National Infrastructure Protection Center CyberNotes

Issue #2002-05 *March 11, 2002*

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 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between February 19 and March 8, 2002. 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
AeroMail[1]	Multiple	AeroMail 0.01.02, 0.01.10, 0.01.20, 0.01.26, 0.01.30, 0.01.40	Multiple vulnerabilities exist: a vulnerability exists when e-mail messages are sent, which could let a remote malicious user execute arbitrary JavaScript; and a vulnerability exists because additional headers can be added to outgoing e-mail messages, which could let a malicious user unencoded attachments.	Upgrade available at: http://the.cushman.net/projects/aeromail/download/aeromail-1.45.zip	AeroMail Multiple Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required.

[1] Securiteam, March 8, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
America OnLine, Inc.[2]	Multiple	AOL Instant Messenger	A vulnerability exists in the AOL Instant Messenger screen, which could let a remote malicious user obtain user passwords.	No workaround or patch available at time of publishing.	AOL Instant Messenger Password Access	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
America OnLine, Inc.[3]	Windows 98/98/ME/ NT 4.0/2000, XP, MacOS 9.0	AOL Instant Messenger 2.0N, 2.0.912, 2.0.996, 2.1.1236, 2.5.1598, 2.5.1366, 3.0N, 3.0.1470, 3.0.1415, 3.5.1808, 3.5.1670, 3.5.1635, 3.5.1856, 4.0, 4.1, 4.1.2010, 4.2, 4.2.1193, 4.3, 4.3.2229, 4.4,-4.7, 4.7.2480, 4.8.2616, 4.8.2646,	A remote Denial of Service vulnerability exists due to an unchecked buffer in 'oscar.dll.'	No workaround or patch available at time of publishing.	AOL Instant Messenger Denial Of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Avenger's News System[4]	Unix	Avenger's News System 2.01, 2.11	Two vulnerabilities exist: a Directory Traversal vulnerability exists, which could let a remote malicious user obtain sensitive information; and a vulnerability exists in a plugin subroutine due to improper input filtering, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Avenger's News System Directory Traversal and Plugin Subroutine Arbitrary Execution	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Directory Traversal vulnerability can be exploited via a web browser. Exploit script has been published for the buffer overflow vulnerability.
BPM Studio[5]	Windows 95/98/ME/ NT 4.0/2000, XP	BPM Studio Pro 4.2	A Directory Traversal vulnerability exists because web requests are not adequately filtered, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	BPM Studio Pro Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[2] NTBugtraq, February 24, 2002.
[3] NtWaK0 & Recon Advisory, February 29, 2002.
[4] Bugtraq, February 21, 2002.
[5] Bugtraq, February 27, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
CacheFlow [6]	Multiple	CacheOS 3.1.02-3.1.10, 3.1.20, 3.1, 3.1.11-3.1.19, 3.1.21, 4.0, 4.0.11-4.0.14	A vulnerability exists in the HTTP CONNECT method, which could let a remote malicious user tunnel arbitrary TCP connections through a HTTP request.	No workaround or patch available at time of publishing.	CacheOS HTTP CONNECT	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Century Software [7]	Unix	Term For Linux 0.06.27.0869	A buffer overflow vulnerability exists due to improper bounds checking, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Term Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Cisco Systems [8]	Multiple	IOS 11.1CC, 12.0T, 12.0ST, 12.0S, 12.0, 12.1T, 12.1E, 12.1, 12.2T, +12.2	A vulnerability exists when Cisco Express Forwarding (CEF) is enabled because information is leaked from previous packets handled by the device, which could let a malicious user obtain sensitive information.	Upgrade available at: http://www.cisco.com	Cisco IOS CEF Sensitive Information	Medium	Bug discussed in newsgroups and websites.
Compaq Computer Corporation [9]	Multiple	ACMS 4.3, 4.4	A vulnerability exists because some process privileges are handled insecurely, which could let a malicious user obtain unauthorized access.	Patch available at: http://www3.compaq.com/support/home/index.asp	ACMS Unauthorized Access	Medium	Bug discussed in newsgroups and websites.
Debian [10]	Unix	CVS Kit CVS Server 1.10.7	A Denial of Service vulnerability exists due to an improperly initialized global variable used by the CVS server.	Upgrade available at: http://security.debian.org/dists/stable/updates/main/	CVS Server Denial Of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Endymion [11]	Unix	MailMan WebMail 3.0, 3.0.1, 3.0.4, 3.0.6-3.0.8, 3.0.10-3.0.16, 3.0.18-3.0.35	A vulnerability exists due to insufficient validation of input supplied to the ALTERNATE_TEMPLATES CGI variable, which could let a remote malicious user obtain sensitive information.	Upgrade available at: http://www.endymion.com/products/mailman/download.htm	MailMan Sensitive Information	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.

[6] Bugtraq, February 19, 2002.
[7] Securiteam, February 25, 2002.
[8] Cisco Security Advisory, 20020227, February 27, 2002.
[9] Compaq Security Advisory, SSRT0813, February 25, 2002.
[10] Debian Security Advisory, DSA 117-1, March 5, 2002.
[11] Securiteam, March 8, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Essen[12]	Windows 95/98/NT 4.0/2000, XP	Essentia Web Server 2.1	Two vulnerabilities exist: a Denial of Service vulnerability exists when an excessively long URL is submitted due to improper bounds checking; and a Directory Traversal vulnerability exists due to improper filtering, which could let a remote malicious user obtain sensitive information.	Upgrade available at: http://www.essencomp.com/Products/Essentia/Essentia.exe	Essentia Web Server Denial Of Service and Directory Traversal	Low/ Medium (Medium for the Directory Traversal vulner-ability)	Bug discussed in newsgroups and websites. Denial of Service vulnerability can be exploited via a web browser. No exploit code is required for the Directory Traversal vulnerability.
Galacti-comm Technol-ogies[13]	Windows	Worldgroup Enterprise Edition 3.20, LITE Personal Server 3.20	Multiple vulnerabilities exist: a remote Denial of Service vulnerability exists if a LIST command is received that includes a long string of characters; and a remote Denial of Service vulnerability exists if a HTTP GET request is received that consists of a long string of arbitrary characters.	No workaround or patch available at time of publishing.	Worldgroup Remote FTP Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Hewlett Packard Systems[14]	Unix	HP9000 Series 700/800 running HP-UX releases 10.20 & 11.x	A vulnerability exists in the Java Runtime Environment, which could let a remote malicious user take any action or combination of actions of his/her choosing.	Patch available at: www.hp.com/go/java	HP-UX Java Applet Browser Traffic Redirect CVE Name: CAN-2002-0058	**High**	Bug discussed in newsgroups and websites.
Hewlett Packard Systems[15]	Multiple	ProCurve Switch 4000M 0.0	A Denial of Service vulnerability exists due to the way port scans are handled.	No workaround or patch available at time of publishing.	ProCurve Switch Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Hotline Commun-ications[16]	Windows 95/98/NT 4.0/2000	Hotline Connect 1.8.5	A vulnerability exists because account information is stored in plaintext, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Hotline Connect Plaintext Password	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[12] Bugtraq, February 26, 2002.
[13] Bugtraq, February 27, 2002.
[14] Hewlett-Packard Company Security Bulletin, HPSBUX0203-186, March 8, 2002.
[15] Bugtraq, February 28, 2002.
[16] Securiteam, March 4, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Ikonboard.com[17]	Unix	Ikonboard 2.17	A Cross-Site Scripting vulnerability exists because images can be included in forum messages, which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	Ikonboard Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Khaled Mardam-Bey[18]	Windows 95/98/ME/ NT 4.0/2000, XP	mIRC 6.0, 6.01	A vulnerability exists when a certain command is issued to the DCC protocol, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	mIRC DCC Sensitive Information	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
KMail[19]	Unix	KDE KMail 1.2	A remote Denial of Service vulnerability exists when an e-mail message is received that contains an excessively long message body.	Upgrade available at: http://www.kde.org/download.html	KMail Denial Of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Luca Deri[20]	Unix	ntop 2.0	A format string vulnerability exists in the 'traceEvent()' function, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://snapshot.ntop.org/tgz/ntop-02-03-01.tgz	ntop Remote Format String	**High**	Bug discussed in newsgroups and websites.
Matt Blaze[21]	Unix	cfs 1.3.3 Sparc, PPC, m68k, ia32, ARM, Alpha	Multiple buffer overflow vulnerabilities exist in the 'cfsd' daemon, which could let a remote malicious user initiate a Denial of Service	**Debian:** http://security.debian.org/dists/stable/updates/main/	CFS Multiple Buffer Overflows	Low	Bug discussed in newsgroups and websites.
Microsoft[22]	Windows 95/98/ME/ NT 4.0/2000, XP	All builds of the Microsoft VM up to and including build 3802	A session hijacking vulnerability exists due to the way Java requests for proxy services are handled, which could let a remote malicious user take any action or combination of actions of his/her choosing.	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/MS02-013.asp	Microsoft Java Applet Browser Traffic Redirect CVE Name: CAN-2002-0058	**High**	Bug discussed in newsgroups and websites.

