# National Infrastructure Protection Center
# CyberNotes

*Issue #2001-02*    *66F-HQ-A1276002 Sub B 2.4*    *January 29, 2001*

**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 January 9, and January 29, 2001. 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 as red and/or italic 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 |
|---|---|---|---|---|---|---|---|
| Allaire[1] | Windows 95/98/NT 4.0/2000, Unix | JRun 3.0 | A vulnerability exists when a malformed URL is sent to the WEB-INF directory, which could let a remote malicious user gain access to sensitive information. | **Windows:**<br>http://download.allaire.com/jrun/jrun3.0/jr30sp2.exe<br>**Unix/Linux:**<br>http://download.allaire.com/jrun/jrun3.0/jr30sp2u.sh | JRun Malformed URL Information Gathering | Medium | Bug discussed in newsgroups and websites. |

[1] Allaire Security Bulletin, ASB01-02, January 25, 2001.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Basilix[2] | Multiple | Webmail 0.9.7beta | A security vulnerability exists in the default configuration for the HTTP server, which could allow malicious users to view sensitive files. | Unofficial workaround (Bugtraq):<br>Class and INC file extensions should be defined as PHP files and be denied read permissions. MySQL port should also be filtered from remote connects. | Webmail Incorrect File Permissions | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |
| Caldera[3] | Unix | eDesktop 2.4, eServer 2.3.1, OpenLinux Desktop 2.3 | A format string vulnerability exists in DHCP (Dynamic Host Configuration Protocol) which could let a remote malicious user execute arbitrary code and potentially gain access. | Upgrade available at: available: ftp://ftp.calderrasystems.com/pub/updates/eDesktop/2.4/current/RPMS | Caldera DHCP Package Format String | **High** | Bug discussed in newsgroups and websites. |
| Check Point Software Technologies[4] | Unix | Firewall-1 4.1, 4.1 SP2, 4.1 SP3 | A Denial of Service vulnerability exists in Firewall-1 installations that have a limited IP license. | **Workaround:**<br>Check Point recommends using the 'fw ctl debug -buf' workaround (http://www.checkpoint.com/techsupport/alerts/ipfrag_dos.html) as an immediate solution. They are currently researching a more permanent solution to the problem. | Firewall-1 Denial of Service | Low/**High**<br>**High if DDoS best practices not in place.** | Bug discussed in newsgroups and websites. Exploit has been published. |

[2] Securiteam, January 16, 2001.
[3] Caldera Systems, Inc. Security Advisory, CSSA-2001-003.0, January 15, 2001.
[4] Bugtraq, January 17, 2001.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Compaq[5] | Windows NT 4.0//2000, Unix | Armada Insight Manager 4.20, 4.20j;<br>Compaq Foundation Agents 1.0, 2.1, 4.0, 4.90;<br>Enterprise Volume Manager/ Command Scripter 1.0, 1.1;<br>Insight Management Desktop Web Agents 3.7;<br>Insight Manager LC 1.3c , 1.50A;<br>Insight Manager XE 1.0, 1.21;<br>Intelligent Cluster Administrator 1.0, 2.1;<br>Management Agents 4.30j, 4.35j, 4.36E, 36j, 4.37E;<br>Open SAN Manager 1.0;<br>SANWorks Resource Monitor 1.0;<br>Storage Allocation Reporter 1.0;<br>Survey Utility 2.17, 2.18, 2.33;<br>System Healthcheck 3.0;<br>Digital (Compaq) TRU64/ DIGITAL UNIX 4.0f, 4.0g, 5.0 | A buffer overflow vulnerability exists in the administration tool, which could let a remote malicious user execute arbitrary code with the privilege level of the system administrator. | Patch available at: http://www5.compaq.com/products/servers/management/agentsecurity.html | Compaq Web Admin Buffer Overflow | **High** | Bug discussed in newsgroups and websites. Exploit script has been published. |

[5] iXsecurity Security Vulnerability Report, 20001120, January 16, 2001.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| eEye Digital Security[6] | Windows 95/98/98SE /NT 4.0/2000 | IRIS 1.0.1 | A Denial of Service vulnerability exists when a maliciously formed packet is sent to the network. | No workaround or patch available at time of publishing. | Iris GET Denial of Service | Low | Bug discussed in newsgroups and websites. Exploit script has been published. |
| Fastream[7] | Windows 95/98/NT 4.0/2000 | FTP++ Server 2.0 | Multiple vulnerabilities exist: a Denial of Service condition, a directory traversal vulnerability; and the storage of unencrypted passwords. | Upgrade available at:<br>http://www.fastream.com | Fastream FTP++ Multiple Vulnerabilities | Low/ Medium | Bug discussed in newsgroups and websites. Exploit has been published. |
| FreeBSD[8] | Unix | FreeBSD 3.0-3.5.1, 4.0-4.1.1, 4.2 | A vulnerability exists in the way FreeBSD interprets the ECE flag in the TCP header which could let malicious users circumvent firewall rules. | Upgrade available at:<br>ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-01:08/ | FreeBSD Ipfw Filtering Evasion | Medium | Bug discussed in newsgroups and websites. Exploit script has been published. |
| GoodTech[9] | Windows 95/98/NT 4.0/2000 | FTP Server NT/2000 3.0.1;<br>FTP Server 95/98 3.0.1 | A Denial of Service vulnerability exists if a malicious user makes an unusual number of connections to the FTP Server. | Upgrade available at:<br>http://www.goodtechsys.com/upgrades.htm | GoodTech FTP Server Denial of Service | Low | Bug discussed in newsgroups and websites. |
| Hewlett-Packard[10] | Unix | HP-UX 10.20, 11.0, 11.11 | A Denial of Service vulnerability exists in the three tools included with the Support Tools Manager (xstm, cstm, and stm). | Patch available at:<br>http://itrc.hp.com<br>PHSS_23067<br>PHSS_23066<br>PHSS_23064<br>PHSS_23065 | HP-UX Support Tools Manager Denial of Service | Low | Bug discussed in newsgroups and websites. |
| Hewlett-Packard[11] | Unix | HP-UX 10.20, 10.24, 11.00, 11.04 | A vulnerability exists in the implementation of the Swait directive, which could allow a malicious user to cause a Denial of Service. | Upgrade available at:<br>http://itrc.hp.com<br>Upgrade with the<br>PHNE_20747<br>PHNE_21699<br>PHNE_21835<br>PHNE_23068 | HP-UX Inetd Swait Denial of Service | Low | Bug discussed in newsgroups and websites. |
| IBM[12] | Multiple | Lotus Domino Mail Server 5.0.5 | A buffer overflow vulnerability exists which could let a remote malicious user cause a Denial-of-Service or execute arbitrary code. | Upgrade available at:<br>http://www.notes.net/r5fixlist.nsf/6d4eae9850a5c2c28525690400551b57/5eea8322c479de968525697d00737ad5?OpenDocument | Lotus Domino Mail Server 'Policy' Buffer Overflow | **High** | Bug discussed in newsgroups and websites. Exploit has been published. |
| iButton[13] | Multiple | Dallas Semiconductor MultiKey iButton DS1991 | A vulnerability exists in the random number generator, which could allow a malicious user to crack passwords and gain unauthorized access to the data. | No workaround or patch available at time of publishing. | Dallas Semiconductor MultiKey iButton insecure password | Medium | Bug discussed in newsgroups and websites. |

