



National Infrastructure Protection Center CyberNotes

Issue #2002-20

October 7, 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 September 17 and between October 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
ACWeb ¹	Windows	ACWeb 1.8, 1.14	A Cross-Site Scripting vulnerability exists which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	ACWeb Cross-Site Scripting	High	Bug discussed in newsgroups and websites.
Alsaplayer ²	Unix	Alsaplayer 0.99.71	Buffer overflow vulnerabilities exist in the way directory and file names are processed due to improper bounds checking, which could let a malicious user execute arbitrary code.	Upgrade available at: http://www.alsaplayer.org/alsaplayer-0.99.72.tar.gz	Alsaplayer Local Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit script has been published.

¹ Illegal Instruction Labs Advisory, September 25, 2002.

² Securiteam, September 24, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Apache Software Foundation ³	Multiple	Apache 2.0, 2.0.28, 2.0.32, 2.0.35-2.0.41	A remote Denial of Service vulnerability exists in the 'mod_dav' component when a malicious HTTP request is issued.	Upgrade available at: http://www.apache.org/dist/httpd/	Apache 2 mod_dav Remote Denial of Service	Low	Bug discussed in newsgroups and websites.
Apache Software Foundation ⁴	Unix	Apache 2.0.39, 2.0.40	A Denial of Service vulnerability exists when a malicious user writes an excessive amount of data to STDERR.	No workaround or patch available at time of publishing.	Apache STDERR Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Apache Software Foundation ^{5,6}	Unix	Tomcat 3.0-4.1, 4.1.3 beta, 4.1.9 beta, 4.1.10	A vulnerability exists in the 'org.apache.catalina.servlets.DefaultServlet' servlet, which could let a malicious user view webroot file contents.	Upgrade available at: http://jakarta.apache.org/builds/jakarta-tomcat-4.0/release/	Tomcat DefaultServlet File Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Appalachian State University ⁷	Multiple	phpWeb Site 0.8.3	A vulnerability exists because HTML IMG tags in a news message are not sufficiently filtered, which could let a remote malicious user execute arbitrary HTML or JavaScript code.	No workaround or patch available at time of publishing.	PHPWebSite News Message HTML Injection	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Appalachian State University ⁸	Unix	phpWeb Site 0.8.3	A Cross-Site Scripting vulnerability exists in the 'article.pho' script due to insufficient sanitization of HTML tags from URI parameters, which could let a malicious user execute arbitrary HTML or JavaScript code.	No workaround or patch available at time of publishing.	PHPWebSite Article.PHP Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Appalachian State University ⁹	Windows, Unix	phpWebsite 0.8.2	A vulnerability exists in the 'modsecurity.php' script when a specially crafted URL request is received, which could let a remote malicious user execute arbitrary code.	Upgrades available at: http://phpwebsite.appstate.edu/downloads/0.8.3/ http://res1.stddev.appstate.edu/horde/chora/cvs.php/phpwebsite	phpWebsite Include Statement CVE Name: CAN-2002-1135	High	Bug discussed in newsgroups and websites. There is no exploit code required.
Apple ¹⁰	MacOS X 10.2	MacOS X 10.2 (Jaguar)	A vulnerability exists due to improper handling of some links, which could let a malicious user execute arbitrary code.	Patch available at: http://download.info.apple.com/Mac_OS_X/061-0223.20020920.Cg69J/2Z/SecurityUpd2002-09-20.dmg.bin	Mac OS X Terminal.APP Telnet Link	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

³ SecurityTracker, September 26, 2002.

⁴ Bugtraq, September 23, 2002.

⁵ Bugtraq, September 24, 2002.

⁶ Gentoo Linux Security Announcement, September 25, 2002.

⁷ ECHU Alert #2, September 25, 2002.

⁸ Bugtraq, October 2, 2002.

⁹ Bugtraq, September 23, 2002.

¹⁰ Apple Security Update, 120150, September 24, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
BEA Systems, Inc. ¹¹	Windows NT 4.0/2000, Unix	WebLogic Express 6.1, 6.1 SP1&2, 7.0.0.1, 7.0, Weblogic Server 6.1, 6.1 SP1&2, 7.0.0.1, 7.0	A vulnerability exists in the buffer mechanism due to HTTP response data being shared among two users, which could unintentionally expose sensitive information.	Upgrade available at: http://commerce.beasys.com/downloads/weblogic_server.jsp#wls	BEA WebLogic Server and Express HTTP Response Information Disclosure	Medium	Bug discussed in newsgroups and websites.
BEA Systems, Inc. ¹²	Windows NT 4.0/2000, Unix	WebLogic Express 7.0.0.1, 7.0; Weblogic Server 7.0.0.1, 7.0	A vulnerability exists when applications that contain Servlets or EJBs are deployed on multiple servers, which could let a malicious user cause security constraints to be removed.	Upgrade available at: http://commerce.beasys.com/downloads/weblogic_server.jsp#wls	WebLogic Server and Express Inadvertent Security Removal	Medium	Bug discussed in newsgroups and websites.
Borland/ Inprise ¹³	Unix	Interbase 4.0, 5.0, 6.0, 6.5	A buffer overflow vulnerability exists in the 'gds_lock_mgr' binary due to improper handling of user-supplied umasks, which could let a malicious user execute arbitrary code with root privileges.	No workaround or patch available at time of publishing.	Interbase GDS_Lock_MGR Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Carlos Sanchez Valle ¹⁴	Multiple	MyNews Groups :) 0.4, 0.4.1	Several Cross-Site Scripting vulnerabilities exist when the subject headers of news group messages are displayed, which could let a malicious user manipulate web content or to steal cookie-based authentication credentials.	No workaround or patch available at time of publishing.	MyNews Groups Subject Header	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Cerulean Studios ¹⁵	Windows 95/98/ME/ NT 4.0/2000	Trillian 0.73, 0.74	A buffer overflow vulnerability exists in the way JOIN commands are processed due to insufficient bounds checking, which could let a malicious user cause a Denial of Service or execute arbitrary code.	No workaround or patch available at time of publishing.	Trillian JOIN Buffer Overflow	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Exploit script has been published.
Cerulean Studios ¹⁶	Windows 95/98/ME/ NT 4.0/2000	Trillian 0.73, 0.74	A remote Denial of Service vulnerability exists due to improper HTML/XML parsing.	No workaround or patch available at time of publishing.	Trillian AIM Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Vulnerability can be exploited via AOL IM.

¹¹ BEA Security Advisory, BEA02-20.00, September 26, 2002.

¹² BEA Security Advisory, BEA02-21.00, October 1, 2002.

¹³ Securiteam, September 26, 2002.

¹⁴ Bugtraq, September 30, 2002.

¹⁵ NTBugtraq, September 20, 2002.

¹⁶ ComputerSecurityNow Advisory, September 23, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Cerulean Studios ¹⁷	Windows 95/98/ME/ NT 4.0/2000	Trillian 0.73, 0.74, 0.725	A buffer overflow vulnerability exists due to improper validation of IRC raw 221 user mode requests, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.	No workaround or patch available at time of publishing.	Trillian IRC Raw 221 Requests Buffer Overflow	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Exploit script has been published.
Cerulean Studios ¹⁸	Windows 95/98/ME/ NT 4.0/2000	Trillian 0.74	Multiple vulnerabilities exist: a remote Denial of Service vulnerability exists due to improper validation of IRC raw messages; a Denial of Service vulnerability exists when messages about a user leaving a non-specified channel or a channel that the user is not currently in is received by the server; and a buffer overflow vulnerability exists when blocks of data that are larger than 4095 bytes are sent to the server, which could let a malicious user cause a Denial of Service and potentially execute arbitrary code.	No workaround or patch available at time of publishing.	Trillian Multiple IRC Denial of Service Vulnerabilities	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Exploit script has been published.
Chost View ^{19,20}	Unix	GhostView 1.3, 1.4, 1.4.1, 1.5; gv 2.7 b1-b5, 2.7.6, 2.9.4, 3.0.0, 3.0.4, 3.1.4, 3.1.6, 3.2.4, 3.4.2, 3.4.3, 3.4.12, 3.5.2, 3.5.3, 3.5.8	A vulnerability exists because file names are not handled properly when a PostScript (PS) or Portable Document Format (PDF) file is contained within a compressed archive, which could let a malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	GhostView GZip Command Execution	High	Bug discussed in newsgroups and websites.
Citrix ²¹	Windows 2000	MetaFrame XP, XP SP1&2	A vulnerability exists which could let a malicious user change the Citrix ICA Client .ICA configuration file to execute arbitrary programs instead of published applications.	No workaround or patch available at time of publishing.	Citrix MetaFrame Client-Specified Published Applications	High	Bug discussed in newsgroups and websites. Exploit has been published.

¹⁷ Bugtraq, September 21, 2002.

¹⁸ NTBugtraq, September 22, 2002.

¹⁹ Gentoo Linux Security Announcement, October 3, 2002.

²⁰ "After" Security Advisory, ASA-0000, October 1, 2002.

²¹ Bugtraq, October 2, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Common Name ²²	Windows	Common Name Toolbar 3.5.2 .0	A vulnerability exists because local Intranet addresses are exposed when the Intranet server name is entered, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	CommonName Toolbar Potential Information Leakage	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Compaq Computer Corporation ²³	Multiple	Compaq TCP/IP Services For OpenVMS 4.2, 5.0 a, 5.1, 5.3	A vulnerability exists in the UCX POP (Post Office Protocol) server, which could let an unauthorized malicious user obtain access to privileges files or unauthorized privileges.	Patch available at: http://ftp1.support.compaq.com/patches/public/vms/axp/v7.3/tcpip/5.3/	OpenVMS UCX POP Server	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Compaq Computer Corporation ²⁴	Windows NT 4.0/2000, XP, Unix	HP WEBES Service Tools 2.0, 3.1, 4.0, 4.0 SP1-SP50	A vulnerability exists which could let a remote malicious user obtain unauthorized file access.	Patch available at: http://www.compaq.com/support/svctools/webes/webes-sp.html	HP WEBES Service Tools Unauthorized File Access	Medium	Bug discussed in newsgroups and websites.
Compaq Computer Corporation ²⁵	Multiple	Insight Management Agents 4.2, 4.37	A Cross-Site Scripting vulnerability exists in the web interface, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	HP Compaq Insight Manager Web Interface Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Coxco Support ²⁶	Unix	Midicart PHP, PHP Maxi, Midicart PHP Plus	A vulnerability exists in the default installation due to insufficient access control on 'admin' folder files, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Midicart Arbitrary File Upload	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Coxco Support ²⁷	Unix	Midicart PHP, PHP Maxi, PHP Plus	A vulnerability exists in the default installation due to insufficient access controls on files in the 'admin' folder, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Midicart Information Disclosure	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
DaCode ²⁸	Multiple	DaCode 1.2.0	A vulnerability exists because HTML IMG tags in a news message are not sufficiently filtered, which could let a remote malicious user execute arbitrary HTML or JavaScript code.	No workaround or patch available at time of publishing.	DaCode News Message HTML Injection	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

²² Bugtraq, October 3, 2002.

²³ Hewlett Packard Security Advisory, SSRT2371, September 25, 2002.

²⁴ Hewlett Packard Security Bulletin, SSRT2362, September 21, 2002.

²⁵ SecurityFocus, September 23, 2002.

²⁶ Bugtraq, October 2, 2002.

²⁷ Bugtraq, October 2, 2002.

²⁸ ECHU Alert #2, September 25, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Drupal ²⁹	Unix	Drupal 4.0.0	A vulnerability exists because HTML IMG tags in a news message are not sufficiently filtered, which could let a remote malicious user execute arbitrary HTML or JavaScript code.	No workaround or patch available at time of publishing.	Drupal News Message HTML Injection	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
EMUMail ³⁰	Windows, Unix	EMUMail for Red Hat Linux 5.0, EMUMail for Unix 5.0, EMUMail for Windows 5.0	A Cross-Site Scripting vulnerability exists in the 'emumail.cgi' script, which could let a remote malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	EmuMail Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Exploit has been published.
EMUMail ³¹	Windows, Unix	EMUMail for Red Hat Linux 5.0, EMUMail for Unix 5.0, EMUMail for Windows 5.0	A vulnerability exists when unexpected characters are inserted into some fields in web mail forms, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	EmuMail Web Root Path Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Eric PrevotEAU ³²	Unix	DCTC 0.83.3	A Denial of Service vulnerability exists due to inadequate checking when processing requests are a string that contains a NULL byte.	Upgrade available at: http://ac2i.tzo.com/dctc/dctc-0.83.4.tar.gz	DCTC NULL Byte Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.

²⁹ ECHU Alert #2, September 25, 2002.

³⁰ AIS advisory # 0005, September 29, 2002.

³¹ AIS advisory # 0004 September 29, 2002.

³² SecurityFocus, September 23, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Eric Raymond ^{33, 34, 35}	Unix	Fetchmail 5.4, 5.6-5.8, 5.9.6-5.9.14, 6.0.0	Multiple vulnerabilities exist: a buffer overflow vulnerability exists due to improper sanitization of user-supplied values for e-mail headers, which could let a remote malicious user cause Fetchmail to improperly allocate space on the system stack or possibly execute arbitrary code; a Denial of Service vulnerability exists due to improper boundary checks when processing e-mail headers in multidrop mode; and a buffer overflow vulnerability exists in the function that is used to parse e-mail headers, which could let a remote malicious user corrupt heap memory with attacker-supplied values and possibly execute arbitrary code.	Eric Raymond: http://www.tuxedo.org/~esr/fetchmail/fetchmail-6.1.0.tar.gz Engarde: ftp://ftp.engardelinux.org/pub/engarde/stable/updates/i386/fetchmail-ssl-6.1.0-1.0.5.i386.rpm	Fetchmail Multiple Vulnerabilities	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites.
Francisco Burzi ³⁶	Unix	PHP-Nuke 6.0	A Cross-Site Scripting vulnerability exists in the 'Search' page because HTML tags are not filtered from links to the 'modules.php' script, which could let a remote malicious user steal a user's cookie-based authentication credentials.	No workaround or patch available at time of publishing.	PHPNuke Cross-Site Scripting	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Francisco Burzi ³⁷	Windows, Unix	PHP-Nuke 6.0	A vulnerability exists because HTML code is not sufficiently filtered from news posts, which could let a remote malicious user execute arbitrary HTML or JavaScript code.	No workaround or patch available at time of publishing.	PHPNuke News Message HTML Injection	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Francisco Burzi ³⁸	Windows, Unix	PHP-Nuke 6.0	A vulnerability exists due to insufficient sanitization of SQL query variables, which could let a malicious user cause a Denial of Service or corrupt database information.	No workaround or patch available at time of publishing.	PHPNuke Modules.PHP SQL Injection	Low/Medium (Medium if the database is corrupted)	Bug discussed in newsgroups and websites. There is no exploit code required.

