003.

⁶⁴ Bugtraq, January 3, 2003.

⁶⁵ Gentoo Linux Security Announcement, 200301-4, January 5, 2003.

⁶⁶ Debian Security Advisory, DSA 228-1, January 14, 2003.

⁶⁷ SuSE Security Announcement, SuSE-SA:2003:0004, January 14, 2003.

⁶⁸ Microsoft Security Bulletin, MS02-070, December 11, 2002.

⁶⁹ Microsoft Security Bulletin, MS02-070 V2.0, January 22, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft ⁷⁰	Windows 98/ME/NT 4.0/2000, XP	Microsoft Outlook 2002, SP1&2	A vulnerability exists due to the way V1 Exchange Server Security certificates are handled when used to encrypt e-mail, which could let a malicious user obtain sensitive information.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-003.asp	Outlook 2002 Exchange Server Security Certificate CVE Name: CAN-2003-0007	Medium	Bug discussed in newsgroups and websites.
Microsoft ⁷¹	Windows NT 4.0/2000, XP	Content Management Server 2001, SP1	A Cross-Site Scripting vulnerability exists when constructing a response page due to insufficient validation of user-supplied input, which could let a malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-002.asp	Content Management Server Cross-Site Scripting CVE Name: CAN-2003-0002	High	Bug discussed in newsgroups and websites.
Microsoft ⁷² <i>Microsoft updates bulletin⁷³</i>	Windows NT 4.0/2000	Data Engine 1.0, 2000, SQL Server 7.0, SQL Server 7.0 SP1-SP4, SQL Server 2000, SQL Server 2000 SP1&2	A vulnerability exists because there is a flaw in the stored procedure that runs web tasks due to the way permissions are handled, which could let a malicious user obtain elevated privileges. In addition, there are weak permissions on the web tasks table that together with the stored procedure could allow a malicious user to run, delete or update a web task. <i>Note: This patch supersedes the one provided in Microsoft Security Bulletin MS02-056, which was also a cumulative patch.</i> <i>Bulletin has been updated to clarify superseded patches information.</i>	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-061.asp <i>Note: This is a cumulative patch that includes the functionality of all previously released patches for SQL Server 7.0, SQL Server 2000, and Microsoft Data Engine (MSDE) 1.0, Microsoft Desktop Engine (MSDE) 2000. In addition, it eliminates one newly discovered vulnerability.</i>	Microsoft SQL Server Web Task Stored Procedure Privilege Escalation CVE Name: CAN-2002-1145	Medium	Bug discussed in newsgroups and websites.

⁷⁰ Microsoft Security Bulletin, MS03-003, January 22, 2003.

⁷¹ Microsoft Security Bulletin, MS03-002, January 22, 2003.

⁷² Microsoft Security Bulletin, MS02-061, October 16, 2002.

⁷³ Microsoft Security Bulletin, MS02-061 V1.1, January 21, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft ⁷⁴	Windows NT 4.0/2000, XP	Windows 2000 Advanced Server, SP1-SP3, 2000 Datacenter Server, SP1-SP3, 2000 Professional, SP1-SP3, 2000 Server, SP1-SP3, Japanese Edition, Terminal Services, SP1-SP3, NT Enterprise Server 4.0, SP1-SP6a, NT Server 4.0, SP1-SP6a, NT Terminal Server 4.0, SP1-SP6a, NT Workstation 4.0, SP1-SP6a, XP 64-bit Edition, SP1, XP Home, SP1, XP Professional, SP1	A buffer overflow vulnerability in the Locator service due to inadequate parameter checks, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/ms03-001.asp	Windows Locator Service Buffer Overflow CVE Name: CAN-2003-0003	Low/High (High if arbitrary code is executed)	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.

⁷⁴ Microsoft Security Bulletin, MS03-001, January 22, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft ⁷⁵ <i>Microsoft updates bulletin to correct link errors</i> ⁷⁶	Windows 95/98/ME/NT 4.0/2000, XP	2000 Advanced Server, SP1-SP3, 2000 Datacenter Server, SP1-SP3, 2000 Professional, SP1-SP3, 2000 Server, SP1-SP3, 2000 Terminal Services, SP1-SP3, Windows 95, 95 SR2, 98, 98SE, ME, NT Enterprise Server 4.0 SP1-SP6a, NT Server 4.0 SP1-SP6a, NT Terminal Server 4.0 SP1-SP6a, NT Workstation 4.0 SP1-SP6a, XP Home SP1, XP Professional SP1	Multiple vulnerabilities exist: a vulnerability exists because it's possible for an untrusted Java applet to access COM objects, which could let a malicious user obtain control over the machine; two vulnerabilities exist because it is possible to spoof the location specified in CODEBASE parameter in the APPLET tag, which could let a malicious user obtain sensitive information; a vulnerability exists due to a flaw in the Virtual Machine's URL parser, which could let a malicious user intercept any traffic that the user would send to the trusted site; a vulnerability exists because Java Database Connectivity APIs don't properly regulate who can call them, which could let a malicious user obtain sensitive information; a Denial of Service vulnerability exists due to insufficient security checks in the VM; a vulnerability exists because VM doesn't prevent untrusted applets from accessing the user.dir system property, which could let a malicious user sensitive information; and a vulnerability exists because it is possible for a Java applet to create an incorrectly initialized Java object, which could let a malicious user cause Internet Explorer to fail.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-069.asp	Java Virtual Machine Multiple Vulnerabilities CVE Names: CAN-2002-1254, CAN-2002-1257, CAN-2002-1258, CAN-2002-1259, CAN-2002-1260, CAN-2002-1261, CAN-2002-1263	Low/Medium/High (Medium if sensitive information can be obtained and High if control can be obtained over the system)	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Middleman ⁷⁷	Unix	Middleman 0.9.9, 1.0, 1.1, 1.2	A vulnerability exists due to an incorrect strncpy() function call in the 'networks.c' file that occurs when looking up the user-provided hostname via the DNS, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	Middleman net_dns() Off-by-One	High	Bug discussed in newsgroups and websites.

⁷⁵ Microsoft Security Bulletin, MS02-069, December 11, 2002.

⁷⁶ Microsoft Security Bulletin, MS02-069 V1.2, January 17, 2003.

⁷⁷ Qitest1 Security Advisory, 006, January 10, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Mozilla ⁷⁸ <i>Debian issues advisory</i> ⁷⁹	Unix	Bugzilla 2.14-2.14.4, 2.16, 2.16.1, 2.17, 2.17.1	Two vulnerabilities exist: a vulnerability exists in the .htaccess files that are provided with the checksetup.pl script because backups are not adequately protected, which could let a remote malicious user obtain unauthorized access to these backup files; and a vulnerability exists because insecure permissions are set on the data/mining directory, which could let a malicious user alter the contents of the data/mining director.	Upgrades available at: http://www.bugzilla.org/download.html <i>Debian:</i> http://security.debian.org/pool/updates/main/b/bugzilla/	Bugzilla LocalConfig Backup File & Data Mining CVE Names: CAN-2003-0012, CAN-2003-0013	Medium	Bug discussed in newsgroups and websites.
mpg123 ⁸⁰	Unix	mpg123 pre0.59s, 0.59 r	A vulnerability exists when playing MP3 files that contain a bitrate of zero, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	mpg123 Zero Bitrate	High	Bug discussed in newsgroups and websites. Exploit has been published.
mpg123.de ⁸¹	Unix	mpg123 pre0.59s	A memory corruption vulnerability exists when certain MP3 files are played, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	mpg123 Memory Corruption	High	Bug discussed in newsgroups and websites. Exploit has been published. Vulnerability has appeared in the press and other public media.
Multiple Vendors ⁸²	Unix	NcFTP Software NcFTPD 2.7.1; ProFTPD Project ProFTPD 1.2.7	A vulnerability exists which could let a remote malicious user remove FTP archive files.	No workaround or patch available at time of publishing.	Multiple FTP Server Virtual User File Removal	Medium	Bug discussed in newsgroups and websites.

⁷⁸ Bugzilla Security Advisory, January 2, 2003.

⁷⁹ Debian Security Advisory, DSA 230-1, January 16, 2003.

⁸⁰ Bugtraq, January 16, 2003.

⁸¹ SecurityTracker Alert ID, 1005918, January 15, 2003.

