



National Infrastructure Protection Center CyberNotes

Issue #2002-09

May 6, 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 April 16 and May 3, 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
Own f0rum ¹	Multiple	Own f0rum 2.1	A vulnerability exists because user-supplied input is not properly stripped of scripting commands, which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	Own f0rum Script Injection	High	Bug discussed in newsgroups and websites.
3Com ²	Multiple	3CDaemon 2.0 revision 10	A buffer overflow vulnerability exists when an unusually large amount of data is submitted to the FTP server, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	3CDaemon Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit script has been published.

¹ SecurityFocus, April 29, 2002.

² Bugtraq, April 30, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Acme Labs ³	Unix	tthttpd 2.20 b	A Cross-Site Scripting vulnerability exists because URLs are not properly checked when generating error pages, which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	tthttpd Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Exploit has been published.
Admanager ⁴	Multiple	Admanager 1.1	Several vulnerabilities exist: a vulnerability exists because the 'add.php3' script does not require authentication, which could let a remote malicious user change banner advertisement content; and a vulnerability exists because script code is not filtered from URL parameters of the 'add.php3' script, which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	Admanager Multiple Vulnerabilities	Medium/ High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. The 'add.php3' script authentication vulnerability can be exploited via a web browser.
America OnLine ⁵	Windows 95/98/ME/NT 4.0/2000, XP	Instant Messenger 2.0 N, 2.0.912, 2.0.996, 2.1.1236, 2.5 .1598, 2.5 .1366, 3.0 N, 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, 4.5-4.7, 4.7.2480, 4.8 .2646, 4.8.2616	A vulnerability exists which could let a remote malicious user intercept connections and steal whatever data the AIM client is transmitting.	<u>Temporary workaround (Bugtraq):</u> Users may change the settings of their AIM client so that different ports are used for direction connections and file transfers.	Instant Messenger Data Interception	Medium	Bug discussed in newsgroups and websites.
Annuaire ⁶	Multiple	Annuaire 1.0	A vulnerability exists because password information is stored in a world readable file, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Annuaire Sensitive Information	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

³ SecurityFocus, April 25, 2002.

⁴ SecurityFocus, April 29, 2002.

⁵ Bugtraq, April 21, 2002.

⁶ SecurityFocus, April 25, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Apache Software Foundation	Unix	Tomcat 3.0, 3.1, 3.1.1, 3.2, 3.2.1-3.2.4, 3.3, 3.3.1, 4.0, 4.0.1-4.0.3, 4.1	A vulnerability exists in a some of the example classes (SnoopServlet and TroubleShooter), which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Tomcat Servlet Path Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Apache Software Foundation	Unix	Tomcat 4.1	A vulnerability exists when malformed requests are submitted, which could let a remote malicious user obtain the absolute path to the web root.	No workaround or patch available at time of publishing.	Tomcat Path Information Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
ATGuard ⁹	Multiple	Personal Firewall 3.2	A vulnerability exists when the restricted web application is renamed with an authorized application name, which could let a malicious user bypass the security restrictions.	No workaround or patch available at time of publishing.	Personal Firewall Connection Restriction Bypass	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
BEA Systems ¹⁰	Windows NT 4.0/2000, Unix	WebLogic Server 4.5.2, 4.5.2 SP1&2, 5.1, 5.15.1 SP1-SP9, 6.1, 6.1SP1&2	A vulnerability exists due to difficulties in parsing certain types of malformed requests, which could let a malicious user obtain JSP script source code.	Patch available at: ftp://ftpna.bea.com/pub/releases/security/	WebLogic Server URL Parsing Sensitive Information	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
BEA Systems ¹¹	Windows NT 4.0/2000, Unix	Weblogic Server 6.1 SP2	A vulnerability exists because the server incorrectly parses certain type of URL requests, which could let a malicious user cause a Denial or Service and obtain sensitive information.	No workaround or patch available at time of publishing.	WebLogic Server URL Parsing Path Disclosure	Low/ Medium (Medium if sensitive information is obtained)	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
BigB ¹²	Multiple	AutoLog 27/07/01	A vulnerability exists when a specially crafted cookie is sent that contains an arbitrary IP address, which could let a remote malicious user cause a false IP to be logged by the script.	No workaround or patch available at time of publishing.	AutoLog IP Spoofing	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

⁷ CHINANSL Security Team, April 22, 2002.

⁸ Securiteam, April 20, 2002.

⁹ ITCP Advisory 13, April 29, 2002.

¹⁰ BEA Security Advisory, BEA02-03.03, April 30, 2002.

¹¹ KPMG-2002016, April 30, 2002.

¹² SecurityFocus, April 30, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Blahz-DNS ¹³	Unix	Blahz-DNS 0.2	A vulnerability exists when scripts included with Blahz-DNS are directly called, which could let a malicious user bypass authentication and gain full access.	Upgrade available at: http://prdownloads.sourceforge.net/blahzdns/blahzdns-0.25.tar.gz	Blahz-DNS Authentication Bypass	High	Bug discussed in newsgroups and websites. Exploit has been published.
CGIScript.NET ¹⁴	Multiple	csMailto	A vulnerability exists because form configuration data is stored in hidden fields in the actual form, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	csMailto Remote Command Execution	High	Bug discussed in newsgroups and websites. Exploits have been published.
CIDER ¹⁵	Unix	Shadow 1.5, 1.6	A vulnerability exists because shell metacharacters are not adequately filtered, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	Shadow Remote Command Execution CVE Name: CAN-2002-0091	High	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Cisco Systems ¹⁶	Windows XP	VPN Client 3.1 & 3.5.1 for Windows	A vulnerability exists because during the installation process the user is advised to change the security settings of unsigned drivers and Windows security settings. If the setting is not reset after the installation process, this could possibly impact system security settings.	As a workaround, users may disregard this advice, or reset the security settings when the VPN Client installation is complete.	VPN Client for Windows Dialog Instructions	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
disipoll ¹⁷	Multiple	disipoll 0.9	A vulnerability exists in the voting poll feature, which could let a malicious user vote more than once.	No workaround or patch available at time of publishing.	disipoll Cookie Security Bypass	Medium	Bug discussed in newsgroups and websites.
DNSTools Software ¹⁸	Unix	DNSTools 2.0 Beta 4, 2.0 Beta 3	A vulnerability exists because an artificially constructed URL can define variables used to track user authentication and administration access, which could let a remote malicious user obtain administrative access.	Update available at: http://www.dnstools.com/dnstools_2.0b5.tar.gz	DNSTools Authentication Bypass	High	Bug discussed in newsgroups and websites. Exploits have been published.
Ethereal Group ¹⁹	Windows 95/98/ME/ NT 4.0, Unix	Ethereal 0.9.1, 0.9.2	A Denial of Service vulnerability exists when malformed ASN.1 messages are parsed.	Upgrade available at: http://www.ethereal.com/distribution/ethereal-0.9.3.tar.gz	Ethereal ASN.1 Denial of Service	Low	Bug discussed in newsgroups and websites.

¹³ PPP-Design Advisory, April 28, 2002.

¹⁴ Bugtraq, April 23, 2002.

¹⁵ eSecurityOnline Security Advisory 2408, April 29, 2002.

¹⁶ SecurityFocus, April 17, 2002.

¹⁷ SecurityFocus, April 25, 2002.

¹⁸ PPP-Design Advisory, April 28, 2002.

¹⁹ Conectiva Linux Security Announcement, CLA-2002:474, April 25, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Foundstone ²⁰	Windows 98/ME/NT 4.0/2000	FScan 1.12	A vulnerability exists because banner data that is supplied by scanned hosts is not properly scanned, which could let a malicious user execute arbitrary code.	Upgrade available at: http://www.foundstone.com/knowledge/proddesc/fscan.html	FScan Banner Format String	High	Bug discussed in newsgroups and websites.
GNU ²¹	Unix	screen 3.9.4, 3.9.8-3.9.11	A buffer overflow vulnerability exists due to insufficient bounds checking by the Braille module, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Screen Braille Module Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit script has been published.
GNU/ Pippmail ²²	Unix	GNU Mailman 1.0, 2.0 beta3-beta5, 2.0.5-2.0.8, 2.0-2.0.3, 2.0.4, 2.0.9, 2.0.10, 2.1 b1; Pippmail 0.05	A vulnerability exists due to insecure permissions, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Pippmail/ Mailman Insecure Permissions	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Gregory Trubetskoy ^{23, 24}	Unix	mod_python 2.7-2.7.7	A vulnerability exists in the 'mod_python' publisher, which may allow a malicious user to access any function that has been included by a previously called script.	Update available at: http://www.modpython.org/dist/mod_python-2.7.8.tgz RedHat: ftp://updates.redhat.com/Conectiva:ftp://atualizacoes.conectiva.com.br/	mod_python Imported Module Access CVE Name: CAN-2002-0185	Medium	Bug discussed in newsgroups and websites.
Hewlett Packard Systems ²⁵	Unix	HP-UX 11.0, 11.11, HP-UX (VVOS) 11.0 4	A Denial of Service vulnerability exists because the password files can be corrupted using the passwd(1) command.	Patch available at: http://itrc.hp.com PHCO_26904 PHCO_25527 PHCO_24839	HP-UX Password File Corruption	Low	Bug discussed in newsgroups and websites.
Hewlett Packard Systems ²⁶	Multiple	MPE/iX 6.0, 6.5, 7.0	A remote Denial of Service vulnerability exists when a malformed packet is received.	Patch available at: http://itrc.hp.com HP Patch NSTGDB0 HP Patch NSTGDB1 HP Patch NSTGDB2	MPE/iX Denial of Service	Low	Bug discussed in newsgroups and websites.
Hewlett Packard Systems ²⁷	Multiple	MPE/iX 6.0, 6.5, 7.0	A vulnerability exists because 'FTPSRVR' does not properly validate certain commands, which may let a malicious user obtain unauthorized access and execute arbitrary commands.	Patch available at: http://itrc.hp.com HP Patch FTPGD91A HP Patch FTPGD92A HP Patch FTPGD93A	MPE/iX FTPSRVR Arbitrary Shell Command Execution	High	Bug discussed in newsgroups and websites.

