



National Infrastructure Protection Center CyberNotes

Issue #2002-07

April 8, 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 March 15 and April 4, 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
Algest ¹	Unix	Algest 1.0	A vulnerability exists because cookies are not properly checked for administrative rights, which could let a remote malicious user obtain administrative access to the guestbook.	No workaround or patch available at time of publishing.	Algest Cookie Verification	High	Bug discussed in newsgroups and websites. There is no exploit code required.

¹ Securiteam, March 26, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Analog ²	Multiple	Analog 3.9 0beta1&2, 4.0 1-4.0 4, 4.1, 4.9 0beta2-4, 4.9 1beta1, 4.11, 4.14-4.16, 5.0-5.0.3, 5.1 a, 5.2	A vulnerability exists because script code is not filtered when logfiles are analyzed, which could let a malicious user execute arbitrary script code.	Upgrade available at: http://www.analog.cx/download.html	Analog Logfile Script Code Injection	High	Bug discussed in newsgroups and websites.
Caldera International, Inc. ³	Unix	nscd 2.2.4	A vulnerability exists in the Name Service Cache Daemon (nscd) if a request is made for a DNS PTR record, which could let a malicious user obtain sensitive information.	Workaround: Caldera suggests disabling the hosts cache in /etc/nscd.conf by adding the line: enable-cache hosts no	nscd Incorrect Hosts Cache Behavior	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Caldera International, Inc. ⁴	Unix	OpenLinux Server 3.1.1, OpenLinux Workstation 3.1.1	A vulnerability exists because the startkde script insecurely initializes the 'LD_LIBRARY_PATH' environment variable, which could let a malicious user obtain sensitive information.	Patch available at: ftp://ftp.caldera.com/pub/updates/	OpenLinux StartKDE Script LD_LIBRARY _PATH	Medium	Bug discussed in newsgroups and websites.
Caldera International, Inc. ⁵	Unix	XFree86 X11R6 4.0.2 -11, 4.1 -11	A vulnerability exists in the MIT-SHM extension, which could let a malicious user obtain read/write access and possibly elevated privileges.	Upgrade available at: ftp://ftp.caldera.com/pub/updates/	XFree86 MIT-SHM	Medium	Bug discussed in newsgroups and websites.
CGI SCRIPT. NET ⁶	Unix	CSSearch 2.5 & prior	A vulnerability exists due to an access validation error in the 'setup.cgi' script, which could let a malicious user execute arbitrary code.	Upgrade available at: http://www.cgiscript.net/download/download.htm	CSSearch Remote Command Execution	High	Bug discussed in newsgroups and websites. Exploit has been published.
Cisco Systems ⁷	Multiple	Call Manager 3.0, 3.1	A Denial of Service vulnerability exists due to a memory leak in the Call Telephone Integration (CTI) Framework authentication.	Upgrade to 3.1(3a) available at: http://www.cisco.com	CallManager CTI Denial of Service	Low	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.

² Debian Security Advisory, DSA 125-1, March 28, 2002.

³ Caldera International, Inc. Security Advisory, CSSA-2002-013.0, March 26, 2002.

⁴ Caldera International, Inc. Security Advisory, CSSA-2002-005.0, April 1, 2002.

⁵ Caldera International, Inc. Security Advisory, CSSA-2002-009.0, March 15, 2002.

⁶ Bugtraq, March 25, 2002.

⁷ Cisco Security Advisory, 20020327-1.2, March 29, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Cisco Systems ⁸	Windows NT 4.0/2000	Cisco Secure ACS for Windows NT 2.6, 2.6.2, 2.6.3, 2.6.4, 3.0.1, 3.0	Two vulnerabilities exist: a vulnerability exists when connecting to port 2002 and sending a crafted URL, which could let a malicious user execute arbitrary code; and a vulnerability exists by using "..\." in the URL, which could let a malicious user obtain sensitive information.	Patch available at: http://www.cisco.com/cgi-bin/tablebuild.pl/cs-acs-win	CiscoSecure ACS Multiple Vulnerabilities	Medium/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites.
Citrix Systems, Inc. ⁹	Multiple	Nfuse 1.51, 1.6	A Cross-Site Scripting vulnerability exists because script code is not filtered from URL parameters in the 'launch.asp' and 'launch.jsp' scripts, which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	NFuse Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Exploit has been published.
Citrix Systems, Inc. ¹⁰	Multiple	Nfuse 1.5	A Directory Traversal vulnerability exists when a specially crafted request is submitted via the 'boilerplate.asp,' which could let a remote malicious user obtain sensitive information.	Upgrade available at: http://www.citrix.com/products/nfuse/default.asp	Nfuse boilerplate.asp Directory Traversal	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Cyrus-Utils ¹¹	Unix	SASL LDAP+MySQL Auth Patch 1.5.24, 1.5.27	A vulnerability exists due to a design problem in the patch, which could let a remote malicious user obtain unauthorized access to the mail accounts of others.	Upgrade available at: http://prdownloads.sourceforge.net/cyrus-utils/sasl-1.5.24-ldap-ssl-filter-mysql-patch4.tgz	SASL LDAP+MySQL Authentication Patch	Medium	Bug discussed in newsgroups and websites.
Darren Reed ¹²	Unix	IPFilter 3.4.25	A vulnerability exists when an attempt is made to connect to a system via TCP on a port that is filtered by IPFilter, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	IPFilter TTL Fingerprinting	Medium	Bug discussed in newsgroups and websites. This vulnerability may be exploited by using one of numerous available portscanning utilities and packet analysis utilities.
Deep Forest Software ¹³	Windows 95/98/NT 4.0/2000	Quik-Serv Webserver 1.1 B	A vulnerability exists because dot-dot-slash requests are not properly handled, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Quik-Serv Web Server Arbitrary File Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.

⁸ Cisco Security Advisory, 2002-04-03, April 3, 2002.

⁹ Securiteam, March 28, 2002.

¹⁰ Bugtraq, March 27, 2002.

¹¹ Bugtraq, April 2, 2002.

¹² Bugtraq, March 31, 2002.