[6] Bugtraq, January 21, 2001.
[7] Strumpf Noir Society Advisories, January 19, 2001.
[8] FreeBSD Security Advisory, FreeBSD-SA-01:08, January 23, 2001.
[9] Defcom Labs Advisory, def-2001-03, January 22, 2001.
[10] Hewlett-Packard Company Security Bulletin, HPSBUX0101-137, January 18, 2001.
[11] Hewlett-Packard Company Security Bulletin, #00136, January 9, 2001.
[12] S.A.F.E.R. Security Bulletin, 010123.EXP.1.10, January 23, 2001.
[13] eSecurityOnline Free Vulnerability Alert 3324, January 23, 2001.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Icecast[14] | Unix | Icecast 1.3.7, 1.3.8 beta2; Red Hat Powertools; Conectiva Linux 4.1, 4.2, 5.0, 5.1, 6.0 | A format string vulnerability exists in the print_client() function of utility.c which could allow a remote malicious user to execute arbitrary code. | **RedHat:**<br>ftp://updates.redhat.com/powertools/<br>**Conectiva Linux:**<br>ftp://atualizacoes.conectiva.com.br/ | Icecast Buffer Overflow | High | Bug discussed in newsgroups and websites. Exploit script has been published. |
| I-Data International[15] | Multiple | Easycom/ Safecom Print Server 1.0 | Multiple vulnerabilities exists which could allow a malicious user to bring down the print server or execute arbitrary code. | No workaround or patch available at time of publishing. | Easycom/ Safecom Print Server Remote Arbitrary Command | High | Bug discussed in newsgroups and websites. |
| **Internet Software Consortium[16, 17]** | **Unix** | **BIND 8.2 -8.2.2 p7** | **Multiple vulnerabilities exist: a buffer overflow in the transaction signature (TSIG) handling code; buffer overflow in nslookupComplain(); an input validation error in nslookupComplain(); and queries to ISC BIND servers may disclose environment variables which could let a remote malicious user gain unauthorized privileged access to the system with superuser privileges, and allow the execution of arbitrary code.** | **Upgrade to BIND version 9.1.0 available at:**<br>**ftp://ftp.isc.org/isc/bind9/9.1.0/bind-9.1.0.tar.gz** | **Bind Multiple Vulnerabilities**<br>**CVE candidate**<br>**CAN-2001-10**<br>**CAN-2001-11**<br>**CAN-2001-12**<br>**CAN-2001-13** | **Very High**<br>**Very High because the majority of name servers in operation today run BIND, these vulnerabilities present a serious threat to the Internet infrastructure.** | **Bug discussed in newsgroups and websites. Exploits have been published.**<br>**Vulnerability has appeared in the press and other public media.** |
| Iomega[18] | Unix | JaZip 0.32-2 | A vulnerability exists due to the failure to properly validate user-supplied input to the DISPLAY environment variable, which could let a malicious user gain root access. | **Debian:**<br>http://security.debian.org/dists/stable/updates/main | JaZip Buffer Overflow | High | Bug discussed in newsgroups and websites. Exploit has been published. |
| LocalWEB[19] | Windows | LocalWEB 2000 v1.1.0 | A directory traversal vulnerability exists which could let a malicious user view files outside the normal directory scope. | Upgrade available at:<br>http://www.intranet-server.co.uk/download.htm | LocalWEB Directory traversal | Low | Bug discussed in newsgroups and websites. Exploit has been published. |

[14] Packet Knights Crew Security Advisory #004, January 21, 2001.
[15] Defcom Labs Advisory, def-2001-06, January 23, 2001.
[16] CERT® Advisory, CA-2001-02, January 29, 2001.
[17] Network Associates, Inc. COVERT Labs Security Advisory, COVERT-2001-01, January 29, 2001.
[18] Debian Security Advisory, DSA-017-1, January 23, 2000.
[19] Strumpf Noir Society Advisories, January 19, 2001.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Matthew Smith[20] | Unix | mICQ 0.4.6; Red Hat Powertools; Debian | Two buffer overflow vulnerabilities exist which could allow a remote malicious user to sniff messages sent from the client to the ICQ server, or to send specially-crafted responses that will trigger the buffer overflow and execute arbitrary code on the victim's machine. | **Red Hat:**<br>ftp://updates.redhat.com/<br>Intel ia32 architecture:<br>**Debian:**<br>http://security.debian.org/dists/stable/updates/main/ | mICQ Remote Buffer Overflow | **High** | Bug discussed in newsgroups and websites. Exploit script has been published. |
| Microsoft[21] | Windows 95/98/ 98SE/NT 4.0/2000 | Internet Explorer 4.0 for Windows 3.1, Outlook 2000, Outlook Express 5.5, Explorer 4.0 for Windows 95, 98, NT 4.0 | A Denial of Service vulnerability exists due to the way Window objects are handled when they are deleted and accessed again. | Temporary workaround (eSecurityOnline ):<br>As a workaround solution, disable Active Scripting. | Microsoft MSHTML. DLL Denial of Service | Low | Bug discussed in newsgroups and websites. Exploit has been published. |
| Microsoft[22] | Windows 95/98/NT 4.0/2000 | Windows Media Player 7 | A security vulnerability exists that is exploitable through IE and Java, which could allow a malicious user to read local files and directories and execute arbitrary programs. This may lead to taking full control over user's computer. | Temporary workaround (Georgi Guninski):<br>Disable Java. | Windows Media Player .WMZ Arbitrary Java Applet | **High** | Bug discussed in newsgroups and websites. Exploit has been published.<br>Vulnerability has appeared in the press and other public media. |
| Microsoft[23] | Windows 95/98/NT 4.0/2000 | PowerPoint 2000 | A security vulnerability exists in the parsing function, which could allow a malicious user to construct a PowerPoint file that, when opened, could potentially run code on the reader's system. | Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq01-002.asp | PowerPoint File Parsing | **High** | Bug discussed in newsgroups and websites. Exploit has been published. |
| Microsoft[24] | Windows 95/98SE/ NT 4.0/2000 | Outlook Express 5.0, 5.01, 5.5; Outlook 98, 2000; Internet Explorer 5.0 for Windows 98, 2000 | A vulnerability exists in the mail and news components that could allow a malicious user to insert a hidden attachment (potentially containing hostile code) in messages. These attachments will be effectively invisible during the message's transport. | No workaround or patch available at time of publishing. | Microsoft Outlook Concealed Attachment | **High** | Bug discussed in newsgroups and websites. Exploit has been published. |