[17] Bugtraq, February 26, 2002.
[18] Bugtraq, March 6, 2002.
[19] Bugtraq, February 26, 2002.
[20] Hologram Security Advisory, H20020304, March 4, 2002.
[21] Debian Security Advisory, DSA 116-1, March 2, 2002.
[22] Microsoft Security Bulletin, MS02-013, March 4, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[23]	Windows 2000, XP	Exchange Server 2000 0.0, 2000 0.0 SP1&2, Advanced Server 0.0. 0.0 SP1&2, Professional 0.0, 0.0SP1&2, 2000 Server 0.0, 0.0SP1&2, XP Professional 0.0	A remote Denial of Service vulnerability exists when certain types of malformed SMTP commands are sent to the server.	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/MS02-012.asp	Microsoft SMTP Service Malformed Data Remote Denial of Service CVE Name: CAN-2002-0055	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Microsoft[24]	Windows NT 4.0/2000	Exchange Server 5.5, 5.5SP1-4, 2000 Advanced Server 0.0, 0.0SP1&2, Datacenter Server 0.0, 0.0SP1&2, Professional 0.0, 0.0SP1&2, 2000 Server 0.0, 0.0SP1&2	A vulnerability exists in the way that the Windows 2000 SMTP service and Microsoft Exchange Server 5.5 interact with the NTLM authentication layer, which could let a malicious user obtain unauthorized user-level access to the SMTP service.	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/MS02-011.asp	Microsoft Windows SMTP Service Authentication CVE Name: CAN-2002-0054	Medium	Bug discussed in newsgroups and websites.
Microsoft[25]	Windows NT 4.0/2000, XP	Microsoft IIS 4.0alpha, 4.0, 5.0, 5.1	A vulnerability exists because it is possible to force the web service to authenticate a user, which could let a remote malicious user launch a brute force attack.	No workaround or patch available at time of publishing.	Microsoft IIS Authentication	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Microsoft[26]	Windows NT 4.0	SQL Server 7.0, 7.0alpha, 7.0SP1-3, 7.0SP1-3 alpha	A buffer overflow vulnerability exists in the 'xp_dirtree' procedure, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Microsoft SQL Server Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

[23] Microsoft Security Bulletin, MS02-012, February 27, 2002.
[24] Microsoft Security Bulletin, MS02-011, February 27, 2002.
[25] NGSSoftware Insight Security Research Advisory, NISR04032002C, March 5, 2002.
[26] NTBugtraq, March 7, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[27] ***Microsoft re-releases bulletin***[28]	**Windows 95/98/NT 4.0/2000, XP**	**Windows 95, 98, 98SE, NT 4.0, NT 4.0 Server, Terminal Server Edition, 2000, XP**	**A buffer overflow vulnerability exists because the component of the SNMP agent service that parses incoming commands contains an unchecked buffer, which could let a malicious user cause a Denial of Service or execute arbitrary code.** ***Microsoft released an updated version of the bulletin announcing the availability of a patch for Windows NT 4.0 and to advise customers that the work-around procedure is no longer needed for that platform. Patches for additional platforms are forthcoming and this bulletin will be re-released to announce their availability.***	**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/MS02-006.asp**	**Windows Unchecked Buffer SNMP Service** **CVE Name: CAN-2002-0053**	**High**	**Bug discussed in newsgroups and websites.** **Vulnerability has appeared in the press and other public media.**
Microsoft[29]	Windows 98/SE/NT 4.0/2000	Windows NT Workstation 4.0, 4.0SP1-6a, Terminal Server 4.0, 4.0SP1-6a, Server 4.0, 4.0SP1-6a, Enterprise Server 4.0, 4.0SP1-6a, 2000 Terminal Services 0.0, 0.0SP1-2, 2000 Server 0.0, 0.0SP1-2, Professional 0.0, 0.0SP1-2, Datacenter Server 0.0, 0.0SP1-2, Advanced Server 0.0, 0.0SP1-2	An unchecked buffer overflow vulnerability exists in one of the functions that helps to locate incompletely removed applications on the system, 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/MS02-014.asp	Microsoft Windows User Shell Buffer Overflow CVE Name: CAN-2001-0070	**High**	Bug discussed in newsgroups and websites.