⁸² Bugtraq, January 17, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors <small>83, 84, 85</small> <i>More updates issued</i> ^{86, 87, 88, 89}	MacOS X 10.2, Unix	Apple MacOS X 10.2 (Jaguar), Easy Software Products CUPS 1.0.4, 1.0.4-8, 1.1.1, 1.1.4-5, 1.1.4-3, 1.1.4-2, 1.1.4, 1.1.6, 1.1.7, 1.1.10, 1.1.12-1.1.15, 1.1.17	Several vulnerabilities exist: vulnerability exists in the HTTP server component of the Common UNIX Printing System (CUPS), which could let a local/remote malicious user obtain root privileges; a race condition exists in the creation of /etc/cups/certs/<pid>, which could let a malicious user create or overwrite any file as root; a vulnerability exists because printers can remotely be added to CUPS by sending a specially crafted UDP packet; a remote Denial of Service vulnerability exists due to negative length memcpy() calls; an integer overflow vulnerability exists in the image handling code, which could let a malicious user obtain elevated privileges; a buffer overflow vulnerability exists in the strncat function call in the setup of the 'options' string, which could let a malicious user obtain root access; a vulnerability exists because CUPS improperly checks for zero width images in filters/image-gif.c, which could let a malicious user execute arbitrary code; and a vulnerability exists because the return values of many file and socket operations are not checked, which could let a malicious user cause a Denial of Service.	<u>Apple:</u> http://www.info.apple.com/kbnum/ <u>Easy Software:</u> http://www.cups.org/software.html <u>SuSE:</u> ftp://ftp.suse.com/pub/suse <u>SCO:</u> ftp://ftp.sco.com/pub/updates/OpenLinux/ <u>Debian:</u> http://security.debian.org/pool/updates/main/c/cupsy/ <u>Mandrake:</u> http://www.mandrakesecurity.net/en/ftp.php <u>RedHat:</u> ftp://updates.redhat.com	CUPS HTTP Multiple Vulnerabilities CVE Names: CAN-2002-1366, CAN-2002-1367, CAN-2002-1368, CAN-2002-1369, CAN-2002-1371, CAN-2002-1372, CAN-2002-1383, CAN-2002-1384	Low/High (High if root access can be obtained or arbitrary code can be executed)	Bug discussed in newsgroups and websites. Exploits have been published.

⁸³ iDEFENSE Security Advisory, December 19, 2002.

⁸⁴ Gentoo Linux Security Announcement, 200212-13, December 29, 2002.

⁸⁵ SuSE Security Announcement, SuSE-SA:2003:002, January 2, 2003.

⁸⁶ SCO Security Advisory, CSSA-2003-004.0, January 21, 2003.

⁸⁷ Debian Security Advisory, DSA 232-1, January 20, 2003.

⁸⁸ Mandrake Linux Security Update Advisory, MDKSA-2003:001, January 10, 2003.

⁸⁹ Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:295-07, January 13, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors ^{90,91} <i>SGI re-releases bulletin⁹²</i>	Mac OS X 10.X, Unix	Apple MacOS X 10.0-10.0.4, 10.1-10.1.5, 10.2 (Jaguar), 10.2.1, MacOS X Server 10.0, 10.2-10.2.1; GNU glibc 2.0-2.0.6, 2.1, 2.1.1-6, 2.1.1-2.1.3, 2.1.3-10, 2.2-2.2.5, 2.3, 2.3.1; SGI IRIX 6.5-6.5.13, 6.5.14 m-6.5.17 m, 6.5.14 f-6.5.14 m <i>SGI IRIX 6.5-6.5.13, 6.5.14 m-6.5.17 m, 6.5.14 f-6.5.14 m</i>	A remote Denial of Service vulnerability exists in multiple libc implementations that are based on Sun RPC due to a failure to provide a time-out mechanism when reading data from TCP connections. <i>The patches referenced in the original bulletin are incompatible with each other, so SGI has created a new series of patches that address these vulnerabilities and are compatible with each other..</i>	<u>SGI:</u> ftp://patches.sgi.com/support/free/security/patches/	Multiple Vendor Sun RPC LibC Remote Denial of Service CVE Name: CAN-2002-1265	Low	Bug discussed in newsgroups and websites.
MyRoom ⁹³	Multiple	MyRoom 3.5 GOLD	A vulnerability exists due to insufficient security checking, which could let a remote malicious user upload arbitrary files to the system.	No workaround or patch available at time of publishing.	MyRoom Arbitrary File Upload	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

⁹⁰ CERT/CC Vulnerability Note VU#266817, November 4, 2002.

⁹¹ SGI Security Advisory, 20021103-01-P, November 8, 2002.

⁹² SGI Security Advisory, 20021103-02-P, January 22, 2003.

⁹³ SecurityFocus, January 20, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
MySQL AB ^{94,95}	Unix	MySQL 3.22.26-3.22.30, 3.22.32, 3.23.3-3.23.5, 3.23.8-3.23.10, 3.23.22-3.23.31, 3.23.33, 3.23.34, 3.23.36-3.23.53, 4.0.0-4.0.3, 4.0.5a	A vulnerability exists in the password authentication mechanism, which could let an malicious user compromise database accounts.	Debian: http://security.debian.org/pool/updates/main/m/mysql/ MySQL AB: http://www.mysql.com/downloads/mysql-3.23.html RedHat: ftp://updates.redhat.com/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Mandrake: http://www.mandrakesecure.net/en/ftp.php SuSE: ftp://ftp.suse.com/pub/suse/ EnGarde: ftp://ftp.engardelinux.org/pub/engarde/stable/updates/ Trustix: ftp://ftp.trustix.net/pub/Trustix/updates/	MySQL Password Account Compromise CVE Name: CAN-2002-1374	Medium	Bug discussed in newsgroups and websites.
Open LDAP ⁹⁶ <i>Vendors release patches^{97,98}</i>	Unix	OpenLDAP 2.0-2.0.23, 2.0.25	Several buffer overflow vulnerabilities exist which could let a malicious user execute arbitrary code.	SuSE: ftp://ftp.suse.com/pub/suse/ Mandrake: http://www.mandrakesecure.net/en/ftp.php Conectiva: ftp://atualizacoes.conectiva.com.br/ Debian: http://security.debian.org/pool/updates/main/o/openldap2/	OpenLDAP Multiple Buffer Overflow CVE Name: CAN-2002-1379	High	Bug discussed in newsgroups and websites.
Palm ⁹⁹	Windows	HotSync Manager 4.0.4	A remote Denial of Service vulnerability exists when configured in network synchronization mode and certain network data is submitted on port 14238.	No workaround or patch available at time of publishing.	HotSync Manager Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
PeopleSoft ¹⁰⁰	Multiple	PeopleTools 8.14-8.18	A vulnerability exists in the Gateway Administration servlet due to insufficient sanitization of user-supplied XML data, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	PeopleSoft Gateway Administration Servlet CVE Name: CAN-2002-1252	Medium	Bug discussed in newsgroups and websites.

⁹⁴ Red Hat, Inc. Red Hat Security Advisory, RHTSA-2002:288-22, January 15, 2003.

⁹⁵ SuSE Security Announcement, SuSE-SA:2003:003, January 2, 2003.

⁹⁶ SuSE Security Announcement, SuSE-SA:2002:047, December 6, 2002.

⁹⁷ Debian Security Advisory, DSA 227-1, January 13, 2003.

⁹⁸ Mandrake Linux Security Update Advisory, MDKSA-2003:006, January 15, 2003.

⁹⁹ Bugtraq, January 23, 2003.

¹⁰⁰ Internet Security Systems Security Advisory, January 20, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
phpBB Group ¹⁰¹	Multiple	phpBB 2.0.3	A vulnerability exists due to insufficient sanitization of user-supplied input, which could let a remote malicious user delete private messages.	Upgrade available at: http://www.phpbb.com/downloads.php	phpBB2 Input Validation	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
phpLinks ¹⁰²	Unix	phpLinks 2.1.2	Several vulnerabilities exist: a vulnerability exists in the 'add.php' script due to insufficient sanitization of HTML and script code, which could let a malicious user execute arbitrary HTML and script code; and a vulnerability exists in the search feature due to insufficient sanitization of HTML and script code, which could let a malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	PHPLinks HTML Injection	High	Bug discussed in newsgroups and websites.
PHPMY Pub ¹⁰³	Multiple	PHPMYPub 1.2.0	A vulnerability exists due to insufficient security checking, which could let a remote malicious user obtain administrative access.	No workaround or patch available at time of publishing.	PHPMYPub Unauthorized Administrative Access	High	Bug discussed in newsgroups and websites. Exploit has been published.
PHPOut-sourcing ¹⁰⁴	Multiple	Zorum 3.0-3.2	A vulnerability exists due to the way PHP includes are handled, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	Zorum PHP Includes	High	Bug discussed in newsgroups and websites. Exploit has been published.
phpPass ¹⁰⁵	Unix	phpPass 2	A vulnerability exists in the 'accesscontrol.php' script due to insufficient sanitization of user-supplied input, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	phpPass AccessControl. PHP SQL Injection	High	Bug discussed in newsgroups and websites. Exploit has been published.
PostgreSQL ^{106, 107}	Unix	PostgreSQL 6.3.2, 6.5.3, 7.0.3, 7.1-7.1.3, 7.2.1	Several buffer overflow vulnerabilities exist: a buffer overflow vulnerability exists with the TZ environment variable, which could let a malicious user cause a Denial of Service or execute arbitrary code; and a buffer overflow vulnerability exists with the SET TIME ZONE environment variable, which could let a malicious user cause a Denial of Service or execute arbitrary code.	RedHat: ftp://updates.redhat.com/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Debian: http://security.debian.org/pool/updates/main/p/postgresql SuSE: ftp://ftp.suse.com/pub/suse	PostgreSQL TZ Environment & SET TIME ZONE Environment Variables Buffer Overflows CVE Name: CAN-2002-1402	Low/High (High if arbitrary code is executed)	Bug discussed in newsgroups and websites.