²⁰ KPMG-2002014, April 19, 2002.

²¹ Gobbles Security Alert, April 21, 2002.

²² Bugtraq, April 16, 2002.

²³ RedHat Security Advisory, RHSA-2002:070-06, May 2, 2002.

²⁴ Conectiva Linux Security Announcement, CLA-2002:477, May 3, 2002.

²⁵ Hewlett-Packard Company Security Bulletin, HPSBUX0204-191, April 23, 2002.

²⁶ Hewlett-Packard Company Security Bulletin, HPSBMP0204-013, April 18, 2002.

²⁷ Hewlett-Packard Company Security Bulletin, HPSBMP0204-014, May 1, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
IcrediBB ²⁸	Multiple	IcrediBB Beta 1.1	A vulnerability exists due to inadequate script code filtering from forum message fields, which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	IcrediBB Script Injection	High	Bug discussed in newsgroups and websites. Exploit has been published.
Ikonboard.com ²⁹	Multiple	Ikonboard 2.1.9	A vulnerability exists if HTML is enabled, which could let a malicious user execute arbitrary JavaScript code.	No workaround or patch available at time of publishing.	Ikonboard Message Body Cross Agent Scripting	High	Bug discussed in newsgroups and websites. There is no exploit code required.
Intel Corporation ³⁰	Multiple	D845BG Motherboard P05-0024, P04-0023, P03-0021, P02-0015, P01-0012, D845HV Motherboard P11-0040, P10-0038, P09-0035, P08-0031, P07-0029, P06-0024, P05-0022, P04-0018, D845PT Motherboard P05-0024, P04-0023, P03-0021, P02-0015, P01-0012, D845WN Motherboard P11-0040, P10-0038, P09-0035, P08-0031, P07-0029, P06-0024, P05-0022, P04-0018	A vulnerability exists when a malicious user hits the F8 key during the POST process because they are presented with a "Please select boot device" dialog, enabling them to boot off of any bootable device in the PC (FDD, HDD, CDROM, Network, etc.).	Upgrade available at: ftp://download.intel.com/design/motherbd	Intel D845 Motherboard BIOS Series Boot Media	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

²⁸ Telhack 026 Inc. Security Advisory #2, April 19, 2002.

²⁹ Bugtraq, April 24, 2002.

³⁰ Bugtraq, April 25, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Internet Security Systems ³¹	Multiple	RealSecure Network Sensor 5.0 XPU 3.4, 5.5 XPU 3.4, 5.5.1 XPU 3.4, 5.5.2 XPU 3.4, 6.0 XPU 3.4, 6.5	A remote Denial of Service vulnerability exists when specially crafted packets are sent to network segments monitored by RealSecure.	Update available at: http://www.iss.net/download/ .	RealSecure DHCP Remote Denial of Service	Low	Bug discussed in newsgroups and websites.
Jon Howell ³²	Multiple	Faq-O-Matic 2.711, 2.712	A Cross-Site Scripting vulnerability exists because malformed queries that contain HTML or script are not properly filtered, which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	Faq-O-Matic Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Exploit has been published.
KillerVault ³³	Multiple	Kv Guestbook 1.0	A Cross-Site Scripting vulnerability exists because URL parameters are not properly filtered from script code, which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	Kv Guestbook Cross-Site Scripting	High	Bug discussed in newsgroups and websites.
KTH ³⁴	Unix	Kerberos 4 1.0.2-1.0.4, 1.1.1	A vulnerability exists in the eBones FTP client due to insufficient bounds checking, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Kerberos4 FTP Bounds Checking	High	Bug discussed in newsgroups and websites. Exploit script has been published.
LEVCGI.COM ³⁵	Unix	MyGuestbook 1.0	A vulnerability exists because script code is not adequately filtered from various fields, which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	MyGuestbook Script Injection	High	Bug discussed in newsgroups and websites. Exploit has been published.
Livre Dor ³⁶	Multiple	Livre Dor' 1.1	A vulnerability exists because the 'config.inc' and 'connexion.inc' files are world readable, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Livre Dor' Information Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Logitech ³⁷	Windows NT 4.0/2000, XP	Cordless Freedom iTouch Keyboard, Cordless iTouch Keyboard	A Denial of Service vulnerability exists when the computer is locked and a malicious user presses one of the buttons a numerous amount of times.	No workaround or patch available at time of publishing.	iTouch Keyboard Command Keys Locked Console Bypass	Low	Bug discussed in newsgroups and websites. There is no exploit code required.

³¹ Internet Security Systems Security Advisory, April 30, 2002.

³² Bugtraq, April 19, 2002.

³³ SecurityFocus, April 30, 2002.

³⁴ Securiteam, April 26, 2002.

³⁵ Securiteam, May 1, 2002.

³⁶ SecurityFocus, April 29, 2002

³⁷ Bugtraq, May 2, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Ludovic STIOT ³⁸	Multiple	Secure 17/09/2001	A vulnerability exists when a specially crafted cookie is sent to the Secure script, which could let a malicious user bypass authentication and obtain unauthorized access.	No workaround or patch available at time of publishing.	Secure Authentication Bypass	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Macro-media ³⁹	Multiple	Flash 6.0	A buffer overflow vulnerability exists if an oversized parameter is included in the URL passed to the ActiveX component, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.macromedia.com/shockwave/download/index.cgi?P1_Prod_Version=ShockwaveFlash	Flash ActiveX Buffer Overflow	High	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Matu ⁴⁰	Multiple	Matu FTP 1.74	A buffer overflow vulnerability exists when a FTP server '220' response is of excessive length, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Matu FTP Client Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Messagerie ⁴¹	Multiple	Messagerie 1.0	Several vulnerabilities exist; a vulnerability exists when a specially crafted URL is submitted, which could let a remote user access user accounts; and a vulnerability exists because file including is permitted, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Messagerie Denial of Service	Medium/ High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft ⁴²	Windows NT	Baseline Security Analyzer 1.0	A vulnerability exists because a report is created as a plain text file and stored in a predictable location after the system is analyzed for security vulnerabilities, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Baseline Security Analyzer Plaintext File	Medium	Bug discussed in newsgroups and websites. Several Proof of Concept exploits have been published. Vulnerability has appeared in the press and other public media.
Microsoft ⁴³	Windows 95/98/ME/NT 4.0/2000	Internet Explorer 5.0, 5.0.1 SP1&2, 5.5, 5.5SP1&2, 6.0	A Denial of Service vulnerability exists due to an indirect recursive calling of an onError event.	No workaround or patch available at time of publishing.	Internet Explorer Recursive Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.

³⁸ SecurityFocus, April 30, 2002.

³⁹ Bugtraq, May 2, 2002.

⁴⁰ Bugtraq, April 22, 2002.

⁴¹ SecurityFocus, April 30, 2002.

⁴² Finjan Software Security Advisory, April 24, 2002.

⁴³ Bugtraq, April 24, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft ⁴⁴	Windows 95/98/ME/NT 4.0/2000	Internet Explorer 5.0, 5.5, 5.5SP1, 6.0	A Denial of Service vulnerability exists due to an error in handling certain self-referential <OBJECT> definitions in HTML documents.	No workaround or patch available at time of publishing.	Internet Explorer Self-Referential Object Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft ⁴⁵	Windows 95/98/ME/NT 4.0/2000	Internet Explorer 6.0, Outlook Express 6.0	A Denial of Service vulnerability exists because malformed XBM image files in webpages are not properly handled.	No workaround or patch available at time of publishing.	Internet Explorer/ Outlook Express XBM Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Microsoft ⁴⁶	Windows	Outlook 2000, 2002	A vulnerability exists because of a flaw in how the WordMail editor handles scripting contained in HTML when an e-mail message is replied to or forwarded, which could let a remote malicious user execute arbitrary script 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/MS02-021.asp	Outlook E-mail Editor Script Execution CVE Name: CAN-2002-1056	High	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Microsoft ⁴⁷ <i>Updated Advisory released⁴⁸</i>	Windows NT 4.0/2000, XP	Outlook 2002	Two vulnerabilities exist: a vulnerability exists because it is possible to embed active content in HTML mail, which could let a malicious user execute arbitrary code; and a vulnerability exists in the MS spreadsheet component in the 'Host()' function, which could let a malicious user write arbitrary files. <i>Microsoft released a security bulletin MS02-021 which resolves part of the vulnerabilities. However, their patch fixes only the Outlook and Word issues and does not fix at least the exploit path through Excel.</i>	No workaround or patch available at time of publishing.	Outlook 2002 HTML Mail Script Execution & Host(). SaveAs() File Creation	High	Bug discussed in newsgroups and websites. Exploits have been published.