[20] Packet Knights Crew Security Advisory #003, January 18, 2001.
[21] eSecurityOnline Free Vulnerability Alert 3302, January 16, 2001.
[22] Georgi Guninski Security Advisory #35, January 15, 2001.
[23] Microsoft Security Bulletin MS01-002, Revised January 25, 2001.
[24] Securiteam, January 23, 2001.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Microsoft[25] | Windows NT 2000 | Windows NT 2000 | A vulnerability exists in EFS (Encrypted File System) which could let a malicious user gain sensitive information. | No workaround or patch available at time of publishing. | Windows 2000 EFS Temporary File Retrieval | Medium | Bug discussed in newsgroups and websites. |
| Microsoft[26] | Windows NT 4.0 | Windows NT 4.0; Windows NT 4.0 Terminal Server Edition | A Denial of Service vulnerability exists due to inappropriate permissions applied to a networking mutex. | Frequently asked questions regarding this vulnerability and the patch can be found at:<br>http://www.microsoft.com/technet/security/bulletin/fq01-003.asp | Windows NT Winsock Mutex Denial of Service | Low | Bug discussed in newsgroups and websites. |
| Microsoft[27] | Windows NT 4.0/2000 | Windows NT 4.0, 2000 Server | A vulnerablity exists which gives any computer on a local network the ability to impersonate a DC (domain controller), and register with a WINS (Windows Internet Naming Service) server as a DC. When this happens, workstations will send authentication requests to it, which allows this DC impersonator to harvest usernames and password hashes passed to it during login attempts. | **Workaround:**<br>Create static records for sensitive records (Domain name controllers, etc). | Windows NT WINS Domain Controller Spoofing | Medium | Bug discussed in newsgroups and websites. Exploit script has been published. |
| **Multiple Vendors[28]**<br>***Patches now available[29, 30]*** | **Unix** | **Debian Linux 2.3; GNU glibc 2.1.9 and greater; RedHat Linux 7.0; Terra Soft Solutions, Inc. Yellow Dog Linux 2.0;** ***Immunix OS 7.0-Beta*** | **A vulnerability exists which could let a malicious user compromise system accounts, elevated privileges, and potentially gain administrative access.** | ***RedHat:***<br>***ftp://updates.redhat.com/***<br>***Wirex Immunix OS 7.0-Beta:***<br>http://www.immunix.org/ImmunixOS/7.0-beta/updates/RPMS/ | **Glibc RESOLV_ HOST_CONF File Read Access** | **Medium** | **Bug discussed in newsgroups and websites. Exploit has been published.** |

[25] eSecurityOnline Free Vulnerability Alert 3323, January 23, 2001.
[26] Microsoft Security Bulletin , MS01-003, January 25, 2001.
[27] Securiteam, January 18, 2001.
[28] Bugtraq, January 10, 2001.
[29] Red Hat, Inc. Red Hat Security Advisory, RHSA-2001:001-05, January 11, 2001.
[30] Immunix OS Security Advisory, IMNX-2000-70-029-01, January 18, 2001.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| **Multiple Vendors**[31]<br>***Linux-Mandrake also vulnerable***[32] | **Unix** | **RedHat Linux 7.0; Wirex Immunix OS 7.0-Beta** | **A race condition vulnerability exists in the creation and handling of /tmp files that could let a malicious user overwrite or append system files.** | **Upgrade available at:**<br>**Wirex Immunix OS 7.0-Beta:**<br>**http://www.immunix.org/ImmunixOS/7.0-beta/updates/RPMS/linuxconf-devel-1.19r2-4_StackGuard_2.i386.rpm**<br>***Linux-Mandrake:***<br>http://www.linux-mandrake.com/en/ftp.php3 | **Linuxconf /tmp File Race Condition** | **Medium** | **Bug discussed in newsgroups and websites.** |
| Multiple Vendors[33] | Unix | Debian Linux 2.2 sparc, powerpc, arm, alpha, 68k;<br>Sam Lantinga splitvt 1.6.4 and Previous | A format string and several buffer overflow vulnerabilities exist which could let a malicious user gain administrative privileges and execute arbitrary code. | **Debian:**<br>http://security.debian.org/dists/stable/updates/main/<br>**Sam Lantinga:**<br>http://www.devolution.com/~slouken/projects/splitvt/ | splitvt Format String | **High** | Bug discussed in newsgroups and websites. Exploit script has been published. |
| Multiple Vendors[34] | Unix | T.C.X Data Konsult MySQL 3.23.23-3.23-30;<br>Debian GNU/Linux 2.2;<br>Red Hat 7.0;<br>Mandrake 7.2;<br>Conectiva Linux 4.0, 4.0es, 4.1, 4.2, 5.0, 5.1, 6.0 | A buffer overflow vulnerability exists which could allow a remote malicious user to cause a Denial of Service or execute arbitrary code. | **MySQL:**<br>http://www.mysql.com/downloads<br>**Debian GNU/Linux 2.2:**<br>http://security.debian.org/dists/stable/updates/main/<br>**MandrakeSoft:**<br>http://www.linux-mandrake.com/en/ftp.php3<br>**Red Hat Linux 7.0:**<br>ftp://updates.redhat.com/7.0/<br>**Conectiva Linux:**<br>ftp://atualizacoes.conectiva.com.br | MySQL Local Buffer Overflow | Low/**High** | Bug discussed in newsgroups and websites. Exploit script has been published. |
| Multiple Vendors[35] | Unix | Pierre Beyssac bing 1.0.4 and Previous | A buffer overflow vulnerablity exists in the gethostbyaddr function, which could let a malicious user gain administrative privileges. | Upgrade available at:<br>http://www.freenix.org/reseau/bing-1.0.5.tar.gz | bing gethostbyaddr Buffer Overflow | **High** | Bug discussed in newsgroups and websites. |
| Multiple Vendors[36] | Unix, BeOS 4.0, 5.0 | Oliver Debon Flash 0.4.9 and Previous | A buffer overflow vulnerability exists in the module, which could allow a malicious user to execute arbitrary code. | No workaround or patch available at time of publishing. | Flash Sound Write-Overflow | **High** | Bug discussed in newsgroups and websites. |