¹⁰¹ Bugtraq, January 17, 2003.

¹⁰² SecurityFocus, January 16, 2003.

¹⁰³ SecurityFocus, January 20, 2003.

¹⁰⁴ Bugtraq, January 22, 2003.

¹⁰⁵ Bugtraq, January 13, 2003.

¹⁰⁶ Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:001-16, January 14, 2003.

¹⁰⁷ Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:010-10, January 14, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Postgre SQL ^{108, 109}	Unix	Postgre SQL 6.3.2, 6.5.3, 7.0.3, 7.1-7.1.3, 7.2, 7.2.1	A buffer overflow vulnerability exists in the date parser due to insufficient bounds checking, which could let a malicious user cause a Denial of Service or execute arbitrary code.	RedHat: ftp://updates.redhat.com/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Debian: http://security.debian.org/pool/updates/main/p/postgresql SuSE: ftp://ftp.suse.com/pub/suse	PostgreSQL Date Parser Buffer Overflow CVE Name: CAN-2002-1398	Low/High (High if arbitrary code is executed)	Bug discussed in newsgroups and websites.
Postgre SQL ^{110, 111}	Unix	Postgre SQL 6.3.2, 6.5.3, 7.0.3, 7.1-7.1.3, 7.2-7.2.3	Several buffer overflow vulnerabilities exist: a buffer overflow vulnerability exists in the 'path_encode()' function, which could let a remote malicious user execute arbitrary commands; and a buffer overflow vulnerability exists with the 'circle_poly' function, which could let a malicious user cause a Denial of Service or execute arbitrary code.	RedHat: ftp://updates.redhat.com/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Debian: http://security.debian.org/pool/updates/main/p/postgresql	PostgreSQL path_encode() & circle_poly Buffer Overflows CVE Name: CAN-2002-1401	Low/High (High if arbitrary code is executed)	Bug discussed in newsgroups and websites.
Postgre SQL ^{112, 113}	Unix	Postgre SQL 6.3.2, 6.5.3, 7.0.3, 7.1-7.1.3, 7.2-7.2.3	A buffer overflow vulnerability exists in the 'path_add()' function due to insufficient bounds checking, which could let a malicious user cause a Denial of Service or execute arbitrary code.	RedHat: ftp://updates.redhat.com/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Debian: http://security.debian.org/pool/updates/main/p/postgresql	PostgreSQL path_add() Buffer Overflow	Low/High (High if arbitrary code is executed)	Bug discussed in newsgroups and websites.
Psunami Bulletin Board ¹¹⁴	Multiple	Psunami Bulletin Board 0.2, 0.2.1, 0.3, 0.3.1, 0.4, 0.5, 0.5.1, 0.5.2	A vulnerability exists in query string parameters due to insufficient sanitization of shell metacharacters, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Psunami Bulletin Board Psunami.CGI Remote Command Execution	High	Bug discussed in newsgroups and websites. Exploit has been published.
Rediff ¹¹⁵	Multiple	Bol 2.0.2	A remote Denial of Service vulnerability exists due to improper handling of some requests.	No workaround or patch available at time of publishing.	Bol Remote Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.

¹⁰⁸ Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:001-16, January 14, 2003.

¹⁰⁹ Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:010-10, January 14, 2003.

¹¹⁰ Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:001-16, January 14, 2003.

¹¹¹ Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:010-10, January 14, 2003.

¹¹² Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:001-16, January 14, 2003.

¹¹³ Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:010-10, January 14, 2003.

¹¹⁴ SecurityFocus, January 14, 2003.

¹¹⁵ SecurityFocus, January 23, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Robert Krawitz ^{116, 117}	Unix	escputil 1.15.2.2	A buffer overflow vulnerability exists in the escputil binary in the parsing of the printer-name command line argument, which could let a malicious user execute arbitrary code with elevated privileges.	Mandrake: http://www.mandrakesecure.net/en/ftp.php	ESCPUtil Printer Name Command Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit has been published.
Sambar Technologies ¹¹⁸	Windows 95/98/ME/NT 4.0/2000	Sambar Server 5.1, 5.2, 5.2 b, 5.3	A Cross-Site Scripting vulnerability exists due to insufficient sanitization of HTML code, which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	Sambar Server Cross-Site Scripting	High	Bug discussed in newsgroups and websites.
Samsung ^{119, 120}	Unix	ml85p Printer Driver 1.0	A race condition vulnerability exists in the ml85p binary when a temporary file is opened, which could let an unauthorized malicious user obtain root privileges.	Mandrake: http://www.mandrakesecure.net/en/ftp.php	ML-85G Race Condition	High	Bug discussed in newsgroups and websites. Exploit has been published.

¹¹⁶ iDEFENSE Security Advisory, 01.21.03, January 21, 2003.

¹¹⁷ Mandrake Linux Security Update Advisory, MDKSA-2003:010, January 21, 2003.

¹¹⁸ SecurityFocus, January 20, 2003.

¹¹⁹ iDEFENSE Security Advisory, 01.21.03, January 21, 2003.

¹²⁰ Mandrake Linux Security Update Advisory, MDKSA-2003:010, January 21, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
SGI ¹²¹ <i>SGI re-releases bulletin¹²²</i>	Unix	IRIX 6.5-6.5.17, 6.5.13 m-6.5.17 m	<p>Multiple vulnerabilities exist: a vulnerability exists in the 'rpcbind' utility because symbolic links are incorrectly followed, which could let a malicious corrupt critical system files and possibly cause a Denial of Service or obtain elevated privileges; a vulnerability exists because temporary desktop files are created with world-writable permissions, which could let a malicious user overwrite and corrupt temporary desktop files; a buffer overflow vulnerability exists in the 'uux' binary, which could let a malicious user execute arbitrary code; a vulnerability exists in the 'fsr_efs' binary because symbolic links are incorrectly followed, which could let a malicious user corrupt critical system files and possibly cause a Denial of Service or obtain elevated privileges; and a vulnerability exists in the 'mv' command because renamed directories are created insecurely, which could let a malicious user overwrite and corrupt critical files on the system.</p> <p><i>The patches referenced in the original bulletin are incompatible with each other, so SGI has created a new series of patches that address these vulnerabilities and are compatible with each other.</i></p>	<p>Upgrades available at: http://www.sgi.com/software/software.html#IRIX Patches available at: ftp://patches.sgi.com/support/free/security/patches</p>	IRIX Multiple Vulnerabilities	<p>Low/Medium/High</p> <p>Low if a Denial of Service; Medium if files are overwritten or elevated privileges obtained; and High if arbitrary code can be executed)</p>	Bug discussed in newsgroups and websites. There is no exploit code required.
Stunnel ¹²³	Unix	Stunnel 3.18, 3.19, 3.21, 3.22, 4.0-4.0 3	A vulnerability exists in the SIGCHLD signal handling routine, which could let a malicious user execute arbitrary code.	Upgrade available at: http://www.stunnel.org/download/stunnel	Stunnel SIGCHLD Signal Handler	High	Bug discussed in newsgroups and websites. Exploit has been published.

¹²¹ SGI Security Advisory, 20020903-01-P, October 14, 2002.

¹²² SGI Security Advisory, 20021103-02-P, January 22, 2003.

¹²³ Bugtraq, January 12, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Sun Microsystems, Inc. ¹²⁴	Unix	Solaris 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86, 9.0	A buffer overflow vulnerability exists in the 'utmp_update' binary due to insufficient bounds checking, which could let a malicious user obtain unauthorized root privileges.	Patches available at: http://sunsolve.sun.com	Sun Solaris UTMP_Update Buffer Overflow	High	Bug discussed in newsgroups and websites.
Sun Microsystems, Inc. ¹²⁵	Unix	Solaris 2.5.1, 2.5.1_x86, 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86, 9.0, 9.0_x86 Update 2	A Directory Traversal vulnerability exists in the Kodak Color Management System (KCMS) KCS_OPEN_PROFILE procedure due to insecure handling of input, which could let a remote malicious user obtain sensitive information.	Workaround: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F50104	Kodak KCMS KCS_OPEN_PROFILE Directory Traversal	Medium	Bug discussed in newsgroups and websites.
Sun Microsystems, Inc. ¹²⁶	Unix	Sun ONE Integration Server EAI Edition 3.0, Unified Development Server 5.0	A vulnerability exists due to the way recursive document type definitions (DTDs) are handled, which could let a malicious user cause a Denial of Service.	Upgrade available at: http://www.sun.com	Sun ONE Unified Development Server Recursive Document Type Definition Denial of Service	Low	Bug discussed in newsgroups and websites.
Sun Microsystems, Inc. ¹²⁷	Unix	Solaris 8.0	A buffer overflow vulnerability exists in the UUCP utility when excessive data is submitted as a user-supplied command line parameter, which could let a malicious user execute obtain elevated privileges and possibly execute arbitrary code with superuser privileges.	No workaround or patch available at time of publishing.	Solaris UUCP Buffer Overflow	Medium/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Symantec ¹²⁸	Windows 2000, XP	Norton Internet Security 2003, 2003 Professional Edition, Personal Firewall 2003	A Denial of Service vulnerability exists when a malicious user sends an excessive number of ICMP packets to the host.	Upgrades are available via LiveUpdate.	Norton Internet Security ICMP Packet Denial of Service	Low	Bug discussed in newsgroups and websites.

