# National Infrastructure Protection Center CyberNotes

*Issue #2001-03* *February 12, 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 23 and February 7, 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 |
|---|---|---|---|---|---|---|---|
| America OnLine, Inc.[1] | Windows 95/98/ME/ NT 4.0/2000, Unix | AOLserver 3.2 | A directory traversal vulnerability exists which could let remote malicious users gain read access to directories outside the root directory of an AOL server. | No workaround or patch available at time of publishing. | AOLserver Directory Traversal | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |
| Apple[2] | Windows 95/98/NT 4.0 | Quicktime plugin - Windows 4.1.2 (Japanese) | A buffer overflow vulnerability exists which could let a malicious user execute arbitrary code. | No workaround or patch available at time of publishing. | Apple Quicktime Plugin Remote Overflow | **High** | Bug discussed in newsgroups and websites. Exploit script has been published. |

[1] Bugtraq, February 6, 2001.
[2] SPS Advisory #41, January 31, 2001.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| AT&T[3] | Windows 98SE/ME/ NT 4.0/2000 | WinVNC Server 3.3.3r7 & previous | A vulnerability exists in the way HTTP requests are handled which could allow a remote malicious user to execute arbitrary code. | Unofficial patch (Core SDI): ftp://ftp.core-sdi.com/pub/patches/VNC-serverBO.patch | AT&T WinVNC Server Buffer Overflow | **High** | Bug discussed in newsgroups and websites. |
| AT&T[4] | Windows 98SE/ME/ NT 4.0/2000 | WinVNC Client 3.3.3r7 & previous | A vulnerability exists in the way the rfbConnFailed packet is handled which could let a remote malicious user execute arbitrary code. | Unofficial patch (CORE SDI): ftp://ftp.core-sdi.com/pub/patches/VNC-clientBO.patch | AT&T WinVNC Client Buffer Overflow | **High** | Bug discussed in newsgroups and websites. |
| AT&T[5] | Windows 98SE/NT 4.0/2000, Unix, MacOS 9.0 | VNC 3.3.3 and previous | A vulnerability exists in the client authentication mechanism, which could allow a remote malicious user to gain unauthorized access to the server, allowing potentially elevated privileges. | It is advisable to tunnel communications between the VNC server and client through a crypto-graphically strong end-to-end authenticated channel. References for doing so are provided in the VNC FAQ located at: http://www.uk.research.att.com/vnc/faq.html and specifics on how to tunnel VNC over SSH are provided at: http://www.uk.research.att.com/vnc/sshvnc.html | AT&T VNC Weak Authentication | Medium | Bug discussed in newsgroups and websites. |
| Cisco[6] | Multiple | WebNS 3.0, 4.0 | A Denial of Service vulnerability exists when a malicious user requests a filename that is the maximum size of the filename buffer. | Upgrade available at: http://www.cisco.com/public/sw-center/sw-web.shtml | Cisco Content Service Switch Long Filename Denial of Service<br><br>CVE name: CAN-2001-0019 | Low | Bug discussed in newsgroups and websites. |
| Cisco[7] | Multiple | WebNS 3.0, 3.1, 4.0, 4.0.1 | A vulnerability exists due to the way user-supplied input is handled which could let a malicious user view sensitive information. | Workaround available at: http://www.cisco.com/warp/public/707/arrowpoint-cli-filesystem-pub.shtml | Cisco Content Services Switch Directory Structure File Reading<br><br>CVE Name: CAN-2001-0020 | Medium | Bug discussed in newsgroups and websites. |