[27] Microsoft Security Bulletin, MS02-006, February 15, 2002.
[28] Microsoft Security Bulletin, MS02-006 (version 3.0), March 5, 2002.
[29] Microsoft Security Bulletin, MS02-014, March 7, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[30]	Windows 95/98/ME/ NT 4.0, XP; Unix	Ethereal Group Ethereal 0.9.1; Gerald Combs Ethereal 0.8.13 and previous	A Denial of Service vulnerability exists when malformed SNMP packets are received.	No workaround or patch available at time of publishing.	Ethereal Malformed SNMP Denial of Service	Low	Bug discussed in newsgroups and websites.
Multiple Vendors[31]	Unix	efingerd 1.3, 1.6.1,	Two vulnerabilities exist: a remote buffer overflow vulnerability exists because domain information is not properly handled, which could let a malicious user execute arbitrary code; and a vulnerability exists when an ".efingerd" file exists and is executable, efingerd will execute the program with the permissions of nobody.	No workaround or patch available at time of publishing.	EFingerD Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Multiple Vendors[32]	Unix	Net-SNMP ucd-snmp 4.1.1, 4.1.2, 4.2.1	Multiple vulnerabilities exist: several buffer overflow vulnerabilities exist in the incoming packet handling code and logging code; a vulnerability exists due to lack of error checking in the command-line parser; and various memory leaks exist in the main agent code. These vulnerabilities could let a remote malicious user cause a Denial of Service, obtain elevated privileges, or execute arbitrary code.	**Debian:** http://security.debian.org/dists/stable/updates/main/ **RedHat:** ftp://updates.redhat.com/ **Mandrake:** ftp://download.sourceforge.net/pub/mirrors/mandrake/updates **Caldera:** ftp://ftp.caldera.com/pub/updates/	Net-SNMP Multiple Vulnerabilities	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Multiple Vendors[33, 34]	Unix	Linux kernel 2.4.9, 2.4.14-2.4.17, 2.4.18pre-1-2.4.18pre-7	A vulnerability exists because the netfilter connection tracking code does not properly handle DCC chats, which could let a malicious user obtain unauthorized access.	**RedHat:** ftp://updates.redhat.com/ **Linux:** http://www.kernel.org/pub/linux/kernel/v2.4/linux-2.4.18.tar.gz	Linux Kernel IRC DCC Arbitrary Connection Access CVE Name: CAN-2002-0060	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[30] Bugtraq, February 19, 2002.
[31] Bugtraq, March 6, 2002.
[32] nCipher Security Advisory #2, February 27, 2002.
[33] Bugtraq, February 27, 2002.
[34] Red Hat Security Advisory, Rhsa-2002:028-13, February 27, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[35]	Multiple	Ascend RADIUS versions 1.16 & prior; Cistron RADIUS versions 1.6.5 & prior; Free RADIUS versions 0.3 & prior; Gnu RADIUS versions 0.95 & prior; ICRADIUS versions 0.18.1 & prior; Livingston RADIUS versions 2.1 & prior ; RADIUS (previously known as Lucent RADIUS) versions 2.1 & prior; RADIUS Client versions 0.3.1 & prior; XTRADIUS 1.1-pre1 & prior; YARD RADIUS 1.0.19 & prior	Several vulnerabilities exist: multiple implementations of the RADIUS protocol contain a digest calculation buffer overflow vulnerability, which could let a remote malicious user execute arbitrary code with the privileges of the victim RADIUS server or client, usually root; and a Denial of Service exists because vendor-specific attributes are not validated adequately.	Patches for the various vendors can be found at: http://www.cert.org/advisories/CA-2002-06.html	Multiple Vendor RADIUS Denial of Service and Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.

[35] CERT® Advisory CA-2002-06, March 4, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[36]	MacOS 7.X, 8.X, 9.X, MacOS X 10.X	Cab Company iCab Pre 2.7, 2.71; Microsoft Internet Explorer Macintosh Edition 4.5MRJ 2.2, 4.5MRJ 2.1.4, 4.5, 5.0; Netscape Netscape 4.77 Mac, 4.78 Mac; Omni Group OmniWeb 4.0.6, 4.1beta11; Opera Software Opera Web Browser 5.0 Mac	A vulnerability exists when the META refresh tag is used, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Multiple Vendor MacOS Browser Auto File Execution	High	Bug discussed in newsgroups and websites. Exploit has been published.
Multiple Vendors[37, 38, 39, 40, 41, 42, 43]	Unix	PHP 3.0.10-3.0.18, 4.0.1-4.0.7, 4.1.0, 4.1.1	Multiple vulnerabilities exist in the "php_mime_split" function due to the way multipart/form-data POST requests are handled, which could let a remote malicious user execute arbitrary code.	**Php.net:** http://www.php.net/downloads.php **Mandrake:** http://www.mandrakesecure.net/en/advisories/2002/MDKSA-2002-017.php?dis=8.0 **RedHat:** ftp://updates.redhat.com/ **SuSE:** ftp://ftp.suse.com/pub/suse **Trustix:** ftp://ftp.trustix.net/pub/Trustix/updates/ **Engarde:** http://ftp.engardelinux.org/pub/engarde/stable/updates/ **Debian:** http://security.debian.org/dists/stable/updates/main/	PHP POST Request Buffer Overflows	High	Bug discussed in newsgroups and websites. Exploit has been published and is being used to actively exploit this vulnerability. Vulnerability has appeared in the press and other public media.

[36] Bugtraq, February 27, 2002.
[37] e-matters GmbH Advisory 012002, February 27, 2002.
[38] Mandrake Linux Security Update Advisory, MDKSA-2002:017, February 28, 2002.
[39] RedHat Security Advisory, RHSA-2002:035-13, February 28, 2002.
[40] SuSE Security Announcement, SuSE-SA:2002:007, February 28, 2002.
[41] Trustix Secure Linux Security Advisory, 2002-0033, February 28, 2002.
[42] EnGarde Secure Linux Security Advisory, ESA-20020301-006, March 1, 2002.
[43] Debian Security Advisory, DSA 115-1, March 2, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [44, 45, 46]	Unix	National Science Foundation Squid Web Proxy 2.0-2.4 STABLE 1&2	Multiple Denial of Service vulnerabilities exist: a remote Denial of Service vulnerability exists if a host is allowed by http_access but denied by miss_proxy; and a remote Denial of Service vulnerability exists when snmpwalk is used to browse empty tables.	**National Science Foundation:** http://www.squid-cache.org/Versions/v2/2.4/squid-2.4.STABLE4-src.tar.gz **Conectiva:** ftp://atualizacoes.conectiva.com.br/7.0/ **Caldera:** ftp://stage.caldera.com/pub/security/openserver/CSSA-2002-SCO.7/ **SuSE:** ftp://ftp.suse.com/pub/suse/	Squid Multiple Denial of Service Vulnerabilities	Low	Bug discussed in newsgroups and websites.
Multiple Vendors [47, 48, 49, 50, 51, 52, 53, 54]	Unix	OpenSSH 2.1-2.3, 2.5-2.5.2, 2.9p2, 2.9p1, 2.9, 2.9.9-3.0.2	A vulnerability exists due to an off-by-one error in the channel code, which could let a malicious user execute arbitrary code or obtain root access.	**OpenSSH:** ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/ **Conectiva:** ftp://atualizacoes.conectiva.com.br/ **Engarde:** ftp://ftp.engardelinux.org/pub/engarde/stable/updates/ **SuSE:** ftp://ftp.suse.de/pub/suse **RedHat:** ftp://updates.redhat.com/ **Mandrake:** http://www.mandrakesecure.net/	OpenSSH Channel Code Off-By-One CVE Name: CAN-2002-0083	**High**	Bug discussed in newsgroups and websites.
Multiple Vendors [55, 56, 57,]	Unix	Apache-SSL Apache-SSL 1.40-1.46, mod_ssl mod_ssl 2.7.1-2.8.6	A buffer overflow vulnerability exists because large cache SSL sessions aren't handled properly, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.apache-ssl.org/ **mod_ssl**: http://www.modssl.org/source/mod_ssl-2.8.7-1.3.23.tar.gz **Trustix:** http://www.trustix.net/pub/Trustix/updates/ **Engarde:** http://ftp.engardelinux.org/pub/engarde/stable/updates **Conectiva:** ftp://atualizacoes.conectiva.com.br/	Apache Mod_SSL/ Apache-SSL Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