⁴⁴ Securiteam, April 20, 2002.

⁴⁵ Bugtraq, April 30, 2002.

⁴⁶ Microsoft Security Bulletin, MS02-021, April 25, 2002.

⁴⁷ Georgi Guninski Security Advisory #53 Version 2.0, April 3, 2002.

⁴⁸ Georgi Guninski Security Advisory #53 Version 3.0, April 28, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft ⁴⁹ <i>Bulletin has been revised⁵⁰</i>	Windows NT 4.0/2000	Windows 2000 Advanced Server, 2000 Advanced Server SP1&2, 2000 Datacenter Server, 2000 Datacenter Server SP1&2, 2000 Server, 2000 Server SP1&2, NT Enterprise Server 4.0, NT Enterprise Server 4.0 SP1-6a, NT Server 4.0, NT Server 4.0 SP1-6a	A vulnerability exists when a trust relationship exists between two domains, the trusting domain will accept the list of Security Identifiers (SIDs) specified within authorization data, which could let a malicious user obtain elevated privileges. <i>Bulletin updated to advise availability of Windows NT 4.0 Server, Terminal Server Edition Security Rollup Package.</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/MS02-001.asp	Windows Trusted Domain Membership CVE Name: CAN-2002-0018	Medium	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.

⁴⁹ Microsoft Security Bulletin, MS02-001, January 30, 2002.

⁵⁰ Microsoft Security Bulletin, MS02-001 V1.1, April 24, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft ⁵ <i>New versions of bulletin released^{52, 53, 54}</i> <i>Bulletin has been updated⁵⁵</i>	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. <i>On March 11, Microsoft released an updated version of the bulletin announcing the availability of a patch for Windows NT 4.0 Terminal Server Edition and to advise customers that the work-around procedure is no longer needed for that platform. On March 14, 2002, Microsoft discovered that the English and German patches for Windows NT 4.0 Terminal Server Edition contained incorrect files. Microsoft released an updated version of the bulletin announcing the availability of a patch for Windows 98 and Windows 98SE and to advise customers that the work-around procedure is no longer needed for that platform.</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/MS02-006.asp <i>It is recommended that customers who have downloaded the Windows NT 4.0 Terminal Server Edition patch in English or German prior to March 14, 2002 install the updated version. Customers who have installed the Windows NT 4.0 Terminal Server Edition patches in any language other than English or German do not need to take any action.</i>	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.
MiniBB ⁵⁶	Multiple	MiniBB 1.2	A Cross-Site Scripting vulnerability exists because script code is not properly filtered from URL parameters, which could let a remote malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	MiniBB Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Exploit has been published.
Mosix Project ⁵⁷	Unix	ClumpOS 5.4	A vulnerability exists because a user is not prompted to set a password when VNC is installed, which could let a remote malicious user obtain root access.	<u>Workaround (Bugtraq):</u> Manually set a VNC password.	ClumpOS Default VNC Password	High	Bug discussed in newsgroups and websites. Vulnerability may be exploited with a VNC client.

⁵¹ Microsoft Security Bulletin, MS02-006, February 15, 2002.

⁵² Microsoft Security Bulletin, MS02-006 (version 3.0), March 5, 2002.

⁵³ Microsoft Security Bulletin, MS02-006 (version 4.0), March 11, 2002.

⁵⁴ Microsoft Security Bulletin, MS02-006 (version 5.0), March 14, 2002.

⁵⁵ Microsoft Security Bulletin, MS02-006 V6.0, April 26, 2002.

⁵⁶ SecurityFocus, April 29, 2002.

⁵⁷ Bugtraq, April 23, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Mosix Project ⁵⁸	Unix	Mosix 1.5.7, OpenMosix 2.4.17	A Denial of Service vulnerability exists because malformed packets are not properly handled.	No workaround or patch available at time of publishing.	Mosix Malformed Packet Denial of Service	Low	Bug discussed in newsgroups and websites.
Mozilla/ Netscape ⁵⁹	Windows 95/98/ME/ NT 4.0, XP, MacOS 9.0/9.0.4. 9.1/9.2/ 9.2.1/9.2.2, MacOS X 10.x	Mozilla Browser 0.9.7, 0.9.8, 0.9.9, 1.0 RC1; Netscape 6.1-6.2.2	A vulnerability exists due to the way HTTP redirects are handled in the XMLHttpRequest object, which could let a remote malicious user obtain sensitive information.	Mozilla Browser: http://ftp.mozilla.org/pub/mozilla/releases/mozilla1.0rc1/src/mozilla-source-1.0.rc1.tar.gz No workaround or patch available for Netscape at time of publishing.	Mozilla / Netscape 6 XMLHttpRequest File Disclosure	Medium	Bug discussed in newsgroups and websites. Exploits have been published. Vulnerability has appeared in the press and other public media.
Multiple Vendors ⁶⁰	Unix	FreeBSD FreeBSD 4.4 –RELENG, 4.5 – STABLE, RELEASE; OpenBSD OpenBSD 2.0-2.3; Sun Solaris 2.5.1, 2.5.1_x86, 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86	A vulnerability exists because BSD-based kernels do not check to ensure that the C library standard I/O file descriptors 0-2 are valid open files before exec()ing setuid images, which could let a malicious user obtain superuser privileges.	FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-02:23/stdio.patch	BSD exec C Library File Descriptor Closure	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Multiple Vendors ⁶¹	Windows 95/98/ME/ NT 4.0, XP, MacOS 9.x, MacOS X 10.x, Unix	Galeon Browser 1.2, 1.2.1; Mozilla Browser 0.9.9, 1.0 RC1; Netscape 6.0-6.2.2	A vulnerability exists when embedding a stylesheet with the <LINK> element, which could let a malicious user circumvent security restrictions and obtain sensitive information.	No workaround or patch available at time of publishing.	Netscape/ Mozilla/Galeon Local File Detection	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published. Vulnerability has appeared in the press and other public media.

⁵⁸ Bugtraq, April 23, 2002.

⁵⁹ GreyMagic Security Advisory, GM#001-NS, April 30, 2002.

⁶⁰ FreeBSD Security Advisory, FreeBSD-SA-02:23, April 22, 2002.

⁶¹ Bugtraq, April 30, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors ⁶²	Multiple	Microsoft Visual C++.Net; StackGuard 1.2, 1.2.1, 2.0.1, 0.7 -beta	Multiple vulnerabilities exist in the stack smashing protection technologies, which could let a malicious user overwrite data.	No workaround or patch available at time of publishing.	Multiple Stack Protection Scheme Function Argument Overwrite	Medium	Bug discussed in newsgroups and websites.
Multiple Vendors ^{63, 64}	Unix	Compaq Tru64 4.0 g, 4.0 f, 5.0 a, 5.1 a, 5.1; HP-UX 10.10, 10.20, 10.24, 11.0 4, 11.0, 11.11; IBM AIX 4.3-4.3.3; Sun Solaris2.4, 2.4_x86, 2.5, 2.5_x86, 2.5.1_x86, 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86	A buffer overflow vulnerability exists when the help menu in the 'dtpriinfo' program is used to perform a volume search with a string of arbitrary length, which could let a malicious user execute arbitrary code.	Compaq: http://ftp1.support.compaq.com/public/unix/ HP-UX: http://itrc.hp.com IBM: IBM APAR IY21539 Sun Microsystems: http://sunsolve.sun.com	CDE DTPrintInfo Buffer Overflow	High	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.

⁶² Core Security Technologies Advisory, CORE-20020409, April 24, 2002.

⁶³ eSecurityOnline Security Advisory 2406, April 29, 2002.