[3] CORE SDI Advisory, CORE-2001011502, January 29, 2001.
[4] CORE SDI Advisory, CORE-2001011503, January 29, 2001.
[5] CORE SDI Advisory, CORE-2001011501, January 23, 2001.
[6] Cisco Security Advisory, CI-01.01, January 31, 2001.
[7] Cisco Security Advisory, CI-01.01, January 31, 2001.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| FreeBSD [8] | Unix | FreeBSD 3.5, 3.5.1, 4.1.1, 4.2; Red Hat Linux 6.2 alpha, i386, sparc | A vulnerability exists in the inetd package, which could allow a malicious user to gain access to restricted resources or elevate their privileges. | Patch available at: **FreeBSD** ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/ **RedHat:** ftp://updates.redhat.com/ | FreeBSD inetd wheel Group File Read | Medium | Bug discussed in newsgroups and websites. |
| FreeBSD [9] | Unix | FreeBSD 4.0-4.2 | A vulnerability exists in the periodic implementation, which could allow a malicious user to cause arbitrary files on the system to be corrupted. | Patch available at: ftp://ftp.freebsd.org/pub/FreeBSD/CERT/patches/SA-01:12/periodic.patch | FreeBSD periodic /tmp File Race Condition | **High** | Bug discussed in newsgroups and websites. |
| GoAhead Software [10] | Windows 95/98/NT 4.0/2000/ CE 2.0/3.0 | GoAhead WebServer 2.0, 2.1 | A directory traversal vulnerability exists which could allow a malicious user to execute arbitrary commands with root privileges. | No workaround or patch available at time of publishing. | GoAhead WebServer Directory Traversal | **High** | Bug discussed in newsgroups and websites. Exploit has been published. |
| Guido Frassato [11] | Windows 95/98/NT 4.0 | SEDUM HTTP Server 2.0 | A directory traversal vulnerability exists which could allow a remote malicious user to break out of the web root. | No workaround or patch available at time of publishing. | Guido Frasseto SEDUM HTTP Server Directory Traversal | Low | Bug discussed in newsgroups and websites. Exploit has been published. |
| Heat-On Software [12] | Windows 95/98/NT 4.0/2000 | HSWeb 2.0 | A vulnerability exists when a specially crafted URL is requested which could let a remote malicious user discover the physical path of the web root if directory browsing is enabled. | No workaround or patch available at time of publishing. | Heat-On HSWeb Web Server Path Disclosure | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |
| IBM [13] | Multiple | Net Commerce 3.0-3.2 | Several security vulnerabilities exist due to user-supplied input requests not being properly validated, which could let a malicious user execute arbitrary commands. | No workaround or patch available at time of publishing. | IBM Net.Commerce Remote Arbitrary Command Execution | **High** | Bug discussed in newsgroups and websites. Exploits have been published. |
| IBM [14] | Multiple | WebSphere | A vulnerability exists when the WebSphere application server shares the same document root as the Netscape Enterprise Server, which could let a malicious user view the source of any JSP file in the document root. | No workaround or patch available at time of publishing. | IBM WebSphere ShowCode | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |

[8] FreeBSD Security Advisory, FreeBSD-SA-01:11, revised January 29, 2001.
[9] FreeBSD Security Advisory, FreeBSD-SA-01:12, January 29, 2001.
[10] Securiteam, February 3, 2001.
[11] Bugtraq, February 4, 2001.
[12] Bugtraq, February 4, 2001.
[13] Securiteam, February 7, 2001.
[14] Securiteam, January 30, 2001.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| IBM[15] | Windows, Unix | IBM HTTP Server 1.3.6.2 under Apache version 1.3.7-dev (Unix), IBM HTTP Server 1.3.6.3 under Apache version 1.3.7-dev (Win32) | A security vulnerability exists which could let a malicious user enter arbitrary JavaScript commands into the output of the WebSphere web server. Information sent from an untrusted web server would appear as if it came from a legitimate server. | No workaround or patch available at time of publishing. | IBM HTTP Server WebSphere Arbitrary Information | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |
| Information Manage-ment Specialists, Inc. [16] | Windows 95 | Informs PicServer 1.0 | A directory traversal vulnerability exists which could let a remote malicious user gain read access to directories outside the root directory. | No workaround or pat ch available at time of publishing. | Informs PicServer Directory Traversal | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |
| iWeb Systems[17] | Windows NT 4.0, Unix | HyperSeek 2000 | A directory traversal vulnerability exists which could let a malicious user gain read permissions. | No workaround or patch available at time of publishing. | iWeb HyperSeek 2000 Directory Traversal | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |
| Martin Stover[18] | Unix | Mars NWE 0.99pl19 | A format string vulnerability exists which could allow a remote malicious user to gain superuser privileges from DOS/Windows workstations attached to the Mars server. | No workaround or patch available at time of publishing. | Mars NWE Format String | **High** | Bug discussed in newsgroups and websites. |
| Microsoft[19] | Windows 98/NT 2000 | Windows 98, Windows NT 2000 | A Denial of Service vulnerability exists due to the lack of restrictions on the allocation of network sockets by user applications. | No workaround or patch available at time of publishing. | Microsoft Windows UDP Socket Denial of Service | Low | Bug discussed in newsgroups and websites. Exploit has been published. |
| Microsoft[20] | Windows NT 2000 | Windows NT 2000, NT 2000 Server, Advanced Server | Anomalies exist in the catalog file (SP2.cat) in the Windows 2000 Post-Service Pack 1 which could cause the removal of some hotfixes and security patches. | Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq01-005.asp | Windows NT Hotfix Packaging Anomalies | Medium | Bug discussed in newsgroups and websites. |