[44] Conectiva Linux Security Announcement, CLA-2002:464, February 27, 2002.
[45] Caldera International, Inc. Security Advisory, CSSA-2002-SCO.7, March 4, 2002.
[46] SuSE Security Announcement, SuSE-SA:2002:008, March 5, 2002.
[47] Conectiva Linux Security Announcement, CLA-2002:467, March 7, 2002.
[48] Debian Security Advisory, DSA-119-1, March 8, 2002.
[49] EnGarde Secure Linux Security Advisory, ESA-20020307-007, March 7, 2002.
[50] Mandrake Linux Security Update Advisory, MDKSA-2002:019, March 8, 2002.
[51] Red Hat Security Advisory, RHSA-2002:043-10, March 8, 2002.
[52] SuSE Security Announcement, SuSE-SA:2002:009, March 7, 2002.
[53] OpenPKG Security Advisory, OpenPKG-SA-2002.001, March 8, 2002.
[54] Pine Internet Security Advisory, PINE-CERT-20020301, March 7, 2002.
[55] Trustix Secure Linux Security Advisory, 2002-0034, February 28, 2002.
[56] EnGarde Secure Linux Security Advisory, ESA-20020301-005, March 1, 2002.
[57] Conectiva Linux Security Announcement, CLA-2002:465, March 4, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
National Science Foundation [58, 59, 60, 61, 62]	Unix	Squid Web Proxy 2.0-2.4	Multiple vulnerabilities exist: a memory leak vulnerability exists in the optional SNMP interface to Squid, which could let a malicious user cause a Denial of Service; a buffer overflow vulnerability exists if users are allowed to proxy ftp://URLs, which could let a remote malicious user cause a Denial of Service or possibly execute arbitrary code; and a vulnerability exists because the optional HTCP interface cannot be properly disabled from 'squid.conf,' which could let an unauthorized malicious user utilize cache resources.	**National Science Foundation:** http://www.squid-cache.org/Versions/v2/2.4/squid-2.4.STABLE4-src.tar.gz **FreeBSD:** ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/i386/packages-4-stable/www/squid-2.4_8.tgz **RedHat:** ftp://updates.redhat.com/6.2/en/os/ **Mandrake:** http://telia.dl.sourceforge.net/mirrorw/mandrake/updates/ **Conectiva:** ftp://atualizacoes.conectiva.com.br/	Squid Web Proxy Multiple Vulnerabilities	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
Noah Grey[63]	Unix	Greymatter 1.2, 1.21b, 1.21a, 1.21	A vulnerability exists in the 'gmrightclick-n.reg' file, which could let a remote malicious user obtain sensitive information and gain full control over the program.	**Workaround:** The vendor has stated that selecting the 'Clear And Exit' button on the relevant administration page will delete all registry files related to the bookmarklet process.	Greymatter Login/ Password Exposure	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Novell[64]	Windows	Groupwise 5.5	A vulnerability exists when a maliciously formatted web request is submitted that contains unexpected variables, which could let a remote malicious user to obtain sensitive information.	No workaround or patch available at time of publishing.	Novell GroupWise Web Access Path Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
OpenBB[65]	Multiple	OpenBB 1.0.beta 1, RC1&RC2	A Cross-Site Scripting vulnerability exists because images can be included in forum messages, which could let a malicious user execute arbitrary script code.	Patch available at: http://www.openbb.net/files/codeparse.zip	OpenBB Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Phorum[66]	Unix	Phorum 3.3.2	A vulnerability exists in the 'stats.php' script, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Phorum Sensitive Information	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[58] Squid Proxy Cache Security Update Advisory, SQUID-2002:1, February 21, 2002.
[59] FreeBSD Security Advisory, FreeBSD-SA-02:12, February 21, 2002.
[60] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:029-09, February 26, 2002.
[61] Mandrake Linux Security Update Advisory, MDKSA-2002:016-1, February 26, 2002.
[62] Conectiva Linux Security Announcement, CLA-2002:464, February 27, 2002.
[63] Securiteam, February 25, 2002.
[64] Bugtraq, February 28, 2002.
[65] Bugtraq, February 25, 2002.
[66] Securiteam, March 2, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Powie[67]	Unix	PForum 1.11-1.14	A Cross-Site Scripting vulnerability exists due to improper checking of user input, which could let a remote malicious user execute arbitrary script code.	Upgrade available at: http://www.powie.de/pm/pmagic.php?pmagic=pforum	Powie PForum Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Real Networks[68]	Windows 95/98/NT 4.0/2000, Unix	RealPlayer 6.0Win32, 6.0 Unix	A Directory Traversal vulnerability exists when a HTTP GET request is submitted, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	RealPlayer Directory Traversal	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Real Networks[69]	Windows 98/NT 4.0/2000, XP	RealPlayer 8.0 Win32	A Denial of Service vulnerability exists when maliciously constructed data is placed into a file named with the .mp3 extension	No workaround or patch available at time of publishing.	RealPlayer Denial of Service	Low	Bug discussed in newsgroups and websites.
ReBB[70]	Multiple	ReBB 1.0	A Cross-Site Scripting vulnerability exists because images can be included in forum messages, which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	ReBB Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Rich Media Technol-ogies[71]	Multiple	JustAdd Commerce Real Time Processing 5.0, Standard 5.0	A vulnerability exists because in the 'rtm.log' file because customer account information is stored in plaintext, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	JustAdd Commerce Information Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Rit Research Labs[72]	Windows 95/98/ME/ NT 4.0/2000, XP	The Bat! 1.53d	A remote Denial of Service vulnerability exists when attachments are saved separately from the message body.	Versions prior to 1.53d appear not to be vulnerable, so affected users may potentially downgrade their e-mail client to an earlier version	The Bat! Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
SH39[73]	Windows 2000	MailServer 1.2.1	A Denial of Service vulnerability exists when a malicious user connects to port 25 and submits an unusual amount of arbitrary data.	Upgrade available at: http://sh39.net/ms/MailServer.zip	MailServer Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Snitz Forums 2000[74]	Windows	Snitz Forums 2000 3.0, 3.1, 3.3.01-3.3.03, 3.3	A Cross-Site Scripting vulnerability exists because images can be included in forum messages, which could let a malicious user execute arbitrary script code.	Patch available at: http://forum.snitz.com/download.asp	Snitz Forums 2000 Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[67] Securiteam, March 2, 2002.
[68] Bugtraq, March 2, 2002.
[69] NtWaK0 Advisory, February 27, 2002.
[70] SecurityFocus, March 4, 2002.
[71] Securiteam, February 22, 2002.
[72] Bugtraq, February 26, 2002.
[73] Bugtraq, March 5, 2002.
[74] Bugtraq, February 27, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Summit Computer Networks[75]	Windows NT 4.0/2000	Lil'HTTP 2.1	A vulnerability exists because a malicious web request can be constructed, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Lil' HTTP Web Server Sensitive Information	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Sun Micro-systems, Inc.[76]	Unix	Cobalt RaQ 2.0-4.0	Multiple vulnerabilities exist: a remote Denial of Service vulnerability exists when excessively long requests are made to ' service.cgi' script; a remote Denial of Service vulnerability exists when a very long URL is received; a Directory Traversal vulnerability exists which could let a remote malicious user obtain sensitive information; and a Cross-Site Scripting vulnerability exists due to insufficient sanitation of input when HTML tags are passed to 'service.cgi' and 'alert.cgi' scripts, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Cobalt RaQ Multiple Vulnerabilities	Low/ Medium/ **High** (Medium for the Directory Traversal Vulner-ability and **High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.