¹³ Securiteam, April 4, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Dynamic Guestbook ¹⁴	Unix	Dynamic Guestbook 3.0	A Cross-Site Scripting vulnerability and an arbitrary command execution vulnerability exists because malicious characters from form fields are not sufficiently sanitized, which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	Dynamic Guestbook Cross-Site Scripting & Arbitrary Command Execution	High	Bug discussed in newsgroups and websites.
Etnus ¹⁵	Unix	TotalView 5.0 .0-4	A vulnerability exists due to insecure permission settings, which could let a malicious user obtain elevated privileges. This could lead to a possible root compromise.	No workaround or patch available at time of publishing.	TotalView Insecure UID/GID Privilege	Medium/ High (High if root compromise)	Bug discussed in newsgroups and websites.
Floosietek ¹⁶	Windows NT	FTGate Office 1.0 5, FTGatePro 1.0 5	Multiple vulnerabilities exist: a Denial of Service vulnerability exists because a mailbox can be locked before authentication via the usage of the POP3 USER command; a Denial of Service vulnerability exists when a large number of 'Rcpt to:' are specified in a SMTP session; and a heap overflow vulnerability exists if an extremely long parameter is supplied to the APOP command, which could let a malicious user execute arbitrary code.	Hotfix available at: FTGatePro: http://www.ftgate.com/download/files/Prohfl280.exe FTGateOffice: http://www.ftgate.com/download/files/officehfl280.exe	FTGate Multiple Vulnerabilities	Low/ High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. There is no exploit code required.
Gravity Storm Software ¹⁷	Windows NT 4.0/2000, XP	Service Pack Manager 2000 6.0, 6.1, 6.3	A vulnerability exists because the software creates a hidden share called 'SPM2000c\$', which could let a remote malicious user obtain read/write access to critical directories of the operating system.	No workaround or patch available at time of publishing.	Service Pack Manager 2000 Directory Permissions	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Hewlett Packard ¹⁸	Multiple	Praesidium Webproxy 1.0	A vulnerability exists when a specially crafted HTTP request is submitted, which could let an unauthorized remote malicious user obtain access to the network.	Patch available at: http://itrc.hp.com (PHSS_26478)	Praesidium Webproxy Unauthorized Access	Medium	Bug discussed in newsgroups and websites.

¹⁴ ITCP Advisory 7, April 3, 2002.

¹⁵ Securiteam, March 26, 2002.

¹⁶ Securiteam, April 4, 2002.

¹⁷ Bugtraq, March 20, 2002.

¹⁸ Hewlett-Packard Company Security Bulletin, HPSBUX0203-189, March 22, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
IBM ¹⁹	Multiple	Lotus Domino 5.0.9a	A vulnerability exists because specially crafted requests for MS-DOS devices are not properly handled, which could let a remote malicious user obtain sensitive information.	Upgrade available at: http://www.notes.net/qmrdow.n.nsf	Lotus Domino MS-DOS Device Path Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Icecast ²⁰	Windows 2000, Unix	Icecast 1.3.10, 1.3.7, 1.3.8 beta2, 1.3.11, WIN32 1.3.7	A buffer overflow vulnerability exists due to improper bounds checking on client sent data, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Icecast Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit script has been published.
LogWatch ²¹	Unix	LogWatch 2.1.1	A vulnerability exists due to a race condition during the temporary directory creation, which could let a malicious user obtain unauthorized root access.	No workaround or patch available at time of publishing.	LogWatch Root Compromise	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Microsoft ²²	Windows NT 4.0/2000	Exchange Server 5.5, 5.5 SP1-4, Exchange Server 2000, 2000SP1&2; RSA Security SecurID 5.0	A vulnerability exists which could let a malicious user bypass SecurID authentication.	No workaround or patch available at time of publishing.	Microsoft Outlook Web Access with RSA SecurID Authentication Bypass	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Microsoft ²³	Windows 95/98/ME/NT 4.0/2000	Internet Explorer 5.0, 5.0.1, 5.0.1SP1&2, 5.5, 5.5SP1&2, 6.0	A vulnerability exists in the implementation of the DYN_SRC attribute because source validity is ignored, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Internet Explorer DYN_SRC File Information Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft ²⁴	Windows 95/98/ME/NT 4.0/2000	Internet Explorer 5.0, 5.0.1, 5.0.1SP1&2, 5.5, 5.5SP1&2, 6.0	A vulnerability exists in the Cascading Style-Sheets (CSS) interpreter, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Internet Explorer Cascading Style Sheet Sensitive Information	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

¹⁹ KPMG-2002006, April 2, 2002.

²⁰ Bugtraq, April 4, 2002.

²¹ Bugtraq, March 27, 2002.

²² NTBugtraq, March 26, 2002.

²³ GreyMagic Security Advisory, GM#003-IE, March 27, 2002.

²⁴ GreyMagic Security Advisory GM#004-IE, April 2, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft ²⁵	Windows 95/98/ME/NT 4.02/000	Internet Explorer 5.0.1SP1&2, 5.5, 5.5SP1&2, 6.0	Two vulnerabilities exist: a vulnerability exists in the zone determination function, which could let a malicious user execute arbitrary script code; and vulnerability exists in the handling of object tags which could let a malicious user invoke an executable already present on the user's system.	Frequently asked questions regarding these vulnerabilities and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms02-015.asp	Internet Explorer Known Local File Script Execution CVE Names: CAN-2002-0077, CAN-2002-0078	Medium 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 ²⁶	Windows 95/98/ME/NT 4.0/2000, XP	Internet Explorer 6.0, Outlook 2000, 2002, Outlook Express 6.0	A vulnerability exists because a malicious user can place a set of files on a system and when decoded and stored in a directory may be arbitrarily executed through the use of MIME base64.	No workaround or patch available at time of publishing.	Microsoft Temporary Internet File Execution	High	Bug discussed in newsgroups and websites.
Microsoft ²⁷	Windows NT 4.0/2000, XP	Outlook 2002	Two vulnerabilities exist: a vulnerability exists because it is possible to embed active content in HTML mail, which could let a malicious user execute arbitrary code; and a vulnerability exists in the MS spreadsheet component in the 'Host()' function, which could let a malicious user write arbitrary files.	No workaround or patch available at time of publishing.	Outlook 2002 HTML Mail Script Execution & Host(). SaveAs() File Creation	High	Bug discussed in newsgroups and websites. Exploits have been published.
Microsoft ²⁸	Windows 2000	Windows 2000 Advanced Server, 2000 Advanced Server SP1&2, 2000 Professional, 2000 Professional SP1&2, 2000 Server, 2000 Server SP1&2	A vulnerability exists in the Microsoft Distributed Component Object Model (DCOM) client, which could let a malicious user obtain sensitive information.	Microsoft knowledge base article can be found at: http://support.microsoft.com/default.aspx?scid=kb;EN-US;q300367	Windows 2000 DCOM Client Sensitive Information	Medium	Bug discussed in newsgroups and websites.
Microsoft ²⁹	Windows NT 4.0/2000, XP	Windows 2000 Server, 2000 Advanced Server, 2000 Datacenter Server	A vulnerability exists because it is possible to lock Group Policy files, which could let a malicious user block the application of Group Policy within a Windows 2000 domain.	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/MS02-016.asp	Windows Group Policy File Block Policy CVE Name: CAN-2002-0051	Medium	Bug discussed in newsgroups and websites.