³³ e-matters GmbH Security Advisory, 03/2002, September 29, 2002.

³⁴ Gentoo Linux Security Announcement, October 1, 2002.

³⁵ EnGarde Secure Linux Security Advisory, ESA-20021003-023, October 3, 2002.

³⁶ Bugtraq, September 24, 2002.

³⁷ ECHU Alert #2, September 25, 2002.

³⁸ Bugtraq, September 25, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Funsoft ³⁹	Windows 95/98/ME	Dino's Webserver 1.2	A Directory Traversal vulnerability exists when an encoded dot-dot-slash sequence is appended to a request, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Dino's Webserver File Disclosure CVE Name: CAN-2002-1133	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Ghost View ⁴⁰	Unix	GhostView 1.3, 1.4, 1.4.1, 1.5, gv 2.7 b1-b5, 2.7.6, 2.9.4, 3.0.0, 3.0.4, 3.1.4, 3.1.6, 3.2.4, 3.4.2, 3.4.3, 3.4.12, 3.5.2, 3.5.3, 3.5.8	A buffer overflow vulnerability exists in the sscanf() function when a malformed postscript or Adobe pdf file is sent, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	GhostView Buffer Overflow CVE Name: CAN-2002-0838	High	Bug discussed in newsgroups and websites. Exploit script has been published.
GNU ^{41, 42, 43}	Unix	tar 1.13.25	A vulnerability exists due to the way pathnames for archived files are handled, which could let a malicious user overwrite arbitrary files.	RedHat: ftp://updates.redhat.com/	GNU Tar Archive Files CVE Name: CAN-2002-0399	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Hewlett Packard Systems ⁴⁴	Unix	LDAP-UX Integration B.03.00, B.02.00	A vulnerability exists in the 'pam-authz' component because r-commands are executed under the wrong user id., which could let a malicious user obtain elevated privileges.	Upgrade available at: http://software.hp.com	LDAP-UX Integration Pam-Authz Privilege Elevation	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Hewlett Packard Systems ⁴⁵	Multiple	Procurve Switch 1600M, 2400M, 2424M, 4000M, 8000M	A Denial of Service vulnerability exists when the switches are used in a stack configuration and the device reset command is issued.	HP has issued an advisory. A temporary fix is available for download. The file, C_09_16.swi is available for download at: ftp://procurve:4000m1@hprc.external.hp.com/ <i>Note: This is a temporary file and will be removed when a product upgrade is available.</i>	Procurve 4000M Switch Device Reset Denial of Service	Low	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.

³⁹ iDEFENSE Security Advisory, 09.23.2002, September 23, 2002.

⁴⁰ iDEFENSE Security Advisory, 09.26.2002, September 26, 2002.

⁴¹ Gentoo Linux Security Announcement, October 1, 2002.

⁴² Hewlett-Packard Company Security Bulletin, HPSBTL0209-068, October 1, 2002.

⁴³ Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:096-24, September 30, 2002.

⁴⁴ Hewlett-Packard Company Security Bulletin, HPSBUX0209-221, September 30, 2002.

⁴⁵ Hewlett Packard Security Advisory, HPSBUX0209-219, September 25, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Hewlett Packard Systems ⁴⁶	Unix	Virtual Vault 4.5, 4.6	A remote Denial of Service vulnerability exists in the mod_ssl module for Apache Web Server due to the way SSL requests are processed.	Patches available at: http://itrc.hp.com PHSS_27627, PHSS_27476	VirtualVault Apache mod_ssl Remote Denial of Service	Low	Bug discussed in newsgroups and websites.
IBM ⁴⁷	Unix	AIX 4.3, 4.3.1, 4.3.2, 4.3.3, 5.1	A buffer overflow vulnerability exists in the 'errpt' command, which could let a malicious user execute arbitrary code with root privileges.	Patch available at: ftp://aix.software.ibm.com/aix/efixes/security/errpt_efix.tar.Z	IBM AIX ERRPT Buffer Overflow	High	Bug discussed in newsgroups and websites.
Info-ZIP ^{48, 49, 50}	Unix	UnZip 5.2, 5.3, 5.31, 5.32, 5.40, 5.42,	A vulnerability exists due to the way pathnames for archived files are handled, which could let a malicious user obtain sensitive information.	RedHat: ftp://updates.redhat.com/	Info-ZIP UnZip Archive Files CVE Names: CAN-2001-1268, CAN-2001-1269	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Invision Power Services ⁵¹	Multiple	Invision Board 1.0, 1.0.1	A vulnerability exists in the 'phpinfo.php' script, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Invision Board ;phpinfo.php' Script	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Jelsoft Enterprises ⁵²	Windows, Unix	VBulletin	A vulnerability exists in the 'calendar.php' script due to improper sanitization of user-supplied input to URI parameters, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	VBulletin Calendar.PHP Command Execution	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Jetty ⁵³	Windows 95/98/ME/ NT 4.0/2000, XP, Unix	Jetty 3.1.6, 3.1.7, 4.1.0RC4	A vulnerability exists in the 'CGIServlet' which could let a malicious user execute arbitrary commands.	Upgrade available at: http://prdownloads.sourceforge.net/jetty/Jetty-4.1.1.zip?download	Jetty CGIServlet Arbitrary Command Execution	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Jetty ⁵⁴	Unix	Jetty 4.1	A Cross-Site Scripting vulnerability exists which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Jetty HTTP Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Exploit has been published.

⁴⁶ Hewlett Packard Security Bulletin, HPSBUX0209-220, September 23, 2002.

⁴⁷ SecurityTracker, Alert ID 1005327, October 1, 2002.

⁴⁸ Gentoo Linux Security Announcement, October 1, 2002.

⁴⁹ Hewlett-Packard Company Security Bulletin, HPSBTL0209-068, October 1, 2002.

⁵⁰ Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:096-24, September 30, 2002.

⁵¹ Bugtraq, September 24, 2002.

⁵² Securiteam, September 24, 2002.

⁵³ Westpoint Security Advisory, wp-02-0011, October 2, 2002.

⁵⁴ Securiteam, September 30, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Jetty ⁵⁵	Unix	Jetty 4.1 .ORC4	A Cross-Site Scripting vulnerability exists due to improper sanitization of user requests, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Jetty Cross-Site Scripting	High	Bug discussed in newsgroups and websites.
KTH⁵⁶ <i>SuSE releases patches⁵⁷</i>	Unix	Heimdal 0.4 a-0.4 e	Several vulnerabilities exist: a vulnerability exists because the Kerberos Forwarding Daemon sends user and file information without integrity protection, which could let a malicious user overwrite any file and possibly exploit root; and a vulnerability exists because information sent from a client to a server is not properly checked for the termination of strings, which could let a malicious user exploit root.	Update available at: ftp://ftp.pdc.kth.se/pub/heimdal/src/heimdal-0.5.tar.gz SuSE: ftp://ftp.suse.com/pub/suse/	Kerberos Forwarding Daemon File Overwriting	Medium/ High (High if root is exploited)	Bug discussed in newsgroups and websites.
MDG Computer Services, Inc. ⁵⁸	Windows NT 4.0/2000, MacOS	Web Server 4D 3.6	A vulnerability exists because various types of credentials for optional modules are stored in plaintext, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	MDG Web Server 4D Insecure Credential Storage	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Michael Schatz ⁵⁹	Multiple	Books 0.6, 0.54	A Cross-Site Scripting vulnerability exists in the Books module, which could let a malicious user execute arbitrary HTML or JavaScript code.	No workaround or patch available at time of publishing.	Books PostNuke Module Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Microsoft ⁶⁰	Windows 95/98/ME/ NT 4.0/2000	Internet Explorer 5.0.1, 5.0.1 SP1&2, 5.0.1 for Windows NT 4.0, 98, 95, 2000, 5.5, 5.5 SP1&2, 5.5 preview, 6.0, 6.0SP1	A vulnerability exists due to the lack of access control checks when access to a document object is attempted through a saved reference, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Internet Explorer Document Reference	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

⁵⁵ Bugtraq, September 28, 2002.

⁵⁶ NetBSD Security Advisory 2002-018, September 17, 2002.

⁵⁷ SecurityFocus, September 30, 2002.

⁵⁸ SecurityOffice Advisories, September 25, 2002.

⁵⁹ Bugtraq, October 2, 2002.

⁶⁰ Bugtraq, October 1, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft ⁶¹	Windows	Internet Explorer 6.0 SP1	A vulnerability exists due the way URL handlers are handled, which could let a malicious user circumvent the restrictions by employing a HTTP redirect to a page which contains one of the restricted URIs.	No workaround or patch available at time of publishing.	Microsoft Internet Explorer URI Handler Restriction Circumvention	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Microsoft ⁶²	Windows NT 4.0/2000	Data Engine 1.0, 2000; SQL Server 7.0, 7.0 SP1-SP4, 2000, 2000 SP1&2	Multiple vulnerabilities exist: a buffer overflow vulnerability exists in the section of code in SQL Server 2000 (and MSDE 2000) associated with user authentication, which could let a malicious user cause a Denial of Service or execute arbitrary code with the privileges of the SQL Server process; a buffer overflow vulnerability exists in the one of the Database Console Commands (DBCCs) that ship as part of SQL Server 7.0 and 2000, which could let a malicious user execute arbitrary code with the privileges of the SQL Server process; and a vulnerability exists due to the way scheduled jobs in SQL Server 7.0 and 2000 are handled, which could let a malicious user execute arbitrary operating system commands with elevated privileges.	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/MS02-056.asp	Multiple Microsoft SQL Server Vulnerabilities CVE Names: CAN-2002-1123, CAN-2002-1137, CAN-2002-1138	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.
Microsoft ⁶³	Windows 98/ME/NT 4.0/2000, XP	Internet Explorer 6.0, 6.0 SP1	A vulnerability exists in the PKI implementation due to the way SSL certificates are processed where information is not available in the certificate or it is available in two places and there is a conflict, which could let a malicious user hijack an SSL session and decrypt messages.	No workaround or patch available at time of publishing.	Microsoft Internet Explorer SSL Certificate Expiration	Medium	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.

⁶¹ SecurityFocus, September 17, 2002

⁶² Microsoft Security Bulletin, MS02-056, October 2, 2002.

⁶³ Bugtraq, September 23, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft ⁶⁴	Windows 2000, XP	FrontPage Server Extensions 2000, 2002, Windows 2000 Advanced Server, 2000 Advanced Server SP1-SP3, 2000 Professional, 2000 Professional SP1-SP3, 2000 Server, 2000 Server SP1-SP3, Windows XP Home, XP Home SP1, XP Professional, XP Professional SP1	A buffer overflow vulnerability exists in the SmartHTML (shtml) interpreter component of FrontPage Server Extensions due to a flaw that could be exposed when processing a request for a particular type of web file, which could let a malicious user cause a Denial of Service (FrontPage Server Extensions 2000) or execute arbitrary code (FrontPage Server Extensions 2002).	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/MS02-053.asp	Microsoft FrontPage Server Extensions SmartHTML Buffer Overflow CVE Name: CAN-2002-0692	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.
Microsoft ⁶⁵	Windows	Virtual Machine 2000 Series, 3000 Series, 3100 Series, 3188, 3200 Series, 3300 Series, 3802 Series, 3805 Series	A vulnerability exists in a Java class that provides ODBC support due to errors in the security checking code, which could let a malicious user obtain unauthorized access.	No workaround or patch available at time of publishing.	Microsoft Virtual Machine Unauthorized ODBC Data Access	Medium	Bug discussed in newsgroups and websites.

⁶⁴ Microsoft Security Bulletin MS02-053 V1.1, September 26, 2002

⁶⁵ SecurityFocus, September 23, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft ⁶⁶	Windows NT 4.0/2000, XP	Microsoft Services for Unix 3.0	Multiple vulnerabilities exist: an integer overflow vulnerability exists in the XDR library function that allocates memory for an External Data Representation (XDR) array, which could let a malicious user cause a Denial of Service or possibly execute arbitrary code; a Denial of Service vulnerability exists when a malicious user sends a RPC request to the RPC server with an improper parameter size check; and a vulnerability exists because an application using the Sun RPC library does not properly check the size of client TCP requests, which could let a malicious user cause a Denial of Service. <i>Note: All three vulnerabilities discussed in this bulletin involve the inclusion of the Sun RPC library in Microsoft's Services for UNIX (SFU) 3.0 on the Interix SDK</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/MS02-057.asp	Multiple Microsoft Services for Unix 3.0 Interix SDK CVE Names: CAN-2002-0391, CAN-2002-1140, CAN-2002-1141	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites.
Microsoft ⁶⁷	Windows 98/ME, XP	Windows 98 With Plus! Pack, Windows ME, XP Home SP1, XP Home	Multiple vulnerabilities exist: a buffer overflow vulnerability exists when a file is being decompressed that contains a malformed filename, which could let a malicious user execute arbitrary code; and a vulnerability exists in the decompression function, which could let a malicious user cause a file to be decompressed in a directory that is neither the user-specified directory or a child of the user-specified directory.	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/ms02-054.asp	Microsoft Windows 98/ME/XP File Decompression Vulnerabilities CVE Names: CAN-2002-0370, CAN-2002-1139	Medium/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites.

⁶⁶ Microsoft Security Bulletin, MS02-057, October 2, 2002.