[75] Securiteam, February 25, 2002.
[76] Securiteam, March 2, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Sun Microsystems, Inc.[77]	Windows, Unix	Windows Production Releases SDK & JRE 1.3.0_02 or earlier, SDK & JRE 1.2.2_010 or earlier, JDK & JRE 1.1.8_007 or earlier, Solaris Operating Environment Reference Releases SDK & JRE 1.2.2_010 or earlier, JDK & JRE 1.1.8_007 or earlier, Solaris Production Releases SDK & JRE 1.3.0_02 or earlier, SDK & JRE 1.2.2_10 or earlier, JDK & JRE 1.1.8_13 or earlier, Linux Production Releases SDK & JRE 1.3.0_02 or earlier, SDK & JRE 1.2.2_010 or earlier	A vulnerability exists in the Java Runtime Environment, which could let a remote malicious user take any action or combination of actions of his/her choosing.	Upgrade available at: http://java.sun.com/j2se	Sun Java Applet Browser Traffic Redirect CVE Name: CAN-2002-0058	**High**	Bug discussed in newsgroups and websites.
Symantec[78]	Windows 98/NT 4.0/2000, XP	Ghost Corporate Edition 7.0	A vulnerability exists because the username and password are stored in plaintext in the Windows registry, which could let a malicious user obtain sensitive information and elevated privileges.	No workaround or patch available at time of publishing.	Ghost Corporate Edition Plaintext Account Information	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[77] Sun Microsystems, Inc. Security Bulletin, SUN-00216, March 5, 2002.
[78] Bugtraq, February 26, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Symantec[79]	Multiple	LiveUpdate 1.4-1.7	A vulnerability exists because authentication credentials are stored in plaintext in the Windows registry, which could let a malicious user obtain elevated privileges.	No workaround or patch available at time of publishing.	LiveUpdate Plaintext Authentication	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Symantec[80]	Windows 98/ME/NT 4.0/2000, XP	Norton AntiVirus 2002 0.0	Multiple vulnerabilities exist: a vulnerability exists because it is possible to bypass Incoming Email Protection by injecting a NULL character into the MIME message; a vulnerability exists because a virus or malicious code can be embedded in certain non-RFC compliant MIME formats causing the scanning to terminate, which could let an infected e-mail to go undetected; a vulnerability exists because the '.nch' and '.dbx' file types, are excluded by default from scanning, which could let a malicious user take a Word macro virus, rename it with an .nch or a .dbx extension, and send it to a victim; and a vulnerability exists when different file names are provided in the Content-Type and Content-Disposition fields it is possible to exclude the file from being scanned.	Symantec is aware of this issue and suggests that the 'Auto Protect' feature will scan active files for viruses, Trojan horses, and worms. In addition, the 'Script Blocking' feature would further prevent any malicious scripts from running on the targeted system. An update for this issue will be released via LiveUpdate.	Symantec Norton AntiVirus Multiple Vulnerabilities	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
TalentSoft [81]	Windows 95/98/NT 4.0, Unix	TalentSoft Web+ Server 4.6, 5.0,	A buffer overflow vulnerability exists due to insufficient bounds checking, which could let a malicious user execute arbitrary code as SYSTEM.	Patches available at: ftp://ftp.talentsoft.com/download/webplus/windows/webplus_46_security_patch2.exe ftp://ftp.talentsoft.com/download/webplus/windows/webplus_50_security_patch.exe	TalentSoft Web+ Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Thatware[82]	Multiple	Thatware 0.5.3	A Cross-Site Scripting vulnerability exists due to the insecure use of the '$root_path' variable in some of the PHP scripts, which could let a remote malicious user to obtain sensitive information.	No workaround or patch available at time of publishing.	Thatware Cross-Site Scripting	Medium	Bug discussed in newsgroups and websites.

[79] Bugtraq, February 25, 2002.
[80] Edvice Security Services, March 7, 2002.
[81] NGSSoftware Insight Security Research Advisory, NISR01032002A, March 5, 2002.
[82] SecurityFocus, February 25, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
The XMB Group[83]	Multiple	XMB Forum 1.6x	A Cross-Site Scripting vulnerability exists because JavaScript and HTML can be entered in messages, which could let a remote malicious user execute arbitrary JavaScript.	No workaround or patch available at time of publishing.	XMB Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Tiny Software[84]	Windows 95/98/ME/ NT 4.0/2000, XP	Personal Firewall 2.0.15	A vulnerability exists when workstations that have been locked are scanned, which could let a malicious user obtain unauthorized access.	No workaround or patch available at time of publishing.	Tiny Personal Firewall Unauthorized Access	Medium	Bug discussed in newsgroups and websites.
Working Resources Inc.[85]	Windows 95/98/ME/ NT 4.0/2000, XP	Deerfield D2Gfx 1.0.2; BadBlue Enterprise Edition 1.5.6 Beta, 1.6 Beta, Personal Edition 1.5.6 Beta, 1.6 Beta	A Directory Traversal vulnerability exists when a specially crafted URL request is sent, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	BadBlue Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Working Resources Inc.[86]	Windows 95/98/ME/ NT 4.0/2000, XP	Deerfield D2Gfx 1.0.2; BadBlue 1.2.7, 1.2.8, 1.5, 1.5.6beta, 1.6.1beta, Enterprise Edition 1.5	Multiple Cross-Site Scripting vulnerabilities exist because URL input is not properly validated and filtered, which could let a remote malicious user execute arbitrary code and gain administrative access.	No workaround or patch available at time of publishing.	BadBlue Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites.
Xtell[87]	Unix	Xtell 2.6.1	Multiple vulnerabilities exist: several buffer overflow vulnerability exist when long strings are received by the client, which could let a remote malicious user execute arbitrary code; a Directory Traversal vulnerability exists because untrusted user input is allowed, which could let a remote malicious user obtain sensitive information; and a race condition vulnerability exists which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	XTell Multiple Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Exploit script has been published for the buffer overflow vulnerabilities. No exploit code is required for the Directory Traversal vulnerability..