[31] Immunix OS Security Advisory, IMNX-2000-70-019-01, January 10, 2001.
[32] Linux-Mandrake Security Update Advisory, MDKSA-2001:011, January 12, 2001.
[33] Bugtraq, January 16, 2001.
[34] eSecurityOnline Free Vulnerability Alert 3327, January 23, 2001.
[35] Bugtraq, January 19, 2001.
[36] Bugtraq, January 15, 2001.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Multiple Vendors[37, 38] | Unix | Trustix Secure Linux 1.1, 1.2; Mandrake Soft Corporate Server 1.0.1, Linux Mandrake 6.0, 6.1, 7.0-7.2; RedHat Linux 6.0-6.2 sparc, i386, alpha | A vulnerability exists in the LD_PRELOAD variable, which could let a malicious user write or overwrite restricted files including system files. | **MandrakeSoft:**<br>http://sunsite.ualberta.ca/pub/Mirror/Linux/mandrake/updates/<br>**RedHat:**<br>ftp://updates.redhat.com/<br>**Trustix**:<br>ftp://ftp.trustix.net/pub/Trustix/updates/ | Glibc LD_ PRE LOAD File Overwriting | Medium/ **High** | Bug discussed in newsgroups and websites. |
| NetCorp[39] | Multiple | PassMaster | A vulnerablity exists in 'password.log' which could let a remote malicious user access username/password files. | Temporary workaround (Securiteam):<br>Use chmod and set the password.log file to 711 (-rwx--x--x). | PassMaster Plaintext Password | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |
| Netscape[40] | Multiple | Netscape Enterprise Server 3.6 with web publishing enabled | A vulnerability exists in the way REVLOG requests are processed by the server that could let a remote malicious user cause a Denial of Service. | Unofficial workaround (eSecurityOnline):<br>Disable Web Publishing, or disable REVLOG request. | Netscape Enterprise Server REVLOG Denial of Service | Low | Bug discussed in newsgroups and websites. Exploit has been published. |
| Netscape[41] | Multiple | FastTrack Server 4.0.1 | A Denial of Service vulnerability exists when nonexistent URLs are continuously requested. | No workaround or patch available at time of publishing. | Netscape FastTrack Cache Module Denial of Service | Low | Bug discussed in newsgroups and websites. |
| Netscape[42] | Windows NT | Enterprise Server 4.1SP5 | A Denial of Service vulnerability exists when a maliciously crafted GET request is composed. | No workaround or patch available at time of publishing. | Netscape Enterprise Server Denial of Service | Low | Bug discussed in newsgroups and websites. Exploit script has been published. |
| Omnicron Technol-ogies Corpora-tion[43] | Windows 95/98/NT 4.0/2000 | Omni HTTPD 2.0.7 | Two vulnerabilities exist in the 'statsconfig.pl' script, which could allow a remote malicious user to corrupt any file in the system or execute arbitrary code. | Temporary workaround (Bugtraq):<br>Erase 'statsconfig.pl' along with any other unnecessary files in your 'cgi-bin'. | OmniHTTPD File Corruption and Command Execution | **High** | Bug discussed in newsgroups and websites. Exploit script has been published. |

[37] Red Hat, Inc. Red Hat Security Advisory, RHSA-2001:002-03, January 16, 2001.
[38] Linux-Mandrake Security Update Advisory, MDKSA-2001:012, January 18, 2001.
[39] Securiteam, January 26, 2001.
[40] eSecurityOnline Free Vulnerability Alert 3343, January 25, 2001.
[41] Defcom Labs Advisory, def-2001-05, January 22, 2001.
[42] Defcom Labs Advisory def-2001-04, January 22, 2001.
[43] Bugtraq, January 16, 2001.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Oracle[44] | Unix | Oracle 8i versions 8.1.6, 8.1.5;<br>Oracle 8 versions 8.0.5, 8.0.4, 8.0.3 | A buffer overflow vulnerability exists in the cmctl (Connection Manager Control) binary, which could let a malicious user gain elevated operating system privileges. | Patch available at:<br>http://metalink.oracle.com | Oracle Cmctl Buffer Overflow | Medium | Bug discussed in newsgroups and websites. |
| Oracle[45] | Windows NT 2000 | XSQL Servlet 1.00 Windows 2000;<br>XSQL Servlet 1.0.1-1.0.3;<br>Oracle 8i 8.1.7.0.0 Enterprise; database server 8.1.7.0.0 | A vulnerability exists in the XSQL servlet, which could allow a remote malicious user to execute arbitrary code. | Upgrade available at:<br>http://otn.oracle.com/tech/xml/xsql_servlet | Oracle XSQL Servlet Arbitrary Java Code | **High** | Bug discussed in newsgroups and websites. Exploit has been published. |
| Oracle[46] | Windows NT 2000 | Oracle8 8.1.7 | A vulnerability exists in the way input is handled by the JSP agent which could let a remote malicious user execute arbitrary .jsp files. | No workaround or patch available at time of publishing. | Oracle JSP/SQLJSP Servlet Execution | **High** | Bug discussed in newsgroups and websites. |
| PHP Development Team[47] | Unix | Mandrake Soft Linux Mandrake 7.2;<br>PHP 4.00-4.0.4;<br>Conectiva Linux 4.0 | Two security vulnerabilities exist in the PHP code that could allow a remote malicious user to view the source code of PHP scripts. | **MandrakeSoft:**<br>http://sunsite.ualberta.ca/pub/Mirror/Linux/mandrake/updates/7.2/RPMS/<br>**PHP:**<br>http://www.php.net/do_download.php?download_file=php-4.0.4pl1.tar.gz&source_site=www.php.net<br>**Conectiva Linux:**<br>ftp://atualizacoes.conectiva.com.br/6.0 | PHP Engine Disable Source Viewing | Medium | Bug discussed in newsgroups and websites. |
| Riada[48] | Windows NT | RiadaLock 1.02 | A security vulnerability exists due to inadequate default permission settings, which could let a remote malicious user access the usernames/passwords file. | Temporary workaround (Securiteam):<br>Check the "encrypt" option in RiadaLock software to better protect records stored inside the lock.txt file. | RiadaLock Java Password Insecurity | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |
| SSH Communications Security[49] | Unix | SSH 1.2.27-1.2.30 | A vulnerability exists when "Secure-RPC" support is used to encrypt a secret key file with the "SUN-DES-1 magic phrase", which could let a malicious user recover this phrase. This seriously weakens the secrecy of a user's private keys. | Patch available at:<br>http://www.ssh.com/products/ssh/patches/patch-ssh-1.2.30-secure.rpc | SSH Secure-RPC Weak Encrypted Authentication | Medium | Bug discussed in newsgroups and websites. Exploit script has been published. |