²⁵ Microsoft Security Bulletin, MS02-015, March 28, 2002.

²⁶ NTBugtraq, March 28, 2002.

²⁷ Georgi Guninski Security Advisory #53 Version 2.0, April 3, 2002.

²⁸ BindView Security Advisory, April 2, 2002.

²⁹ Microsoft Security Bulletin, MS02-016, April 4, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft ³⁰	Windows NT 4.0/2000, XP	Windows NT 4.0 Workstation, 4.0 Server, 4.0 Server, Enterprise Edition, Terminal Server Edition, 2000 Professional, 2000 Server, 2000 Advanced Server, XP Professional	A buffer overflow vulnerability exists due to improper input checking in the Multiple UNC Provider, which could let a malicious user gain complete over the machine.	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/MS02-017.asp	Windows Multiple UNC Provider Buffer Overflow CVE Name: CAN-2002-0151	High	Bug discussed in newsgroups and websites.
Multiple Vendors ³¹	Unix	Linux kernel 2.2-2.2.20, 2.3, 2.3.99, 2.4- 2.4.18	A vulnerability exists in the 'd_path()' function if the fixed length buffer is exceeded, which could let a malicious user bypass security.	No workaround or patch available at time of publishing.	Linux Kernel d_path() Path Truncation	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
National Science Foundation ³²	Unix	Squid Web Proxy 2.0, 2.1, 2.2 STABLE5, 2.2, 2.3 STABLE 2-5, 2.3, 2.3.1, 2.4, 2.4 STABLE 1-4, 2.4 STABLE6	A Denial of Service vulnerability exists when a maliciously formed compressed DNS answers messages.	Upgrade available at: http://www.squid-cache.org/Versions/v2/2.4/squid-2.4.STABLE6-src.tar.gz	Squid Compressed DNS Denial of Service	Low	Bug discussed in newsgroups and websites.
NetBSD ³³	Unix	NetBSD 1.0-1.5.2	A vulnerability exists in 'talkd' due to the lack of user validation for incoming requests, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Multiple Vendor TalkD User Validation	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
NEWLOG ³⁴	Windows 95/98/ME/ NT 4.0/2000	NetSupport Manager 5.5, 6.10	A Directory Traversal vulnerability exists, which could let a remote malicious user obtain sensitive information.	Upgrade available at: http://www.newlock.com/	NetSupport Manager Directory Traversal	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

³⁰ Microsoft Security Bulletin, MS02-017, April 4, 2002.

³¹ Securiteam, March 26, 2002.

³² Squid Proxy Cache Security Update Advisory, SQUID-2002:2, March 26, 2002.

³³ Securiteam, April 4, 2002.

³⁴ Securiteam, March 23, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Novell ³⁵	Multiple	Netware 5.1, 6.0	A buffer overflow vulnerability exists if a HTTP Basic Authentication request is sent with extremely long values for the username or password field, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Netware Buffer Overflow	High	Bug discussed in newsgroups and websites. There is no exploit code required. Vulnerability has appeared in the press and other public media.
OpenBSD ³⁶	Unix	OpenBSD 3.0	A vulnerability exists when an attempt is made to connect to a system via TCP on a port that is filtered by PF, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	OpenBSD PF Fingerprinting	Medium	Bug discussed in newsgroups and websites. This vulnerability may be exploited by using one of numerous available portscanning utilities and packet analysis utilities.
Oracle Corporation ³⁷	Multiple	Oracle Configurator 11.0 i	Multiple vulnerabilities exist: A Cross-Site Scripting vulnerability exists when a string that is not a recognized argument is passed to the 'test' parameter using the 'oracle.apps.cz.servlet.UiServlet' servlet, which could let a malicious user obtain sensitive information; a Cross-Site Scripting vulnerability exists in the Text Features and the DHTML user interface because HTML tags are not properly filtered from input boxes, which could let a malicious user execute arbitrary script code; and a vulnerability exists if you pass a 'test=version' argument to the 'oracle.apps.cz.servlet.UiServlet' servlet, which could let a malicious user obtain sensitive information.	Patch available at: http://otn.oracle.com/deploy/security/htdocs/oconfigvul.html	Oracle Configurator Multiple Vulnerabilities	Medium/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites.

³⁵ iXsecurity Security Vulnerability Report, iXsecurity.20020313, April 2, 2002.

³⁶ Bugtraq, March 31, 2002.