[83] Bugtraq, February 22, 2002.
[84] Bugtraq, February 28, 2002.
[85] Strumpf Noir Society Advisories, February 26, 2002.
[86] Srumpf Noir Society Advisories, February 26, 2002.
[87] Securiteam, March 4, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Yahoo! Incorp-orated[88]	Windows 95/98/NT 4.0/2000, XP	Yahoo! Messenger 5.0	Multiple vulnerabilities exists: several remote Denial of Service vulnerabilities exist due to buffer overflows in the message field and IMvironment field of the Yahoo protocol; and a vulnerability exists which could allow a remote malicious user to send messages using a spoofed username.	No workaround or patch available at time of publishing.	Yahoo! Messenger Multiple Vulnerabilities	Low	Bug discussed in newsgroups and websites.
Zero One Tech[89]	Multiple	P100s PrintServer 5.31.13E	A vulnerability exists in the SNMP community read string even if the SNMP string has been disabled, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	ZOT P100s PrintServer SNMP Community String	Medium	Bug discussed in newsgroups and websites. Vulnerability may be exploited using a SNMP client.
Zope[90]	Unix	Zope 2.2.0-2.2.5, 2.3.0-2.3.3, 2.4.0-2.4.4b1, 2.5.0, 2.5.1b1	A vulnerability exists because the context of the user who creates a proxy role is not taken into account when determining access to the object with the proxy role assigned, which could let a malicious user obtain elevated privileges.	Hotfix available at: http://www.zope.org/Products/Zope/Hotfix_2002-03-01/Hotfix_2002-03-01.tgz	Zope Proxy Elevated Privileges	Medium	Bug discussed in newsgroups and websites.

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

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

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

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

[88] Bugtraq, February 21, 2002.
[89] Bugtraq, February 21, 2002.
[90] Bugtraq, March 1, 2002.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between February 21 and March 7, 2002, 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, 26 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
March 7, 2002	Winfingerprint-0.4.2.zip	Advanced remote Windows OS detection that includes these features: Determine OS using SMB Queries, PDC (Primary Domain Controller), BDC (Backup Domain Controller), NT member server, NT Workstation, SQLServer, Novell Netware Server, Windows for Workgroups, Windows 9X, Enumerate Servers, Enumerate Shares including Administrative ($), Enumerate Global Groups, Enumerate Users, Displays Active Services, Ability to Scan Network Neighborhood, and Ability to establish NULL IPC$ session with host.
March 6, 2002	Phpxpl.c	Script that exploits the remote root format string overflow vulnerability in Linux.
March 5, 2002	Amap-0.95.tar.gz	A scanning tool that allows you to identify the applications that are running on specific ports. It does this by connecting to the port(s) and sending trigger packets.
March 5, 2002	H07adv-Sphere.txt	Exploit for the SphereServer Ultima Online Roleplay Server Denial of Service vulnerability.
March 5, 2002	Onesixtyone-0.2.tar.gz	A SNMP scanner which utilizes a sweep technique to achieve good performance. It finds SNMP devices on your network and brute-forces the community strings using a dictionary.
March 4, 2002	Apache_php.c	Proof of concept exploit for the PHP Post POST Request Buffer Overflows vulnerability.
March 4, 2002	**Colbalt-raq-v4.txt**	**Exploits for the Cobalt RaQ Multiple Vulnerabilities.**
March 4, 2002	Elfsh-0.39b.tgz	An automated reverse engineering tool for the ELF format. Sophisticated output with cross references using .got, .ctors, .dtors, .symtab, .dynsym, .dynamic, .rel.* and many other with an integrated hexdump.
March 4, 2002	Ethereal-0.9.2.tar.gz	A GTK+-based network protocol analyzer, or sniffer, that lets you capture and interactively browse the contents of network frames.
March 4, 2002	**Xtell.c**	**Script which exploits the XTell Multiple Vulnerabilities.**
March 3, 2002	John-1.6.31-dev.tar.gz	John the Ripper is a very fast password cracker that is available for Unix, DOS, Win32, and BeOS.
February 27, 2002	**Ftp_dos.c**	**Script which exploits the Worldgroup Remote FTP Denial of Service vulnerability.**
February 27, 2002	**Ftp_www.c**	**Script which exploits the Worldgroup Remote FTP Denial of Service vulnerability.**
February 27, 2002	Mssmtp_dos.pl	Perl script which exploits the Microsoft SMTP Service Malformed Data Remote Denial of Service vulnerability.
February 26, 2002	Mimedefang-2.6.tar.gz	This is a flexible MIME e-mail scanner.
February 26, 2002	Nbtenum20.zip	NetBIOS Enumeration Utility v2.0 is a utility for Windows which can be used to enumerate NetBIOS information from one single host or an entire class C subnet. The information that is enumerated includes the account lockout threshold, local groups and users, global groups and users, and shares.

Date of Script (Reverse Chronological Order)	Script name	Script Description
February 26, 2002	Sendip-2.1.tar.gz	This is a commandline tool to send arbitrary IP packets. It has a large number of command line options to specify the content of every header of a TCP, UDP, ICMP, RIP or raw IPv4/IPv6 packet. It also allows any data to be added to the packet.
February 26, 2002	Snax.fixed.c	Exploit script for the UCD-SNMP vulnerability.
February 26, 2002	Snmp-audit-0.1.tar.gz	This is a Perl SNMP scanner that is a collection of scripts that can be used to scan an arbitrary set of networks.
February 25, 2002	Chap.pdf	This is a document that explains the weaknesses in the CHAP protocol as used within PPP and PPTP.
February 25, 2002	**Ex-callin.c**	**Script which exploits the Term Buffer Overflow vulnerability.**
February 25, 2002	Kismet-1.4.1.tar.gz	Kismet is a 802.11b wireless network sniffer.
February 25, 2002	Oat-source-1.1.0.zip	A set of tools that can be used to audit Oracle databases running on the Microsoft Windows platform.
February 25, 2002	Sortelnetd.tgz	Sortelnetd is a working telnetd 0.17 exploit.
February 25, 2002	Sqlat-src-1.0.0.tar.gz	SQLAT is a suite of tools that could be useful for pen-testing a MS SQL Server. The tools do dictionary attacks, upload files, read registry and dump the SAM.
February 21, 2002	**Ans.pl**	**Perl script which exploits the Avenger's News System Directory Traversal and Remote Command Execution vulnerability.**