⁶⁴ Compaq Computer Corporation Security Bulletin, SSRT-541, April 18, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors ^{65, 66, 67, 68, 69, 70, 71}	Unix	Todd Miller Sudo 1.5.9, 1.6-1.6.2, 1.6.3 p1-1.6.3 p7, 1.6.3, 1.6.4 p1-1.6.4 p2, 1.6.4, 1.6.5 p1-1.6.5 p2, 1.6.5	A vulnerability exists in the customized password prompt feature, which could let a malicious user obtain root privileges.	Todd Miller: ftp://ftp.sudo.ws/pub/sudo/sudo-1.6.6.tar.gz RedHat: ftp://updates.redhat.com/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Debian: http://security.debian.org/dists/stable/updates/main/ Mandrake: http://www.mandrakesecurity.net/en/ftp.php Engarde: http://ftp.engardelinux.org/pub/engarde/stable/updates/ Trustix: http://www.trustix.net/pub/Trustix/updates/ SuSE: ftp://ftp.suse.com/pub/suse/i386/update/ Slackware: ftp://ftp.slackware.com/pub/slackware/	Sudo Password Prompt Heap Overflow CVE Name: CAN-2002-0184	High	Bug discussed in newsgroups and websites.
National Instruments ⁷²	Windows 98/2000, Unix	LabVIEW 5.1.1, 6.0, 6.1	A Denial of Service vulnerability exists when a malformed HTTP request is received.	Vendor workaround available at: http://digital.ni.com/public.nsf/websearch/4C3F86E655E5389886256BA00064B22F?OpenDocument	LabVIEW HTTP Request Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Netscape/Mozilla ⁷³	Windows 95/98/NT 4.0, Unix	Mozilla Browser 0.9.9, 1.0 RC1; Netscape Communicator 6.0, 6.0.1, 6.1	A buffer overflow vulnerability exists when an exceptionally long request is handled for a channel using the IRC protocol, which could cause the server to crash.	No workaround or patch available at time of publishing.	Netscape/Mozilla IRC Buffer Overflow	Low	Bug discussed in newsgroups and websites. Exploit has been published. Vulnerability has appeared in the press and other public media.

⁶⁵ Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:072-07, April 25, 2002.
⁶⁶ Conectiva Linux Security Announcement, CLA-2002:475, April 26, 2002.
⁶⁷ Debian Security Advisory, DSA-128-1, April 26, 2002.
⁶⁸ Mandrake Linux Security Update Advisory, MDKSA-2002:028, April 26, 2002.
⁶⁹ EnGarde Secure Linux Security Advisory, ESA-20020429-010, April 29, 2002.
⁷⁰ Trustix Secure Linux Security Advisory, TSLSA-2002-0046, April 29, 2002.
⁷¹ SuSE Security Announcement, SuSE-SA:2002:014, April 30, 2002.
⁷² Bugtraq, April 22, 2002.
⁷³ GreyMagic Security Advisory, GM#001-NS, April 30, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
NullSoft ⁷⁴	Windows 95/98/ME/ NT 4.0/2000, XP	Winamp 2.79	A buffer overflow vulnerability exists because HTML tags can be included in the title/artist/album fields, which could let a malicious user execute arbitrary data.	Upgrade available at: http://www.winamp.com/download/	Winamp Minibrowser Buffer Overflow	High	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
OpenSSH ⁷⁵	Unix	OpenSSH 2.1, 2.1.1, 2.2, 2.3, 2.5, 2.5.1, 2.5.2, 2.9 p2, 2.9 p1, 2.9, 2.9.9, 3.0, 3.0.1, 3.0.2, 3.1, 3.2	A buffer overflow vulnerability exists due to the way Kerberos 4 TGT/AFS tokens are handled, which could let an unauthorized remote/local malicious user obtain privileged access.	Patch available at: ftp://ftp.openbsd.org/pub/OpenBSD/patches/2.9/common/024_sshafs.patch	OpenSSH Kerberos 4 TGT/AFS Token Buffer Overflow	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Outfront ⁷⁶	Windows NT	Spooky Login 2.0-2.5	A vulnerability exists in the authentication component, which could let a remote malicious user circumvent the authentication mechanism.	No workaround or patch available at time of publishing.	Spooky Login Password Manipulation	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Philip Chinery ⁷⁷	Multiple	Guestbook 1.1	A vulnerability exists because script code is not properly filtered from form fields, which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	Guestbook Script Injection	High	Bug discussed in newsgroups and websites. Exploit has been published.
PHP ⁷⁸	Multiple	Gratuit Recherche 1.3	A Cross-Site Scripting vulnerability exists because script code is not properly filtered from URL parameters, which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	Recherche Cross-Site Scripting	High	Bug discussed in newsgroups and websites.
PHP ⁷⁹	Unix	PHP 4.0-4.0.7, 4.1.0-4.1.2	A vulnerability exists in Posix_* functions because they do not restrict the usage of posix_getpwnam and posix_getpwuid, which could let a malicious obtain sensitive information.	No workaround or patch available at time of publishing.	PHP posix_getpwnam / posix_getpwuid safe_mode Circumvention	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

⁷⁴ Sandblad Advisory #5, April 26, 2002.

⁷⁵ Bugtraq, April 21, 2002.

⁷⁶ Securiteam, May 2, 2002.

⁷⁷ Bugtraq, April 21, 2002.

⁷⁸ SecurityFocus, April 30, 2002

⁷⁹ Securiteam, April 23, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
PHPProjekt ⁸⁰	Multiple	PHPProjekt 2.0-3.1	Multiple vulnerabilities exist: a vulnerability exists in some of the scripts, which could let an unauthorized malicious user access these scripts; a vulnerability exists due to insufficient validation of variables in the upload functions, which could let a malicious user execute arbitrary files; and a vulnerability exists because user-supplied data is not properly sanitized before it is passed into SQL queries, which could let a malicious user launch SQL injection attacks.	Upgrade available at: http://www.phprojekt.com/modules.php?op=modload&name=Downloads&file=index&req=viewdownload&cid=1	PHPProjekt Multiple Vulnerabilities	Medium/ High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser. There is no exploit code required for the upload function vulnerability.
PHP-Survey ⁸¹	Unix	PHP-Survey prebeta-20000327, 20000615, 20000614b, 20000614, 20000421, 20000420	A vulnerability exists in the 'global.inc' script when it is requested via HTTP, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	PHP-Survey Information Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
PhpWeb Gallery ⁸²	Multiple	PhpWeb Gallery 1.0	A vulnerability exists because cookies that are used for authentication are stored in a non-encrypted format, which could let a malicious user obtain unauthorized access to the administrative account.	No workaround or patch available at time of publishing.	PhpWeb Gallery Cookie Manipulation Compromise	High	Bug discussed in newsgroups and websites.
Post Calendar Development Team ⁸³	Multiple	Post Calendar 3.0	A Cross-Site Scripting vulnerability exists because HTML or user-supplied script is not properly filtered, which could let a malicious user execute arbitrary script code.	Patch available at: http://www.bahraini.tv/modules.php?op=modload&name=Downloads&file=index&req=getit&lid=86	PostCalendar Cross-Site Scripting	High	Bug discussed in newsgroups and websites.

⁸⁰ Bugtraq, April 25, 2002.

⁸¹ Securiteam, April 29, 2002.

⁸² SecurityFocus, April 29, 2002.

⁸³ Bugtraq, April 20, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
PostBoard ⁸⁴	Unix	PostBoard 2.0, 2.0.1	Multiple vulnerabilities exist: Cross-Site Scripting vulnerabilities exist because code that is submitted between IMG tags and message title input is not adequately sanitized, which could let a malicious user execute arbitrary script code; and a Denial of Service vulnerability exists in the implementation of BBcode if adequate resource limits are not in place.	No workaround or patch available at time of publishing.	PostBoard Multiple Vulnerabilities	Low/High (High if arbitrary script code can be executed)	Bug discussed in newsgroups and websites. Cross-Site Scripting vulnerabilities can be exploited via a web browser. There is no exploit code required for the Denial of Service vulnerability.
Progress ⁸⁵	Windows NT 4.0/2000, Unix	Database 9.1 C	A buffer overflow vulnerability exists in the '_probrkr' program, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Progress _probrkr Buffer Overflow	High	Bug discussed in newsgroups and websites.
psyBNC ⁸⁶	Unix	psyBNC 2.3	A remote Denial of Service vulnerability exists when a password of 9000 or more characters is sent to the server.	Upgrade available at: http://www.psychoid.lam3r.z.de/psyBNC2.3.tar.gz	PsyBNC Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Punknews.org ⁸⁷	Multiple	phpAnyVote 1.0	A vulnerability exists because cookies may be modified in order to vote more than once, which could let a malicious user corrupt the poll data.	No workaround or patch available at time of publishing.	phpAnyVote Cookie Security Bypass	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Qualcomm ⁸⁸	Unix	qpopper 4.0.3, 4.0.4	A buffer overflow vulnerability exists to insufficient bounds checking on some data, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	QPopper Bulletin Name Buffer Overflow	High	Bug discussed in newsgroups and websites.
RedHat ⁸⁹	Unix	DocBook-utils 0.6-13, 0.6.9-2, 1.54.13	A vulnerability exists in the default stylesheet because an insecure option is enabled, which could let a malicious user overwrite arbitrary files.	Update available at: ftp://updates.redhat.com/	DocBook Tools Default Stylesheet Arbitrary File Write CVE Name: CAN-2002-0169	Medium	Bug discussed in newsgroups and websites.