³⁷ Oracle Security Alert #31, April 1, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Oracle Corporation ³⁸	Unix	Oracle8i 8.1.5	A buffer overflow vulnerability exists when an oversized command line parameter is sent, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Oracle 8i TNS Listener Local Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Oracle Corporation ³⁹	Multiple	Oracle9i 9.0, 9.0.1	A remote Denial of Service vulnerability exists when a one-byte packet is sent to the TNS Listener on port 1521.	No workaround or patch available at time of publishing.	Oracle 9i TNS Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
phpBB Group ⁴⁰	Unix	phpBB 1.0 .0, 1.2 .0, 1.2.1, 1.4 .0, 1.4.1, 1.4.2, 1.4.4	A vulnerability exists because image tags are not adequately filtered, which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	phpBB Image Tag User-Embedded Scripting	High	Bug discussed in newsgroups and websites.
phpBB Group ⁴¹	Multiple	phpBB 1.0.0, 1.2.0, 1.2.1, 1.4.0, 1.4.1, 1.4.2, 1.4.4	Two vulnerabilities exist: a Denial of Service vulnerability exists when phpBB processes BBcode; and vulnerability exists in BBcode, which could let a malicious user inject garbage data into the database.	No workaround or patch available at time of publishing.	phpBB BBCode Denial Of Service & Database Corruption	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
phpBB Group ⁴²	Multiple	phpBB 2.0 Beta 1, 2.0 RC1-RC3,	Vulnerabilities exist because the 'phpbb_root_path' variable accepts scripts from external servers, which could let a remote malicious user execute arbitrary commands.	Upgrade available at: http://prdownloads.sourceforge.net/phpbb/phpBB-2.0-RC4.tar.gz	phpBB2 Remote Extension Command	High	Bug discussed in newsgroups and websites.
PHPGroup Ware ⁴³	Multiple	PHPGroup Ware 0.9.12	A vulnerability exists due to insufficient checking of input, which could let a remote malicious user execute arbitrary SQL commands.	No workaround or patch available at time of publishing.	PHP Groupware Login SQL Command Execution	High	Bug discussed in newsgroups and websites. There is no exploit code required.
Posadis ⁴⁴	Unix	Posadis m5pre1	A format string vulnerability exists in the 'log_print' function, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.	Upgrade available at: http://prdownloads.sourceforge.net/posadis/posadis-m5pre2.tar.gz	Posadis DNS Server Format String	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites.
PostNuke Development Team ⁴⁵	Multiple	PostNuke 0.7.0.3	A vulnerability exists in the 'user.php' script, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	PostNuke Remote Command Execution	High	Bug discussed in newsgroups and websites. Exploit has been published.

³⁸ Bugtraq, April 1, 2002.

³⁹ Bugtraq, March 28, 2002.

⁴⁰ ITCP Advisory 5, March 21, 2002.

⁴¹ Whitecell Security Systems, WSS-Advisories-02003, April 4, 2002.

⁴² Bugtraq, March 18, 2002.

⁴³ Bugtraq, April 3, 2002.

⁴⁴ Securiteam, March 28, 2002.

⁴⁵ Bugtraq, March 28, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
PostNuke Development Team ⁴⁶	Multiple	PostNuke 7.0.3 & prior	Cross-Site Scripting vulnerabilities exist in the 'index.php' and 'modules.php' scripts, which could let a malicious user execute arbitrary script code.	Patch available at: www.postnuke.com	PostNuke Cross-Site Scripting	High	Bug discussed in newsgroups and websites. There is no exploit code required.
Progress ⁴⁷	Windows NT 4.0/2000, Unix	Database 9.1 B, 9.1 C	A buffer overflow vulnerability exists in the 'sqlcpp' program, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Progress sqlcpp Local Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Qualcomm ⁴⁸	Windows 95/98/NT 4.0/2000	Eudora 5.1	A vulnerability exists when a Media Player file is referenced within a <video> tag, which could let a malicious user execute arbitrary JavaScript commands.	No workaround or patch available at time of publishing.	Eudora WebBrowser Control Embedded Media Player File	High	Bug discussed in newsgroups and websites.
RCA ⁴⁹	Multiple	Digital Cable Modem DCM225E, DCM225	Two vulnerabilities exist: a remote Denial of Service vulnerability exists when a malicious user connects to the 10.x.x.x IP address on port 80; and an information leakage vulnerability exists because public access to SNMP interface is allowed on the 10.x.x.x IP address, which could let a remote malicious user connect, view, and modify modem configuration data.	No workaround or patch available at time of publishing.	Digital Cable Modem Remote Denial of Service & Sensitive Information	Low/ Medium (Medium if sensitive information is obtained)	Bug discussed in newsgroups and websites. There is no exploit code required.
Sambar Technologies ⁵⁰	Windows 95/98/ME/NT 4.0/2000	Sambar Server 5.0 beta1-6, 5.1,	Multiple vulnerabilities exist: a buffer overflow vulnerability exists if extremely long strings are sent for the authentication username and password which could let a malicious user execute arbitrary code with SYSTEM privileges; and several Denial of Service vulnerabilities exist when an overly long string is supplied to a specific HTTP header field.	Upgrade available at: http://www.sambarserver.com/download/sambar51p.exe	Sambar Server Multiple Vulnerabilities	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites.

⁴⁶ Bugtraq, March 22, 2002.

⁴⁷ Bugtraq, April 1, 2002.

⁴⁸ GreyMagic Security Advisory, GM#002-IE, March 22, 2002.

⁴⁹ Bugtraq, March 27, 2002.

⁵⁰ NGSSoftware Insight Security Research Advisory, NISR01042002, April 1, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
SGI ⁵¹	Unix	IRIX 6.5, 6.5.1, 6.5.2-6.5.14, 6.5.2m-6.5.14m, 6.5.2f-6.5.14f, 6.5.15m, 6.5.15f	A buffer overflow vulnerability exists when a malformed SNMP request is sent to the server, which could let a remote malicious user execute arbitrary code.	Patch available at: ftp://patches.sgi.com/support/free/security/patches/6.5/	IRIX SNMP Daemon Buffer Overflow CVE Name: CAN-2002-0013, CAN-2002-0017	High	Bug discussed in newsgroups and websites.
SGI ⁵²	Unix	IRIX 6.5-6.5.10, 6.5.11m-6.5.15m, 6.5.11f-6.5.15f	Two vulnerabilities exist: a Denial of Service vulnerability exists in the 'portman' and 'rpcbind' daemons when malformed RPC requests are sent with invalid lengths; and a Denial of Service vulnerability exists if 'HOSTALIASES' is set to a maliciously constructed value.	Patch available at: http://support.sgi.com/irix/sw/updates/	SGI IRIX Denial of Service Vulnerabilities CVE Names: CAN-2002-0039, CAN-2002-0040	Low	Bug discussed in newsgroups and websites.
SouthWest ⁵³	Windows 95/98/NT 4.0	SouthWest 1.0 .0	A remote Denial of Service vulnerability exists when a specially crafted HTTP request is received by the handling service.	No workaround or patch available at time of publishing.	SouthWest Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Squirrel Mail ⁵⁴	Unix	SquirrelMail 1.2.5	A vulnerability exists because the variable used to select a user's theme can be corrupted, which could let a malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	SquirrelMail Theme Remote Command Execution	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Sun Microsystems ⁵⁵	Unix	Solaris 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86	A buffer overflow vulnerability exists in XSun when processing a command line parameter "-co," which could let a malicious user execute arbitrary code with root user/root group privileges.	No workaround or patch available at time of publishing.	Solaris XSun Buffer Overflow CVE Name: CAN-2002-0158	High	Bug discussed in newsgroups and websites.
Symatec ⁵⁶	Multiple	popper_mod 1.0, 1.2, 1.2.1	A vulnerability exists in the default installation because public access is granted to the administration pages.	Upgrade available at: http://www.symatec-computer.com/popper_mod/popper_mod-1.2.3.tgz http://www.symatec-computer.com/popper_mod/popper_mod-1.2.3.zip	Popper_Mod Default Administrative Access	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

⁵¹ SGI Security Advisory, 20020201-01-P, April 3, 2002.