Trends

The National Infrastructure Protection Center is aware of potential vulnerabilities existing within the Simple Network Management Protocol (SNMP) -- a protocol used by routers, switches and hubs on the Internet and other related equipment. For more information, see NIPC ALERT 02-001, located at: http://www.nipc.gov/warnings/alerts/2002/02-001.htm.
Numerous vulnerabilities have been reported in multiple vendors' SNMP implementations. For more information, see CERT® Advisory CA-2002-03, located at: http://www.cert.org/advisories/CA-2002-03.html.
The National Infrastructure Protection Center (NIPC) has received reporting that infrastructure related information, available on the Internet, is being accessed from sites around the world. While in and of itself this information is not significant, it highlights a potential vulnerability. For more information, see NIPC ADVISORY 02-001, located at: http://www.nipc.gov/warnings/advisories/2002/02-001.htm.
The CERT/CC has received credible reports of scanning and exploitation of Solaris systems running the CDE Subprocess Control Service buffer overflow vulnerability identified in CA-2001-31 and discussed in VU#172583. For more information, see CERT® Advisory CA-2002-01, located at: http://www.cert.org/advisories/CA-2002-01.html.
NIPC has updated their advisory, NIPC Advisory 01-030, regarding what Microsoft refers to as a critical vulnerability in the universal plug and play (UPnP) service in Windows. For more information see, NIPC ADVISORY 01-030.3, located at: www.nipc.gov/warnings/advisories/2001/01-030-2.htm.

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.*

VBS/Britney-A (Aliases: VBS/Breetnee, VBS/BritneyPic@MM, worm/BritneyPic) (Visual Basic Script Worm): This is a mass-mailing worm which spreads via both Microsoft Outlook and IRC networks. It copies itself to BRITNEY.CHM in the Windows folder and then e-mails itself to all addresses in the Outlook address list. The e-mails will have the following characteristics:

Subject Line: RE: Britney Pics
Body Text: Take a look at these pics ...
Attachment: BRITNEY.CHM

The worm requires ActiveX to be enabled for the VBS to run and prompts the user to enable ActiveX with the message "Enable ActiveX To See Britny Pictures." VBS/Britney-A searches the C:, D:, and E: drives for the presence of a file called MIRC.INI. If it finds this file, the worm creates a SCRIPT.INI file, which will then attempt to send copies of the files to other IRC users.

W32/CTX-A (Aliases: Win32.CTX.6886, W95/CTX.7207, W32/CTX, PE_Cholera.CTX) (Win32 File Virus): This is a Win32 executable file virus that uses several techniques designed to evade detection by anti-virus software products. If the current day and hour are the same as those at the time of infection, and the current month is six months after the month of infection, then the virus will change the Desktop background color.

W32/Gibe-A (Alias: W32/Gibe@MM) (Win32 File Worm): This is a worm that is attached to a message that appears to come from Microsoft. The e-mail will have the subject line: "Internet Security Update." The e-mail message leads you to believe that it is the latest version of a security update. The update will eliminate all known security vulnerabilities affecting Internet Explorer and MS Outlook/Express and contains descriptions of several well-known vulnerabilities. If the attachment is run, it will display the message "This will install a Microsoft Security Update. Do you wish to continue?" It then copies itself to the q216309.exe in the Windows folder and vtnmsccd.dll in the Windows system folder. The worm also drops and executes the bctool.exe, winnetw.exe, and gfxacc.exe in the Windows folder and creates the file 02_n803.dat in which it stores information about e-mail recipients. Bctool.exe and winnetw.exe attempt to send out the e-mails. Gfxacc.exe runs as a background process and opens port 12387, which could allow an intruder to gain remote access and control over the machine. The worm sets the following registry keys:

HKLM\Software\AVTech\Settings\Default Address = <default address>
HKLM\Software\AVTech\Settings\DefaultServer = <default server>
HKLM\Software\AVTech\Settings\Installed = ...by Begbie
HKLM\Software\Microsoft\Windows\CurrentVersion\Run\3dfx Acc = <path to gfxacc.exe>
HKLM\Software\Microsoft\Windows\CurrentVersion\Run\LoadDBackup = <path to bctool.exe>

W32/MyLife-A (Win32 Worm): This worm arrives in an e-mail. When run, the worm will copy itself to C:\windows\system\My Life.scr and add the registry key:

HKCU\Software\Microsoft\Windows\CurrentVersion\Run\strmgr = C:\windows\system\My Life.scr.

It will then e-mail itself to addresses from the Outlook address book. Finally the worm will display a painting of a young girl.

W32/Sharp-A (Alias: W32/Sharpie@mm) (Win32 File Virus): This virus arrives in an e-mail message that contains an attachment, MS02-010.EXE. When W32/Sharp-A is executed, it copies itself to C:\MS02-010.EXE and drops and executes sharp.vbs in the current directory. The script sends the e-mail to everyone in the Outlook address book. If the virus detects the Microsoft .NET runtime, it drops and executes the file cs.exe in the Windows directory. This file infects .EXE files with W32/Sharp-A and creates the file sharp.vbs in the Windows startup folder. This file displays a message box with the title "Sharp" and the text "You're infected with Win32.HLLP.Sharp, written in C#, by Gigabyte/Metaphase."
The virus also creates the registry key HKLM/Software/Sharp that contains the name of the viral file that was run.

W32.Fully.3424 (Win32 Virus): This is a Windows 32-bit virus that appears to have been written in assembly language. The virus contains several bugs and is unlikely to spread.

W32.Simile (Alias: W32.Etap) Win32 Virus): This is a very complex virus that uses entry-point obscuring, metamorphism, and polymorphic decryption. It infects files in folders on all fixed and remote drives that are mapped at the time that the virus is executed. The virus contains no destructive payload, but infected files may display messages on certain dates.

W97M.SMDM.A (Word 97 Macro Virus): This is a macro virus that only replicates to the Microsoft Word Normal.dot template. On the 5th of March, June, September, or December it will add instructions to the Autoexec.bat file to delete all files and folders on the C drive upon the next reboot.

WM97/Ethan-EO (Word 97 Macro Virus): This is a variant of the WM97/Ethan Word macro virus. This virus may change the file properties of infected Word documents as follows:

Title: Ethan Frome
Author: EW/LN/CB
Keywords: Ethan

WM97/Marker-HW (Word 97 Macro Virus): This virus has been reported in the wild. It is a corrupted but viable variant of WM97/Marker-C.

WM97/Onex-G (Word 97 Marco Virus): WM97/Onex-G is a Word macro virus. There is a 1 in 8 chance that the virus will repeatedly minimize and maximize the active Word document.

WORM_ALCARYS.B (Aliases: SEXSOUND.C, SEXSOUND, W32.Alcarys.B@mm, ALCARYS.B, ALCARYS) (Internet Worm): This destructive, memory-resident worm propagates via e-mail. It overwrites *.EXE, *.COM, *.SCR, and *.HTML files. It also has macro components.