⁶⁷ Microsoft Security Bulletin, MS02-054, October 2, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft ⁶⁸	Windows 2000, XP	Windows 2000 Advanced Server, 2000 Advanced Server SP1-SP3, 2000 Datacenter Server, 2000 Datacenter Server SP1-SP3, 2000 Professional, 2000 Professional SP1-SP3, 2000 Server, 2000 Server SP1-SP3, 2000 Terminal Services, 2000 Terminal Services SP1-SP3, XP Home, XP Home SP1, XP Professional, XP Professional SP1	A buffer overflow vulnerability exists in the PPTP (Point to Point Tunneling Protocol) implementation when a specially crafted PPTP packet is sent to the PPTP service listening on port 1723, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code.	No workaround or patch available at time of publishing.	Microsoft PPTP Server Buffer Overflow	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites.

⁶⁸ phion Security Advisory, September 26, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft ⁶⁹	Windows 98/ME/NT 4.0/2000, XP	Windows 2000 Advanced Server, SP1-SP3, 2000 Professional, SP1-SP3, 2000 Server, SP1-SP3, 2000 Terminal Services, SP1-SP3, 98, 98 a/b/j, 98SE, ME, NT Server 4.0, NT Server 4.0 SP1-SP6a, NT Terminal Server 4.0, alpha, SP1-SP6a, NT Workstation 4.0, 4.0 SP1-SP6a, Windows XP, XP 64-bit Edition, SP1, XP Home, SP1, XP Professional, SP1	Two vulnerabilities exist: a buffer overflow vulnerability exists in a function that is exposed in an ActiveX control, which could let a malicious user execute arbitrary code; and a vulnerability exists due to flaws associated with the handling of compiled HTML Help (.chm) files that contain shortcuts, which could let a malicious user execute arbitrary commands.	Frequently asked questions regarding this vulnerability and the patch can be found at:	Microsoft Windows Help Facilities CVE Names: CAN-2002-0693, CAN-2002-0694	High	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.
Microsoft ⁷⁰	Windows 95/98/ME/NT 4.0/2000, XP	Word 2000, Word 2000 SR1&1a, Word 2000 SP2, Word 2002, Word 2002 SP1, Word 95, Word 97, Word 97 SR1&2	A vulnerability exists if the 'INCLUDEPICTURE' Field Code is included in a document and references a URL, which could let a remote malicious user insert arbitrary URLs into a document and obtain sensitive information.	No workaround or patch available at time of publishing.	Microsoft Word INCLUDE PICTURE Document Sharing File Disclosure	Medium	Bug discussed in newsgroups and websites. Exploits have been published.
Monkey ⁷¹	Unix	Monkey HTTP Daemon 0.1.4	A vulnerability exists when a malicious query is passed to the server, which could let a malicious user obtain sensitive information.	Upgrade available at: http://monkeyd.sourceforge.net/download.php?vrs=M C41LjA=	Monkey HTTP Server Sensitive Information	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

⁶⁹ Microsoft Security Bulletin, MS02-055, October 2, 2002.

⁷⁰ Bugtraq, September 19, 2002.

⁷¹ Illegal Instruction Labs Advisory, September 25, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Monkey ⁷²	Unix	Monkey HTTP Daemon 0.1.4, 0.4-0.4.2, 0.5	A Cross-Site Scripting vulnerability exists in the 'test2.pl' CGI script, which could let a malicious user execute arbitrary code	No workaround or patch available at time of publishing.	Monkey HTTP Server Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Mozilla ⁷³	Multiple	Bugzilla 2.14-2.14.4, 2.16	Multiple vulnerabilities exist: a vulnerability exists due to insufficient sanitization of apostrophes from e-mail address during account creation, which could let a malicious user obtain sensitive information or database corruption; a vulnerability exists in the 'usebuggroups' feature when a new product is added to a site that has many bug groups, the new group will be created with extra privileges set, which could let a malicious user obtain access to other group privileges; and a vulnerability exists in the 'bugzilla_e-mail_append.pl' script, which could let a malicious user execute arbitrary commands.	Upgrade available at: http://ftp.mozilla.org/pub/webtools/bugzilla-2.16.1.tar.gz	Bugzilla Multiple Vulnerabilities	Medium/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. There is no exploit code required for the 'usebuggroups' vulnerability.
Mozilla ⁷⁴	Multiple	Mozilla Browser 1.0	Multiple vulnerabilities exist that have been patched. These vulnerabilities could let a malicious user cause a Denial of Service, obtain sensitive information or cause arbitrary code to be executed. For a complete list of these vulnerabilities, see http://mozilla.org/releases/mozilla1.0.1/security-fixes-1.0.1.html .	Upgrade available at: http://www.mozilla.org/releases/	Mozilla Multiple Vulnerabilities	Low/Medium/High (Low if a Denial of Service, Medium if sensitive information is obtained and High if arbitrary code can be executed)	Bug discussed in newsgroups and websites.

⁷² Illegal Instruction Labs Advisory, September 30, 2002.

⁷³ Bugzilla Security Advisory, October 1, 2002.

⁷⁴ Bugtraq, September 18, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors ⁷⁵	Multiple	Aladdin Systems Inc. Stuffit Expander 6.5.2; Lotus Notes Client R6, R5, 4.5 & prior, 5.0-5.0.5, 5.0.9a, 5.10, 5.11; Windows 98 With Plus! Pack, ME, XP Home, SP1, XP Professional, SP1; Verity Inc. KeyView Viewing SDK; WinZip WinZip 7.0	A vulnerability exists in libraries from multiple vendors because they behave unpredictably when processing ZIP files having entries with long filenames, which could let a malicious user cause a Denial of Service and possibly execute arbitrary code.	Microsoft: Microsoft has incorporated the fix for the malformed filename buffer overflow into Windows XP SP1 available at: http://www.microsoft.com/windows98/downloads/contents/WUCritical/q329048/default.asp Apple: Apple has released Security Advisory APPLE-SA-2002-10-02. Users of Stuffit Expander 6.5.2 and earlier are advised to upgrade to Stuffit Expander 7.0 available at: http://www.stuffit.com/expander/cert.html	Multiple Vendor ZIP Files Long Filename Buffer Overflow CVE Name: CAN-2002-0370	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites.
Multiple Vendors ⁷⁶	Unix	Apache Software Foundation Tomcat 3.2-3.2.4; HP Virtual Vault 4.5, 4.6	A vulnerability exists when the Tomcat server 3.2.x is accessed with a special URL, which could let a remote malicious user obtain sensitive information.	Hewlett Packard: http://itrc.hp.com PHSS_27921, PHSS_27922	Tomcat Directory Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.

⁷⁵ Rapid 7, Inc. Security Advisory, October 3, 2002.

⁷⁶ Hewlett-Packard Company Security Bulletin, HPSBUX0209-222, September 30, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors ^{77, 78}	Windows NT 4.0/2000, Unix	Apache Software Foundation Apache 1.3.20, 1.3.22-1.3.26; Oracle Internet Application Server 1.0.2.1, 1.0.2.0, 8i Enterprise Edition 8.1.7.1.0, 8.1.7.0.0, 9i Application Server, 1.0.2.2, 1.0.2.1s, 1.0.2, 9.0.2, 9.0.2 release 2, 9iAS Reports 9.0.2 .1, Oracle8 8.1.7, 8.1.7.1, 8.1.7, Oracle9i Release 2 9.2 .2, 9.0.2	Multiple vulnerabilities exist: a Denial of Service vulnerability exists due to the way the Apache scorecare is handled; a Cross-Site Scripting vulnerability exists due to improper sanitization of SSI error pages, which could let a malicious user execute arbitrary HTML or JavaScript code; and a buffer overflow vulnerability exists in the ab.c web benchmarking support utility , which could let a malicious user execute arbitrary code.	Apache Software Foundation: http://www.apache.org/dist/httpd/apache_1.3.27.tar.gz Oracle Corporation: Oracle has stated that fixes for affected software will be available October 8, 2002 through metalink. OpenPKG: ftp://ftp.openpkg.org/release/1.0/UPD/	Apache Web Server Multiple Vulnerabilities CVE Names: CAN-2002-0839, CAN-2002-0840, CAN-2002-0843	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites.
MySimple News ⁷⁹	Unix	MySimple News 1.0	Several vulnerabilities exist: a vulnerability exists in the 'users.php' script file due to improper sanitization of URI parameters, which could let a malicious user execute arbitrary code; a vulnerability exists because the administrative password is stored in cleartext, which could let a remote malicious user obtain the administrator password; and a vulnerability exists in the 'vider.php3' file because it can be accessed by unauthenticated remote malicious users.	No workaround or patch available at time of publishing.	MySimple News Multiple Vulnerabilities	Medium/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Exploits have been published. There is not exploit required for the vider.php3 file vulnerability.

⁷⁷ iDEFENSE Security Advisor, 10.03.2002, October 3, 2002.

⁷⁸ OpenPKG Security Advisory, OpenPKG-SA-2002.009, October 4, 2002.

⁷⁹ SecurityFocus, October 2, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
MySQL AB ⁸⁰	Windows NT	MySQL 3.23.49, 4.0.0, 4.0.1	A buffer overflow vulnerability exists when an overly long string is supplied for the 'datadir' parameter in my.ini, which could let a malicious user execute arbitrary commands.	Upgrade available at: http://www.mysql.com/downloads/index.html	MySQL Buffer Overflow	High	Bug discussed in newsgroups and websites.
NetGear ⁸¹	Multiple	FVS318 1.1	A vulnerability exists when the device is configured to backup configuration settings because usernames and passwords are stored in cleartext, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	FVS318 Username/ Password Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Net-SNMP ⁸²	Unix	Net-SNMP 5.0.1, 5.0.3, 5.0.4 .pre2	A Denial of Service vulnerability exists due to improper handling of some requests.	Upgrade available at: http://sourceforge.net/project/showfiles.php?group_id=12694	Net-SNMP Denial of Service CVE Name: CAN-2002-1170	Low	Bug discussed in newsgroups and websites.
NPDS ⁸³	Multiple	NPDS 4.8	A vulnerability exists because HTML IMG tags in a news message are not sufficiently filtered, which could let a remote malicious user execute arbitrary HTML or JavaScript code.	No workaround or patch available at time of publishing.	NPDS News Message HTML Injection	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
NullLogic ⁸⁴	Windows, Unix	Null HTTPd 0.5	A buffer overflow vulnerability exists when a negative 'content length' value is passed to the server, which could let a remote malicious user crash the web server or execute arbitrary code.	Upgrade available at: http://prdownloads.sourceforge.net/nullhttpd/nullhttpd-0.5.1.tar.gz	Null HTTPd Remote Heap Overflow	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Exploit script has been published.
NullSoft ⁸⁵	Windows ME	Winamp 3.0	A buffer overflow vulnerability exists inside the XML parser DLL that could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Winamp Skin File Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit has been published.

⁸⁰ Westpoint Security Advisory, wp-02-0003, October 2, 2002.

⁸¹ Bugtraq, September 27, 2002.

⁸² iDEFENSE Security Advisory, 10.02.2002, October 2, 2002.

⁸³ ECHU Alert #2, September 25, 2002.

⁸⁴ Netric Security Advisory, September 22, 2002.

⁸⁵ Illegal Instruction Labs Advisory, September 29, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
OpenBSD ⁸⁶	Unix	OpenBSD 2.0-3.1	A vulnerability exists in the setitimer(2) system call due to an error in the way signed integers are handled, which could let a malicious user obtain root privileges.	Patch available at: ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.1/common/015_kerntime.patch <i>Note: Apply by doing: cd /usr/src patch -p0 < 015_kerntime.patch And then rebuild your kernel.</i>	OpenBSD setitimer(2) Kernel Memory Overwrite	High	Bug discussed in newsgroups and websites.
phpMyNews Letter ⁸⁷	Unix	phpMyNewsLetter 0.6.10	A vulnerability exists in the 'customize.php' script, which could let a malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	phpMyNews Letter Remote File Include	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
PostNuke Development Team ⁸⁸	Unix	PostNuke 0.721	A Cross-Site Scripting vulnerability exists, which could let a malicious user execute arbitrary HTML and script code.	Patch available at: http://developers.postnuk e.com/cgi-bin/viewcvs.cgi/*checkout*/postnukedevel/html/includes/pnAPI.php?rev=HEAD&content-type=text	PostNuke Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.
PostNuke Development Team ⁸⁹	Unix	PostNuke 0.721	A vulnerability exists due to insufficient sanitization of variables used in SQL queries, which could let a remote malicious user cause a Denial of Service or corrupt the database information.	Patch available at: http://developers.postnuk e.com/cgi-bin/viewcvs.cgi/*checkout*/postnukedevel/html/includes/pnAPI.php?rev=HEAD&content-type=text	PostNuke Remote SQL Injection	Low/ Medium (Medium if the database is corrupted)	Bug discussed in newsgroups and websites. There is no exploit code required.
Power Phlogger ⁹⁰	Unix	Power Phlogger 2.0.9, 2.2.1, 2.2.2 a	A vulnerability exists in the 'showhits.php3' script, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	PowerPhlogger showhits.php3 Script	High	Bug discussed in newsgroups and websites.
Py-Membres ⁹¹	Multiple	Py-Membres 3.1	A vulnerability exists due to inadequate checking of URI parameters, which could let a remote malicious user obtain administrative privileges.	No workaround or patch available at time of publishing.	Py-Membres Index.PHP Unauthorized Access	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Rudi Benkovic ⁹²	Unix	JAWmail 1.0 -rc1, 1.0, 1.0.1	A Cross-Site Scripting vulnerability exists due to insufficient HTML code filtering of e-mail messages, which could let a malicious user execute arbitrary script code.	Upgrade available at: http://prdownloads.sourceforge.net/jawmail/jawmail-2.0rc3.tar.gz?download	JAWMail Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

⁸⁶ SecurityFocus, October 2, 2002.

⁸⁷ SecurityFocus, October 3, 2002.

⁸⁸ Bugtraq, September 25, 2002.

⁸⁹ Bugtraq, September 25, 2002.

⁹⁰ Bugtraq, October 2, 2002.

⁹¹ Bugtraq, October 2, 2002.