⁵² SGI Security Advisory, 20020306-01-P, March 28, 2002.

⁵³ Securiteam, March 26, 2002.

⁵⁴ Bugtraq, March 28, 2002.

⁵⁵ NSFOCUS Security Advisory, SA2002-01, April 2, 2002.

⁵⁶ Bugtraq, March 30, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Understroem ⁵⁷	Unix	Instant Web Mail 0.59 & prior	Two vulnerabilities exist: a vulnerability exists due to inadequate character filtering in the function command(), which could let a malicious user execute arbitrary POP3 commands; and a vulnerability exists due to inadequate character filtering in the 'write.php' script, which could let a malicious user embed attachments via other means than those provided by the normal interface.	Upgrade available at: http://understroem.dk/instantwebmail/instantwebmail.tar.bz2	Instant Web Mail POP3 Commands & Mail Filters	High	Bug discussed in newsgroups and websites.
Veridis ⁵⁸	Multiple	OpenKey Server 1.2	A Cross-Site Scripting vulnerability exists due to the way key queries are handled, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	OpenKey Server Cross-Site Scripting	High	Bug discussed in newsgroups and websites. There is no exploit code required.
Webmin ⁵⁹	Unix	Webmin 0.93 & prior	A vulnerability exists because authentication credentials are stored in plaintext, which could let a remote malicious user obtain sensitive information and elevated privileges.	No workaround or patch available at time of publishing.	Webmin Plaintext Authentication	Medium	Bug discussed in newsgroups and websites.
WebSight Directory System ⁶⁰	Unix	WebSight Directory System 0.1	A Cross-Site Scripting vulnerability exists because script code is not properly filtered from URL parameters, which could let a remote malicious user execute arbitrary script code.	Upgrade available at: http://prdownloads.sourceforge.net/websight/WebSight-0.1.1.zip	WebSight Directory System Cross-Site Scripting	High	Bug discussed in newsgroups and websites.
WWWIsis ⁶¹	Unix	WWWIsis 3.3, 3.45,	Two vulnerabilities exist: a vulnerability exists because query parameters can be forged to have WWWIsis execute any (shell) command and display any readable file as allowed for the user of the cgi process, which could let a remote malicious user execute arbitrary commands; and a file disclosure vulnerability exists due to inadequate validation of user input, which could let a remote malicious user obtain sensitive information.	Upgrade available at: http://www.bireme.br/wwwisis/1/download.htm	WWWIsis Remote Command Execution & File Disclosure	Medium/ High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.

⁵⁷ Bugtraq, March 23, 2002.

⁵⁸ Securiteam, March 26, 2002.

⁵⁹ Bugtraq, March 20, 2002.

⁶⁰ Bugtraq, March 25, 2002.

⁶¹ Bugtraq, March 28, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
X-Chat ⁶²	Unix	X-Chat 1.8.1, 1.8.6-1.8.8	A vulnerability exists because IRC server responses are not filtered when a /dns query is executed, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	XChat DNS Command Execution	High	Bug discussed in newsgroups and websites.
Zone Labs ⁶³	Windows 98/ME/NT 4.0/2000, XP	ZoneAlarm 3.0	Several vulnerabilities exist which could let a malicious user bypass e-mail protection.	Update available at: http://www.zonelabs.com/download/index.html	ZoneAlarm MailSafe Filtering Bypass	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

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

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

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

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

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between March 26 and April 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, 14 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
April 4, 2002	Talkspooftar.gz	Exploit for the Multiple Vendor TalkD User Validation vulnerability.
April 3, 2002	Concept.c	Script which exploits the Windows remote command execution vulnerability.
April 3, 2002	Icx.c	Script which exploits the Icecast Buffer Overflow vulnerability.

⁶² Bugtraq, March 27, 2002.

⁶³ Bugtraq, April 2, 2002.

Date of Script (Reverse Chronological Order)	Script name	Script Description
April 3, 2002	Logwatch211.sh	Script which exploits the LogWatch Root Compromise vulnerability.
April 3, 2002	Wellenreiter-v09.tar.gz	A GTK/Perl program that makes the discovery and the auditing of 802.11b wireless-networks much easier. It has an embedded statistics engine for the common parameters provided by the wireless drivers, enabling you to view details about the consistency and signal strength of the network. A scanner window can be used to discover access-points, networks, and ad-hoc cards.
April 2, 2002	Nmap-2.54beta32.tgz	A utility for port scanning large networks that supports Vanilla TCP connect() scanning, TCP SYN (half open) scanning, TCP FIN, Xmas, or NULL (stealth) scanning, TCP ftp proxy (bounce attack) scanning, SYN/FIN scanning using IP fragments (bypasses some packet filters), TCP ACK and Window scanning, UDP raw ICMP port unreachable scanning, ICMP scanning (ping-sweep), TCP Ping scanning, Direct (non portmapper) RPC scanning, Remote OS Identification by TCP/IP Fingerprinting, and Reverse-ident scanning.
April 1, 2002	Sqlcpx.c	Script which exploits the Progress sqlcpx Local Buffer Overflow vulnerability.
April 1, 2002	Tnslsnrx.c	Script which exploits the Oracle 8i TNS Listener Local Buffer Overflow vulnerability.
March 30, 2002	Ethereal-0.9.3.tar.gz	A GTK+-based network protocol analyzer, or sniffer, that lets you capture and interactively browse the contents of network frames.
March 30, 2002	Libwhisker-1.3.tar.gz	A Perl module for performing whisker CGI vulnerability checks.
March 29, 2002	Osshchan.tgz	Script which exploits the OpenSSH channel_lookup() off by one vulnerability.
March 28, 2002	Sq125x	Exploit for the SquirrelMail Theme Remote Command Execution vulnerability.
March 27, 2002	Lcrzoex-4.07-src.tgz	A toolbox for network administrators and network malicious users that contains over 200 functionalities using network library lerzo.
March 26, 2002	Dpathx.c	Script which exploits the Linux Kernel d_path() Path Truncation vulnerability.