WORM_Alcarys.C (Aliases: W32.Alcays.C, W32.Palco.A) (Internet Worm): This virus attempts to disguise itself as an "anti-malicious macro" macro. When it is executed, the virus inserts a macro module into the Normal.dot file. This macro module inserts two components into Microsoft Word documents as they are closed: an executable component of the virus and a macro component that runs the executable component.

WORM_BEZILOM.A (Aliases: BEZILOM.A, Win32.HLLW.Bezilom, Win32.HLLW.Bezilom.dr, W32/Bezilom-A) (Internet Worm): This worm drops WORM_BEZILOM.A1 and WORM_BEZILOM.A2. To propagate, it propagates by writing itself to floppy disks accessed on the infected system.

WORM_FBOUND.A (Aliases: I-WORM.ZCRYPT, CRYPTZ.A, CRYPTZ, Win32.Fbound) (Internet Worm): This worm uses its own SMTP engine to mass-mail copies of itself to all e-mail addresses listed in the infected user's Windows Address book. It arrives as the attachment CHECK.EXE or IMPORTANT.ZIP. CHECK.EXE is a copy of the worm and IMPORTANT.ZIP is a password protected zip file containing CHECK.EXE.

WORM_FBOUND.B (Aliases: FIDAO.A, FIDAO, W32/Fbound.b@MM, Win32/Japanize.Worm, I-Worm.Zircon.B (Internet Worm): This worm mass-mails itself to all e-mail addresses listed in the infected user's Windows Address Book (WAB). It arrives in an e-mail with a subject that it randomly selects from a group of Japanese language phrases if the e-mail address of the recipient ends with .jp. Otherwise, the subject is “Important.” The name of the attachment it arrives with is PATCH.EXE.

WORM_GLUTON.A (Aliases: GLUTON.A, GLUTON) (Internet Worm): This Internet worm uses Internet Relay Chat (IRC) to propagate copies of itself to users connected to the same IRC channel as the infected user.

WORM_KITRO.A (Aliases: I-Worm.Kitro, KITRO.A, KITRO) (Internet Worm): This UPX-compressed worm, compiled in Delphi, uses Microsoft MSN Messenger to propagate. It arrives as the file "PSYCHO.SCR."

WORM_KLEZ.E (Aliases: W32.Klez.E@mm, KLEZ) (Internet Worm): This destructive mass-mailing worm propagates copies of itself across network drives. Upon execution, it drops two executable files, WINK*.EXE and WQK.EXE, in the Windows System folder. It also creates registry entries that allow it to run at system startup. This worm terminates processes, and occasionally deletes files associated with certain antivirus programs. On the sixth (6) day of every odd-numbered month (January, March, May, July, September, and November) it overwrites files with the following extensions: TXT, HTM, HTML, WAB, DOC, XLS, CPP, C, PAS, MPEG, MPG, BAK, MP3, and JPG.

WORM_SHARPEI.A (Aliases: BLUNT.A, Blunt, Sharp, Win32.HLLP.Sharp, VBS_SHARPEI.A) (Internet Worm): This non-destructive worm propagates via Microsoft Outlook, and arrives in an e-mail with the attachment "MS02-010.exe." This worm is only activated if the Microsoft .NET Framework is installed.

WORM_STOPIN.A (Aliases: I-Worm.Stopin, STOPIN, STOPIN.A) (Internet Worm): This is a UPX-compressed worm compiled in Borland C++ that propagates via e-mail. It can disable some antivirus and monitoring programs.

WORM_WARGA.A (Aliases: W32/Warga@MM, WARGA.A, WARGA) (Internet Worm): This Internet worm uses Microsoft Outlook to propagate by sending e-mails to all addresses in the infected user's address book, with itself as an attachment. It arrives as the attachment "Article.doc.exe."

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table starts with Trojans discussed in CyberNotes #2002-01, and items will be 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 #
APStrojan.sl	N/A	CyberNotes-2002-03
Backdoor.EggHead	N/A	CyberNotes-2002-04
Backdoor.G_Door.Client	**N/A**	**Current Issue**
Backdoor.IISCrack.dll	N/A	CyberNotes-2002-04
Backdoor.NetDevil	N/A	CyberNotes-2002-04
Backdoor.Palukka	N/A	CyberNotes-2002-01
Backdoor.Subwoofer	N/A	CyberNotes-2002-04
Backdoor.Surgeon	N/A	CyberNotes-2002-04
Backdoor.Systsec	N/A	CyberNotes-2002-04
BackDoor-AAB	N/A	CyberNotes-2002-02
BackDoor-FB.svr.gen	N/A	CyberNotes-2002-03
BKDR_SMALLFEG.A	N/A	CyberNotes-2002-04
DlDer	N/A	CyberNotes-2002-01
DoS-Winlock	N/A	CyberNotes-2002-03
Hacktool.IPStealer	N/A	CyberNotes-2002-02
Irc-Smallfeg	N/A	CyberNotes-2002-03
JS/Seeker-E	N/A	CyberNotes-2002-01
JS_EXCEPTION.GEN	N/A	CyberNotes-2002-01
SecHole.Trojan	N/A	CyberNotes-2002-01

Trojan	Version	CyberNotes Issue #
Troj/Download-A	N/A	CyberNotes-2002-01
Troj/ICQBomb-A	**N/A**	**Current Issue**
Troj/Msstake-A	N/A	CyberNotes-2002-03
Troj/Optix-03-C	N/A	CyberNotes-2002-01
Troj/Sub7-21-I	N/A	CyberNotes-2002-01
Troj/WebDL-E	N/A	CyberNotes-2002-01
TROJ_CYN12.B	N/A	CyberNotes-2002-02
TROJ_DANSCHL.A	N/A	CyberNotes-2002-01
TROJ_DSNX.A	N/A	CyberNotes-2002-03
TROJ_FRAG.CLI.A	N/A	CyberNotes-2002-02
TROJ_ICONLIB.A	N/A	CyberNotes-2002-03
TROJ_SMALLFEG.DR	N/A	CyberNotes-2002-04
Trojan.Badcon	N/A	CyberNotes-2002-02
Trojan.StartPage	N/A	CyberNotes-2002-02
Trojan.Suffer	N/A	CyberNotes-2002-02
VBS.Gascript	N/A	CyberNotes-2002-04
VBS_THEGAME.A	N/A	CyberNotes-2002-03
W32.Alerta.Trojan	**N/A**	**Current Issue**

Backdoor.G_Door.Client (Aliases: Backdoor.G_Door.b, Backdoor.G_Door.d): This is a utility that is used to control the Backdoor.G_Door Trojan. This utility is nonviral, and it does not cause harm to the malicious user who is using it to control the Trojan. However, because deployment of this utility is usually harmful to the victim of an attack, it is therefore considered a threat by network administrators.

W32.Alerta.Trojan: This is a Trojan that displays messages in Spanish. The messages have a pink background that covers the entire Windows desktop.

Troj/ICQBomb-A: This is a tool that can be used to instantly send a large number of messages to an ICQ user's account. The malicious user simply needs to enter the victim's unique ICQ user id number, a message to send and the number of times they wish that message to be delivered.