⁸⁴ Bugtraq, April 16, 2002.

⁸⁵ Bugtraq, May 2, 2002.

⁸⁶ Bugtraq, April 22, 2002.

⁸⁷ SecurityFocus, April 17, 2002.

⁸⁸ Bugtraq, April 29, 2002.

⁸⁹ RedHat Security Advisory, RHSA-2002:062-08, May 1, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
SAP ⁹⁰	Multiple	SAP R/3	A vulnerability exists due to a weak default installation on Oracle, which could let a malicious user read, write, and modify SAP data.	No workaround or patch available at time of publishing.	SAP R/3 with Oracle Unauthorized Data Access	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
SGI ⁹¹	Unix	IRISconsole 2.0	A vulnerability exists because incorrect passwords may allow login to the 'icadmin' account, which could let a remote malicious user obtain unauthorized access.	Patch available at: http://patches.sgi.com/support/free/security/patches/6.5/	IRISConsole icadmin Unauthorized Access CVE Name: CAN-2002-0171	Medium	Bug discussed in newsgroups and websites.
SGI ⁹²	Unix	IRIX 5.0-5.3, 6.0-6.5.10, 6.5.2 m-6.5.10 m, 6.5.2 f-6.5.10 f	A buffer overflow vulnerability exists in the 'CPR' program, which could let a malicious user execute arbitrary code with elevated privileges.	Upgrade to IRIX 6.5.11 or later located at: http://freeware.sgi.com/	Irix CPR Buffer Overflow CVE Name: CAN-2002-0173	High	Bug discussed in newsgroups and websites.
SGI ⁹³	Unix	IRIX 6.5, 6.5.1-6.5.9	A remote Denial of Service vulnerability exists in the 'syslogd' process when a large number of connections and log entries are made.	Upgrade to IRIX 6.5.11 or later located at: http://freeware.sgi.com/	Irix syslogd Remote Denial of Service CVE Names: CAN-1999-0171, CVE-1999-0566	Low	Bug discussed in newsgroups and websites.
SGI ⁹⁴	Unix	IRIX 6.5-6.5.10	A remote Denial of Service vulnerability exists when a large string of arbitrary data is sent to the /usr/etc/pmcd daemon.	Upgrade to a 6.5.11 or a later version located at: http://freeware.sgi.com/	Irix Performance Co-Pilot Remote Denial of Service CVE Name: CAN-2000-1193	Low	Bug discussed in newsgroups and websites. Exploit has been published.
SGI ⁹⁵	Unix	IRIX 6.5-6.5.10	A Denial of Service vulnerability exists because the /dev/MAKEDEV script creates the ipfilter device with world-read permission by default. A malicious user may also obtain unauthorized access to the device.	Upgrade to IRIX 6.5.11 or later located at: http://freeware.sgi.com/	Irix Insecure IPFilter Device Permissions CVE Name: CAN-2002-0172	Low/ Medium (Medium if unauthorized access is obtained)	Bug discussed in newsgroups and websites.

⁹⁰ Bugtraq, April 27, 2002.

⁹¹ SGI Security Advisory, 20020406-01-P, April 24, 2002.

⁹² SGI Security Advisory, 20020409-01-I, April 30, 2002.

⁹³ SGI Security Advisory, 20020405-01-I, April 24, 2002.

⁹⁴ SGI Security Advisory, 20020407-01-I, April 30, 2002.

⁹⁵ SGI Security Advisory, 20020408-01-I, April 30, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
SGI ⁹⁶	Unix	IRIX 6.5-6.5.10	A vulnerability exists in the debugging feature implemented in NSD, which could let a malicious user corrupt any file on the filesystem.	Upgrade to versions 6.5.11 or greater. available at: http://freeware.sgi.com/	Irix NSD Symbolic Link CVE Name: CAN-2002-0174	Medium	Bug discussed in newsgroups and websites.
SGI ⁹⁷	Unix	snmpd.sw.h p 1.1.2, 1.1.3	A vulnerability exists in the 'hpsnmpd' binary, which could let a remote malicious user cause a Denial of Service.	Patch available at: ftp://patches.sgi.com/support/free/security/patches/	Irix hpsnmpd Denial of Service CVE Names: CAN-2002-0012, CAN-2002-0013	Low	Bug discussed in newsgroups and websites.
SLRN Development Team ⁹⁸	Unix	SLRN 0.9.6 .2 - 0.9.6 .4	A buffer overflow vulnerability exists in spool directory names, which could let a malicious user obtain elevated privileges and execute arbitrary code.	Upgrade available at: http://prdownloads.sourceforge.net/slrn/slrn-0.9.7.4.tar.gz	SLRNPull Spool Directory Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Snapgear ⁹⁹	Multiple	Lite+ Firewall 1.5.3, 1.5.4	Several Denial of Service vulnerabilities exist: a Denial of Service vulnerability exists if external web management or PPTP are enabled and more than 50 simultaneous connections are made; a Denial of Service vulnerability exists when a 0 length UDP packet is sent to UDP port 500 and IPSEC is enabled; and a Denial of Service vulnerability exists when a malicious user sends a stream of approx. 7000 packets with malformed IP options.	Upgrade available at: http://www.snapgear.com/ftp/snapgear/firmware/SnapGearLITE_LITE+ v1.6.0_20020429_netflash.exe	Lite+ Firewall Denial of Service Vulnerabilities	Low/High (High if DDoS best practices not in place)	Bug discussed in newsgroups and websites. There is no exploit code required.
Snitz Forums 2000 ¹⁰⁰	Windows	Snitz Forums 2000 3.0, 3.1, 3.3.01-3.3.03, 3.3	A vulnerability exists in the 'members.asp' page because the input (M_NAME) is not checked for malicious code, which could let a remote malicious user obtain sensitive information and execute arbitrary code.	The vendor has provided fix information at the following location: http://forum.snitz.com/forum/topic.asp?TOPIC_ID=26776	Snitz Forums 2000 Members.ASP SQL Injection	Medium/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Proof of concept exploit has been published. Vulnerability can be exploited via a web browser.

⁹⁶ SGI Security Advisory, 20020501-01-I, May 1, 2002.
⁹⁷ SGI Security Advisory, 20020404-01-P, April 24, 2002.
⁹⁸ Bugtraq, April 22, 2002.
⁹⁹ KPMG-2002017, May 2, 2002.
¹⁰⁰ Bugtraq, April 19, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Summit Computer Networks ¹⁰	Windows NT 4.0/2000	Lil'HTTP 2.1, 2.2	A Directory Traversal vulnerability exists which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Lil' HTTP Server Directory Traversal	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Sun Micro Systems, Inc. ¹⁰²	Unix	Solaris 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86	A Denial of Service vulnerability exists in the RPC server component of the Cache File System if an RPC request is made for an invalid procedure.	No workaround or patch available at time of publishing.	Solaris cachefsd Denial of Service CVE Name: CAN-2002-0085	Low	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Sun Micro Systems, Inc. ¹⁰³	Unix	Solaris 2.6, 7.0, 8.0	A buffer overflow vulnerability exists in the 'admintool' due to insufficient bounds checking of the media installation path, which could let a malicious user execute arbitrary code and obtain elevated privileges.	No workaround or patch available at time of publishing.	Solaris AdminTool Buffer Overflow CVE Name: CAN-2002-0088	High	sBug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Sun Micro Systems, Inc. ¹⁰⁴	Unix	Solaris 8.0, 8.0_x86	A buffer overflow vulnerability exists in 'lbp proxy' due to insufficient bounds checking of the display name command line option, which could let a malicious user execute arbitrary code and obtain elevated privileges.	Patch available at: http://sunsolve.sun.com Sun Patch 108653-41 Sun Patch 108652-51	Solaris LBXProxy Buffer Overflow CVE Name: CAN-2002-0090	High	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Sun Micro Systems, Inc. ¹⁰⁵	Unix	Solaris 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86	A buffer overflow vulnerability exists in the 'cachefsd' mount file due to insufficient bounds checking on user-supplied mounts, which could let a malicious user obtain root privileges.	No workaround or patch available at time of publishing.	Solaris cachefsd Buffer Overflow CVE Name: CAN-2002-0084	High	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.

¹⁰¹ Securiteam, April 22, 2002.

¹⁰² eSecurityOnline Security Advisory 4197, April 29, 2002

¹⁰³ eSecurityOnline Security Advisory 4123, April 29, 2002.