[44] eSecurityOnline Free Vulnerability Alert, January 19, 2001.
[45] Georgi Guninski security advisory #34, January 9, 2001.
[46] Georgi Guninski Security Advisory #36, January 22, 2001.
[47] Securiteam, January 16, 2001.
[48] Securiteam, January 26, 2001.
[49] Bugtraq, January 16, 2001.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Sun Microsystems, Inc.[50] | Unix | Solaris 2.4-2.6, 2.4-2.6 x86, 7.0, 7.0_x86 | A buffer overflow vulnerability exists in the arp utility, which could let a malicious user execute arbitrary code and gain root privilege. | Patch available at: http://sunsolve.sun.com/securitypatch | Solaris Arp Buffer Overflow | **High** | Bug discussed in newsgroups and websites. Exploit script has been published. |
| Sun Microsystems, Inc.[51] | Unix | Solaris 2.4, 2.5, 22.5.1, 2.6, 7.0, 8.0 | A buffer overflow vulnerability exists in the /usr/bin/cu command which could let a malicious user gain root access. | No workaround or patch available at time of publishing. | Solaris cu Buffer Overflow | **High** | Bug discussed in newsgroups and websites. |
| Sun Microsystems, Inc.[52] | Unix | Solaris 7 | A buffer overflow vulnerability exists in the second argument /usr/bin/write receives which could let a malicious user execute arbitrary commands. | Upgrade available at: http://sunsolve.sun.com/seccuritypatch | Solaris /usr/bin/write Buffer Overflow | **High** | Bug discussed in newsgroups and websites. Exploit script has been published. |
| SuSE[53] | Linux | Linux 6.1-6.4,7.0 | A race condition vulnerability exists in the rctab (Run Control Tab) script which could allow a malicious user to elevate their privileges or append to and corrupt system files. | **Temporary workaround:** Remove the only occurrence of the string "-p " in the file /sbin/rctab. Change the line:<br>*mkdir -p ${tmpdir}*<br>to read<br>*mkdir ${tmpdir}* | SuSE Rctab Race Condition | **High** | Bug discussed in newsgroups and websites. Exploit scripts have been published. |
| Tinyproxy[54] | Unix | Tinyproxy 1.3.2, 1.3.3 | A heap overflow vulnerability exists which could allow a remote malicious user to cause a Denial of Service or execute arbitrary code. | Upgrade available at: http://tinyproxy.sourceforge.net/tinyproxy-1.3.3a.tar.gz | Tinyproxy Heap Overflow | **High** | Bug discussed in newsgroups and websites. Exploit script has been published. |
| Trend Micro[55] | Unix | InterScan VirusWall for Unix 3.0.1, 3.6x | Multiple vulnerabilities exist: insecure password change mechanism, weak authentication method allows password recovery; and predictable file names for root-owned temporary files which could let a malicious user gain root access. | No workaround or patch available at time of publishing. | Interscan VirusWall Multiple Vulnerabilities | **High** | Bug discussed in newsgroups and websites. |
| Ultra Scripts[56] | Multiple | UltraBoard 2.11 | A vulnerability exists due to improperly set directory permissions, which could let a malicious user copy malicious cgi scripts to the directory and compromise data. | No workaround or patch available at time of publishing. | Ultraboard Incorrect Directory Permissions | Medium | Bug discussed in newsgroups and websites. |

[50] Sun Microsystems, Inc. Security Bulletin, Sun-00200, January 12, 2001.
[51] Bugtraq, January 17, 2001.
[52] Securiteam, January 26, 2001.
[53] Bugtraq, January 13, 2001.
[54] Packet Knights Advisory 002, January 17, 2001.
[55] Bugtraq, January 16, 2001.
[56] Bugtraq, January 11, 2001.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Umut Gokbayrak[57] | Unix | Postaci 1.1.2, 1.1.3 | A vulnerability exists due to lack of checking for malicious SQL code in user-supplied variables when deleting address book contacts, bookmarks and notes which could let a malicious user execute arbitrary commands. | No workaround or patch available at time of publishing. | Postaci Arbitrary SQL Command Injection | **High** | Bug discussed in newsgroups and websites. Exploit has been published. |
| Veritas Software[58] | Windows 95/98/NT 4.0/2000, Unix | Backup 4.5 | A Denial of Service vulnerability exists when a remote malicious user connects to TCP socket 8192 but does not send any data. | No workaround or patch available at time of publishing. | Backup Denial of Service | Low | Bug discussed in newsgroups and websites. |
| Watch Guard Technol-ogies[59] | Multiple | FireboxII Firmware 4.0-4.5 | A vulnerability exists in the way passwords are handled which could let a remote malicious user gain elevated privileges. | Upgrade available at: https://www.watchguard.com/esupport.htm | FireboxII Password Retrieval | Medium/ **High**<br>**High if DDoS best practices not in place.** | Bug discussed in newsgroups and websites. |

*Risk is defined in the following manner:

**High** - A vulnerability that will allow an intruder to immediately gain privileged access (e.g., sysadmin, and root) to the system and/or the intruder can execute or alter arbitrary system files. An example of this would be a vulnerability in which a sequence of instructions is sent to a machine by an unauthorized user and the machine responds with a command prompt.

**Medium** - A vulnerability that will allow an intruder immediate access to the system that is not privileged access. This allows the intruder the opportunity to continue the attempt to gain root access. An example would be a configuration error that allows an intruder to capture the password file.

**Low** - A vulnerability that provides information to an intruder that could lead to further compromise attempts or a Denial-of-Service (DoS) attack. The reader should note 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 as a "High" threat.

## *Recent Exploit Scripts/Techniques*

The table below contains a representative sample of exploit scripts and How to Guides, identified between January 12, and January 26, 2001, 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, 27 scripts, programs, and net-news messages containing holes or exploits were identified.

[57] Securiteam, January 20, 2001.
[58] Securiteam, January 17, 2001.
[59] Bugtraq, January 20, 2001.