¹²⁴ Sun(sm) Alert Notification, 50008, January 16, 2003.

¹²⁵ Intercept Ricochet Advisory, January 22, 2003.

¹²⁶ Sun(sm) Alert Notification, 49922, January 16, 2003.

¹²⁷ SecurityTracker Alert ID, 1005920, January 14, 2003.

¹²⁸ Bugtraq, January 11, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Thomas Krebs ¹²⁹	Windows NT 4.0/2000	Nite Server 1.83	A Directory Traversal vulnerability exists, which could let a remote malicious user obtain sensitive information.	Upgrade available at: http://come.to/niteserversite	Nite Server Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Trend Micro ¹³⁰	Windows NT 4.0/2000	Virus Control System 1.8	A Denial of Service vulnerability exists in the 'activesupport.exe' when a malicious user submits numerous requests.	The vendor has reported that TVCS has been replaced with TCM (Trend Micro Control Manager). Users are advised to migrate to TCM, as it is not affected by this issue.	Virus Control System Denial Of Service	Low	Bug discussed in newsgroups and websites.
Trend Micro ¹³¹	Windows NT 4.0/2000	Virus Control System 1.8	An information disclosure vulnerability exists because log files that are generated can be accessed, which could let a malicious user obtain sensitive information.	The vendor has reported that TVCS has been replaced with TCM (Trend Micro Control Manager). Users are advised to migrate to TCM, as it is not affected by this issue	Virus Control System Information Disclosure	Medium	Bug discussed in newsgroups and websites.
Trend Micro ¹³²	Multiple	ScanMail for Microsoft Exchange 3.8	A vulnerability exists which could let a remote malicious user bypass authentication mechanisms to obtain unauthorized access to the management system.	This issue is addressed in ScanMail for Microsoft Exchange versions 3.81/6.1 and later. Information on upgrading available at: http://kb.trendmicro.com/solutions/solutionDetail.asp?solutionId=13352	ScanMail For Exchange Authentication Bypass	Medium	Bug discussed in newsgroups and websites.
Trend Micro ¹³³	Windows 95/98/ME/ NT 3.1.4.0/2000	OfficeScan Corporate Edition 3.0, 3.5, 3.11, 3.13, 3.54, Corporate Edition for Windows NT Server 3.0, 3.1.1, 3.5, 3.11, 3.13, Virus Buster Corporate Edition 3.52-3.54	A vulnerability exists due to insufficient permissions, which could let a malicious user obtain sensitive information.	A tool (CGI_NTFS.exe) is provided with OfficeScan that provides utilities to lock down CGI directory permissions and secure OfficeScan. Further details about this tool can be found at the following location: http://kb.trendmicro.com/solutions/solutionDetail.asp?solutionId=13353	OfficeScan CGI Directory Insufficient Permissions	Medium	Bug discussed in newsgroups and websites.
United Admins ¹³⁴	Multiple	ClanMod 1.80.19 Beta, 1.81.11 Beta	A format string vulnerability exists in the 'cm_log' command, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	ClanMod 'cm_log' Format String	High	Bug discussed in newsgroups and websites. Exploit script has been published.

¹²⁹ Securiteam, January 19, 2003.

¹³⁰ SecurityFocus, January 15, 2003.

¹³¹ SecurityFocus, January 15, 2003.

¹³² SecurityFocus, January 15, 2003.

¹³³ SecurityFocus, January 15, 2003.

¹³⁴ void.at Security Advisory, VSA0301, January 10, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
United Admins ¹³⁵	Multiple	AdminMod 2.50.25 a, 2.50.50	A format string vulnerability exists in commands that call the 'selfmessage()' function, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	AdminMod Plugin Remote Format String	High	Bug discussed in newsgroups and websites. Exploit script has been published.
United Admins ¹³⁶	Multiple	StatsMe 2.6.9, 2.6.16 Beta, 2.6.17 Beta unstable, 2.6.19 Beta	Two vulnerabilities exist: a buffer overflow vulnerability exists in 'CMD_ARGV,' which could let a remote malicious user execute arbitrary code; and a format string vulnerability exists in 'statsme.cpp,' which could let a malicious user obtain unauthorized access.	No workaround or patch available at time of publishing.	StatsMe Plug-in Buffer Overflow & Format String	Medium/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Exploit script has been published.
URLogy ¹³⁷	Windows NT 4.0/2000	a.shop.Kart 2.0.3	A vulnerability exists in the 'addcustomer.asp,' 'addprod.asp,' and 'process.asp' scripts due to insufficient sanitization of user-supplied input passed to SQL queries, which could let a remote malicious user corrupt the database or obtain sensitive information.	No workaround or patch available at time of publishing.	A.ShopKart Multiple SQL Injection	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Valve Software ¹³⁸	Windows 98/NT 4.0	Half-Life 1.1.0.9, 1.1.0.8, 1.1.1.0	A format script vulnerability exists when messages are received from an administrator through the AdminMod add-on package, 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.	Half-Life Client Server Message Format String	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Exploit script has been published.
Valve Software ¹³⁹	Unix	Half-Life Dedicated Server 3.1.1.0 Linux	A remote Denial of Service vulnerability exists when a malicious user submits a specially crafted packet to the host.	No workaround or patch available at time of publishing.	Half-Life HLTV Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
VIM Development Group ¹⁴⁰	Unix	VIM 5.0-5.8, 6.0, 6.1	A vulnerability exists in the modelines function due to insufficient handling of input, which could let a remote malicious user execute arbitrary code. <i>Note: A conceptual worm has been reported that explicitly illustrates how this vulnerability could be further exploited to act as a mass mailing worm.</i>	RedHat: ftp://updates.redhat.com/	VIM ModeLines Arbitrary Command Execution CVE Name: CAN-2002-1377	High	Bug discussed in newsgroups and websites. VIM Worm has been published that exploits this vulnerability.

¹³⁵ void.at Security Advisory, VSA0301, January 10, 2003.

¹³⁶ void.at Security Advisory, VSA0303, January 11, 2003.

¹³⁷ Centaura Technologies Security Research Lab Advisory, CTADVIIIC046, January 8, 2003.

¹³⁸ void.at Security Advisory, VSA0304, January 10, 2003.

¹³⁹ void.at Security Advisory, VSA0305, January 10, 2003.

¹⁴⁰ Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:297-17, January 16, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
WinRar ¹⁴¹	Windows	WinRar 2.90, 3.0.0, 3.10	A buffer overflow vulnerability exists in the 'winrar.exe' if an archive is opened that contains a file with an overly long file extension, which could let a malicious user execute arbitrary instructions.	Upgrade available at: http://www.rarlab.com/rar/wrar311.exe	WinRar Archive File Buffer Overflow	High	Bug discussed in newsgroups and websites.
Xynph FTP Server ¹⁴²	Multiple	Xynph FTP Server 1.0	A Directory Traversal vulnerability exists, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Xynph FTP Directory Traversal	Medium	Bug discussed in newsgroups and websites.
YaBB SE ¹⁴³	Unix	YaBB SE 1.4.1	A Cross-Site Scripting vulnerability exists in the 'Reminder.php' script due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and JavaScript code.	No workaround or patch available at time of publishing.	YABB SE Reminder.PHP Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Exploit has been published.
YaBB SE ¹⁴⁴		YaBB SE 1.4.1, 1.5 .0	A vulnerability exists in the 'Packages.php' file, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	YABB SE Packages.PHP Remote File Include	High	Bug discussed in newsgroups and websites. Exploit has been published.

*"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.

¹⁴¹ Bugtraq, January 21, 2003.

¹⁴² Bugtraq, January 11, 2003.

¹⁴³ void.at Security Advisory, VSA0306, January 11, 2003.