¹⁰⁴ eSecurityOnline Security Advisory 3761, April 29, 2002

¹⁰⁵ eSecurityOnline Security Advisory 4198, April 29, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Sun Micro Systems, Inc. ¹⁰⁶	Unix	Sun Solaris 2.5, 2.5_x86, 2.5.1, 2.5.1_x86, 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86	Multiple buffer overflow vulnerabilities exist: a buffer overflow vulnerability exists in ' admintool' binary which may allow a malicious local user to gain elevated privileges and root access; and a buffer overflow vulnerability exists due to a lack of bounds checking for the PRODVERS argument in the 'cdtoc' file, which could let a malicious user obtain root access.	Patch available at: http://sunsolve.sun.com	Solaris Local Buffer Overflows CVE Name: CAN-2002-0089	High	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Sun Micro Systems, Inc. ¹⁰⁷	Unix	Sun Solaris 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86	A vulnerability exists in the 'rpc.rwalld' daemon when malicious format strings are sent from one system to another, which could let a remote malicious user execute arbitrary code and obtain root access.	No workaround or patch available at time of publishing.	Sun Solaris RWall Daemon Syslog Format String	High	Bug discussed in newsgroups and websites. Exploit has been published. Vulnerability has appeared in the press and other public media.
Trend Micro, Inc. ¹⁰⁸	Unix	InterScan eManager 3.6 For Sun & Linux	A vulnerability exists when an e-mail message being sent is identified as Spam, which could let a malicious user obtain addresses in the BCC field.	No workaround or patch available at time of publishing.	InterScan eManager Bcc Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Vincent Courcelle ¹⁰⁹	Multiple	Trackeur de visiteurs 1.0	A vulnerability exists when the "no track" flag is enabled via a specially crafted cookie or cookie manipulation, which could let a remote malicious user disable tracking the web activity of certain users.	No workaround or patch available at time of publishing.	Trackeur De Visiteurs Tracking Evasion	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
vqSoft ¹¹⁰	Windows 95/98/NT 4.0	vqServer for Windows 1.9, 1.9.30, 1.9.47, 1.9.55	Multiple Cross-Site Scripting vulnerabilities exist in some of the demo CGIs, which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	vqServer CGI Demo Program Script Injection	High	Bug discussed in newsgroups and websites. Exploit has been published.

¹⁰⁶ eSecurityOnline Security Advisory 2397, April 29, 2002.

¹⁰⁷ CERT Advisory, CA-2002-10, May 1, 2002.

¹⁰⁸ Bugtraq, April 24, 2002.

¹⁰⁹ SecurityFocus, April 29, 2002.

¹¹⁰ Securiteam, April 22, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Workforce ROI ¹¹¹	Windows	Xpede 4.1	Multiple vulnerabilities exist: a vulnerability exists because authentication credentials are not required for non-administrative users when they attempt to access an administrative script, which could let a malicious user obtain unauthorized access to the administrative facilities; a vulnerability exists in the 'datasource.asp' script, which could let a malicious user access the database without authentication; a vulnerability exists because the 'datasource.asp' script provides an interface for changing the user's password, which could let a remote malicious brute-force the account; a vulnerability exists because when a user submits an expense claim the file is saved in the world-readable '/reports/temp' directory, which could let a remote malicious user obtain sensitive information; a vulnerability exists in the 'sprc.asp' script, which could let a malicious user to launch SQL injection attacks; and a vulnerability exists in the 'ets_app_process.asp' script due to the lack of adequate authentication, which could let a remote malicious user access the time sheets of other users.	No workaround or patch available at time of publishing.	XPede Multiple Vulnerabilities	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser. No exploit code is required.
X-Crew ¹¹²	Multiple	Ultimate PHP Board 1.0 Beta, 1.1	Several vulnerabilities exist: a vulnerability exists in the private message system, which could let a malicious user read private messages; and a vulnerability exists because encrypted UPB user passwords are included in files which may be accessible to a malicious user.	Upgrade available at: http://www.tritanium-scripts.de/download/download_ad.php?script_id=1	Ultimate PHP Board Multiple Vulnerabilities	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.

¹¹¹ Bugtraq, April 19, 2002.

¹¹² SecurityFocus, April 25, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
X-Crew ¹¹³	Multiple	Ultimate PHP Board 1.0 Beta, 1.1	A vulnerability exists because script code is not properly filtered from image tags, which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	Ultimate PHP Board Image Tag Script Injection	High	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.

*“Risk” is defined by CyberNotes in the following manner:

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

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

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

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between April 21 and May 4, 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, 30 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
May 4, 2002	Cisco677.pl	Perl script which exploits the Cisco 677/678 Telnet Overflow Denial of Service vulnerability.
May 4, 2002	Tomas.zip	A commandline tool to crack the secret passwords on Cisco routers.

¹¹³ SecurityFocus, April 25, 2002.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
May 4, 2002	Nmap-2.54BETA34.tgz	A utility for port scanning large networks that supports Vanilla TCP connect() scanning, TCP SYN (half open) scanning, TCP FIN, Xmas, or NULL (stealth) scanning, TCP ftp proxy (bounce attack) scanning, SYN/FIN scanning using IP fragments (bypasses some packet filters), TCP ACK and Window scanning, UDP raw ICMP port unreachable scanning, ICMP scanning (ping-sweep), TCP Ping scanning, Direct (non portmapper) RPC scanning, Remote OS Identification by TCP/IP Fingerprinting, and Reverse-ident scanning.
May 4, 2002	Ppp-2.4.1+Bf.patch	A patch which adds PPP authentication brute force password guessing support to Linux pppd.
May 4, 2002	Mimedefang-2.9.tar.gz	A flexible MIME e-mail scanner designed to protect Windows clients from viruses and other harmful executables.
May 1, 2002	Tgt_v1_x86Lnx.Tar.gz	Script which exploits the OpenSSH Kerberos 4 TGT/AFS Token Buffer Overflow vulnerability.
May 1, 2002	Food_for_the_poor.c	Exploit for the KTH eBones Kerberos4 FTP Client Passive Mode Heap Overflow vulnerability.
May 1, 2002	pUll.pl	Perl script which exploits the SLRNPull Spool Directory Command Line Parameter Buffer Overflow vulnerability.
May 1, 2002	X2.tgz	Script which exploits the SSH Restricted Shell Escaping Command Execution vulnerability.
May 1, 2002	Msh3comdos.c	Script which exploits 3Com 3CDaemon Buffer Overflow vulnerability.
April 27, 2002	Wellenreiter-V11.tar.gz	A GTK/Perl program that makes the discovery and auditing of 802.11b wireless networks much easier.
April 27, 2002	Nmap-2.54BETA33.tgz	A utility for port scanning large networks that supports Vanilla TCP connect() scanning, TCP SYN (half open) scanning, TCP FIN, Xmas, or NULL (stealth) scanning, TCP ftp proxy (bounce attack) scanning, SYN/FIN scanning using IP fragments (bypasses some packet filters), TCP ACK and Window scanning, UDP raw ICMP port unreachable scanning, ICMP scanning (ping-sweep), TCP Ping scanning, Direct (non portmapper) RPC scanning, Remote OS Identification by TCP/IP Fingerprinting, and Reverse-ident scanning.
April 24, 2002	Epop.c	Exploit for the WiredRed e/pop v2.0.3 vulnerability.
April 24, 2002	Backstealth.zip	A tool that bypasses outbound restrictions of personal firewalls by embedding an HTTP client in a dll.
April 24, 2002	Iischeck.pl	Perl script which checks for the Microsoft IIS .HTR heap overflow vulnerability to determines if patch MS02-018 has been applied.
April 24, 2002	Screen-stuff.tgz	Exploit for the GNU Screen Braille Module Buffer Overflow vulnerability.
April 24, 2002	Remotefmt-howto.txt	How to Remotely Exploit Format String Bugs tutorial that includes information on guessing the offset, guessing the address of the shellcode in the stack, using format string bugs as debuggers, and examples, etc.
April 24, 2002	Evelyne.sh	Local root exploit for the Suid application execution vulnerability.
April 24, 2002	Iosmash.c	Script which exploits the BSD exec C Library Standard I/O File Descriptor Closure vulnerability.
April 24, 2002	Nessus-1.2.0.tar.gz	A full featured remote security scanner for Linux, BSD, Solaris and some other systems that is multithreaded, plugin-based, has a nice GTK interface, and currently performs over 900 remote security checks.
April 24, 2002	Ettercap-0.6.5.tar.gz	A network sniffer/interceptor/logger for switched LANs that uses ARP poisoning and the man-in-the-middle technique to sniff all the connections between two hosts.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
April 22, 2002	Pos_expl2.c	Script that exploits the Posadis m5pre2 local format string vulnerability.
April 22, 2002	Promiscdetect.exe	PromiscDetect for Windows NT 4.0 / 2000 / XP checks if your network adapter(s) is in promiscuous mode.
April 22, 2002	Sambar.fileparse.txt	Example URLs for the Sambar Server Script Source Disclosure vulnerability.
April 22, 2002	Matuftp_exploit.pl	Perl script which exploits the Matu FTP Client Buffer Overflow vulnerability.
April 22, 2002	Slrnpull-ex.pl	Perl script which exploits the SLRNPull Spool Directory Command Line Parameter Buffer Overflow vulnerability.
April 22, 2002	Fragroute-1.2.tar.gz	Fragroute intercepts, modifies, and rewrites egress traffic destined for a specified host, implementing most of the attacks described in the Secure Networks "Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection" paper of January 1998.
April 22, 2002	Psybnc2.3.pl	Perl script which exploits the PsyBNC Oversized Passwords Denial Of Service vulnerability.
April 21, 2002	Own-screen.c	Script which exploits the GNU Screen Braille Module Buffer Overflow vulnerability.
April 21, 2002	Tgt-X86linux.tar	Exploit for the OpenSSH Kerberos 4 TGT/AFS Token Buffer Overflow vulnerability.