| Date of Script (Reverse Chronological Order) | Script name | Script Description |
|---|---|---|
| January 26, 2001 | Ecepass.tar.gz | Proof of concept exploit for the FreeBSD ipfw+ECE vulnerability. |
| **January 26, 2001** | **Glibc-resolve-tr.sh** | Shell script that exploits the glibc vulnerability using the Openssh-2.3.0p1 binary. |
| January 26, 2001 | Mscreen.c | Script which exploits the SCO OpenServer v5.0.5 /usr/bin/mscreen vulnerability. |
| **January 26, 2001** | **Ns-shtml.pl** | Perl script which exploits the Netscape Enterprise Server 4.0 vulnerability. |
| January 26, 2001 | Write.c | Proof of concept exploit for the Solaris 7 /usr/bin/write overflow vulnerability. |
| January 25, 2001 | Nessus-1.0.7.tar.gz | Full featured remote security scanner for Linux, BSD, Solaris and some other systems which is multithreaded, plugin-based, performs over 531 remote security checks. |
| January 25, 2001 | Pwdump3.zip | Combines the functionality of pwdump and pwdump2 and is capable of extracting the password hashes from a remote Windows NT 4.0 or 2000 box. |
| January 25, 2001 | Safer.010123.EXP.1.10 | Perl exploit script for the Lotus Domino SMTP Server buffer overflow vulnerability. |
| **January 24, 2001** | **Iris-dos.c** | Denial of service attack against the Iris The Network Traffic Analyzer vulnerability. |
| January 24, 2001 | Thong.pl | Perl script that exploits several vulnerabilities found in Cisco products. Includes the Cisco Catalyst ssh Protocol Mismatch DoS, Cisco 675 Web Administration DoS, Cisco Catalyst 3500 XL command execution, and the Cisco IOS Software HTTP Request DoS. |
| January 23, 2001 | Mysql.ploit.c | Script which exploits the MySQL Local Buffer Overflow vulnerability. |
| January 21, 2001 | PKCicecast-ex.c | Script which exploits the Icecast Buffer Overflow vulnerability. |
| January 18, 2001 | Micq-exp.c | Script which exploits the mICQ Remote Buffer Overflow vulnerability. |
| **January 18, 2001** | **Wins2.pl** | Perl script which exploits the Microsoft WINS Domain Controller Spoofing vulnerability. |
| January 17, 2001 | Passive.pdf | Technique to rapidly identify target operating systems and version, as well as vectors of attack, based on data sent by client applications. |
| January 17, 2001 | PKCtiny-ex.c | Script which exploits the Tinyproxy Heap Overflow vulnerability. |
| **January 16, 2001** | **perl omnismash.pl** | Perl script which exploits the OmniHTTPD File Corruption and Command Execution vulnerability. |
| January 16, 2001 | Spitvt.c | Script which exploits the splitvt Format String vulnerability. |
| January 16, 2001 | Ssh1-Exploit.c | Script which exploits the SSH Secure-RPC Weak Encrypted Authentication vulnerability. |
| January 15, 2001 | Host-detection.txt | Techniques To Validate Host-Connectivity. Advanced host mapping bypasses many forms of intrusion detection systems, filters, and routers, essentially enabling an attacker to map and discover previously unknown firewalled hosts. |
| January 14, 2001 | Tcpdump-xploit.c | Tcpdump v3.5.2 remote root exploit script. |
| January 13, 2001 | Arpexp.C | Solaris /usr/sbin/arp local root stack overflow exploits script. |
| **January 13, 2001** | **changerc.sh** | Script which exploits the SuSE Rctab Race Condition vulnerability. |
| January 13, 2001 | Ethereal-0.8.15.tar.gz | A GTK+-based network protocol analyzer that lets you capture and interactively browse the contents of network frames. |
| **January 13, 2001** | **rcshell.sh** | Script which exploits the SuSE Rctab Race Condition vulnerability. |
| January 12, 2001 | Enabler.C | Attempts to find the enable password on a Cisco system via brute force. |

| Date of Script (Reverse Chronological Order) | Script name | Script Description |
|---|---|---|
| January 12, 2001 | Pudding01.tar.gz | Pudding is a proxy that recodes HTTP requests using most of RFP's IDS evasion encoding methods, plus random UTF-8 encoding support and allows any web aware program/exploit/cgi-scanner to evade IDS without modification of the original code. |

## *Trends*

**Probes/Scans:**

The CERT/CC has received reports of extensive probing to port 515/tcp. For more information see CERT Advisory CA-2000-22 Input Validation Problems in LPRng, located at: http://www.cert.org/advisories/CA-2000-22.html.

**Other:**

**The CERT/CC has recently learned of four vulnerabilities spanning multiple versions of the Internet Software Consortium's (ISC) Berkeley Internet Name Domain (BIND) server. Because the majority of name servers in operation today run BIND, these vulnerabilities present a serious threat to the Internet infrastructure. For more information, please see CERT® Advisory CA-2001-02 located at:** http://www.cert.org/advisories/CA-2001-02.html**.**

**Several reports have been received from sites that recovered an intruder toolkit called 'ramen' from hosts that been compromised by a self-propagating worm known as Ramen. Ramen has been discussed in several public forums and exploits well-known holes (wu-ftp, rpc.statd, and LPRng). For more information, please see CERT® Incident Note IN-2001-01 located at: http://www.cert.org/incident_notes/IN-2001-01.html.**

Several instances of remote self-updating viruses have been reported. In addition, the most recent version of one of these viruses incorporates strong cryptography to avoid detection.

## *Viruses*

A list of viruses infecting two or more sites as reported to various anti-virus vendors and virus incident reporting organizations has been 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 tables list 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. These types of malicious code will also now be included in the table. Following this table are write-ups of new viruses and updated versions discovered in the last two weeks. WARNING: at times, viruses may contain names or content that may be considered offensive.

Note: Virus reporting may be weeks behind the first discovery of infection. A total of **228** distinct viruses are currently considered "in the wild" by anti-virus experts, with another **612** 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.

| Ranking | Common Name | Type of Code | Trends | Date |
|---|---|---|---|---|
| 1 | VBS/Kakworm | Script | Slight increase | December 1999 |
| 2 | W32/Hybris | Worm | New to table | November 2000 |
| 3 | VBS/LoveLetter | Script | Slight decrease | March 2000 |
| 4 | PE_MTX.A | File Infector, Trojan | Slight decrease | September 2000 |
| 5 | W32/Navidad | File, Worm | New to table | November 2000 |
| 6 | VBS/Stages | Script | Slight decrease | June 2000 |
| 7 | W32/Prolin | Worm | New to table | December 2000 |
| 8 | W97M/Melissa.A-BG | Macro | Return to table | April 1999 |
| 9 | W97M/Marker | Macro | Decrease | August 1998 |
| 10 | W32/SKA | File | Decrease | March 1999 |

**BAT_ATARIS.D (Aliases: EXITWIN.A, BAT.Ataris.D, ATARIS.D) (Batch File):** A batch file which is inserted by the Visual Basic Worm VBS_LOVELETTR.BG which attempts to delete several antivirus files when Windows is restarted.

**HTML_SATANIK.A (Alias: SATANIK.A) (VBS Script Worm):** This is the Hyper Text Markup Language (HTML) counterpart of the VBS_LOVELETTR.BG, which is a variant of the LoveLetter virus. It is a Visual Basic worm that spreads copies of itself via MS Outlook. The worm drops a copy of itself in the Windows and Systems directories and adds several registry entries so that it executes upon Windows start up. The worm does not have a destructive payload, but it displays a warning message about a new destructive Internet Worm.