¹⁴⁴ Bugtraq, January 21, 2003.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between January 10 and January 23, 2003, listed by date of script, script names, script description, and comments. Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing. During this period, 11 scripts, programs, and net-news messages containing holes or exploits were identified. Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
January 23, 2003	Core_format_strings.pdf	Vulnerabilities in Your Code Part II - Format string vulnerabilities and exploitation shows the exact location of the vulnerabilities, providing detailed explanations and exploits for each one found.
January 23, 2003	Ethereal-0.9.9.tar.gz	A GTK+-based network protocol analyzer, or sniffer, that lets you capture and interactively browse the contents of network frames.
January 20, 2003	Middle2.c.gz	Program that allows you to recover SMB password in clear text (from the network) when they should be encrypted. It operates a man in the middle attack with complete traffic redirection that does not need forwarding with transparent proxy.
January 20, 2003	Virus-writing-HOWTO-2003-01-08.tar.gz	The Linux Virus Writing HOWTO describes how to write parasitic file viruses which infect ELF executables on Linux/i386 and contains source code.
January 19, 2003	Arpoison-0.6.tar.gz	A network analysis tool that sends ARP packets to and from specified hardware and protocol addresses.
January 17, 2003	Phpbb-exploit.pl	Perl script that exploits the phpBB2 Input Validation vulnerability.
January 17, 2003	W00nf-stunnel.c	Exploit for the STunnel Client Negotiation Protocol Format String vulnerability.
January 16, 2003	Hoagie_dhcpd.c	Script that exploits the ISC DHCPD NSUPDATE Remote Buffer Overflow vulnerability.
January 11, 2003	Hoagie_statsme.c	Script that exploits the StatsMe Plug-in Buffer Overflow & Format String vulnerabilities.
January 10, 2003	Hoagie_adminmod_client.c	Script that exploits the Half-Life Client Server Message Format String vulnerability.
January 10, 2003	Hoagie_clanmod.c	Script that exploits the ClanMod 'cm_log' Format String vulnerability.

Trends

- NIPC has issued an advisory regarding the propagation of an SQL worm. The self-propagating malicious code exploits multiple vulnerabilities in the Resolution Service of Microsoft SQL Server 2000. This worm activity appears to have caused various levels of network degradation across the Internet. In addition to the compromise of vulnerable machines; the apparent effects of this fast-spreading, virus-like infection has overwhelmed the world's digital pipelines and interfered with Web browsing and delivery of e-mail. For more information, see Virus Section, WORM_SQLP1434.A description and NIPC Advisory 03-001.1, located at: <http://www.nipc.gov/warnings/advisories/2003/03-001.1updates.htm>. For patch information, see:**
 - <http://www.microsoft.com/security/slammer.asp>
 - <http://www.microsoft.com/technet/security/bulletin/MS02-061.asp>
 - <http://www.microsoft.com/technet/security/bulletin/MS02-039.asp>

- The CERT/CC has released an advisory regarding a buffer overflow vulnerability in the Microsoft Windows Shell. For more information, see Bugs, Holes & Patches table entry, “Windows XP WMA/MP3 Buffer Overflow” and CERT® Advisory CA-2002-37, located at: <http://www.cert.org/advisories/CA-2002-37.html>.
- The CERT/CC has released an advisory regarding multiple vendors' implementations of the secure shell (SSH) transport layer protocol contain vulnerabilities that could allow a remote malicious user to execute arbitrary code with the privileges of the SSH process or cause a denial of service. The vulnerabilities affect SSH clients and servers, and they occur before user authentication takes place. For more information, see Bugs, Holes & Patches table entry “Multiple Vendor SSH2 Implementation” and CERT® Advisory CA-2002-36, located at: <http://www.cert.org/advisories/CA-2002-36.html>.
- The CERT/CC has received reports of increased scanning for NetBIOS services. Probes to port 137/udp may be indicative of such activity.

Viruses

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

BAT.Vandeed.Worm (Aliases: Bat/Vandeed.worm, BAT.Darn) (Batch Script Worm): This worm attempts to spread itself through the KaZaA file-sharing network. When BAT.Vandeed.Worm is executed, it adds the value, “darn C:\DARN.BAT,” to the registry key:

- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that the worm runs each time you start Windows. It also adds the values:

- dir0 012345:C:\\ProgramFlies
- dir99 012345:C:\Windows\Desktop
- DisableSharing 0

to the registry key:

- HKEY_CURRENT_USER\SOFTWARE\KAZAA\LocalContent

If the infected computer has KaZaA installed, this will give access to the C:\\ProgramFlies and C:\Windows\Desktop folders to other KaZaA users. The subfolder ProgramFiles is created in the folder from which the worm is executed. It copies itself as C:\ProgramFlies\Darn.bat and C:\Windows\Desktop\GameWarez.bat and copies itself to all the drives that exist on the infected computer. This worm also pings mail.yahoo.com.

HLLP.Gartin.9680 (DOS Virus): This is a parasitic DOS virus that is written in a high-level language, such as Pascal. When HLLP.Gartin.9680 is executed, it searches for and infects a small number of files that have an MZ Header, such as the .exe and .dll files. The virus looks for these files on the root of the drives A, B, C, and D. When HLLP.Gartin.9680 infects a new host file, it copies 9,680 bytes from the beginning of the file to the end of the file, and then replaces the first 9,680 bytes with itself. If the virus is active in memory, it randomly flashes the Num Lock, Caps Lock, and Scroll Lock LED's of the keyboard. HLLP.Gartin.9680 also contains two strings that probably give the author's name and home city in Poland.

JS/Spth (JavaScript Worm): This is a JavaScript worm that is able to spread on the Internet using e-mail, ICQ, and P2P networks. Many different variants exist as a kit generates the worm that is available in different versions that produces highly customized worms. The worm does not carry any payload but, being JavaScript, it's easy to modify the generated worm and add destructive capabilities.

VBS_LICHAR.A (Aliases: VBS.Heart, VBS/VBSVG.Mirc.Worm,VBS/Croatia.A, VBS/VBSWG.gen@MM) (Visual Basic Script Worm): This Visual Basic Script (VBS) malware propagates copies of itself via the Mirabilis Internet Relay Chat application (mIRC). It is designed to send copies of itself to all e-mail addresses found in the Outlook Address Book of the infected system. The subject of the e-mail that this worm sends is:

- "News from Eugene Kaspersky"

However, due to bugs in its codes, this worm does not execute its mass-mailing routine. On the system dates, 1, 5, 10, 15, 20, 25, 30 of the month, it changes the Registered Owner of the PC and overwrites all files with the following extension in all drives and directories: DOC, XLS, PPT, MDB, ERT, HTM, HTML, ASP, VBS, and VBE.

VBS.Keinef (Visual Basic Script Worm): This worm may modify the registry or the Win.ini file, or it can copy itself to your computer or to network drives. Additionally, it may attempt to send Windows password files to a pre-defined e-mail address.

VBS_REDLOF.B (Visual Basic Script Worm): This polymorphic Visual Basic Script (VBScript) malware infects files with the following extensions: VBS, HTML, HTM, ASP, PHP, JSP, and HTT. To propagate, it infects the stationery file, BLANK.HTM, on Microsoft Outlook Express. It then configures the e-mail client to use this stationery for outgoing e-mail. As a result, outgoing e-mail messages are infected with this malware. This VBS malware runs on Windows 95, 98, NT, 2000, ME and XP.

W32.Bokya.Int (Win32 Worm): This is an intended worm that attempts to disguise itself as a picture folder. This threat is written in the Microsoft Visual Basic (VB) programming language and is compressed with UPX. Because this threat has been modified, it cannot be unpacked by UPX itself. The VB run-time libraries must be installed on the computer for it to execute.

W32.Buffy.D (Alias: I-WORM.Buffy.d) (Win32 Worm): This is a worm that uses mIRC to spread. When the worm runs, it copies itself as C:\BTVS.exe. It also drops C:\Mirc\Script.ini. Finally, the worm drops C:\Windows\Winstart.bat and C:\Windows\StartMenu\Programs\Startup\Start.vbs, but they are not malicious.

W32/Eslac.worm (Win32 Worm): This is a network-share propagating worm. Using Netbios, it attempts to connect to systems on the same Class B subnet by querying random IP addresses. Upon connecting successfully, a copy of the worm, MAIN.EXE [24,576 bytes], is written to the share.

W32.HLLW.Backzat.G (Win32 Worm): This is a mass-mailing worm that uses Microsoft Outlook to send itself to all the contacts in the Microsoft Outlook Address Book. It also attempts to spread itself through the Grokster, eDonkey2000, BearShare, Morpheus, and KaZaA file-sharing networks. This worm may distribute itself across the mapped drives and through AIM95, mIRC, and ICQ. It deletes the security software from your computer. The e-mail it sends has the following characteristics:

- Subject: Fw: Hello there.
- Message: Hey, I just received a screen saver in the mail and it is really cute. Take a loot.
- Attachment: CuteKirby.Scr

This threat is written in the Microsoft C++ programming language and is compressed with UPX.

W32.HLLW.Eissa (Win32 Worm): This worm attempts to spread using the KaZaA file-sharing network. When the worm is executed, it displays a message and copies itself as %Windir%\CassieWorm.exe. It adds the values:

- CassieWorm %Windir%\CassieWorm.exe
- KAZAA <path to Kazaa>\Kazaa.exe /SYSTRAY

to the registry key:

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

so that the worm runs when you start Windows and sends e-mail to the author of the worm.

W32.HLLW.GOP.G@mm (Win32 Worm): This is a mass-mailing worm that copies itself to the hard drive as %System%\WindowsAgent.exe. It also searches the network drives and copies itself to \Recycled\Notdelw.i.n.v.e.r.y.i.f.y.exe on any mapped drive on which it can find an operating system. Then, W32.HLLW.GOP.G@mm modifies the Win.ini file to run the worm at startup.