Trends

- The National Infrastructure Protection Center (NIPC) continues to monitor a mass-mailing worm called Klez.h. The NIPC is issuing this alert due to information received from industry partners, combined with the striking number of infections reported in the wild. For more information, see NIPC ALERT 02-002, located at: <http://www.nipc.gov/warnings/alerts/2002/02-002.htm>.
- The CERT/CC has received reports of social engineering attacks on users of Internet Relay Chat (IRC) and Instant Messaging (IM) services. Intruders trick unsuspecting users into downloading and executing malicious software, which allows the intruders to use the systems as attack platforms for launching distributed Denial of Service (DDoS) attacks. For more information, see http://www.cert.org/current/current_activity.html#IM.
- The Computer Emergency Response Team (Cert) has released a report pinpointing the six fastest evolving trends in the black hat world of Internet security. The most notable trend to evolve over recent years is the automation and speed of attack tools. The full report can be found at: http://www.cert.org/archive/pdf/attack_trends.pdf.
- The CERT/CC has received reports of social engineering attacks on users of Internet Relay Chat (IRC) and Instant Messaging (IM) services. Intruders trick unsuspecting users into downloading and executing malicious software, which allows the intruders to use the systems as attack platforms for launching distributed denial-of-service (DDoS) attacks. The reports to the CERT/CC indicate that tens of thousands of systems have recently been compromised in this manner. For more information, see CERT® Incident Note IN-2002-03, located at: http://www.cert.org/incident_notes/IN-2002-03.html.

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.*

PE_CIH.1049 (Alias: W95/CHIS-1049) (File Infector Virus): On the system date, August 2 of any year, this variant of the CIH virus corrupts the hard disk and destroys the flash BIOS of the infected system. W95/CIH-1049 is a new variant of W95/CIH-10xx family of viruses.

VBS/Dracv.a@MM (Visual Basic Script Worm): This virus may arrive as an e-mail attachment, 'vcards.vbs,' and will send e-mail using Outlook to all recipients in address list. On executing the virus, the following message is displayed, "Do you want to see your VCard?" If the user chooses no, the virus will not proceed. If yes is chosen, the following message is then displayed, "Enter a message for people getting your card" and user can enter a message. The virus creates the directory C:\wcache and saves the files vcrd01.vcrd, vcrd02.vcrd, and vcrd03.vcrd. It goes on to search the hard drive for three .jpg files and then creates the file imgDisplay.html to display the pictures found. The virus then checks to see if the registry key "HKEY_CURRENT_USER\software\vcards\mailed" = "1" and if not proceeds to send the e-mail out to all in addresses. Once this has finished, the virus will then edit the registry key:
HKEY_CURRENT_USER\software\vcards\mailed" "1"

VBS/Horty-A (Aliases: VBS-KAGRA.A, VBS.Kagra.A@mm) (Visual Basic Script Worm): This is an e-mail worm that uses Microsoft Outlook to spread. The worm sends an e-mail to all contacts in the user's Windows address book. The e-mail has the following characteristics:

- Subject line: Jenna Jameson pornstar free superf**k+photo address
- Message text: Do you wanna see super pornstar, Jenna Jameson, in a special superf**k? Double click on the attachment of this mail, and get also some interesting sex-sex-sex addresses...
- Attached file: JENNA-JAMESON-FREE-SUPERF**K.TXT.vbs

The worm will create the following registry entry so that it runs on Windows startup:
HKLM\Software\Microsoft\Windows\CurrentVersion\Run\WUpdate

VBS/Jord.a (Visual Basic Script Worm): The virus copies itself as ORD.doc.vbs, ORD_photo.jpg.vbs, and JERRY.vbs to the Windows Font directory. It then edits the following registry keys:

HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Please..., <WINDOWS font directory>\JERRY.vbs"

The virus checks to see if the value of "HKEY_CURRENT_USER\Control Panel\International\iCountry = 34," and if not creates the key "HKEY_LOCAL_MACHINE\Software\Singapore,""0." If the registry key does equal 34, then the virus creates the key "HKEY_LOCAL_MACHINE\Software\Singapore,""1." If the registry key "HKEY_LOCAL_MACHINE\Software\Singapore" does not equal 1, the virus then proceeds with the damaging payload routine. If day is 12th of June, a message will be displayed.

VBS/Redlof@M (Aliases: HTML.Redlof.A, VBS.Redlof, VBS_REDLOF.A) (Visual Basic Script Worm): This is a file infecting VBScript that sets a default, infected, stationary file for the Microsoft Outlook and Outlook Express e-mail client programs. It exploits the Microsoft VM ActiveX Component Vulnerability. The script arrives in an e-mail message, hidden from the user, or can be present on websites that contain infected .HTM files. The virus uses the BODY ONLOAD event to trigger the infection. .HTM, and .HTT files on the local system are infected by appending them with the encrypted, viral code. .HTT files are prepended with the BODY ONLOAD trigger, while this action is placed at the beginning of the virus body in .HTM files. The default mail account is retrieved from the registry and a stationary file is created, "BLANK.HTM," and is set as the default stationary file. The VBScript virus body is saved to the file KERNEL.DLL in the WINDOWS SYSTEM directory and a registry run key is created to load the script at startup:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\
Run\Kernel32=C:\WINDOWS\SYSTEM\Kernel.dll

W32/Denis.worm (Aliases: DenisBee worm, W32.Denisbee, W32/Denisbee, W32/Denisbee.68608, Win32.Denisbee, Win32.HLLW.Denis, Worm.DenisBee, Worm/Win32.Denisbee) (Win32 Worm): This worm browses the network connections to spread to other machines that allow passwordless write

access to open shares over NetBIOS, and copies itself into the folder with one of the following names: trojan.exe, pager.exe, crack.exe, lines99.exe, worm.exe, draw.exe, mpeg.exe, low.exe, byte.exe, visual.exe, word.exe, done.exe, horse.exe, express.exe, toy.exe, com.exe, or friday.exe. After the worm gets executed, it copies itself into %Windir%\System\ with one of filenames mentioned above. It creates these keys in the registry :

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\App Paths\n0.exe\@="%VirusPath%"
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\%VName%="%VirusPath%"
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Network\DisablePwdCaching="1"

%VName% is randomly selected from one of these strings: winapp, netbios, wapihlp, msxapp, dsgrun, winver32, gk32ctrl, or Netvx.

W32/ElKern-C (Alias: W32.ElKern.4926) (Win32 Executable File Virus): This virus has been reported in the wild. It is an executable file virus very similar to W32/ElKern-A. W32/ElKern-C works under Windows 98, Windows ME, Windows 2000 and Windows XP. It is capable of infecting file cavities, meaning that it may not change the size of files it infects. The virus is dropped into the Program Files folder and run by W32/Klez-H. The virus contains routines to disable the on-access component of virus scanners developed by major anti-virus software vendors. The body of the virus contains the text "Win32 Foroux V1.0" in an encrypted format.

W32/Sowsat@MM (Alias: I-Worm.Sowsat) (Win32 Executable File Virus): This e-mail virus sends itself to addresses extracted from .HTM* files in the Windows directory of the victim machine. The worm is also capable of spreading via IRC, via a dropped SCRIPT.INI file. The worm contains its own SMTP engine, and uses a public SMTP server (address hardcoded within the worm) for mailing. It may arrive in an e-mail formatted in a number of ways. The worm contains the string:

- I-Worm/Cow
- [Team A] kicks [Team B]'s ass!

WM97/Marker-KG (Office 97 Macro Virus): This is a corrupted but viable variant of WM97/Marker-C. Whenever a document is closed, the virus attempts to FTP user information from Word to the Codebreakers site and appends this information to the bottom of the macro as comments.

W95/Sledge (Word 95 Macro Virus): This is a PE (Portable Executable) appending virus. When run it attempts to infect .EXE files on the local system under Windows 95/98/ME.

WORM_MALDAL.K (Internet Worm): This non-encrypted and non-destructive worm uses Microsoft Outlook to mass-mail itself to all e-mail addresses listed in the infected user's address book.

WORM_KLEZ.I (Aliases: I-Worm.Klez.i, W32/Klez.gen@mm, KLEZ.I) (Internet Worm): This variant is a slight modification of WORM_KLEZ.H. This mass-mailing worm uses SMTP to propagate via e-mail. The subject line of the e-mail it arrives with is randomly selected from a list of possible choices. It also drops a copy of PE_ELKERN.D that is the Windows file infector.