⁹² Bugtraq, September 23, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
SafeTP ⁹³	Windows 2000, Unix	SafeTP Server 1.46	A vulnerability exists when a passive session is initiated in a specific manner, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	SafeTP Passive Mode Sensitive Information	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Sendmail Consortium ⁹⁴	Unix	Sendmail 8.12.0-8.12.6	A vulnerability exists due to improper handling of long idents, which could let a remote malicious user bypass mail logging.	No workaround or patch available at time of publishing.	Sendmail Ident Logging Circumvention	Low	Bug discussed in newsgroups and websites.
Sendmail Consortium ⁹⁵	Unix	Sendmail 8.12.0-8.12.6	A vulnerability exists in SMRSH, which could let a malicious user bypass security checks and possibly execute arbitrary commands.	Patch available at: http://www.sendmail.org/patches/smrsh-20020924.patch	Sendmail SMRSH Security Bypass CVE Name: CAN-2002-1165	Medium/ High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Exploit script has been published.
Shana Corporation ⁹⁶	Windows, MacOS, Unix	Informed Designer 3.5, Informed Filler 3.5	A vulnerability exists when an encrypted document that was created by Informed is opened in a hex editor, which could let a malicious user obtain sensitive information.	Upgrade available at: http://www.shana.com	Shana Informed Information Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Sun Microsystems / Astaware Technologies Inc. ⁹⁷	Unix	Sun ONE Starter Kit 2.0; ASTAware SearchDisc 3.1	A Directory Traversal vulnerability exists in the search engine facility, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Sun ONE Starter Kit / ASTAware SearchDisc Search Engine Directory Traversal	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser. Proofs of Concept exploits have been published.
Sun Microsystems, Inc. ⁹⁸	Unix	Solaris 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86	A vulnerability exists in 'TTYPROMPT' environment variable, which could let a remote malicious user bypass authentication and obtain local access, including root if remote root logins are permitted.	No workaround or patch available at time of publishing.	Sun Solaris TTYPROMPT Authentication Bypass	Medium/ High (High if root access can be obtained)	Bug discussed in newsgroups and websites. There is no exploit code required.

⁹³ Bugtraq, September 27, 2002.

⁹⁴ Bugtraq, September 21, 2002.

⁹⁵ iDEFENSE Security Advisory, 10.01.02, October 1, 2002.

⁹⁶ Bugtraq, September 25, 2002.

⁹⁷ Bugtraq, September 29, 2002.

⁹⁸ Bugtraq, October 2, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Surf Control ⁹⁹	Windows NT 4.0/2000	SuperScout Web Filter for Windows NT/2000 3.0, 3.0.3, 4.0, 4.1	Multiple vulnerabilities exist: a vulnerability exists because some types of information is stored insecurely in an unrestricted directory, which could let a remote malicious user obtain sensitive information; a vulnerability exists in the EncryptString function due to weak encryption, which could let a malicious user obtain sensitive information; a Denial of Service vulnerability exists when a malicious user sends multiple overly long GET requests; a Directory Traversal vulnerability exists in the Reports Server due to improper filtering of triple-dot-slash sequences, which could let a malicious user obtain sensitive information; and a SQL injection vulnerability exists in the Reports Server due to insufficient input validation, which could let a remote malicious user obtain sensitive information or corrupt the database.	No workaround or patch available at time of publishing.	SuperScout Multiple Vulnerabilities CVE Names: CAN-2002-0705, CAN-2002-0706, CAN-2002-0707, CAN-2002-0708, CAN-2002-0709	Low/ Medium (Medium if sensitive information is obtained)	Bug discussed in newsgroups and websites. There is no exploit code required.
Tight Auction ¹⁰⁰	Multiple	TightAuction 3.0	A vulnerability exists because the configuration file can be retrieved via a web request, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	TightAuction Configuration File Information Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Trolltech Qt ¹⁰¹	Multiple	Assistant 1.0	A vulnerability exists because an unfiltered port (#7358) is opened when executed from the QT Designer program, which could let a remote malicious user obtain unauthorized access.	Contact the vendor about obtaining upgrades.	Trolltech Qt Assistant Default Port Unauthorized Access	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Ultimate PHP Board ¹⁰²	Unix	Ultimate PHP Board 1.0 b	A vulnerability exists due to insufficient input validation, which could let a malicious user obtain unauthorized access to data files.	No workaround or patch available at time of publishing.	Ultimate PHP Board Information Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.

⁹⁹ Westpoint Security Advisory, wp--02-0005, October 2, 2002.

¹⁰⁰ Bugtraq, October 2, 2002.

¹⁰¹ Bugtraq, September 29, 2002.

¹⁰² Bugtraq, October 2, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Unisys ¹⁰³	Multiple	Clearpath	A Denial of Service vulnerability exists when a port scan is initiated with NMap or similar tools.	No workaround or patch available at time of publishing.	Unisys 'Clearpath' Denial of Service	Low	Bug discussed in newsgroups and websites. Vulnerability can be exploited with NMap or similar portscanning utilities.
WASD ¹⁰⁴	Multiple	WASD HTTP Server 7.1-7.2.3, 8.0	<p>Multiple vulnerabilities exist in the default installation:</p> <ul style="list-style-type: none"> • Universal directory traversal • Instant access to the entire web server tree • Trivial bypassing of access control rules • Getting the location of the document root • Read access to the whole web server configuration • Read access to all web server logs • Disclosure of directories supposed to be hidden • Getting the list of all CGI scripts • Getting the sources of all CGI scripts • Read access to OpenVMS system files • User home directories might be readable • One very serious flaw in a CGI script enabled by default • Some problems with other cgi-scripts enabled by default. <p>Exploitation of these vulnerabilities by a remote malicious user could range from information disclosure to varying degrees of compromise. When combining different vulnerabilities, a remote SYSTEM (root) compromise is possible</p>	Upgrade available at: http://wasd.vsm.com.au/wasd/	Multiple OpenVMS WASD HTTP Server Vulnerabilities	<p>Medium/High</p> <p>(High if root is compromised)</p>	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.

¹⁰³ Bugtraq, October 2, 2002.

¹⁰⁴ Securiteam, October 1, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Watch Guard ¹⁰⁵	Multiple	Rapid Stream 8000, 6000, 500, 4000, 2000; Watch Guard Firebox V10, V100, V60, V80	Two vulnerabilities exist: a format string vulnerability exists in the VClass and legacy RSSA line of security appliances due to inadequate checking of user-supplied input for passwords in the CLI (command line interface) binary, which could let a remote malicious user execute arbitrary code with root privileges; and a vulnerability exists in CLI binary due to a failure to close a connection when an administrative user logs in with the -N option, which could let a malicious user obtain access to the CLI with administrative privileges.	Hotfix available at: ftp://RSSA:RS_s0ftware@ftp.watchguard.com/	WatchGuard Firebox VClass CLI Interface Vulnerabilities	High	Bug discussed in newsgroups and websites. There is no exploit code required for the CLI binary connection closure vulnerability.
WN Server ¹⁰⁶	Multiple	WN Server 1.18.2-1.18.7, 1.19.0-1.19.9, 2.0.0	A buffer overflow vulnerability exists due to insufficient bounds checking of data received in HTTP GET requests, which could let a malicious user execute arbitrary code.	Upgrade available at: http://hopf.math.nwu.edu/wn-2.4.4.tar.gz	WN Server Buffer Overflow CVE Name: CAN-2002-1166	High	Bug discussed in newsgroups and websites.
Xerox ¹⁰⁷	Windows	DocuShare 2.2	Several vulnerabilities exist: a vulnerability exists in the Upload Helper Utility, which could let a remote malicious user obtain sensitive information; and a vulnerability exists in the configuration settings, which could let a remote malicious user obtain unauthorized access.	No workaround or patch available at time of publishing.	Xerox DocuShare Vulnerabilities	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Ximian ¹⁰⁸	Unix	Evolution 1.0.3-1.0.8	A vulnerability exists in the camel component due to the failure to reauthenticate previously accepted SSL certificates when a connection is reestablished, which could let a malicious user inject a maliciously constructed certificate and intercept and modify SSL traffic.	No workaround or patch available at time of publishing.	Evolution SSL Certificate	Medium	Bug discussed in newsgroups and websites.
Xoops ¹⁰⁹	Unix	Xoops 1.0 RC3	A vulnerability exists due to insufficient filtering of HTML code from posted messages, which could let a malicious user execute arbitrary HTML or JavaScript code.	Upgrade available at: http://www.xoops.org/modules/mydownloads/visit.php?lid=231	XOOPS HTML Injection	High	Bug discussed in newsgroups and websites. Exploit has been published.

¹⁰⁵ Securiteam, September 30, 2002.

¹⁰⁶ iDEFENSE Security Advisory, 09.30.2002, September 30, 2002.

¹⁰⁷ Bugtraq, October 3, 2002.

¹⁰⁸ Bugtraq, October 3, 2002.

¹⁰⁹ Bugtraq, September 24, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Zope ¹¹⁰	Unix	Zope 2.1.x, 2.1.1, 2.1.7, 2.2.0, 2.2 beta1, 2.2-2.2.5, 2.3.0-2.3.3, 2.4.0-2.4.4 b1, 2.5.0, 2.5.1 b1, 2.5.1	A remote Denial of Service vulnerability exists in systems that permit users to write "Through The Web Code" due to insufficient input validation.	Hotfix available at: http://www.zope.org/Products/Zope/Hotfix_2002-04-15/Hotfix_2002-04-15.tgz	Zope "Through The Web" Remote Denial of Service CVE Name: CAN-2002-0687	Low	Bug discussed in newsgroups and websites.
Zope ¹¹¹	Windows, Unix	Zope 2.3.2, 2.3.3, 2.4.0-2.4.3, 2.4.4 b1, 2.5.0, 2.5.1	A vulnerability exists because XML-RPC requests are not handled properly, which could let a malicious user obtain sensitive information.	Upgrades available at: http://www.zope.org/Products/Zope/2.6.0b1/	Zope XML-RPC Request	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Zope ^{112, 113}	Unix	Zope 2.4.0-2.4.3, 2.4.4 b1, 2.5.0, 2.5.1	A vulnerability exists in the ZCatalog plug-in due to insecure default settings, which could let a remote malicious user bypass access control restrictions.	Hotfix available at: http://www.zope.org/Products/Zope/Hotfix_2002-06-14/Hotfix_2002-06-14.tgz <u>RedHat:</u> SRPMS: ftp://updates.redhat.com/	Zope ZCatalog Plug-In Access Control CVE Name: CAN-2002-0688	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.

¹¹⁰ Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:060-17, September 24, 2002.

¹¹¹ Bugtraq, October 1, 2002.

¹¹² Zope Alert 2002-06-14, September 26, 2002.

¹¹³ Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:060-17, September 24, 2002.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between September 20 and October 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, 38 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
October 4, 2002	Bearshare.4.0.6.txt	Exploit URL for the Bearshare Directory Traversal vulnerability.
October 4, 2002	Telnet.c	Script which exploits the Sun Solaris TTYPROMPT Authentication Bypass vulnerability.
October 4, 2002	Tl004.txt	Denial of Service exploit information for the Microsoft Windows Help Facility vulnerability.
October 4, 2002	Ward18.c	War dialer that scans a list of phone numbers, finding the ones where a modem is answering the call and generates phone numbers lists based on a user-supplied mask, in incremental or random order.
October 3, 2002	Kismet-2.6.1.tar.gz	Wireless network sniffer that is capable of sniffing using almost any wireless card supported in Linux, FreeBSD, OpenBSD and Mac OS X systems.
October 3, 2002	Sara-4.1.1.tgz	Security Auditor's Research Assistant (SARA) is a security analysis tool based on the SATAN model.
October 2, 2002	Pubappbrute.tar.gz	Exploit for the Citrix MetaFrame Client-Specified Published Applications vulnerability.
October 2, 2002	Solaris.login.txt	A document that describes how to compromise Solaris systems prior to version 9 by using a Telnet client only.
October 1, 2002	Idefense.smrsh.txt	Exploit techniques for the Sendmail SMRSH Security Bypass vulnerability.
October 1, 2002	Lcrzoex-4.15-src.tgz	A toolbox for network administrators and network malicious users that contains over 200 functionalities using network library lcrzo.
October 1, 2002	Rnmap_0.9.tar.gz	A python client/server package which allows many authorized clients to connect to a centralized NMap server to do their port scanning.
September 30, 2002	Gv-exploit.pdf	Exploit for the GhostView Buffer Overflow vulnerability.
September 30, 2002	Openssl-bsd.c	Script which exploits the Apache + OpenSSL vulnerability.
September 29, 2002	Cinik.tgz	A modified version of the Slapper worm.
September 29, 2002	Ethereal-0.9.7.tar.gz	A GTK+-based network protocol analyzer, or sniffer, that lets you capture and interactively browse the contents of network frames.
September 29, 2002	Nslconf.c	Exploit script for the Linuxconf v1.28r3 and below local exploit that uses the ptrace method for offset.
September 29, 2002	Openbsd-select-bug.txt	Denial of Service exploit for the OpenBSD select() vulnerability.
September 29, 2002	Spikeproxy-1.3.tar.gz	A web application analysis tool which uses the SPIKE API to help reverse engineer new and unknown network protocols.
September 29, 2002	Winfingerprint-0.5.3.zip	Advanced remote windows OS detection that can determine OS.
September 27, 2002.	Nullhttpd.c	Exploit for the Null HTTPd Remote Heap Overflow vulnerability.
September 26, 2002	Interbase-gds-exploit.c	Script which exploits the Interbase GDS_Lock_MGR Buffer Overflow vulnerability.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
September 25, 2002	Airsnot-0.2.1b.tar.gz	A tool for wireless LANs which recovers encryption keys by passively monitoring transmissions, computing the encryption key when enough packets have been gathered.
September 25, 2002	Apache-ssl-bug.c	Exploit for the Apache Buffer Overflow OpenSSL vulnerability..
September 25, 2002	Monkey014.pl	Perl script which exploits the Monkey HTTP Server Sensitive Information vulnerability.
September 25, 2002	Zyxb Brut.c	A brute force program written for the ZyXel router Telnet service.
September 24, 2002	Gspoofer-2.1.1.tar.gz	A GTK+ program written in C which makes easy and accurate the building and the sending of TCP packets with or without a data payload.
September 24, 2002	Php2.c	Script which exploits the VBulletin Calendar.PHP Command Execution vulnerability.
September 23, 2002	Alsaplayer-suid.c	Exploit for the Alsaplayer Local Buffer Overflow vulnerability.
September 23, 2002	Apache-stderr-dos.c	Exploit script for the Apache STDERR Denial of Service vulnerability.
September 23, 2002	Bakkum.c	Script which exploits the Null HTTPd Remote Heap Overflow vulnerability.
September 23, 2002	Netric-adv009.txt	Exploit for the Null HTTPd Remote Heap Overflow vulnerability.
September 23, 2002	Wireless_scan.txt	A document that defines how an intruder would identify a suitable open network to launch a malicious attack and what common methods are used.
September 22, 2002	Trillian-dos.c	Script which exploits the Trillian Multiple IRC Denial of Service Vulnerabilities.
September 21, 2002	Guardadv.db4web.txt	Exploit URL for the DB4Web Directory Traversal vulnerability.
September 21, 2002	Ngsniff-1.0.zip	A command line sniffer for Windows 2000 that does not require any packet driver.
September 21, 2002	Nidsfindshellcode.tgz	Proof of concept code based on the "Polymorphic shellcodes vs. Applications IDS" white paper.
September 21, 2002	Trillian-221.c	Script which exploits the Trillian JOIN Buffer Overflow vulnerability.
September 20, 2002	Trillian-join.c	Script which exploits the Trillian JOIN Buffer Overflow vulnerability.