**Linux/Ramen (Aliases: Linux/Ramen.Worm, Linux.Ramen) (Linux Worm):** This is an Internet worm for Linux. The worm attempts to use three remote exploits to gain access to computers running Red Hat 6.2 and 7.0. Once it has access on the computer it downloads a copy of itself to /tmp/ramen.tgz and extracts itself to the /usr/src/.poop directory. It appends a line to /etc/rc.d/rc.sysinit so it is executed on startup. Once executed the worm remains running until the machine is switched off. While the worm is active it will choose a class B Internet network at random and probe all addresses in the range looking for machines to infect. The worm may delete /usr/sbin/lpd or /sbin/rpc.statd or /usr/sbin/rpc.statd to close the exploit it used to gain access to the system. In order to propagate copies of itself it installs a service named asp, either by appending a line to /etc/inetd.conf or by overwriting the file /etc/xinetd.conf. The worm replaces all index.html files on the computer with an HTML file containing the text:

'Hackers looooooooooooooooooove noodles.'

**Melissa-X (Aliases: W2001MAC/Melissa.W-mm, WM97/Melissa-X, Mid/Melissa-X, ANNIV, ANNIV.DOC) (Word 2001 Macro Virus):** This virus has been reported in the wild and is contained in an infected Microsoft Office 2001 file (Microsoft Office for Macintosh). This variant came about when a Macintosh user who had a file infected with WM97/Melissa-X, saved it using Office 2001. The file (ANNIV.DOC) was then sent to a colleague running Microsoft Office 97 or 2000. When the file was opened the viral macro code ran (even though the file format was still Office 2001), and the mass-mailing part of the virus code executed. Although this virus was originally created in a Macintosh version of Word, it can also infect Microsoft Word users running Windows. The virus sends a message to the first 50 addresses in all of the address books accessible by Outlook. This message has the subject line:

'Important Message From <username>'

(where <username> is taken from the current user information settings) and the message text reads:

'Here is that document you asked for ... don't show anyone else ;-)'.

Accompanying this message is an attachment: a copy of the infected document from which the virus is launched. The virus infects class modules in Word and is Word 2000 aware. Versions of Word prior to

Word 97 will not be affected by the Melissa virus. The virus uses the appropriate new security features in Word 2000 to disable the macro security warnings. If, when a document is opened, the minute and the day are the same (for example, the time is 10:05 on 5 March), the virus will insert the text 'twenty-two, plus triple-word-score, plus fifty points for using all my letters. Game's over. I'm outta here.' into the document.

**VBS/Davinia-A (Aliases: LittleDavinia, JS/Davinia-A, WM97/Davinia-A, HTML/LittleDavinia) (Visual Basic Script Worm):** Users can be initially infected by this worm by either browsing an infected website or reading an infected HTML e-mail that would attempt to access an infected website. The infected website contains code that exploits the Microsoft "Office 2000 UA Control" Vulnerability (details of this vulnerability and how to patch against it are documented at http://www.sophos.com/support/news/index.html#uacontrol). This vulnerability allows websites to run Word macros silently. If macros are allowed to run, a Visual Basic Script will attempt to overwrite the files in subdirectories of all local and remote network drives.

**VBS_LOVELETTR.BG (Aliases: LOVELETTR.BG, VBS/LoveLetter@MM, I-Worm.Loveletter) (Visual Basic Script Worm):** This is a variant of the VBS_LOVELETTER virus that spreads copies of itself via MS Outlook. It drops copies of itself in the Windows and Systems directories. It adds several registry entries so that it executes upon Windows start up. Upon execution, it displays a warning message on the screen about a new destructive Internet Worm, while it drops another batch file virus, BAT_ATARIS.D.

**VBS_MILL.F (Aliases: MILL.F, SeasonGreeting Worm) (Visual Basic Script Worm):** This destructive worm spreads via MS Outlook and Internet Relay Chat (mIRC). It sends a copy of itself as an attachment named “SeasonGreeting.txt.vbs” to everyone listed in the Messaging Application Interface (MAPI) address list of the infected user. It then creates duplicates of non Visual Basic Script (VBS) files in certain directories and appends the extension .TXT.VBS to these duplicates. The worm also modifies the registry so that it can make changes to the desktop wallpaper, mouse buttons, and others.

**W32/Demig-A (Aliases: W32/Demiurg, W32.Demiurg.16354, Mid/Demig-A, XM97/Demig-A) (Windows 32 Executable File Virus and Excel 97 Macro Virus):** When an infected file is run, the virus copies the file kernel32.dll from the Windows System directory to the Windows directory and infects it. If Microsoft Excel is installed in the default path, the virus will also drop an Excel spreadsheet file DEMIURG.XLS infected with XM97/Demig-A into the XLSTARTUP directory. The next time the computer is restarted, the infected kernel32.dll file is loaded and the virus will be active in memory and infect files with EXE, COM and BAT extensions. The virus infects DOS and Win16 executable format files in addition to Win32 executables., . The Excel macro part of the virus infects all spreadsheets with a macro, which drops and runs C:\DEMIURG.EXE, a virus dropper. Infected COM and BAT files as well as DOS and Win16 executable files act as virus droppers and drop and run the C:\DEMIURG.EXE file.

**W32/Navidad-C (Win32 Worm):** This is a variant of the W32/Navidad-B e-mail-aware worm. The only difference is that this sample is also infected with W32/Demig-A virus.

**W97M_ASSILEM.B (Aliases: ASSILEM.B, W97M/Melissa.W, WM97/Melissa-X, WM97/Melissa-X, MacOffice2001, W97M/MELISSA.VARIANT, Mid/Melissa-X) (Word 97 Macro Virus):** This direct infecting and overwriting macro virus infects Microsoft Word 97 and Word 2000 documents. It infects in both Windows and Macintosh platforms. This virus spreads via e-mail as an infected Word document attachment. If the current system day is equal to the current system minute, the virus overwrites the first part of the active document.

**W97M_XTHREE.A (Aliases: W97M/Xthree.A, XTHREE.A) (Word 97 Macro Virus):** This Word 97 macro virus is not destructive and only infects documents when they are closed.

**WM97/Class-FE (Word 97 Macro Virus):** When an infected document is closed on January 26th the virus displays a message box with the title "Face Of Evil" and the message "ReT}{@SoFt Inc Lda 87/99" 15 times.

**WM97/Eight941-T (Word 97 Macro Virus):** This is a minor variant of the Eight941 family of viruses. It is an unremarkable macro virus, which spreads but does not have a working payload.

**WM97/Story-AD (Word 97 Macro Virus):** This is a variant of the WM97/Story Word macro virus. If C:\MIRC\MIRC32.EXE exists WM97/Story-AD will delete the file SCRIPT.INI from the C:\MIRC subdirectory. It will then write a new SCRIPT.INI file containing the mIRC/Story virus. The active document within Word will be saved as C:\WINDOWS\STORY.DOC if it does not already exist. mIRC/Story will send the infected Word document C:\WINDOWS\STORY.DOC to the currently connected IRC (Internet Relay Chat) channel. The script then sends boastful messages to various e-mail addresses.