[15] Securiteam, February 3, 2001.
[16] Bugtraq, February 5, 2001.
[17] NerF Security gr0up Advisory, January 28, 2001.
[18] Bugtraq, January 26, 2001.
[19] Georgi Guninski Security Advisory #37, February 6, 2001.
[20] Microsoft Security Bulletin, MS01-005, January 30, 2001.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Microsoft[21] | Windows NT 2000 | Windows NT 2000 Server, Advanced Server | A Denial of Service vulnerability exists in the implementation of the Remote Data Protocol (RDP) when multiple malformed packets are submitted. | Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq01-006.asp | Windows NT 2000 Invalid RDP Data | Low | Bug discussed in newsgroups and websites. |
| Microsoft[22] | Windows NT 2000 | Windows NT 2000, Server, SP1, Professional, Advanced Server, Terminal Services | A vulnerability exists in the way the Network Dynamic Data Exchange (DDE) Agent processes requests, which could let a malicious user execute arbitrary code or take complete control over the local machine. | Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq01-007.asp | Windows NT 2000 Network DDE Agent Request | **High** | Bug discussed in newsgroups and websites. Exploit script has been published. |
| Microsoft[23] | Windows NT 4.0 | Windows NT 4.0 Workstation, Server, Enterprise Edition, Server, Terminal Server Edition | A vulnerability exists in the NTLM Security Support Provider (NTLMSSP) service which could allow a malicious user to gain administrative control over the system. | Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq01-008.asp | Windows NT NTLMSSP Privilege Elevation<br><br>CVE Name: CVE CAN-2001-0016 | Medium | Bug discussed in newsgroups and websites. |
| Microsoft[24] | Windows NT 4.0/2000 | Internet Information Service (IIS) 4.0, 5.0 | A new variant of the 'File Fragment Reading via .HTR' vulnerability exists which could allow a remote malicious user to read fragments of files from a web server. Previous variants of this vulnerability were discussed in Microsoft Security Bulletins MS00-031 and MS00-044. | Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq01-004.asp | IIS File Fragment Reading via .HTR | Medium | Bug discussed in newsgroups and websites. |
| Multiple Vendors[25] | Unix | Debian Linux 2.2 sparc, powerpc, arm, alpha, 68k; SuSE Linux 6.3, 6.4, 7.0 | A vulnerability exists due to the handling of format strings by the -l argument of the man command, which could let a local malicious user execute arbitrary code and potentially gain administrative access. | No workaround or patch available at time of publishing. | Linux man -l Format String | **High** | Bug discussed in newsgroups and websites. |