Trends

- The National Infrastructure Protection Center (NIPC) is issuing this advisory to heighten the awareness of an e-mail-borne worm known as W32.Bugbear or I-Worm.Tanatos. For more information, see NIPC Advisory 02-008, located at: <http://www.nipc.gov/warnings/advisories/2002/02-008.htm> and Virus Section.
- The National Infrastructure Protection Center (NIPC) has been coordinating with the anti-virus and security community on the life cycle of "Slapper," the OpenSSL/Apache worm and all its variants. For more information, see NIPC ASSESSMENT 02-003, located at: <http://www.nipc.gov/warnings/assessments/2002/02-003.htm>.
- The SANS Institute and the National Infrastructure Protection Center (NIPC) have updated the list containing the Twenty Most Critical Internet Security Vulnerabilities. This list is broken into two categories: the ten most commonly exploited vulnerable services in Windows, and the ten most commonly exploited vulnerable services in Unix. For more detailed information, see: <http://www.sans.org/top20>.

- A record number of malicious hacking attempts were made during September with more than 4,157 attacks, and anti-American groups are responsible. Systems running Microsoft Windows suffered more attacks than all other operating systems combined, with only 1,740 attacks on Linux, 933 attacks on BSD and 229 attacks on Solaris.
- The CERT/CC has received reports of self-propagating malicious code that exploits a known buffer overrun vulnerability in the Secure Sockets Layer 2.0 (SSLv2) handshake process in OpenSSL. This malicious code has been referred to as Apache/mod_ssl worm, linux.slapper.worm, and bugtraq.c worm. For more information see CERT® Advisory CA-2002-27, located at: <http://www.cert.org/advisories/CA-2002-27.html>. Please ensure that you've applied the appropriate patch.
- Statistical weaknesses exist in TCP/IP Initial Sequence Numbers. For more information, see CERT® Advisory CA-2001-09, located at: <http://www.cert.org/advisories/CA-2001-09.html>.
- The Microsoft Product Support Services (PSS) Security Team has issued an alert regarding an increased level of hacking activity. These hacking attempts show similar symptoms and behaviors involving the detection of Trojans such as Backdoor.IRC.Flood and its variants, and the modification of the security policy on domain controllers.
- Web CGI exploits and Microsoft vulnerabilities continue to be two of the more frequent ways which external malicious sources conduct their probes in their attempt to gain access to networks.
- According to data compiled by its regional Global Command Centers (GCCs), which monitor and protect client networks from cyber-attacks, there has been a surge in cyber-attacks originating from Malaysia over the last quarter. The majority of these attacks were mainly Apache exploit attempts to execute arbitrary codes, which could lead to possible Denial-of-Service (DoS) attacks.
- The National Infrastructure Protection Center (NIPC) has issued an advisory to heighten the awareness of multiple buffer overflows in OpenSSL (Open Secure Sockets Layer). For more information, see NIPC Advisory 02-006, located at: <http://www.nipc.gov/warnings/advisories/2002/02-006.htm>.

Viruses

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. **To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available.** The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported during the latest three months), and approximate date first found. During this month, a number of anti-virus vendors have included information on Trojan Horses and Worms. Following this table are descriptions of new viruses and updated versions discovered in the last two weeks. *NOTE: At times, viruses may contain names or content that may be considered offensive.*

Ranking	Common Name	Type of Code	Trends	Date
1	W32/Klez	Worm	Stable	January 2002
2	W32/Nimda	File, Worm	Slight Increase	September 2001
3	Elkern	File Infector	Slight Increase	October 2001
4	W32/Yaha	Worm	Slight Decrease	February 2002
5	W32.Badtrans.B	Worm	Slight Increase	April 2001
6	Worm_BugBear.A	Worm	New to Table	September 2002
7	W32/Magistr	File, Worm	Slight Decrease	March 2001
8	W32/SirCam	Worm	Slight Decrease	July 2001
9	JS/NoClose	Trojan	Slight Increase	May 2002
10	Funlove	File	Slight Increase	November 1999

Note: Virus reporting may be weeks behind the first discovery of infection. A total 198 distinct viruses are currently considered "in the wild" by anti-virus experts, with another 361 viruses suspected. "In the wild" viruses have been reported to anti-virus vendors by their clients and have infected user machines. The additional suspected number is derived from reports by a single source.

HTML.Reality.D (Aliases: VBS/Reality, VBS.SVBVC-Based) (HTML Virus): This is a virus that attempts to prepend itself to .html, .htt, .asp, .hta, .htm, and .htx files on the infected computer. This script virus also disables security settings for Microsoft Word 2000. The virus writes itself to the beginning of any such files that it finds. It opens the Normal.dot file and infects it so that Microsoft Word documents are infected when you open or close them. On December 14 of any year, the virus creates a file named Porous.vbs in the Start Menu folder. On a random basis, the virus:

- Displays a harmless message
- Creates a link to an external Web page
- Changes the registered owner to "Porous"

Due to bugs in the code, this virus does not always run.

Linux/Devnull-A (Aliases: Linux/Slapper.E, Linux.Kaiten.Worm) (Linux Worm): This is a worm which spreads by exploiting the OpenSSL vulnerability in Apache mod_SSL module similarly to Linux/Slapper-A. The worm consists of four files. Three of these: shell.sh, sslx.c, and devnull, are used to spread; the fourth, k, is a Linux backdoor Trojan with distributed Denial of Service capabilities. The worm starts to spread when devnull runs and generates a random IP address. Once a valid address is generated, devnull calls the compiled sslx that runs the exploit code. The exploit, running on a remote machine, connects to a website and downloads the shell script shell.sh. The script shell.sh attempts to download, unpack and run two other files: k.gz and devnull.tar.gz.

Linux.Slapper.D (Alias: Linux/Slapper.worm.d) (Linux Worm): This is a worm that uses an OpenSSL buffer overflow exploit to run a shell on a remote computer. The worm targets vulnerable installations of the Apache Web server on Linux operating systems, which include versions of SuSe, Mandrake, RedHat, Slackware, and Debian. When Linux.Slapper.D attacks a computer, it attempts to connect on port 80. It sends an invalid GET request to the server to identify the Apache system. After the worm finds an Apache system, it tries to connect on port 443 to send the exploit code to the SSL service that is listening on the remote computer. The worm uses a Linux shell code exploit, which runs only on Intel platforms. This code requires the presence of the /bin/sh shell command in order to execute properly. The worm attempts to download a shell script from a Web site that no longer exists. The worm then appears to download and decompress two different .gz files, and execute two ELF files: "devnull" and "k." It appears to compile the file "sslx.c" using the "gcc" program. This program, "sslx," is then executed on the remote server in an attempt to spread from that machine. The "k" file runs as an IRC server on the remote machine and awaits commands from an IRC channel. The worm sweeps class B-sized networks, looking for Apache servers. The first byte of the network address is chosen randomly from the following list, and the second byte is

random: 3, 4, 6, 8, 9, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 24, 25, 26, 28, 29, 30, 32, 33, 34, 35, 38, 40, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 61, 62, 63, 64, 65, 66, 67, 68, 80, 81, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, 193, 194, 195, 196, 198, 199, 200, 201, 202, 203, 204, 205, 206, 207, 208, 209, 210, 211, 212, 213, 214, 215, 216, 217, 218, 219, 220, 224, 225, 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 236, 237, 238, 239.

VBS/Corica-A (Aliases: VBS/Corica@MM, VBS_CORICA.A, VBS.Corica) (Visual Basic Script Worm): This is a VBScript worm that sets the following registry entry so that any attempt to edit a file with a VBS extension using the default option of Notepad.exe will display the file

C:\Windows\Microsoft.txt:

- HKLM\Software\Classes\VBSfile\Shell\Edit\Command = C:\Windows\notepad.exe
%C:\Windows\Microsoft.txt

Microsoft.txt contains nothing but a nonsense of dots and dashes and is created by VBS/Corica-A. The worm sets the Internet Explorer start page to <http://www.latingua.com> and modifies the Windows Desktop wallpaper so that a large red, white and blue banner displaying the message "Costa Rica, es un pais libre y democratico." appears in the centre of the screen and the message "Viva Costa Rica!" scrolls along the bottom of the screen in red text. VBS/Corica-A copies itself to C:\Windows\Microsoft.vbs and creates a shortcut in the current folder, called Microsoft.Lnk, to run this VBS file. VBS/Corica-A attempts to e-mail itself to all contacts in the Outlook address book. The e-mail will have one of the following two sets of characteristics:

- Subject: Hi
- Message body: Please open the attachment is very important.
- Attached file: Microsoft.vbs

or

- Subject: Hola
- Message body: Aqui te mando un anexo muy importante que lo abras.
- Attached file: Microsoft.vbs

VBS/Corica-A also sets the following registry entry:

- HKCU\AutoSetup\Land = "Costa Rica"

VBS/Kakworm-F (Aliases: I-Worm.KakWorm.z, JS/Kak@M, JS.KakWorm.Z, JS_KAKWORM.F) (Visual Basic Script Worm): This worm has been reported in the wild. It is a variant of VBS/Kakworm, a worm that exploits security vulnerabilities in Microsoft Internet Explorer and Microsoft Outlook in a way similar to VBS/BubbleBoy-A. Microsoft have released a patch to deal with this security problem which we strongly recommend users install. For further information and to download the patch please view Microsoft Security Bulletin (MS99-032). The worm will run if the user has Internet Explorer, Outlook or Outlook Express, but it will only spread to other users if Outlook Express is used to send e-mail. Even if you receive an infected message, you cannot be affected unless you have an Internet Explorer based product installed. The worm arrives embedded in an e-mail message as the message HTML signature. The recipient of the message cannot see any visible symptoms as there is no displayable text in the signature. If the user opens or previews the infected e-mail message the worm drops file KAK.HTA into the Windows start-up folder. KAK.HTA runs the next time Windows is started, creates the C:\WINDOWS\KAK.HTM file and changes the Microsoft Outlook Express registry settings so that the KAK.HTM is automatically included in every outgoing message as a signature. The KAK.HTA also changes the Windows registry that it includes the name of the worm file. On the 1st of any month after 5 p.m. the worm displays the message "Kagou-Anti-Kro\$oft says not today" and runs Windows shutdown.

VBS.Pelic.Worm (Alias: IRC.Worm.Generic) (Visual Basic Script Worm): This worm spreads through mIRC and also the file-sharing network KaZaA. It tries to delete antivirus software on the infected computer.

W32.Ameter@m (Win32 Worm): This is a worm that requires Borland C++ 6.0 runtime libraries be installed for it to run. It overwrites all .exe files (except for Emm386.exe and Setver.exe) that reside in the %windir% folder. It also sends itself to an e-mail address that is contained within the worm. This e-mail message has the following characteristics:

- Subject: Brigada Ocho Bitmap Tools
- Attachment: <original worm file name>

W32/Blinkom-A (Aliases: WORM_BLINKOM.A, Worm.P2P.Blinkom, W32/Blinkom, Win32/Blinkom.worm, Win32/Venzu.Worm, Win32.Venzu.A) (Win32 Worm): This is a worm which attempts to spread via SMTP, IRC channels, KaZaA peer-to-peer shared folders, ICQ shared folders and by copying itself to drive A:. E-mails may arrive with messages in either English or Spanish and have various characteristics. W32/Blinkom-A may drop copies of itself to the numerous folders and drives. The worm also attempts to disable certain firewall programs (ZoneAlarm, BlackIce, Tiny and Sygate), delete files related to anti-virus software, disable registry settings related to macro security within Microsoft Office and run itself on system restart by adding an entry to SYSTEM.INI. W32/Blinkom-A attempts to add the following entries to the registry:

- HKEY_LOCAL_MACHINE\Software\KasperskyLab\SharedFiles\avpfolder = "Blink Folder"
- HKEY_LOCAL_MACHINE\Software\KasperskyLab\SharedFiles\avpfolder\VEDataFilePath = "The Blink Path"
- HKEY_LOCAL_MACHINE\Software\KasperskyLab\SharedFiles\avpfolder\VEIndexFilePath = "The Plink, the Blink, the Oink"
- HKEY_LOCAL_MACHINE\Software\KasperskyLab\SharedFiles\avpfolder\MainDir = "Blink virus & the Batch company"
- HKEY_LOCAL_MACHINE\Software\KasperskyLab\SharedFiles\avpfolder\Folder = "Plink it's the Blink guitarist yeeeee!"
- HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Options\EnableMacroVirusProtection = "0"
- HKEY_CURRENT_USER\Software\Microsoft\Office\8.0\Word\Options\EnableMacroVirusProtection = "0"
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RegisteredOwner = "Blink"
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RegisteredOwnerRegisteredOrganization = "The Blink company inc."