W32.HLLW.Oror.C@mm (Alias: I-Worm.Roron.4997)(Win32 Worm): This is a mass-mailing worm and a variant of W32.HLLW.Oror@mm. This worm attempts to spread using e-mail, mIRC, KaZaA, network shares, and mapped drives. It also attempts to terminate and remove various security products from the infected computer. This threat is written in the C++ language and is compressed with UPX. The uncompressed size is about 166 KB.

W32.HLLW.Onewol (Win32 Worm): This is a worm that uses the IRC and P2P networks to spread. The worm attempts to delete many different security programs from the infected system

W32.HLLW.Veedna.B (Win32 Worm): This worm spreads through the KaZaA file-sharing network and copies itself to floppy disks. It also has backdoor capabilities. W32.HLLW.Veedna.B is written in the Microsoft Visual Basic programming language and is compressed with UPX. When W32.Bokya.Int is executed, it creates a hidden window and displays a message. W32.Bokya.Int contains code designed to use Windows Scripting to do the following:

- Modify the registry to execute itself every time you start Windows.
- Copy itself to the root folder of all the drives as Pictures.exe.
- Delete the files Regedit.exe and Regedit.com from the %system% folder.

W32.Horo@mm (Aliases: W32/Horo@MM, WORM_WCONN.B) IWin32 Worm): This is a mass-mailing worm that uses Microsoft Outlook to spread. This worm is written in Microsoft Visual Basic, version 6, and is packed with FSG. The e-mail message has the following characteristics:

- Subject: Today's free horoscope
- Attachment: Horoscope.scr

W32.Netspree.Worm (Win32 Worm): This is a worm that spreads over the network shares that are protected with trivial passwords. It also uses IRC to notify the remote malicious users when it infects a new system. This action may allow a malicious user to download programs to the infected computer. The worm may also enable the malicious user to use the infected computer as a drone for attacks against other Internet-connected computers. W32.Netspree.Worm does not spread from Windows 95/98/ME systems, although it functions normally in every other way on those platforms.

W32/Oror-L (Win32 Worm): This is a worm that spreads by network shares and e-mail. The e-mails subject line, message text, and attachment names are randomly chosen from a variety of possibilities. The worm attempts to exploit a known vulnerability in Internet Explorer versions 5.01 and 5.5, so that the attachment is launched automatically when the e-mail is selected for viewing. To prevent reinfection, users of Microsoft Outlook and Outlook Express should install the following patch available from Microsoft: <http://www.microsoft.com/technet/security/bulletin/MS01-027.asp>. This patch fixes a number of vulnerabilities in Microsoft's software, including the one exploited by this worm. When first run, the worm displays a message box with the text "Windows," "Cannot open file: it does not appear to be a valid program If you downloaded this file, try downloading file again." The worm copies itself to the Windows folder with a name that is a combination of 'Cmd', the computer's name backwards and "16.exe." The worm creates the following registry entry so that it is run automatically each time Windows is restarted:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\LoadProfile = Cmdtrid16.exe powrprof.dll,LoadCurrentPwrScheme

The worm also prepends its pathname to the registry entry:

- HKCR\exefile\shell\open\command\,

so that the worm is run before any executable file is run. W32/Oror-L chooses a random sub-folder of the Program Files folder and copies itself to this folder using the sub-folder name concatenated with "16.exe," "32.exe" or ".exe." If the chosen folder name contains spaces, only the beginning of the folder name is used. The worm adds the pathname to this executable under the registry key:

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

so that this copy of the worm is run automatically on startup. The worm also copies itself to the Windows System folder using the name of a randomly selected file from the System folder, but with "16.exe," "32.exe" or ".exe" in place of the file's extension. The worm runs this copy of itself automatically on startup by adding the line, "run=<path to worm>," to the [Windows] section of WIN.INI file. W32/Oror-L spreads over the local network by copying itself to shared folders using random filenames. During this process the worm may create additional entries under the registry key:

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

The worm attempts to spread via file sharing on KaZaA networks by copying itself to any KaZaA shared folders that it finds using various filenames. W32/Oror-L also creates new versions of the mIRC files MIRC.INI and REMOTE.INI. These files allow a remote malicious user access to the computer via IRC channels. The worm will attempt to terminate several anti-virus programs.

W32/Sahay-A (Alias: Win32.HLLP.YahaSux) (Win32 Worm): This is a worm that replicates by creating and executing the temporary file yahasux.vbs in the Windows folder (detected as VBS/Sahay-A), which sends an e-mail to all contacts in the Windows Address Book. The e-mail has the following characteristics:

- Attached file: MathMagic.scr
- Subject line: Fw: Sit back and be surprised..

W32/Sahay-A copies itself as MathMagic.scr to the root folder and may attempt to disinfect a variant of W32/Yaha if the virus is present on the computer. This procedure will cause the computer to restart.

W97M.Lakko (Word 97 Macro Virus): This is a macro virus that spreads from the Microsoft Word Normal.dot template to Microsoft Word documents. If the month is March, June, September, or December, the virus creates the C:\Windows.sys file and logs the date and time of the infection.

WM97/Replug-F (Aliases: Macro.Word97.Replug, W97M.Replug.E) (Word 97 Macro Virus): This is a member of the WM97/Replug family. The virus will attempt to run I:\Eudora\Sys\Server.exe and create the file I:\Rep.log - a log file which will record the date of the infection.

Worm/Ainjo.e (Alias: Win32.Hunch.A@mm) (Internet Worm): This is an Internet worm that spreads through e-mail by using addresses it collects in the Microsoft Outlook Address Book, as well as, through the use of the mIRC network and through the file-sharing program KaZaA. It also copies itself over all mapped drives. If executed, the worm copies itself in the \windows\ directory under the filenames "kernelw32.exe" and "blank.scr." It will also copy itself under "C:\recycled\de3.exe.scr" and "c:\pictures.exe." Additionally, the following files are added:

- C:\zip.com
- C:\freepic.zip (zip file with the packed 'pictures.exe')
- C:\windows\t.bat

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

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
"Kernelw"="C:\\WINDOWS\\Kernelw32.exe"

In order to use the mIRC network, it modifies the mirc.ini file in the MIRC directory. It will then copy itself under random files names with a .exe file extension to the My Shared Folder directory in the KaZaA directory making itself available for download through the file sharing application. Then, the worm copies itself using the same filenames of all .EXE, .HTM, and .DOC files in locates in the same directory in all local drives and directories.

Worm/Clown.B (Internet Worm): Worm/Clown.B is an Internet worm that spreads through e-mail by using addresses it collects in the Microsoft Outlook Address Book, as well as, through the KaZaA file-sharing network. If executed, Worm/Clown.B infects all files in C:\windows\Samples\Wsh*.vbs and sets this directory to a shared folder for the P2P application, Kazaa. The worm will then attempts to send itself with Microsoft Outlook. The following registry key will get added:

- HKEY_CURRENT_USER\Software\Kazaa\LocalContent
"Dir2"="012345:C:\\WINDOWS\\SAMPLES\\WSH" "DisableSharing"="0"

Worm/Herpes (Internet Worm): This is an Internet worm that spreads through the use of many of the popular file-sharing networks including, KaZaA, Morpheus, BearShare, and Grokster.

Worm/Opasoft.O (Alias: W32.Opaserv.O) (Internet Worm): This is a variant of Worm/Opasoft, a network aware Internet worm that spreads through the use of network shares. If executed, the worm copies itself in the \windows\ directory under the filename, "SRV32.EXE." So that it gets run each time a user restart their computer the following registry key gets added:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices "Srv32"="C:\\WINDOWS\\Srv32.exe"

Additionally, the file C:\Windows\win.ini gets modified as follows:

- Modifies:
- run=
- run=c:\windows\SRV32.EXE

It will then attempt to delete prior Opasoft related files and registry keys. Worm/Opasoft.O copies itself on shared "C" drives on other machines to \windows\ directory under SRV32.EXE and changes their win.ini file. Due to a vulnerability the virus has the ability to copy itself on password protected machines as well. This vulnerability only exists under Windows 95/98/ME machines.

WORM_SQLP1434.A (Aliases: SQLP1434.A, W32/SQLSlammer, W32.SQLExp.Worm, Worm.SQL.Helkern, DDOS_SQLP1434.A) (Internet Worm): This worm has been reported in the wild. It attacks targets systems that use Microsoft SQL Server 2000, allowing affected SQL Servers to send the malicious packet to other SQL Servers and thereby causing a slowdown, or even failure, in the affected network. The code that executes the Denial of Service attack resides only in memory of affected Microsoft SQL servers, and there are no file counterparts. Because of this, antiviral scanners that do not support memory scanning will not be able to detect the code. There is no pattern file required. Unpatched machines installed with the Microsoft SQL Server 2000 Desktop Engine (MSDE) are also vulnerable to this malware. MSDE is based on core SQL Server technology and runs on the following platforms:

- Windows 98
- Windows ME
- Windows NT 4.0
- Windows 2000 Professional

This worm does not drop files or send copies of itself via e-mail that is the usual worm routine.