WORM_WITHOUT.A (Aliases: I-Worm.Without.a, W32/PetTick.bat, VBS/GenMail.D) (Internet Worm): This destructive worm is written in Visual Basic Script (VBS) and uses Microsoft Outlook to propagate copies of itself via e-mail. It overwrites batch files on the infected system's available drives

X97M/Fixen.a (Excel 97 Macro Virus): The virus contains one module, v123 that, infects Excel97/2000 workbooks. It saves a copy of itself as 'v123.xls' into the Excel Application path. The virus also creates the file 'v123.vbs' that is also found in the Excel Application path. The script file will export the viral code of 'v123.xls' to 'v123.bas' file. This .bas file is not viral. It then finds all .xls files in the Windows Recent folder and imports the viral code to these files. The virus will then delete all .xls.lnk from the Recent folder. If the day is greater than the 30th of May 2002, a message will be displayed. If the user chooses OK, the following registry keys will be changed:

HKLM\Software\Microsoft\Windows\CurrentVersion\ProductName, "Microsoft Windows 0.1"
 HKLM\Software\Microsoft\Windows\CurrentVersion\RegisteredOrganization,"
 "Completely no good system company"
 HKLM\Software\Microsoft\Windows\CurrentVersion\Version," "Windows 0.1"
 HKLM\Software\Microsoft\Windows\CurrentVersion\VersionNumber," "0.00.0001"
 HKLM\Software\Microsoft\Windows\CurrentVersion\SystemRoot," "C:"

The following registry key is also changed:

HKLM\Software\Microsoft\Windows\CurrentVersion\Run\v123, EXCEL Path
 Application\v123.vbs"

which will enable the virus to execute on the next reboot of the system.

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
Arial	N/A	CyberNotes-2002-08
Backdoor.EggHead	N/A	CyberNotes-2002-04
Backdoor.Evilbot	N/A	Current Issue
Backdoor.G Door.Client	N/A	CyberNotes-2002-05
Backdoor.IISCrack.dll	N/A	CyberNotes-2002-04
Backdoor.NetDevil	N/A	CyberNotes-2002-04
Backdoor.Palukka	N/A	CyberNotes-2002-01
Backdoor.RemoteNC	N/A	Current Issue
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-ABH	N/A	CyberNotes-2002-06
BackDoor-ABN	N/A	CyberNotes-2002-06
BackDoor-FB.svr.gen	N/A	CyberNotes-2002-03
BDS/Osiris:	N/A	CyberNotes-2002-06
BKDR_INTRUZZO.A	N/A	Current Issue
BKDR_LITMUS.C	N/A	Current Issue
BKDR SMALLFEG.A	N/A	CyberNotes-2002-04
BKDR WARHOME.A	N/A	CyberNotes-2002-06
Dewin	N/A	CyberNotes-2002-08
DI Der	N/A	CyberNotes-2002-01
DoS-Winlock	N/A	CyberNotes-2002-03
Downloader-W	N/A	CyberNotes-2002-08
Hacktool.IPStealer	N/A	CyberNotes-2002-02

Trojan	Version	CyberNotes Issue #
Irc-Smallfeg	N/A	CyberNotes-2002-03
IRC-Smev	N/A	CyberNotes-2002-08
JS/Seeker-E	N/A	CyberNotes-2002-01
JS_EXCEPTION.GEN	N/A	CyberNotes-2002-01
mIRC/Gif	N/A	CyberNotes-2002-08
Multidropper-CX	N/A	CyberNotes-2002-08
QDel227	N/A	Current Issue
SecHole.Trojan	N/A	CyberNotes-2002-01
Troj/Diablo	N/A	Current Issue
Troj/Download-A	N/A	CyberNotes-2002-01
Troj/ICQBomb-A	N/A	CyberNotes-2002-05
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_JUNTADOR.B	N/A	CyberNotes-2002-06
TROJ_OPENME.B	N/A	Current Issue
TROJ_SMALLFEG.DR	N/A	CyberNotes-2002-04
Trojan.Badcon	N/A	CyberNotes-2002-02
Trojan.Fatkill	N/A	Current Issue
Trojan.StartPage	N/A	CyberNotes-2002-02
Trojan.Suffer	N/A	CyberNotes-2002-02
VBS.Gascript	N/A	CyberNotes-2002-04
VBS_CHICK.B	N/A	CyberNotes-2002-07
VBS_THEGAME.A	N/A	CyberNotes-2002-03
W32.Alerta.Trojan	N/A	CyberNotes-2002-05
W32.Delalot.B.Trojan	N/A	CyberNotes-2002-06
W32.DSS.Trojan	N/A	Current Issue
W32.Maldal.J	N/A	CyberNotes-2002-07
W32.Tendoolf	N/A	Current Issue
WbeCheck	N/A	Current Issue

Backdoor.Evilbot: This is a backdoor Trojan. It is used as a remote attack tool by malicious users using IRC. When Backdoor.Evilbot is executed, it copies itself as \%SYSTEM%\Sysedit.exe. NOTE: %System% is a variable. The worm locates the \Windows\System folder (by default this is C:\Windows\System or C:\Winnt\System32) and copies itself to that location. It also adds the value, "sysyemdl \%system%\sysedit.exe" to the registry key:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
Backdoor.Evilbot allows access to the infected computer by a malicious user.

Backdoor.RemoteNC: This is a backdoor Trojan that can allow a malicious user to gain access to your system. When Backdoor.RemoteNC is executed, it opens a random (usually it is 1025, 1035, 1041, 1047, 1054, or similar) port and listens for a connection. The malicious user then can connect and have access to your system to delete, rename, copy, execute, and any other commands that can be used by Cmd.exe.

NOTE: This backdoor Trojan does not function properly on Windows 95/98/Me systems. On these systems it allows a malicious user to connect to the infected system, but they cannot send any damaging commands to the infected system. This is because Windows 95/98/Me systems do not use the Cmd.exe file, but instead use the Command.com file. The Trojan is coded to use only Cmd.exe and its commands, which will function only on Windows NT/2000/XP systems.

BKDR_INTRUZZO.A (Aliases: Backdoor.Intruzzo, Backdoor.Intrzo.A, W32/Intruzzo.1_0, BackDoor-ADM): This backdoor hacking tool is written in Visual Basic and has a server component and a client component. The server component installs itself on the target computer and then enables the malicious user access to the target computer. It compromises network security.

BKDR_LITMUS.C (Aliases: LITMUS.B, Backdoor.Litmus.203): This is the server component of a backdoor malware. It drops a MSGSRV320.EXE file in a C:\Windows\LITMUS folder. It does not have a destructive payload.

QDel227: This is a Windows PE Trojan written in Visual Basic 5, with a damaging file deletion payload. It runs on both 9x and NT/2000 machines. When executed on the victim machine, the following fake message box is displayed, "Sorry Your Operating System is not Supported." Once 'OK' is clicked, the Trojan attempts to delete files from the C: drive. The Trojan contains the string:

For my love in her birthday :-))

Troj/Diablo: This is a backdoor Trojan horse. If the Trojan server is installed on a computer, it will monitor and log all keyboard keystrokes made by the user. The keystrokes are logged into a file, which can be send via e-mail or FTP to the potential attacker. The attacker can be notified by ICQ when log files are uploaded onto an FTP server. The filename and extension used by the Troj/Diablo server are configurable. Possible Troj/Diablo file extensions can be: EXE, SCR, PIF, COM, CMD and BAT. When the Trojan server is run, it copies itself into the Windows Startup folder so that it automatically runs every time Windows is started.

TROJ_OPENME.B (Alias: OPENME.B): This Trojan opens Internet Explorer on the infected user's system. It drops the file INDEX.HTM that it then uses to pop-up an advertisement for pornographic Web sites. It also sends HTML packets and consumes memory resources.

Trojan.Fatkill: When Trojan.Fatkill is run, it corrupts the hard disk. Trojan.Fatkill is a DOS program that overwrites the File Allocation Table of the hard disk so that it becomes corrupted. This may result in the computer being unable to restart.

W32.DSS.Trojan: This is a Trojan horse that inserts a small web page onto your system. This web page is then launched in a hidden Internet Explorer window. The inserted web page contains code that waits for a given period of time. When the time period has expired, the web page activates another web page, which contains a link to an advertising page for an adult web site. The web page downloads a new phone dialer onto your computer. This Trojan is most likely to arrive in an e-mail message, which included an attachment named, "Openme.exe."

W32.Tendoolf: This is a variant of the Backdoor.Subseven Trojan, which appears to be able to spread through e-mail. The e-mail message has the following characteristics:

- Subject: Thoughts...
- Message: I just found this program, and, i dont know why... but it reminded me of you. check it out.
- Attachment: Cute.exe

WbeCheck (Alias: Trojan.Win32.WbeCheck): This Trojan installs a spying component file, 'pbsysie.dll,' to Internet Explorer. The DLL file is usually located in the \Windows\ folder. This DLL filters HTTP requests of IE and it makes some changes in HTTP traffic.