W32/Bugbear-A (Aliases: WORM_BUGBEAR.A, Win32.Bugbear, W32/Bugbear@MM, I-Worm.Tanatos, W32/Bugbear, Tanatos, Tanat, WORM_NATOSTA.A, I-Worm/Keywo) (Win32 Worm): This worm has been reported in the wild. It is a network-aware worm. W32/Bugbear-A spreads by sending e-mails containing attachments and by locating shared resources on your network to which it can copy itself. Note that W32/Bugbear-A tries to copy itself to all types of shared network resource, including printers. Printers cannot become infected, but they will attempt to print out the raw binary data of W32/Bugbear-A's executable code. This usually results in many wasted pages. The worm attempts to exploit a MIME and an IFRAME vulnerability in some versions of Microsoft Outlook, Microsoft Outlook Express, and Internet Explorer. These vulnerabilities allow an executable attachment to run automatically, even if you do not double-click on the attachment. Microsoft has issued a patch that secures against these attacks. The patch can be downloaded from Microsoft Security Bulletin MS01-027. (This patch was released to fix a number of vulnerabilities in Microsoft's software, including the ones exploited by this worm.) If the worm activates, several new files will appear on your computer. Their names consist of letters of the alphabet randomly chosen by the worm. You will find:

- xxx.EXE (usually 50688 bytes) in the Startup folder
- yyyy.EXE (usually 50688 bytes) in the System folder
- zzzzzz.DLL (usually 5632 bytes) in the System folder

The two EXE files are executable copies of the worm. The DLL is a keystroke logging tool that is used by the worm when it is activated. The worm not only adds itself to the Startup folder, but also adds an entry to the following registry key:

- HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce

This means that the worm will be reactivated when your computer is rebooted. The worm spreads itself via e-mail. The e-mails can look like normal e-mails or they could have no body text and have various subject lines. Attachments can have the same filename as another file on the victim's computer but they may contain the various strings. The attachments have double extensions with the final extension being EXE, SCR or PIF. Please note that the worm can spoof the From and Reply To fields in the e-mails it sends. W32/Bugbear-A has a thread running in the background that attempts to terminate anti-virus and security programs. The keylogging component of W32/Bugbear-A (the DLL) hooks the keyboard input so that it records keystrokes to memory. When the user next connects to the Internet using a dial-up connection, the worm sends this information to one various remote e-mail addresses. W32/Bugbear-A opens port 36794 and listens for commands from a remote machine. The remote user may also attempt to open port 80 (HTTP) on the victim's computer, then connect to the backdoor web server (possibly an Apache 1.3.26-type web server) provided by W32/Bugbear-A and thus achieve a level of control over the infected computer.

W32.Cazinat@mm (Alias: I-Worm.Cazinat) (Win32 Worm): This is a worm that sends e-mail to addresses that it retrieves from .htm files. It also attempts to spread across the KaZaA file-sharing network. W32.Cazinat@mm is a Visual Basic application that is compiled to native code. The e-mail would arrive with the following characteristics:

- Subject: Screen Saver Canapa
- Attachment: Canapa.scr

W32.Elet (Win32 Virus): This is a virus that copies itself as %windir%\Pstnoop.exe and randomly deletes .exe files from the %windir% and the %system% folders. It performs this action repeatedly. The virus then copies itself to the %windir% folder using the deleted file names. For example, if it deletes the files %windir%\Test1.exe and %system%\Test2.exe, it will copy itself as %windir%\Test1.exe and %windir%\Test2.exe. It then sleeps for a while and then repeatedly performs the delete-and-copy routine.

W32.Gillich.Mirc (Win32 Worm): This is a worm that spreads using mIRC, the Windows Internet Relay Chat (IRC) client. This worm attempts to disable various antivirus software processes if they are running.

W32.HLLP.Flate.D (Alias: W32.HLLP.Flate): This is a variant of W32.HLLP.Flate. It is a prepender virus that is written in C# and which infects only .NET executable files. The virus functions only if the .NET Framework is installed. Security Response has not received any reports of this virus in the wild. When the virus is executed, it displays the message, “::: now infecting dotnet files only :P :::”

W32.HLLP.Ipamor (Win32 Worm): This is a virus that attempts to prepend itself to .exe files. The virus may also attempt to terminate some antivirus and firewall processes. It is written in the Microsoft C++ programming language. When W32.HLLP.Ipamor runs, it creates the file C:\%windir%\Mswdm.exe, which is the pure viral body of the virus. The attribute of the file is set to hidden. It adds the value, “WDM MSWDM.EXE,” to both of these registry keys:

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

so that the virus runs when you restart Windows. The virus searches for the file named C:\Mswdm.pro. If this file exists, the virus will not infect any files. Otherwise, it tries to create the file Sys.try file in the root of each logical drive beginning from drive D. If it successfully creates the file, it then searches for all .exe file on those drives and prepends itself to the host files that it finds. It also appends 18 bytes to the end of each host file.

W32/Hobbit.a@MM (Win32 Virus): Written in Visual Basic, this virus attempts to spread by mailing itself to e-mail addresses extracted from the temporary Internet files, and sharing itself over KaZaA networks. The original source code has been released leading to multiple compilations of this virus. One such variant is described below. When run on the victim machine, the virus copies itself to %WinDir%\KN0X.EXE a Registry key is added in order to run the virus at subsequent system startup, for example:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
"WinSrv" = C:\WINDOWS\kn0x.exe

The virus queries the Registry to obtain information concerning the system default SMTP settings:

- SMTP Server
- SMTP Display Name
- User
- SMTP E-mail Address

E-mail addresses are extracted from the temporary Internet files on the machine, and written to the file E-MAIL.TXT. The virus copies itself to the current directory with one of various filenames. This file may take various filenames, with .theme or .bat extension. The virus mails itself to addresses in E-MAIL.TXT. In testing, the outgoing messages contained From:, To: and Subject: headers followed by the message body text and two UUEncoded file attachments (no MIME headers). If either of these directories exist on the victim machine:

- C:\PROGRAM FILES\KAZAA\MY SHARED FOLDER
- C:\KAZAA\MY SHARED FOLDER

the virus copies itself there multiple times with various filenames. The virus also attempts to download a file compressor utility from a remote URL (saved locally as ZIPPY.EXE).

W32/Hobbit.b@MM (Win32 Virus): This virus is written in Visual Basic, this virus attempts to spread by mailing itself to e-mail addresses extracted from the temporary Internet files, and sharing itself using the KaZaA peer-to-peer file sharing network. The original source code has been released, leading to multiple compilations of this virus. This worm arrives as in an e-mail message containing the following information:

- Subject: AntiVirus Updates:
- Body: A Removal to scan for the new BugBear Virus. Recommended by%senders name% (note there is no space after the word "by")
- Attachments: One of numerous theme files and one of numerous non-.theme files.

When one of the .BAT, .EXE, .PIF, or .SCR files is run, the worm copies itself to the %WinDir% directory as Shizzle.exe and a registry run key is created to load the worm at startup:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\
Run "WinSrv"=C:\WINDOWS\Shizzle.exe

The .theme files that are attached to the message are also dropped on the infected system. They contain a 21 byte BAT file with the following instructions:

- @echo off
- cty nul

The virus contains a payload to use PING to initiate a Denial of Service attack against www.dokfleed.net.

W32.Hobble@mm (Alias: Worm.Alcaul.z) (Win32 Worm): This is a worm that attempts to spread across the KaZaA file-sharing network. It has mass-mailing capabilities, and can send itself to the e-mail addresses that it retrieves from the .htm and .html files that it finds in the Internet Explorer cache. W32.Hobble@mm is a Visual Basic application.

W32.Molim@mm (Win32 Worm): This is a mass-mailing worm that uses Microsoft Outlook to send itself to all contacts in the Microsoft Outlook Address Book. The e-mail message has the following characteristics:

- Subject: Vazna informacija!
- Attachment: Crack32.exe

This threat is written in the Microsoft Visual Basic (VB) programming language. When W32.Molim@mm runs, it tries to copy itself as:

- C:\%system%\Crack.exe
- C:\%system%\Crack32.exe

W32/Opaserv-A (Alias: Opasoft, WORM_OPASOFT.A, W32/Opaserv.worm, Win32.Opaserv, Worm.Win32.Opasoft) (Win32 Worm): This virus has been reported in the wild. It spreads via network shares. When executed the worm will create a file called scrsvr.exe in the Windows folder on the current drive. W32/Opaserv-A then adds the following registry entry to run itself when the system starts:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\ScrSvr =
C:\WINDOWS\ScrSvr.exe

The worm attempts to copy itself to the Windows folder on networked computers with open shared drives. It then modifies the win.ini file on the remote machine to ensure the copied file will be run on system start. The worm searches local IP addresses for open C: shares and attempts to copy itself to the Windows folder of the share. W32/Opaserv-A also attempts to connect to a website that is currently unavailable. This attempted connection is most likely intended as a means of updating the worm executable. The following three non-viral files may be found in the root folder of infected systems:

- tmp.ini
- scrsin.dat
- scrsout.dat

W32/Opaserv-B (Aliases: Worm.Win32.Opasoft.b, WORM_OPASOFT.B, BackDoor-ALB Trojan)

(Win32 Worm): This worm has been reported in the wild. It is a variant of W32/Opaserv-A and is a worm that spreads via network shares. When executed the worm will create a file called scrsvr.exe in the Windows folder on the current drive. W32/Opaserv-B then adds the following registry entry to run itself when the system starts:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\ScrSvr = C:\WINDOWS\ScrSvr.exe

The worm attempts to copy itself to the Windows folder on networked computers with open shared drives. It then modifies the win.ini file on the remote machine to ensure the copied file will be run on system start. The worm also searches local IP addresses for open C: shares and attempts to copy itself to the Windows folder of the share. W32/Opaserv-B also attempts to connect to a website that is currently unavailable. This attempted connection is most likely intended as a means of updating the worm executable. The following three non-viral files may be found in the root folder of infected systems:

- tmp.ini
- scrsin.dat
- scrsout.dat

W32/Opaserv.D.Worm (Aliases: WORM_OPASOFT.D, Backdoor.Opasoft, OPASOFT,

Worm.Win32.Opasoft.d) (Win32 Worm): This worm propagates across networks via shared C:\ drives. It attempts to download an executable file, which is likely an update of itself, from a specific site. The download site is currently not accessible and may have either been blocked or shut down. Upon execution, this worm drops a copy of itself named SCRSVR.EXE in the Windows directory of both the local machine and all the remote machines with shared drives. It then deletes the copy that was originally executed, provided that this copy is not located in the Windows directory. It also drops the following files in the root directory of drive C.

- SCRSIN.DAT
- SCRSOUT.DAT
- SCRLOG2

It uses these files during the information exchange with <http://www.op<blocked>soft.com>. The third file, SCRLOG2, is the new file dropped by this OPASOFT variant, and is not dropped by earlier versions of the worm. On the local machine, this worm creates the following registry entry so that it automatically executes at every Windows startup:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
ScrSvr = "%Windows%\SCRSVR.EXE"

*where %Windows% is the Windows directory, which is usually C:\Windows or C:\WINNT. At the same time, on the remote machines, this worm creates a file named TMP.INI in the C:\ directory and copies the content of the configuration file, WIN.INI, located in the Windows directory into this file. It then adds the following entry in the [windows] section of TMP.INI:

- run = C:\%Windows%\SCRSVR.EXE"

Afterwards, this worm copies back the contents of TMP.INI to WIN.INI. These changes enable SCRSVR.EXE to execute during Windows startup.

W32.Osapex (Alias: Win32.HLLW.Osapex) (Win32 Worm): This is a virus that copies itself back and forth from drives A and C. It copies itself as Vga32.exe. The virus has no damaging payload. Upon execution, it adds the line, "load=%windir%\Vga32.exe," to the %windir%\Win.ini file so that the virus runs each time that you start a Windows 95/98/Me-based computer. When copying itself to drive A, it

searches for any .doc files in the C:\Misdoc~1" folder. If it finds any such files, it appends the .exe extension to them, and copies itself as that file name to drive A drive.

W97M.Furio.B (Word 97 Macro Virus): This is a macro virus that infects documents created in Microsoft Word 97 and later. The virus infects when documents are opened or closed. The virus does not contain a malicious payload. W97M.Furio.B infects Microsoft Word 97 documents when they are opened or closed. Unlike many Microsoft Word macro viruses, it does not infect by way of the Normal.dot template; instead, it creates a file named Furio.dot in the Office\Startup folder. It then exports its code to Furio.driv and imports the code from Furio.driv when it infects documents. When seconds = minutes on the system clock and if the macro is running at that time, the virus opens a Notepad window and attempts to display a message. It also changes the Microsoft Word window to white lettering on a blue background. If the window was already white on blue, the virus changes it to black letters on a white background. The virus also changes the registered owner of the system to "The Walrus" and disables macro protection when you open documents.

WORM_ALCAUL.N (Aliases: CHILLER.A, I-Worm.Alcaul.n., Win32/Alcaul.AL.Worm, Win32/Alcaul@mm, W32/Alcaul-F, W32.Alcarys.F@mm) (Internet Worm): This worm uses Microsoft Outlook to e-mail copies of itself to all addresses listed in the infected user's address book. The details of the e-mail it arrives with are as follows:

- Subject: 101 Reasons Why You Should Have Sex When You're Drunk
- Attachment: 101 Reasons

This UPX-compressed worm is written in Visual Basic. Upon execution, this worm browses all drives and folders, including mapped folders on the network. It then displays a .GIF image with a cartoon of a man drinking beer and the text. This worm contains destructive code that does not execute properly.

WORM_CIANAM.A (Alias: CIANAM.A) (Internet Worm): This worm propagates via Internet Relay Chat and KaZaA, the popular peer-to-peer file sharing application. It also sends copies of itself via e-mail using Microsoft Outlook. The e-mail that it sends out is any combination of the various subjects and message bodies. The attachment also has various names. This file attachment, however, is actually BINARY.EXE, which is a copy of this worm. Upon execution, this worm displays a message box with the following text strings:

- W32.Join.A@mm - Coded by mANiAC89 [SpiderMan]/IndoVirus

It then drops a copy of itself as COOL_FILE.EXE in the root directory of drive C and modifies the registry to enable its automatic execution every system startup. The modified registry appears as follows:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run Join.A = "%Malware Directory%\BINARY.EXE"

*where %Malware Directory% is the directory where its copy, BINARY.EXE, is located.