Trends

- Windows users should be suspicious of a new Internet worm that is disguised as a Microsoft security bulletin. The "W32/Gibe" worm masquerades as an "Internet Security Update" from Microsoft Corporation.
- The CERT/CC has received reports of social engineering attacks on users of Internet Relay Chat (IRC) and Instant Messaging (IM) services. Intruders trick unsuspecting users into downloading and executing malicious software, which allows the intruders to use the systems as attack platforms for launching distributed denial-of-service (DDoS) attacks. The reports to the CERT/CC indicate that tens of thousands of systems have recently been compromised in this manner. For more information, see CERT® Incident Note IN-2002-03, located at: http://www.cert.org/incident_notes/IN-2002-03.html.
- The National Infrastructure Protection Center is aware of potential vulnerabilities existing within the Simple Network Management Protocol (SNMP) -- a protocol used by routers, switches and hubs on the Internet and other related equipment. For more information, see NIPC ALERT 02-001, located at: <http://www.nipc.gov/warnings/alerts/2002/02-001.htm>.

- The National Infrastructure Protection Center (NIPC) has received reporting that infrastructure related information, available on the Internet, is being accessed from sites around the world. While in and of itself this information is not significant, it highlights a potential vulnerability. For more information, see NIPC ADVISORY 02-001, located at: <http://www.nipc.gov/warnings/advisories/2002/02-001.htm>.
- The CERT/CC has received credible reports of scanning and exploitation of Solaris systems running the CDE Subprocess Control Service buffer overflow vulnerability identified in CA-2001-31 and discussed in VU#172583. For more information, see CERT® Advisory CA-2002-01, located at: <http://www.cert.org/advisories/CA-2002-01.html>.
- NIPC has updated their advisory, NIPC Advisory 01-030, regarding what Microsoft refers to as a critical vulnerability in the universal plug and play (UPnP) service in Windows. For more information see, NIPC ADVISORY 01-030.3, located at: www.nipc.gov/warnings/advisories/2001/01-030-2.htm.

Viruses

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

Actem (E-mail Worm): This is a worm virus spreading via the Internet as an infected e-mail attachment. The worm itself is a Windows PE EXE file about 61Kb in size, written in Visual Basic. The infected message body is empty. The e-mail subject is, "Try this, pretty cool." There are two files attached to the e-mail. One is a copy of the worm, "ActiveM.exe." While the other is a text file, "list.txt." Actem activates from the infected e-mail only if a user clicks on the attached file. If activated, the worm installs itself into the system and displays false messages. The worm hides itself as an "Active Mouse" application and displays several false messages and menus when the infected file is run. Actem does not install itself to the system and is not active after having run unless a user clicks on the infected attachment again. To send out infected messages Actem uses MS Outlook to send messages to all addresses found in the Outlook address book.

HLLW.Dervice (Win32 Worm): This is not a dangerous Win32 worm virus. The virus itself is a Windows PE EXE file about 20Kb in size and written in Delphi. The virus copies itself to the Windows directory under the name "DWService.exe," and to the A: floppy disk under the name "DW.exe." The virus spreads from floppy disks to hard drives (only in the event that a user runs the infected file on the floppy disk), and from hard drives to floppy disks. The virus also registers a copy of itself "DWService.exe" in the system registry auto-run key:

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Run ServiceInternet =
%WindowsDir%\DWService.exe
```

While spreading the virus sends out 'beeps' via the PC speaker. The file, "WINSTART.BAT" is also created in the Windows directory and an "echo" command is written there that displays the following text upon Windows boot up:

```
"You are welcomed by the manager of the disk drive of windows."
```

HLLP.DH.7199: This is a dangerous, non-memory resident parasitic virus. It is written in the high level language Pascal. The virus looks for EXE files in the directories from the PATH environment variable and writes itself to the beginning of EXE files. It marks infected files with last four bytes: DH)! It doesn't infect files with length less than 7195 bytes. On the 13th, 14th, and 15th day of each month the virus erases all files in the subdirectories of the directories from the PATH environment variable.

Kaze.2056 (Win32 Virus): This is a dangerous non-resident parasitic Win32 virus. The virus is written in Assembly language. It searches for and tries to infect all Win32 executable applications (PE EXE files) in the current directory and all its sub-directories. During the "infecting" process, the virus writes itself to the end of the file. However, if the current date is the 22nd day in a month the worm writes the word "KAMIKAZE" or up to eight zeroes at the beginning of any found EXE files instead of infecting them. Kaze.2056 doesn't contain any specific text string.

Netres (Internet Worm): This is a dangerous worm that functions only under Win32 systems. The worm spreads over local networks and copies itself to shared network drives. Some versions of the worm also copy themselves to subdirectories on the local drive and to floppy disks in the A: drive. There are at least ten different known versions of Netres. Netres copies itself with different randomly selected names, some of them have many spaces before the ".exe" extension, and most of the names are in Russian. Other names are also used that are randomly constructed from three parts - Name1 + Ext1 + ".exe." Netres moves all files from the Windows SYSTEM directory to a new "restop" directory:

```
C:\windows\system\*. * -> c:\windows\restop\
```

The worm also creates a log file and writes to this file a report logging its actions. The name of the log file depends on the specific worm version.

VBS_JADRA.A (Aliases: VBS.Jadra, VBS.Madonna.a) (Visual Basic Script Malware): This destructive Visual Basic Script (VBS) malware overwrites all VBS files in the directory where it is executed. It modifies registry settings so that the following files execute upon Windows startup:

- DEFRA.G.EXE
- WINFILE.EXE
- EXPLORER.EXE
- CDPLAYER.EXE
- COMMAND.COM

It also displays a series of message boxes and popup windows.

VBS_JADRA.B (Aliases: JADRA.B, VBS.Annod.B, VBS.Ardin.C) (Visual Basic Script Malware):

This destructive Visual Basic Script malware overwrites critical files located in the Windows directory and the system folder. If it does not find its target files, it copies itself to the filenames of its target files.

VBS_LEE.D (Aliases: VBS/Anjulie.gen@MM, I-Worm.Lee-Based, Bloodhound.VBS.Worm) (Visual Basic Script Malware): This Visual Basic Script malware uses Microsoft Outlook to propagate copies of itself via e-mail. It sends itself as an attachment in an e-mail that is sent to all recipients listed in the infected user's address book. It can also send itself via Internet Relay Chat (IRC). This malware copies itself into the %Windows% directory and modifies the Startup page of Internet Explorer.

VBS_REGRESIDE.A (Aliases: VBS/Anjulie.gen@MM, VBS.Entice) (Visual Basic Script Malware): This Visual Basic Script (VBS) malware uses Microsoft Outlook to propagate copies of itself via e-mail. It sends a copy of itself as attachment in the e-mail it sends to all e-mail recipients listed in the infected user's address book. It also encodes a copy of itself in a registry key and drops a decoder script in the root directory. The root directory usually refers to the C:\.

VBS_VBSWG.D (Alias: VBSWG.D) (Visual Basic Script Malware): This Visual Basic Script malware replicates via Internet Relay Chat (IRC) and e-mail. It arrives in a semi-encrypted format, in an e-mail with the attachment "syashin2.jpg.vbs."

VBS.Hart@mm (Visual Basic Script Worm): This VBS worm spreads by sending itself to all addresses in the Microsoft Outlook address book. It also copies itself to all local or mapped network drives, and spreads through mIRC.

VBS.Krim@mm (Visual Basic Script Worm): This is a Visual Basic Script (VBS) worm that uses Microsoft Outlook MAPI to mail itself to all contacts in the Outlook address book. This attachment is a batch file. When it is executed, it does the following:

- It creates the folder C:\Windows\Mk
- It creates the following files:
- C:\Windows\Mirko.vbs
- C:\Windows\Mirko.reg
- C:\Windows\Mk\Mirko.vbs
- C:\Windows\Desktop\Mirko.txt

The worm then copies itself as C:\Windows\Mk\Mirko.bat. Next, it appends the following line to the end of the C:\Autoexec.bat file:

```
@call C:\windows\system\mirko.bat
```

The worm then attempts to add the value "mirko c:\windows\mk\mirko.bat" to the registry key:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
```

The worm searches for the file "C:\Windows\Desktop\Mirko.txt." If the worm cannot find this file on the desktop, it begins to perform a quick format of drive C. Next, the worm uses the file, "C:\Windows\Mirko.vbs," to mail itself to all contacts in Outlook address book.

VBS.Vbswg2b.B@mm (Visual Basic Script Worm): This is a worm that was created by the VBS worm generator, Vbswg Version 3. It spreads using Microsoft Outlook and mIRC.

W32/Goround.worm (Win32 Worm): This is a network aware worm that can put an infected system into a reboot loop. When the worm is run, typically the filename is "OLDNEWS.EXE." It also checks for the presence of the file, "C:\BOOTMGR.SYS." If this file is not present (which is typically the case), the worm drops a 1 bytes file, "C:\BOOTMGR.SYS," and attempts to copy itself to other systems using the following network shares:

- C\$\windows\startup\oldnews.exe (note: this is an invalid startup folder)
- C\$\WINNT\Profiles\All Users\Start Menu\Programs\Startup\oldnews.exe
- C\$\Documents and Settings\All Users\Start Menu\Programs\Startup\oldnews.exe

The 2nd time the worm is run, "C:\BOOTMGR.SYS" is present and the worm immediately shuts down the machine. Once the worm has successfully copied itself to an active Startup folder, the machine will shutdown as soon as Windows has loaded. The worm is also designed to mass e-mail itself to all users in the Microsoft Outlook Address book. However, due to a bug in the program, this routine does not function properly and no messages are sent.

W32/MyLife-C (Alias: W32/MyLife.c@mm) (Win32 Worm): This worm has been reported in the wild. It is a Win32 worm that copies itself to the Windows system directory as "List.TXT.scr" and sets the following registry key to run the copy on restart:

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
```

If List.TXT.scr is executed, the worm displays the false error message "Error Notepad.dll ##." It then sends itself to addresses from the Outlook address book, using an e-mail with the subject line, "The List" and an attachment, "List.TXT." It may format drives and delete files depending on the system time.

W32/MyLife-D (Alias: W32/MyLife.d@MM) (Win32 Worm): W32/MyLife-D is a Win32 worm which copies itself to the Windows system directory as "Screen.scr" and sets the following registry key to run the copy on restart:

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Screen
```

If Screen.scr is executed, the worm displays a messagebox with the title "Error" and the text "Error 1452544 File Not Found." It then sends itself to addresses from the Outlook address book, using an e-mail with subject line, "New Screen Saver," and an attached file, "Screen.scr."

W32/MyLife-E (Alias: W32/MyLife.e@MM) (Win32 Worm): W32/MyLife-E is a Win32 worm which copies itself to the Windows system directory as "Screen.scr" and sets the following registry key to run the copy on restart:

HKCU\Software\Microsoft\Windows\CurrentVersion\Run

If Screen.scr is executed, the worm displays the false error message "Error 1452544 File Not Found." It then sends itself to addresses from the Outlook address book, using an e-mail with the subject line, "sexxyyy Screen Saver" or "New Screen Saver" and an attached file, "Screen.scr."

W32/MyLife-F (Alias: W32/MyLife.f@MM) (Win32 Worm): W32/MyLife-F is a Win32 worm which copies itself to the Windows system directory as "list480.txt.scr" and sets the following registry key to run the copy on restart:

HKLM\Software\Microsoft\Windows\CurrentVersion\Run\sys

The worm displays a message box with the title "Error" and the text "Error Notepad.dll ##." It then sends itself to addresses from the Outlook address book, using an e-mail with the subject line, "the list" and an attached file, "list480.txt.scr." Depending on the system time, it may format drives and delete files.

W97M.Cisi.A (Word 97 Marco Virus): This is a macro virus that infects open Microsoft Word documents and the global template, Normal.dot. When you close an infected document, the message "Thank's for Not Deleting Cisi_Lupi" appears. Once the virus infects the global template, it hides any other virus infections (in other documents) by turning off macro virus protection just before it opens documents, and then turning it on again after any macros have executed. During FileOpen and AutoOpen, this virus changes the title bar text "Microsoft Office" to "Micro\$oft Word" and then to "Bappebti Microsoft Word." This virus also sets the following options:

- "Check grammar as you type" is set to Off.
- "Check spelling as you type" is set to Off.
- "Check grammar with spelling" is set to Off.
- The default file path for user templates is set to C:\Program Files\Microsoft Office\Templates.