**WM97/Vmpck1-DZ (Word 97 Macro Virus):** The virus deletes all Word document templates (.DOT files) from the Office Startup and Templates directories.

**XM97/Barisada-N (Excel 97 Macro Virus):** This is an Excel macro virus that stores its viral macros in a file called HD.XLS. On the 25th of any month the virus displays a dialog box with the text: "Question : Hyundai Unicorns left from Incheon, What do you think of it? Answer : Hyundai is SOB ". If the user chooses the 'Yes' answer button then the text: Good! You're pretty good guy!!" is displayed. If the user chooses 'No' then: Oh! no, Next question is last time for you" is displayed, followed by: "We do not buy Hyundai's product, is it right?". Answering 'Yes' displays the text: "You got it! You have right answer". Answering 'No' causes the virus to display: "Wrong Answer, Your file will be deleted! You are SOB, too". The virus will then delete all the entries in the current workbook.

**XM97/Slacker-B (Excel 97 Macro Virus):** This virus has been reported in the wild. The virus contains code that attempts to delete files on the C: drive.

## *Trojans*

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table starts with Trojans discussed in CyberNotes #2001-01, 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 # |
|---|---|---|
| Backdoor-JZ | | Current Issue |
| BAT_EXITWIN.A | | CyberNotes-2001-01 |
| Flor | | Current Issue |
| PHP/Sysbat | | Current Issue |
| PIF_LYS | | Current Issue |
| Troj/KillCMOS-E | | CyberNotes-2001-01 |
| TROJ_AOL_EPEX | | CyberNotes-2001-01 |
| TROJ_AOLWAR.B | | CyberNotes-2001-01 |
| TROJ_AOLWAR.C | | CyberNotes-2001-01 |
| TROJ_AZPR | | CyberNotes-2001-01 |
| TROJ_BAT2EXEC | | CyberNotes-2001-01 |
| TROJ_BKDOOR.GQ | | CyberNotes-2001-01 |
| TROJ_GLACE.A | | CyberNotes-2001-01 |
| TROJ_GTMINESXF.A | | Current Issue |
| TROJ_ICQCRASH | | Current Issue |
| TROJ_JOINER.15 | | Current Issue |

| Trojan | Version | CyberNotes Issue # |
|---|---|---|
| TROJ_NAVIDAD.E | | CyberNotes-2001-01 |
| TROJ_QZAP.1026 | | CyberNotes-2001-01 |
| TROJ_SUB7.401315 | | CyberNotes-2001-01 |
| TROJ_SUB7.MUIE | | CyberNotes-2001-01 |
| TROJ_SUB7.V20 | | Current Issue |
| TROJ_SUB7DRPR.B | | CyberNotes-2001-01 |
| TROJ_TWEAK | | Current Issue |
| TROJ_WEBCRACK | | Current Issue |

**Backdoor-JZ:** This, UPX packed, Trojan opens TCP/IP port 30005 on a victim's machine. An attacker can then open, execute and delete files on the user's local system. He can also shutdown windows and send out pings. This program copies itself to the WINDOWS directory as "traywnd.exe" and adds the following registry key value to allow the program to load at startup:
HKLM\Software\Microsoft\Windows\CurrentVersion\
Run\Taskschd=%WINDIR%\traywnd

**Flor:** This is a memory resident Trojan written in Visual Basic. The VB5 (or higher) runtime files are required for this program to function. Once the program is loaded into memory, it attempts every 60 seconds to copy itself to "A:\Pornografia.exe" and to "C:\windows\menu iniciar\programas\iniciar\ .exe" (the STARTUP folder on the Portuguese version of Windows). Additionally, the Trojan attempts to access a URL in the http://www3.cybercities.com domain.

**PHP/Sysbat:** This Trojan is written in PHP, which is a server-side scripting language used to generate dynamic Web page content. Computers that do not run a PHP interpreter are immune to this threat. When PHP/Sysbat is allowed to execute, the user may see the text, "This program performed an illegal operation".

**PIF_LYS (Aliases: LYS, Pif/Lys, WinPIF.Lys, PIF.Lys):** This Program InFormation (PIF) Trojan infects PIF files in the working directory. Whenever it finds a PIF file, it copies the file and overwrites it the PIF it found earlier. For example, in its working directory, it has the following shortcuts and their original contents:

PIF1 = One
PIF2 = Two
PIF3 = Three

When the Trojan finds PIF1, it copies the contents of that file and overwrites it to the earlier PIFs it has found. However, because it is the first one, it does not overwrite anything. When the Trojan finds PIF2, it copies the contents of that file and overwrites it to PIF1 and PIF2. The contents of the shortcuts or PIF files after it finds PIF2 would then be:

PIF1=Two
PIF2=Two
PIF3=Three

When the Trojan finds PIF3, it overwrites it to PIF1, PIF2 and PIF3. The contents of the shortcuts or PIF files after it finds PIF3 would then be:

PIF1=Three
PIF2=Three
PIF3=Three

Since this is a shortcut file and the virus is not embedded within a file, this Trojan executes the command line of the PIF file and uses the working directory as its search parameter.

**TROJ_GTMINESXF.A** (Aliases: IRC/Winhelp.INI, GTMINESXF.A, IRC/Winhelp): This is a variant of TROJ_GTMINE_SFX. It is a Windows Trojan that uses Internet Relay Chat mIRC to compromise the security of an infected user's computer . It sets up various network services such as file servers, IRC bouncers/spoofers, port scanners, and ICQ flooders.

**TROJ_ICQCRASH (Aliases: Flooder.Win32ICQCrash, ICQCRASH):** This is a UNIX hacker tool that is ported to Windows. It only functions in systems with the Cygnus Runtime library (CYGWIN.DLL). It launches a distributed denial of service (DDoS) attack by flooding the infected user's ICQ port with a huge number of messages.

**TROJ_JOINER.15 (Aliases: JOINER, Multidropper.cfg.a,):** This Win32 hacking tool allows merging a normal executable file with a Trojan executable file so that the Trojan file may be distributed without being detected.

**TROJ_SUB7.V20 (Aliases: BackDoor_G2.svr.gen, SUB7.V20, SubSeven.backdoor.v20):** This destructive server side hacking tool allows a remote hacker access to an infected user's computer. It makes itself active in memory when executed and then compromises an infected user's network system security.

**TROJ_TWEAK (Aliases: TWEAK, AdClicker, Trojan.Win32.Tweak):** This network-enabled Trojan is designed to connect to a Trojan author's Web site that contains banner advertisements. It runs in the background and consumes computer resources. This Trojan is written in MS Visual Basic.

**TROJ_WEBCRACK (Alias: WEBCRACK):** This Win32 hacking tool attacks password-protected Web sites using dictionary attack or brute force to guess passwords and gain access.