Trojans

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

Trojan	Version	CyberNotes Issue #
Backdoor.Amitis	N/A	CyberNotes-2003-01
Backdoor.Assasin.D	D	CyberNotes-2003-01
Backdoor.Beasty	N/A	Current Issue
Backdoor.Colfuser	N/A	CyberNotes-2003-01
Backdoor.Cow	N/A	CyberNotes-2003-01
Backdoor.Cybspy	N/A	CyberNotes-2003-01
Backdoor.Deftcode	N/A	CyberNotes-2003-01
Backdoor.Drator	N/A	CyberNotes-2003-01
Backdoor.FTP.Casus	N/A	Current Issue

Trojan	Version	CyberNotes Issue #
Backdoor.Hethat	N/A	CyberNotes-2003-01
Backdoor.Hornet	N/A	CyberNotes-2003-01
Backdoor.IRC.Aladinz	N/A	Current Issue
Backdoor.Lala	N/A	CyberNotes-2003-01
Backdoor.Massaker	N/A	Current Issue
Backdoor.NetDevil.B	B	CyberNotes-2003-01
Backdoor.NetTrojan	N/A	CyberNotes-2003-01
Backdoor.Ohpass	N/A	CyberNotes-2003-01
Backdoor.OICQSer.165	N/A	CyberNotes-2003-01
Backdoor.OICQSer.17	17	CyberNotes-2003-01
Backdoor.OptixPro.10.c	10.c	CyberNotes-2003-01
Backdoor.Remohak.16	16	CyberNotes-2003-01
Backdoor.RemoteSOB	N/A	CyberNotes-2003-01
Backdoor.Rephlex	N/A	CyberNotes-2003-01
Backdoor.Sdbot.C	C	Current Issue
Backdoor.Servsax	N/A	CyberNotes-2003-01
Backdoor.Sixca	N/A	CyberNotes-2003-01
Backdoor.Talex	N/A	Current Issue
Backdoor.Upfudoor	N/A	CyberNotes-2003-01
Backdoor.VagrNocker	N/A	CyberNotes-2003-01
Backdoor.Vmz	N/A	CyberNotes-2003-01
Backdoor.Xenozbot	N/A	CyberNotes-2003-01
Backdoor.Zdemon	N/A	Current Issue
Backdoor.Zix	N/A	Current Issue
Backdoor-AOK	N/A	CyberNotes-2003-01
BDS/AntiPC	N/A	Current Issue
BDS/Backstab	N/A	Current Issue
Downloader-BO.dr.b	N/A	Current Issue
Downloader-BS	N/A	Current Issue
IRC/Backdoor.e	E	CyberNotes-2003-01
IRC/Backdoor.f	f	Current Issue
IRC-OhShootBot	N/A	CyberNotes-2003-01
JS.Seeker.J	J	CyberNotes-2003-01
KeyLog-TweakPan	N/A	Current Issue
MultiDropper-FD	N/A	CyberNotes-2003-01
PWSteal.ALight	N/A	CyberNotes-2003-01
PWSteal.Rimd	N/A	CyberNotes-2003-01
PWS-Tenbot	N/A	CyberNotes-2003-01
QDel359	N/A	CyberNotes-2003-01
TR/Fake.YaHoMe.1	N/A	Current Issue
TR/WinMx	N/A	Current Issue
Troj/Dloader-BO	N/A	Current Issue
Troj/Qzap-248	N/A	CyberNotes-2003-01
TROJ_JBELLZA	N/A	Current Issue
TROJ_KILLBOOT.B	B	CyberNotes-2003-01
Trojan.Dasmin	N/A	CyberNotes-2003-01
Trojan.Downloader.Inor	N/A	Current Issue
Trojan.Ivanet	N/A	Current Issue
Trojan.KKiller	N/A	CyberNotes-2003-01

Trojan	Version	CyberNotes Issue #
Trojan.Poldo.B	B	Current Issue
Trojan.PSW.Platan.5.A	N/A	CyberNotes-2003-01
Trojan.PWS.QQPass.D	N/A	Current Issue
Trojan.Qforager	N/A	Current Issue
Trojan.Qforager.Dr	N/A	Current Issue
Trojan.Qwe	N/A	Current Issue
Trojan.Snag	N/A	Current Issue
Trojan.Unblockee	N/A	CyberNotes-2003-01
VBS.Moon.B	B	Current Issue
VBS.StartPage	N/A	Current Issue
W32.Socay.Worm	N/A	Current Issue
W32.Xilon.Trojan	N/A	CyberNotes-2003-01

Backdoor.Beasty: This is a backdoor Trojan that allows complete access to the infected computer. By default, the Trojan listens on port 666 and notifies the malicious user through ICQ.

Backdoor.FTP.Casus (Aliases: Backdoor.FTP.Casus.23, Backdoor-KZ): This Trojan allows unauthorized access to the infected computer. By default, it attempts to listen on port 1919. It is written in the Delphi programming language and is packed with ASPack. When Backdoor.FTP.Casus runs, it adds the value, "SystemSpy <Path\file name>," to the registry key:

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

It also adds several values to the registry key:

- HKEY_CURRENT_USER\Software\Spy\SystemS

Next it opens port 1919 and sends the ICQ or e-mail notification to the malicious user. This Trojan steals the network passwords and ICQ user ID.

Backdoor.IRC.Aladinz (Aliases: Backdoor.IRC.Aladinz.30, Backdoor:IRC/Aladinz, IRC/Flood):

This is a backdoor Trojan that gives a third party full control over the victim's computer. It uses the mIRC client to connect to the Internet, where it notifies the attacker of its presence. During the execution of the initial insertion program of Backdoor.IRC.Aladinz, it will create the folder, %Windir%\FONTS\FONTS. Backdoor.IRC.Aladinz also creates the registry value, "Arialfont %windir%\FONTS\FONTS\Arialfont.exe," under the key:

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

so that the Trojan runs when you start Windows.

Backdoor.Massaker: This is a backdoor Trojan that allows complete access to the infected computer. By default it listens on port 7119. In addition, this Trojan horse attempts to terminate the processes of several security products. It is written in the Microsoft Visual Basic (VB) programming language and compressed with UPX. The VB run-time libraries must be installed on the computer for it to execute.

Backdoor.Sdbot.C (Alias: Backdoor.Sdbot.gen): This is a backdoor Trojan that is a variant of Backdoor.Sdbot. This variant has been packed and encrypted eight times using four different run-time packers and run-time encryptors. This process has ostensibly been done to evade detection and to make it more difficult to analyze this backdoor Trojan.

Backdoor.Talex (Aliases: Backdoor.Talex.287, Backdoor-ZE): This backdoor Trojan allows complete access to the infected computer. It is written in the Delphi programming language and is packed with ASPack. When Backdoor.Talex is executed, it copies itself as %Windir%\Regscan.exe and adds the value, "RegScan %Windir%\Regscan.exe," to the registry key:

- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that the Trojan runs when you start Windows. Next it modifies the run= line of the Win.ini file on Windows 95/98/ME computers, as, "run=%Windir%\regscan.exe," so that the Trojan starts when you start Windows. This Trojan then waits for commands from the malicious user to perform

Backdoor.Zdemon (Alias: Backdoor.Zdemon.10): This Trojan allows a malicious user to remotely control your computer. Backdoor.Zdemon can listen on any port, though, by default, it listens on ports 31556 and 6051. When Backdoor.Zdemon is executed, by default, it copies itself as %Windows%\SystemReg.exe and adds the SystemReg value to the registry key:

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

so that it runs when you start Windows. The Trojan opens a port allowing a malicious user to remotely control the infected computer.

Backdoor.Zix: This is a backdoor Trojan that allows a malicious user to run arbitrary commands on the infected computer. The Trojan sends information an e-mail message from the infected computer to a specific e-mail address. It also downloads files from an e-mail account and then executes them on the computer. When executed, the Trojan copies itself to, “%System%\zy6server.exe,” and adds the value, “iez,” to the registry key:

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

It attempts to register itself as a service and sends system information to an e-mail address at 163.com through the mail server, smtp.163.com. It also downloads e-mail messages with encoded information from the POP server at pop.163.com, which instructs the computer to perform arbitrary commands.

BDS/AntiPC: Like other backdoor programs, BDS/AntiPC would potentially allow someone with malicious intent backdoor access to your computer. Once executed, BDS/AntiPC remains in memory. It does not create or modify any registry keys.

BDS/Backstab: Like other backdoors, BDS/Backstab would potentially allow someone with malicious intent backdoor access to your computer. It is a remote administration tool. If executed, it will copy itself to the /windows/ directory under the filename “<random>server.exe.” Additionally, it will modify the file “C:\Windows\win.ini” with the following changes:

- run=
- run=C:\Windows\Server.EXE

Downloader-BO.dr.b: This threat has been known to have been SPAMMED to many users. The message may arrive as follows:

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

The MESSAGES.HTA attachment displays a blank Window. This HTA file contains an embedded VBScript. The script will drop the file C:\mware.exe and execute it.