WORM_CHILLER.B (Aliases: CHILLER.B, CHILLER) (Internet Worm): This UPX-compressed worm is created in Visual Basic and is a variant of the WORM_CHILLER.A. It uses Microsoft Outlook to e-mail itself to all e-mail addresses listed in the infected user's address book. The details of the e-mail it arrives with are as follows:

- 101 Reasons Why You Should Have Sex When You're Drunk...
- To: me_john_doe@
- Cc: _____
- Subject: 101 Reasons Why You Should Have Sex When You're Drunk
- Attachment: a letter within a letter, 101 Reasons

Worm/BritneyPic.2 (Alias: I-Worm.Brit.b) (Internet Worm): This is a slight variation of Worm/BritneyPic, an Internet worm that spreads through e-mail by using addresses it collects in the Microsoft Outlook Address Book, as well as, through mIRC. Worm/BritneyPic.2 is displayed in the Spanish language and comes as a compiled HTML file, "caifanes.chm." The worm arrives through e-mail in the following format:

- Subject: RE:Nuevo video de Caifanes
- Body: Caifanes regresa y te muestra su nuevo video musical ...
Regards,
<USER NAME>
- Attachment: caifanes.chm

Worm/Newbiero (Internet Worm): This is an Internet worm that arrives under the original filename "Bsgk.exe." If executed, the worm copies itself in the \windows\%system% directory under the filename "bsgk.exe." This file runs each time a user restarts their computer. The following registry key gets added:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
Microsoft Diagnostic=C:\Windows\System\bsgk.exe

WORM_PETIK.M (Alias: PETIK.M) (Internet Worm): This UPX-compressed worm is a variant of WORM_PETIK.A. It propagates via Internet Relay Chat (IRC) channels and e-mail using Microsoft Outlook. It does not have a destructive payload.

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table starts with Trojans discussed in CyberNotes #2002-01, and items will be added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on Trojans and Trojan variants that anti-virus software detects. *Note: At times, Trojans may contain names or content that may be considered offensive.*

Trojan	Version	CyberNotes Issue #
APStrojan.sl	N/A	CyberNotes-2002-03
Backdoor.EggHead	N/A	CyberNotes-2002-04
Backdoor.G_Door.Client	N/A	CyberNotes-2002-05
Backdoor.IISCrack.dll	N/A	CyberNotes-2002-04
Backdoor.NetDevil	N/A	CyberNotes-2002-04
Backdoor.Palukka	N/A	CyberNotes-2002-01
Backdoor.Subwoofer	N/A	CyberNotes-2002-04
Backdoor.Surgeon	N/A	CyberNotes-2002-04
Backdoor.Systsec	N/A	CyberNotes-2002-04
BackDoor-AAB	N/A	CyberNotes-2002-02
BackDoor-ABH	N/A	CyberNotes-2002-06
BackDoor-ABN	N/A	CyberNotes-2002-06
BackDoor-FB.svr.gen	N/A	CyberNotes-2002-03
BDS/Osiris:	N/A	CyberNotes-2002-06
BKDR_SMALLFEG.A	N/A	CyberNotes-2002-04
BKDR_WARHOME.A	N/A	CyberNotes-2002-06
DIDer	N/A	CyberNotes-2002-01
DoS-Winlock	N/A	CyberNotes-2002-03
Hacktool.IPStealer	N/A	CyberNotes-2002-02
Irc-Smallfeg	N/A	CyberNotes-2002-03
JS/Seeker-E	N/A	CyberNotes-2002-01
JS_EXCEPTION.GEN	N/A	CyberNotes-2002-01
SecHole.Trojan	N/A	CyberNotes-2002-01
Troj/Download-A	N/A	CyberNotes-2002-01
Troj/ICQBomb-A	N/A	CyberNotes-2002-05
Troj/Msstake-A	N/A	CyberNotes-2002-03
Troj/Optix-03-C	N/A	CyberNotes-2002-01
Troj/Sub7-21-I	N/A	CyberNotes-2002-01
Troj/WebDL-E	N/A	CyberNotes-2002-01
TROJ_CYN12.B	N/A	CyberNotes-2002-02
TROJ_DANSCHL.A	N/A	CyberNotes-2002-01
TROJ_DSNX.A	N/A	CyberNotes-2002-03

Trojan	Version	CyberNotes Issue #
TROJ_FRAG.CLI.A	N/A	CyberNotes-2002-02
TROJ_ICONLIB.A	N/A	CyberNotes-2002-03
TROJ_JUNTADOR.B	N/A	CyberNotes-2002-06
TROJ_SMALLFEG.DR	N/A	CyberNotes-2002-04
Trojan.Badcon	N/A	CyberNotes-2002-02
Trojan.StartPage	N/A	CyberNotes-2002-02
Trojan.Suffer	N/A	CyberNotes-2002-02
VBS.Gascript	N/A	CyberNotes-2002-04
VBS_CHICK.B	N/A	Current Issue
VBS_THEGAME.A	N/A	CyberNotes-2002-03
W32.Alerta.Trojan	N/A	CyberNotes-2002-05
W32.Delalot.B.Trojan	N/A	CyberNotes-2002-06
W32.Maldal.J	N/A	Current Issue

VBS_CHICK.B (Aliases: CHM_BRIT.A, CHICK.B): This Trojan propagates via MAPI commands, and arrives as a Compiled HTML Help File with the subject line "RE:Nuevo video de Caifanes....." It overwrites the SCRIPT.INI file in the mIRC folder. If a SCRIPT.INI file does not exist, it creates one, and sends the file, "C:\Windows\BRITNEY.CHM," to users connected in the same mIRC channel as the infected user.

W32.Maldal.J: This is a mass-mailing Trojan Horse that also logs keystrokes. It sends an e-mail message to all addresses that it finds in the Microsoft Outlook address book, the MSN Messenger list, and in .html files on the infected computer. The e-mail message contains an HTML link to a file named FixerData.exe. FixerData.exe then downloads the file Data.exe from a particular Web site and runs it. Data.exe is the mass-mailing component of W32.Maldal.J.