WORM_P2PBONET.A (Aliases: W32.HLLW.Kazdot, Worm_P2PBonet, Worm.P2P.Bonet, W32/PeaTwoPea.worm, Win32.Kazdot worm) (Internet Worm): This worm, which only runs under the .NET framework, propagates via KaZaA, the popular peer-to-peer file sharing utility. Upon execution under a .NET framework environment, this worm shares the folder where it is located over the KaZaA file-sharing network. It does this by creating this registry entry:

- HKEY_CURRENT_USER\Software\Kazaa\LocalContent Dir0 = 012345: <worm's folder>

It then drops several copies of itself in the KaZaA shared folder using various filenames. By sharing the folder where it is located over the KaZaA network, it makes itself easily downloadable to all other users of KaZaA.

WORM_VEEDNA.A (Alias: SUSMIO.A) (Internet Worm): This Internet worm propagates via e-mail and KaZaA, the popular peer-to-peer file sharing utility. It sends itself as an attachment in an e-mail message with the following details:

- FROM: god
- TO: god@yahoo.com
- ATTACHMENT: <copy of worm from root directory>

Whenever an executable file is run, this worm opens the Web browser to an adult site.

XM97/Divi-AS (Excel 97 Macro Virus): XM97/Divi-AS creates the viral file 874.xls in the XLSTART folder.

Trojans

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

Trojan	Version	CyberNotes Issue #
AIM-Flood	N/A	CyberNotes-2002-16
Arial	N/A	CyberNotes-2002-08
Backdoor.Anakha	N/A	CyberNotes-2002-13
Backdoor.AntiLam	N/A	CyberNotes-2002-12
Backdoor.AntiLam.20	20	CyberNotes-2002-18
Backdoor.Armageddon.B	N/A	Current Issue
Backdoor.Assasin	N/A	CyberNotes-2002-14
Backdoor.Cabro	N/A	CyberNotes-2002-17
Backdoor.Cabrotor	N/A	CyberNotes-2002-18
Backdoor.Crat	N/A	CyberNotes-2002-12
Backdoor.Cyn	N/A	CyberNotes-2002-18
Backdoor.DarkFtp	N/A	CyberNotes-2002-19
Backdoor.DarkSky.B	N/A	Current Issue
Backdoor.Delf	N/A	CyberNotes-2002-16
Backdoor.Delf.B	B	CyberNotes-2002-16
Backdoor.Delf.C	C	CyberNotes-2002-17
Backdoor.Ducktoy	N/A	CyberNotes-2002-15
Backdoor.Easyserv	N/A	CyberNotes-2002-16
Backdoor.Elitem	N/A	Current Issue
Backdoor.Evilbot	N/A	CyberNotes-2002-09
Backdoor.Expjan	N/A	CyberNotes-2002-18
Backdoor.Fearic	N/A	CyberNotes-2002-16
Backdoor.FTP_Ana	N/A	Current Issue
Backdoor.FTP_Ana.B	B	Current Issue
Backdoor.FTP_Bmail	N/A	CyberNotes-2002-12
Backdoor.FunFactory	N/A	CyberNotes-2002-19
Backdoor.G_Door.Client	N/A	CyberNotes-2002-05
Backdoor.Goster	N/A	Current Issue
Backdoor.GRM	N/A	CyberNotes-2002-13
Backdoor.GSpot	N/A	CyberNotes-2002-12
Backdoor.Helios	N/A	CyberNotes-2002-19
Backdoor.Kaitex.B	N/A	Current Issue
Backdoor.Kavar	N/A	CyberNotes-2002-16
Backdoor.Kryost	N/A	CyberNotes-2002-18
Backdoor.Laphex	N/A	CyberNotes-2002-18

Trojan	Version	CyberNotes Issue #
Backdoor.Laphex.Client	N/A	CyberNotes-2002-18
Backdoor.Lastdoor	N/A	CyberNotes-2002-18
Backdoor.Latinus	N/A	CyberNotes-2002-12
Backdoor.Latinus.B	B	CyberNotes-2002-18
Backdoor.Litmus.2a	2a	Current Issue
Backdoor.Miffice	N/A	CyberNotes-2002-18
Backdoor.Mirab	N/A	CyberNotes-2002-13
Backdoor.Mite	N/A	CyberNotes-2002-18
Backdoor.MLink	N/A	CyberNotes-2002-16
Backdoor.Ndad	N/A	CyberNotes-2002-17
Backdoor.NetControle	N/A	CyberNotes-2002-13
Backdoor.Nota	N/A	CyberNotes-2002-12
Backdoor.Omed.B	B	CyberNotes-2002-11
Backdoor.Optix.04	04	CyberNotes-2002-19
Backdoor.OptixPro.10	10	CyberNotes-2002-18
Backdoor.OptixPro.11	11	Current Issue
Backdoor.OptixPro.12	12	CyberNotes-2002-18
Backdoor.Osirdoor	N/A	CyberNotes-2002-17
Backdoor.Pest.Cli	N/A	Current Issue
Backdoor.Pestdoor	N/A	Current Issue
Backdoor.Phoenix	N/A	CyberNotes-2002-19
Backdoor.Ptakks.B	N/A	CyberNotes-2002-18
Backdoor.RCServ	N/A	CyberNotes-2002-19
Backdoor.RemoteNC	N/A	CyberNotes-2002-09
Backdoor.RMFDoor.Cli	N/A	Current Issue
Backdoor.Robi	N/A	CyberNotes-2002-18
Backdoor.Roxrat.10	N/A	Current Issue
Backdoor.Sazo	N/A	CyberNotes-2002-13
Backdoor.Scanboot	N/A	CyberNotes-2002-17
Backdoor.Seamy	N/A	CyberNotes-2002-18
Backdoor.Sparta	N/A	CyberNotes-2002-13
Backdoor.Sparta.B	B	CyberNotes-2002-19
Backdoor.Tela	N/A	CyberNotes-2002-17
Backdoor.Theef	N/A	CyberNotes-2002-15
Backdoor.Tron	N/A	CyberNotes-2002-12
Backdoor.Ultor	N/A	CyberNotes-2002-13
Backdoor.WinShell	N/A	CyberNotes-2002-16
Backdoor.Y3KRat.15	N/A	CyberNotes-2002-17
Backdoor.Zenmaster	N/A	CyberNotes-2002-19
BackDoor-ABH	N/A	CyberNotes-2002-06
BackDoor-ABN	N/A	CyberNotes-2002-06
Backdoor-AKO	N/A	Current Issue
BackDoor-AKR	N/A	CyberNotes-2002-19
Banan.Trojan	N/A	CyberNotes-2002-15
Bck/Litmus.201	N/A	CyberNotes-2002-14
BDS/ConLoader	N/A	CyberNotes-2002-12
BDS/EHKSLogger	N/A	CyberNotes-2002-19
BDS/Osiris	N/A	CyberNotes-2002-06

Trojan	Version	CyberNotes Issue #
BDS/Pestdoor.4	N/A	Current Issue
BDS/Sporkbot	N/A	Current Issue
BKDR_EMULBOX.A	N/A	CyberNotes-2002-10
BKDR_INTRUZZO.A	N/A	CyberNotes-2002-09
BKDR_LITMUS.C	N/A	CyberNotes-2002-09
BKDR_WARHOME.A	N/A	CyberNotes-2002-06
Bneo.Trojan	N/A	CyberNotes-2002-18
Cardst	N/A	CyberNotes-2002-17
Cytron	N/A	Current Issue
Dewin	N/A	CyberNotes-2002-08
Downloader-W	N/A	CyberNotes-2002-08
FakeGina.Trojan	N/A	CyberNotes-2002-16
Fortnight	N/A	CyberNotes-2002-10
IIS.Beavuh-Exploit	N/A	CyberNotes-2002-17
IRC.kierz	N/A	CyberNotes-2002-16
IRC-Smev	N/A	CyberNotes-2002-08
Jekord	N/A	CyberNotes-2002-19
JS/NoClose	N/A	CyberNotes-2002-11
Liquid.Trojan	N/A	CyberNotes-2002-14
mIRC/Gif	N/A	CyberNotes-2002-08
Multidropper-CX	N/A	CyberNotes-2002-08
Netbus.160.Dropper	N/A	CyberNotes-2002-17
PWS-AOLFake	N/A	CyberNotes-2002-15
PWS-MSNCrack	N/A	CyberNotes-2002-18
PWS-MSNSteal	N/A	CyberNotes-2002-17
PWS-Ritter	N/A	CyberNotes-2002-16
PWSteal.BStroj	N/A	Current Issue
PWSteal.Kaylo	N/A	CyberNotes-2002-17
PWSteal.Netsnake	N/A	CyberNotes-2002-17
PWSteal.Profman	N/A	CyberNotes-2002-17
PWSteal.SoopSpy	N/A	CyberNotes-2002-18
QDel227	N/A	CyberNotes-2002-09
QDel234	N/A	CyberNotes-2002-11
RCServ	N/A	CyberNotes-2002-10
Reboot-R	N/A	CyberNotes-2002-18
StartPage-B	N/A	CyberNotes-2002-16
Swporta.Trojan	N/A	CyberNotes-2002-13
TR/EvilDX	N/A	CyberNotes-2002-19
TR/Win32.Rewin	N/A	CyberNotes-2002-12
Tr/WiNet	N/A	CyberNotes-2002-10
TR/WLoader	N/A	Current Issue
TR/Zirko	N/A	CyberNotes-2002-10
Trj/GhostGirl	N/A	CyberNotes-2002-19
Troj/Apher-A	N/A	CyberNotes-2002-17
Troj/Diablo	N/A	CyberNotes-2002-09
Troj/DSS-A	N/A	CyberNotes-2002-12
Troj/FireAnv-A	N/A	CyberNotes-2002-19
Troj/Flood-O	N/A	CyberNotes-2002-14
Troj/ICQBomb-A	N/A	CyberNotes-2002-05

Trojan	Version	CyberNotes Issue #
Troj/Kbman	N/A	CyberNotes-2002-10
Troj/Momma-B	N/A	CyberNotes-2002-11
Troj/Ritter-A	N/A	CyberNotes-2002-17
Troj/Tobizan-A	N/A	CyberNotes-2002-16
Troj/Unreal-A	N/A	CyberNotes-2002-16
TROJ_DOAL.A	N/A	CyberNotes-2002-14
TROJ_JUNTADOR.B	N/A	CyberNotes-2002-06
TROJ_JUNTADOR.G	N/A	CyberNotes-2002-10
TROJ_OPENME.B	N/A	CyberNotes-2002-09
TROJ_SMALL.J	N/A	CyberNotes-2002-10
TROJ_SMBNUKE.A	N/A	CyberNotes-2002-18
TROJ_SQLSPIDA.B	N/A	CyberNotes-2002-11
TROJ_SUOMIA.A	N/A	CyberNotes-2002-18
TROJ_WORTRON.10B	N/A	CyberNotes-2002-12
Trojan.Adclicker	N/A	CyberNotes-2002-19
Trojan.Adnap	N/A	CyberNotes-2002-17
Trojan.Allclicks.A	N/A	CyberNotes-2002-13
Trojan.Avid	N/A	CyberNotes-2002-19
Trojan.Beway	N/A	CyberNotes-2002-15
Trojan.Crabox	N/A	CyberNotes-2002-17
Trojan.DiabKey	N/A	CyberNotes-2002-18
Trojan.Diskfil	N/A	CyberNotes-2002-19
Trojan.Fatkill	N/A	CyberNotes-2002-09
Trojan.IrcBounce	N/A	CyberNotes-2002-19
Trojan.Junnan	N/A	CyberNotes-2002-16
Trojan.Lovead	N/A	CyberNotes-2002-19
Trojan.Nullbot	N/A	CyberNotes-2002-19
Trojan.Portacopo:br	N/A	CyberNotes-2002-16
Trojan.Prova	N/A	CyberNotes-2002-10
Trojan.PSW.Ajim bbs	N/A	CyberNotes-2002-19
Trojan.PSW.CrazyBilets	N/A	CyberNotes-2002-12
Trojan.PSW.M2	N/A	CyberNotes-2002-13
Trojan.Starfi	N/A	CyberNotes-2002-16
Trojan.Win32.Filecoder	N/A	CyberNotes-2002-18
Trojan.Win32.MSNTrick	N/A	CyberNotes-2002-17
Trojan.WinReboot	N/A	Current Issue
VBS.Lavra.B.Worm	N/A	CyberNotes-2002-19
VBS.Zevach	N/A	CyberNotes-2002-15
VBS_CHICK.B	N/A	CyberNotes-2002-07
W32.Alerta.Trojan	N/A	CyberNotes-2002-05
W32.Azak	N/A	CyberNotes-2002-16
W32.Cbomb	N/A	CyberNotes-2002-16
W32.Click	N/A	CyberNotes-2002-15
W32.Delalot.B.Trojan	N/A	CyberNotes-2002-06
W32.DSS.Trojan	N/A	CyberNotes-2002-09
W32.Estrella	N/A	CyberNotes-2002-13
W32.Evala.Worm	N/A	CyberNotes-2002-14
W32.IRCBot	N/A	CyberNotes-2002-14
W32.Kamil	N/A	CyberNotes-2002-16

Trojan	Version	CyberNotes Issue #
W32.Kotef	N/A	CyberNotes-2002-16
W32.Libi	N/A	CyberNotes-2002-10
W32.Maldal.J	N/A	CyberNotes-2002-07
W32.Nuker.Winskill	N/A	CyberNotes-2002-15
W32.Tendoolf	N/A	CyberNotes-2002-09
W32.Wabbin	N/A	CyberNotes-2002-15
WbeCheck	N/A	CyberNotes-2002-09
Winshell	N/A	CyberNotes-2002-15
Worm/Garra	N/A	Current Issue

Backdoor-AKO: This is a remote access Trojan targets Windows NT/2000/XP. When run, it opens port 22 for remote access. Possible actions that could occur are:

- Upload/download files to/from victim's system
- List current running processes
- Install other Trojans
- Steal username and password

Backdoor.Armageddon.B: Backdoor.Armageddon.B allows unauthorized access to the infected computer. When it is run, it disables antivirus and firewall software. Backdoor.Armageddon.B is a variant of a zoo Trojan. It is a server that is accessed through any number of known clients. When it runs, the executable moves itself to %windir%\System\Notify.exe. It modifies the %windir%\System.ini file so that it will run when you restart Windows. In the [boot] section of the file, it appends %windir%\system\Notify.exe to the shell= line. Typically this line is shell=explorer.exe, although some systems have additional boot shells loaded. When the infected computer is started, the Trojan notifies the malicious user. This Trojan uses port 6969.