Downloader-BS: When executed on the victim machine, this downloader Trojan attempts to download files via HTTP. The files it tries to download from this HTTP site are porndialers. The Trojan copies itself to the C:\WINDOWS\SYSTEM directory as MSFINDOS.EXE and creates the following registry run keys to load itself at startup:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
"msfindosa.exe" C:\WINDOWS\SYSTEM\msfindosa.exe
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
"msfindosa.exe" C:\WINDOWS\SYSTEM\msfindosa.exe

IRC/Backdoor.f : This is a backdoor Trojan for mIRC that allows a malicious user to execute any mIRC commands on the victim machine. It opens port 33 UDP and listens for incoming commands. Every command is executed immediately. The Trojan requires the IRC chatprogram mIRC to be installed.

KeyLog-TweakPan: This is a privacy invading Trojan. It is designed to capture typed keystrokes and send the information to e-mail address qq@chat.ru using its own SMTP engine. When run, the Trojan copies itself to the WINDOWS SYSTEM (%SysDir%) as MSKHPK.EXE and MSKHPK.DLL. A registry run key is created to load the worm at startup:

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

TR/Fake.YaHoMe.1: This Trojan would potentially allow someone with malicious intent backdoor access to your computer. It is a Yahoo! password stealer. So that it gets run each time a user restart their computer the following registry key gets added:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
"Yahoo! Pager"="C:\\XXX\\AYPAGER.exe"

Additionally, the following key gets created:

- HKEY_CURRENT_USER\Software\HRVG "e-mail"=asd@ydf.de
"path"="C:\\Program Files\\Yahoo!\\Messenger\\ypager.exe -quiet"

TR/WinMx: Like other Trojans, TR/WinMx would potentially allow someone with malicious intent backdoor access to your computer. It is a WinMx sharing program. If executed, it will copy itself to the /windows/ directory under the filename "syscom.com." The file "library.dat" will also get created. So that it gets run each time a user restart their computer the following registry key gets added:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
"Syscom"="C:\\windows\\syscom.com"

Finally, it attempts to copy all the files from local the disk to C:\\kernel\\.

Troj/Dloader-BO (Aliases: TrojanDownloader.Win32.Inor, Downloader-BO, W32/Maz.A, Tr/Mastaz, Maz, Mastaz, W32/Maz.B): Troj/Dloader-BO downloads and executes a file from the website masteraz.hypermart.net within three days of being run for the first time. It has been seen in the files MASTERAZ.EXE, JIMKRE.EXE, and messages.hta. The Trojan adds the following entry to the registry:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\
.inr\5Nzg1mOWKzFnuvu6 = "C:\\<path to Trojan>."

This will run the Trojan on system restart. The Trojan also creates the following entry within the registry:

- HKLM\Software\CLASSES\.inr\5Nzg1mOWKzFnuvu6.

TROJ_JBELLZ.A (Aliases: Trojan.Linux.JBellz, Exploit-Jbellz, MP3.Jbellz Trojan): This Trojan exploits a vulnerability in version pre0.59 of mpg123 players. It can append its code to MP3 files. Also, it displays the following messages in the user's console:

- rm -rf ~ in 5 seconds .. CTRL-C to abort
- :PpPpPpPpPp ...

The Trojan is written in the C language and operates on Linux systems, usually SuSE 8.0 and Slackware 8.0, but can be modified for use in other Linux systems like Red Hat.

Trojan.Downloader.Inor: This Trojan horse that attempts to contact a web site that will determine and then display the language settings of your computer. It tries to download a file from a certain Web site. At the time that this write-up was written, Trojan.Downloader.Inor downloads the Trojan.Qwe file. Trojan.Downloader.Inor spreads as a .hta file. When this file is executed, it creates the C:\\Mware.exe file, and then executes it. When Mware.exe runs, first it contacts a Web site that contains a script.

Trojan.Ivanet: This Trojan Horse attempts to disguise itself as an .avi file. It is written in Delphi and is compressed with UPX. When Trojan.Ivanet is executed, it adds the value, "winnet C:\\WINDOWS\\SYSTEM\\mui\\040c\\winnet.pif," to the registry key:

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

The Trojan may also add the value, "winnet C:\\WINDOWS\\SYSTEM\\mui\\040c\\winnet.pif," to the registry key:

- HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Windows\\CurrentVersion\\RunServices

It attempts to force the local time of the infected computer to be 06:06:06 A.M and delete the file C:\\Windows\\Regedit.exe. If the Trojan fails to delete this file, it displays a message. Next it searches for the file C:\\Windows\\System\\Mmui\\040c\\Winnet.pif. If the Winnet.pif does not exist on the computer, the Trojan attempts to copy the file C:\\Windows\\Command\\Format.sys.bat to C:\\Windows\\System\\Mui\\040c\\Winnet.pif and attempts to copy the file C:\\Windows\\System\\mui\\040c\\Winnet.pif to the following files:

- C:\\Windows\\Command\\Format.sys.bat
- A:\\ayanami.avi.exe

- a:\Bikinis.avi.exe
- A:\Lauraleon.avi.exe
- A:\Nancycristy_18.avi.exe
- A:\Sakura.avi.exe
- A:\Xxx.avi.exe

Trojan.Qforager: This is a Trojan horse that attempts to steal the password for the QQ instant messenger program and e-mail it to the malicious user. When Trojan.Qforager is executed, it adds the value, "AudioHQ <path to the Trojan>," to the registry key:

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

so that the Trojan runs each time you start Windows. It also attempts to steal the passwords for the QQ instant messenger program and e-mail it to the malicious user.

Trojan.Qforager.Dr: This is a Trojan dropper that inserts Trojan.Qforager on the computer.

Trojan.Qwe: This is a Trojan horse that monitors key strokes, saves them in a log file, and then sends the log file to a certain e-mail address. It downloads and installs this Trojan on the system and consists of two files:

Mskhpk.exe

Mskhpk.dll

When Trojan.Qwe was installed, the value, "TwkCplDaemon," was added to the registry key:

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

to make the Trojan run when you start Windows. When Trojan.Qwe runs, it saves all the keystrokes to a log file, and then attempts to e-mail the log file to the malicious user.

Trojan.Poldo.B (Alias: Trojan.Win32.Dasmin.b): This is a variant of Trojan.Poldo and Trojan.Dasmin. When Trojan.Poldo.B runs, it searches the following registry keys:

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

for one of the following values:

- MSAdmin
- MSConfigr
- VirusCheckII

If the value is found and it points to an .exe file, the Trojan attempts to terminate that process and delete the file. Next it copies itself to the %System% folder, with the Hidden attribute set, as:

- IEXPRES.EXE
- REGCPM32.EXE

and adds the values:

- MSStartOptimizer %System%\IEXPRES.EXE
- RegCompres %System%\REGCPM32.EXE

to the registry keys:

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

It also adds the value, "OEMCurrentVersion currentVersion," to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion

and attempts to access a specific URL to increase the Web site's counter. This Trojan attempts to download a settings file from a specific FTP server. If it is successful, it attempts to download and execute a file.

Trojan.PWS.QQPass.D: This is a password-stealing Trojan that steals passwords and user information. The Trojan is a Visual Basic application that requires the presence of Microsoft Visual Basic run-time libraries for it to run. When Trojan.PWS.QQPass.C is executed, it copies itself to the file, “%Windir%\Notepad.exe,” and modifies %Windir%\System.ini file by changing: shell=Explorer.exe to: shell=Explorer.exe Notepad.exe so that the Trojan runs when you start Windows (Window 95/98/ME only). It also adds the value, “sesteym %Windir%\Notepad.exe,” to the registry key:

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

so that the Trojan runs when you start Windows. This Trojan attempts to steal the QQ passwords and send them to the author of the Trojan.

Trojan.Snag (Alias: Trojan.Spy.Snag.02): This is a Trojan horse that attempts to steal the CDKeys of the following games:

- Battlefield 1942
- Black & White
- Counter-Strike
- Gunman Chronicles
- Half-Life
- Medal Of Honor - Allied Assault
- NeedForSpeed - Hot Pursuit 2
- Unreal Tournament 2003

VBS.Moon.B: This is a Trojan Horse that is similar to VBS.Moon@mm. It uses the Windows file Wscript.exe to run its instructions and copies itself to the \Windows folder. VBS.Moon.B also reduces the security level of Internet Explorer, sets the speaker mode of the modem, and changes the Internet Explorer home page.

VBS.StartPage: This Trojan horse alters the Microsoft Internet Explorer default home page without permission. The Trojan horse arrives as a file with the .vbs extension. When VBS.StartPage is executed, it makes changes to the registry key:

- HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Start Page

W32.Socay.Worm: This is a backdoor Trojan that contains worm functionality. It attempts to send itself to all the addresses in the Microsoft Outlook Address Book. The e-mail characteristics are:

- Subject: Re:VISA DE TRABAJO
- Attachment: <Original file name>

The worm also tries to copy itself to drive A as Visa de Trabajo <multiple spaces> .exe. The backdoor component listens on port 8,520 for remote connections.