Backdoor.DarkSky.B (Alias: Backdoor.DarkSky): This is a Trojan that is used to gain unauthorized access to an infected computer. It opens ports 5418 and 5419. This allows a malicious user to gain unauthorized access to the infected system. It first runs as a service and then copies itself to the \Windows\System folder as these files:

- Notepad.exe
- Knrel32.exe
- SysArchive.exe

It sets the attributes of these files to system, read-only, and hidden. This Trojan makes several changes to the Windows registry. It adds the value, "SysArchive SysArchive.exe," to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
- so that the Trojan runs each time that you start Windows. In the registry key:

- HKEY_LOCAL_MACHINE\Software\Classes\exe\shell\open\command

it changes the (Default) value to, "\Windows\System\Notepad.exe \"%1\" %*," so that the Trojan runs each time that you run an .exe file. It creates the registry key:

- HKEY_CLASSES_ROOT\.txt\shell\open\command

with the (Default) value of \Windows\System\Notepad.exe "%1" so that the Trojan runs each time that you open a .txt file. In these registry keys:

- HKEY_CLASSES_ROOT\txtfile\shell\open\command
- HKEY_CLASSES_ROOT\txtfile.txt\shell\open\command

it changes the (Default) value to, "\Windows\System\Notepad.exe \"%1\"," so that the Trojan runs each time that you open a .txt file.

Backdoor.Elitem: This is a Trojan horse that works under MSN Messenger. It allows a malicious user to remotely control an infected computer. It is written in the Microsoft Visual Basic (VB) programming language. Backdoor.Elitem consists of two parts: the server part that runs on the infected computer, and the client part that is run by the malicious user. It adds the value, "Wincfg.exe C:%Windir%\System32\Wincfg.exe," to the registry key:

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

so that the Trojan runs each time that you start Windows. When the Trojan runs on a computer on which MSN Messenger is installed, it allows the malicious user to remotely perform any of the following actions:

- Enable/disable the Trojan
- Open Notepad or Internet Explorer multiple times
- Enable/disable/swap mouse buttons
- Change the MSN user name
- View or obtain the MSN contact list
- Monitor MSN messages
- Send MSN messages
- Steal system information
- Log keystrokes

When the server part of Backdoor.Elitem runs, it copies itself as C:\%windir%\System32\Wincfg.exe. The attribute of this file is set to hidden.

Backdoor.FTP_Ana (Aliases: Backdoor.AnaFTP.01, BKDR_ANAFTP.A, BackDoor-ADW): This is a backdoor Trojan that gives an attacker unauthorized access to an infected computer. This Trojan copies itself as %system%\Run32dll.exe. The Trojan creates the value, “winstro %system%\RUN32DLL.exe,” in the registry key:

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

so that the Trojan starts when you start or restart Windows. It creates the value, “StubPath %system%\RUN32DLL.exe ASC,” in the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components\Winstro

The Trojan notifies the client side using ICQ pager. After it is installed, Backdoor.FTP_Ana awaits commands from the remote client. The commands give a malicious user full access to the file system of the infected computer.

Backdoor.FTP_Ana.B (Aliases: Backdoor.Ftp.Lana.01, Backdoor-ADW): This is a Trojan that gives an attacker unauthorized access to an infected computer. Once the Trojan is installed, the attacker is notified of the compromised system via ICQ pager. When Backdoor.FTP_Ana.B runs, it moves itself to %system%\MS_IIS.exe. It creates the value, “MS IIS 5.01 %system%\MS_IIS.exe,” in the registry keys:

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

so that the Trojan starts when you start or restart Windows. It modifies the Win.ini file by adding these lines in the [windows] section:

- run=%system%\MS_IIS.exe
- load=%system%\MS_IIS.exe

It modifies the [boot] section of the System.ini file as follows:

- shell=explorer.exe %system%\MS_IIS.exe

The Trojan notifies the client side using ICQ pager. After it is installed, Backdoor.FTP_Ana.B awaits commands from the remote client. The commands give a malicious user full access to the file system of the infected computer.

Backdoor.Goster: This is a backdoor Trojan that works under ICQ Messenger. It allows a malicious user to remotely control an infected computer. It is written using the Microsoft Visual Basic programming language. When Backdoor.Goster runs, it copies itself as C:\Windows\Command\Command.exe. It adds the value, “Currency <Trojan path and the file name>,” to the registry key:

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

so that the Trojan runs each time that you start Windows. When the Trojan runs on a computer on which ICQ is installed, it allows the malicious user to remotely perform any of the following actions:

- Enable/disable keyboard and mouse
- Swap mouse buttons
- Open/close the CD-ROM drive
- Send ICQ messages

This Trojan also creates C:\Windows\Sysnt.dll. This file is a text file; it is not viral itself, and as such, is not detected by Symantec antivirus products. If Backdoor.Goster infected your computer, delete this file.

NOTE: This Trojan may not work properly under Windows NT/2000/XP.

Backdoor.Kaitex.B [(Alias: W32.Kaiten.D): This is a backdoor Trojan that uses a randomly changed TCP port to connect to IRC servers of the malicious user choice. It allows the malicious user to remotely take control of the infected computer. When Backdoor.Kaitex.B runs, it adds this Trojan reference value, "Service <the Trojan file path and name>," to the registry key:

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

so that the Trojan runs each time that you start Windows. The Trojan opens a randomly changed TCP port to connect to IRC servers of the malicious user's choice and joins the #lerler IRC channel. It then waits for commands from the malicious user. The commands (which can include, but are not limited to the following) allow the malicious user to:

- Perform Distributed Denial of Service (DDoS) attacks
- Download files from a Web site of the malicious user's choice
- Run commands or files of the malicious user's choice
- Send private IRC messages
- Terminate the Trojan

Backdoor.Litmus.2a (Aliases: BackDoor-JZ, Backdoor.Litmus.II, BKDR_LITMUS2.A, Troj/Litmus-II): This is a backdoor Trojan that gives an attacker unauthorized access to an infected computer. This Trojan copies itself as %windir%\VxD\Blah.exe. The Trojan creates the value. "Windows %windir%\VxD\blah.exe," in the registry key:

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

so that the Trojan starts when you start or restart Windows. If the operating system is Windows 95/98/ME, the Trojan registers itself as a service process so that it continues to run after you log off. In this case, Backdoor.Litmus.2a closes only when the system is shut down. In addition, Backdoor.Litmus.2a attempts to obtain an access to the password cache that resides on the local computer. The cached passwords include modem and dial-up passwords, URL passwords, share passwords, and others. The Trojan connects to an IRC server and awaits for the commands that the malicious user transmits using IRC. The commands allow the malicious user to perform multiple actions, such as download and execute files, manage the installation of the backdoor Trojan, and so on.

Backdoor.OptixPro.11 (Alias: BackDoor-ACH): This is a backdoor Trojan that gives an attacker unauthorized access to an infected computer. By default it opens port 50021 on the compromised computer. Backdoor.OptixPro.11 is a Delphi application and is packed with tElock v0.98. It copies itself as %windir%\Win32loader.exe.

Backdoor.Pestdoor (Aliases: Backdoor.Pestdoor.10, Backdoor-AHS): This is a backdoor Trojan that allows a malicious user to remotely control an infected computer. It is written using the Delphi programming language. When Backdoor.Pestdoor runs, it copies itself as %system%\Winregse.exe. It adds the value, "winregse %System%\winregse.exe," to the registry key:

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

so that the Trojan runs each time that you start Windows. It opens two ports. One is for controlling the infected computer, and another is used to upload or download files. The malicious user controls an infected computer with the client program, which is detected as Backdoor.Pest.Cli.

Backdoor.Pest.Cli: This is the client part of a backdoor Trojan horse. This is the part that a malicious user uses to control an infected computer. When Backdoor.Pest.Cli runs, it displays a graphical user interface (GUI). From within this GUI, a malicious user can connect to computers that are infected with the server part of this backdoor Trojan horse. After the connection is made, the malicious user can perform various malicious actions. These include, but are not limited to, the following:

- Shut down or restart Windows
- Log the user out of Windows
- Transfer files
- Log keystrokes

- Get cached and saved passwords
- Clear the CMOS (this can potentially destroy the CMOS and leave the computer unusable)
- Take screen shots
- Disable the keyboard
- Disable the mouse

Backdoor.RMFDoor.Cli: This is the client for the backdoor Trojan RMFdoor (the server).

Backdoor.RMFdoor.Cli is used by the malicious user to remotely control computers that have been infected with the server part of this backdoor Trojan. When Backdoor.RMFDoor.Cli runs, it opens a graphical user interface (GUI). From this GUI the malicious user can control any computer that has been infected with the server part of this backdoor Trojan. This backdoor Trojan allows the malicious user to scan IP ranges for infected computers. After a connection to an infected computer has been made, the malicious user can perform many actions. They include, but are not limited to, the following:

- Send messages
- Open, play and stop the CD-ROM drive
- Restart, shut down, log off or display a blue screen on Microsoft Windows
- Open a URL in the default Web browser
- Run applications
- Send many messages to the infected computer to make it unstable
- Download, delete, or execute files
- Take screen shots

Backdoor.Roxrat.10 (Aliases: Backdoor.Roxrat, Backdoor.AIQ): Backdoor.Roxrat.10 allows unauthorized access to the infected computer. It also disables antivirus and firewall products. Backdoor.Roxrat.10 is written in Delphi and allows unauthorized access to the infected computer. When it runs, it copies itself as %windir%\System\Runvxd32.exe and %windir%\Pic.jpg.exe. It configures itself to run by each time that you start Windows by adding the value, "lol = %windir%\pic.jpg.exe," to these registry keys:

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

It also modifies the registry key:

- HKEY_LOCAL_MACHINE\Software\classes\txtfile\shell\open\command

so that the (Default) value is "@=%windir%\system\runvxd32.exe /notepad %1." As a result of this modification, Runvxd32.exe runs each time that you open a text file, and the text file opens in Notepad. In addition to the registry key modifications, the Trojan modifies the following startup files (on Windows 95/98/ME-based computers only) so that it runs when you restart Windows: System.ini. In the [boot] section of the System.ini file, it appends %windir%\pic.jpg.exe to the "shell=" line. Win.ini: In the [Windows] section of the Win.ini file, it adds the line run=%windir%\pic.jpg.exe. The Trojan uses port 5050 and TCP port 60552.

BDS/Pestdoor.4: Like other Trojans, BDS/Pestdoor.4 would potentially allow someone with malicious intent backdoor access to your computer. If executed, the Trojan adds the following file to the \windows\ directory, "msHtml.exe." So that it gets run each time a user restart their computer the following registry key gets added:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
MS HTML=C:\\WINDOWS\\msHtml.exe

BDS/Sporkbot: Like other Trojans, BDS/Sporkbot would potentially allow someone with malicious intent backdoor access to your computer. If executed, the Trojan adds the following file to the \windows%\system%\ directory, "Wintwdmu.exe." So that it gets run each time a user restart their computer the following registry keys get added:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
"MS Shell Services"="C:\\WINDOWS\\SYSTEM\\WINTWDMU.EXE"
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
"MS Shell Services"="C:\\WINDOWS\\SYSTEM\\WINTWDMU.EXE"

Cytron: A recent (09/30/02) ploy to get users to run this Trojan involved sending out fake messages saying that they had received a E-Card, and that they had to go to a specific site to pick it up. When they went to that site, a message said that they had to run an ActiveX control to view the card. If they accepted the ActiveX control, the Trojan would be installed on their system. The file is a CAB file containing a POTD.DLL. It installs as a browser helper object, and displays pop-ups while viewing web sites.

PWSteal.BStroj (Alias: Trojan.PSW.BStroj.19): This is password-stealing Trojan horse. It collects user passwords for MSN Messenger or Yahoo! Messenger and sends them to the malicious user. PWSteal.BStroj is written in Microsoft Visual Basic version 6.

Trojan.WinReboot: This is a Trojan horse that causes Windows to continuously restart the computer at the end of the startup process. Because it is written in Visual Basic, it requires the VB runtime libraries to execute. Also, Windows must be installed in C:\Windows. The file name for Trojan.WinReboot is Close.exe. When Trojan.WinReboot runs, it drops itself using the hard-coded path and file name C:\Windows\Close.exe. It modifies the C:\Windows\Win.ini file by adding the line.

“load=c:\windows\Close.exe,” to the [windows] section. As a result, the Trojan is executed at the end of computer's startup process, causing an immediate system reboot. This loop continues until you stop it. Because the Trojan prevents the Windows desktop from appearing, you cannot do anything to prevent the reboot unless a program or dialog box is open and waiting for response. If such a dialog box did appear, you could press Ctrl+Alt+Delete one time and End Task on the WINDOW~1 process, (which would stop the forced reboot), and then follow the Removal Instructions in this document. Windows NT/2000/XP are affected by this Trojan only if the operating system was installed in the C:\Windows folder. (This is the default for Windows XP; Windows NT/2000 are installed by default in C:\Winnt). In any case, even if the file were copied to these operating systems, at most you would see an error message such as "Run-time error '53': File not found." The Trojan cannot cause a Windows NT-based system to reboot, and it cannot attach itself to the normal boot or login process.

TR/WLoader: Like other Trojans, TR/WLoader would potentially allow someone with malicious intent backdoor access to your computer. If executed, the Trojan adds the following file to the \windows\ directory, "loadwmgr.exe." So that it gets run each time a user restart their computer the following registry key gets added:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
LoadWinMgr="C:\\WINDOWS\\loadwmgr.exe

Worm/Garra: This is a Trojan that can be exchanged through the P2P network KaZaA. It disguises itself by appearing as the video game Pac-Man. If executed, the worm renames the following files:

- C:\COMMAND.COM -> C:\VIRUS.EXE
- C:\WINDOWS\WIN.COM -> C:\WINDOWS\WIN.TXT
- C:\WINDOWS\COMMAND.COM -> C:\WINDOWS\MENU.TXT

Once the Worm/Garra file is ran, Pac2000 remains as an active process that allows it to continuously open and close the cd-rom drive. It then tries to power down the operating system. Upon execution, it will display a GIF image.