[21] Microsoft Security Bulletin, MS01-006, January 31, 2001.
[22] Microsoft Security Bulletin, MS01-007, revised February 9, 2001.
[23] Microsoft Security Bulletin, MS01-008, February 7, 2001.
[24] Microsoft Security Bulletin, MS01-004, January 29, 2001.
[25] Bugtraq, January 31, 2001.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Multiple Vendors[26] | Unix | Mandrake Soft Linux Mandrake 6.0-7.2, Corporate Server 1.0.1; Red Hat Powertools; Martin Schwenkes gnuserv 3.12 & previous | A buffer overflow vulnerability and weak security exists in the MIT-MAGIC-COOKIE authentication mechanism which could let a remote malicious user execute arbitrary commands. | **MandrakeSoft:** http://www.linux-mandrake.com/en/ftp.php3 **RedHat:** ftp://updates.redhat.com/powertools/6.2 **Martin Schwenkes**: http://www.xemacs.org/Releases/21.1.14.html | Gnuserv MIT-MAGIC-COOKIE Remote Buffer Overflow | **High** | Bug discussed in newsgroups and websites. |
| **Multiple Vendors[27]** ***Debian releases patch[28]*** | **Unix** | **RedHat Linux 7.0; Wirex Immunix OS 7.0-Beta** ***Debian GNU/Linux 2.2*** | **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: Wirex Immunix OS 7.0-Beta: http://www.immunix.org/ImmunixOS/7.0-beta/updates/RPMS** ***Debian:*** ftp://ftp.debian.org/debian/dists/stable/*/binary-$arch/ | **Apache /tmp File Race** | **High** | **Bug discussed in newsgroups and websites.** |
| Netopia[29] | Multiple | Netopia R9100 Firmware version 4.6 | A Denial of Service vulnerability exists when a remote malicious user telnets to the router. | Upgrade to firmware 4.8.2 or later. (See "Upgrading Netopia Router Firmware") located at: http://www.netopia.com/support/technotes/hardware/NIR_055.html | Netopia Router Denial of Service | Low | Bug discussed in newsgroups and websites. |
| Netscape[30] | Multiple | Enterprise Server 3.0, 4.0 | A vulnerability exists when the Web Publishing feature is installed by default which could let a remote malicious user gain sensitive information. | Unofficial workaround (S.A.F.E.R.): Disable Web Publishing, or disable INDEX request. | Netscape Enterprise Server 'Index' Disclosure | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |
| QNX Software Systems[31] | Unix | QSSL QNX RTP | A vulnerability exists in the ftp daemon which could allow a malicious user to execute arbitrary code. | No workaround or patch available at time of publishing. | QNX RTP ftpd stat Buffer Overflow | **High** | Bug discussed in newsgroups and websites. |
| SSH Communi-cations Security[32] | Unix | SSH 1.2.30 | A vulnerability exists in the implementation of the SSH1 daemon which could allow a remote malicious user to gain access to any account, including potentially the root account. | No workaround or patch available at time of publishing. | SSH1 Daemon Logging Failure | **High** | Bug discussed in newsgroups and websites. Exploit script has been published. |
| Sun Micro-systems, Inc.[33] | Unix | Solaris 7.0, 7.0_x86, 8.0, 8.0_x86 | A buffer overflow vulnerability exists in the shared library "ximp40," which could allow a local malicious user to obtain root privileges. | No workaround or patch available at time of publishing. | Solaris ximp40 Library Buffer Overflow | **High** | Bug discussed in newsgroups and websites. Exploit script has been published. |

[26] Securiteam, February 5, 2001.
[27] Immunix OS Security Advisory, IMNX-2000-70-016-01, January 10, 2001.
[28] Debian Security Advisory, DSA-021-1, January 26, 2001.
[29] Securiteam, January 30, 2001.
[30] S.A.F.E.R. Security Bulletin, 010124.EXP.1.11, January 25, 2001.
[31] Securiteam, February 4, 2001.
[32] Crimelabs Security Note, CLABS200101, February 5, 2001.
[33] SPS Advisory #40, January 31, 2001.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Washington University [34] | Unix | wu-ftpd 2.4.1 -2.6 | A format string vulnerability exists which could let a remote malicious user get root access on the victim host. | Upgrade available at: http://security.debian.org/dists/stable/updates/main/binary-i386/wu-ftpd_2.6.0-5.2.1_i386.deb | Wu-Ftpd Debug Mode Client Hostname Format String | **High** | Bug discussed in newsgroups and websites. Exploit has been published. |
| WhitSoft Development [35] | Windows 95/98/NT 4.0/2000 | SlimServe HTTPd 1.0 | A Denial of Service vulnerability exists when a remote malicious user submits an unusually long GET request. | No workaround or patch available at time of publishing. | WhitSoft SlimServe HTTPd Server Denial of Service | Low | Bug discussed in newsgroups and websites. Exploit has been published. |
| XMail [36] | Unix | XMail 0.66 & prior | Several buffer overflow vulnerabilities exist in the CTRLServer tool which could let a remote malicious user execute arbitrary code with root privileges. | Patch available at: http://www.mycio.com/davidel/xmail | XMail CTRLServer Buffer Overflow Vulnerabilities | **High** | Bug discussed in newsgroups and websites. Exploit script has been published. |

*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 27 and February 9, 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, 26 scripts, programs, and net-news messages containing holes or exploits were identified. NOTE: At times, scripts/techniques may contain names or content that may be considered offensive.

| Date of Script (Reverse Chronological Order) | Script name | Script Description |
|---|---|---|
| February 9, 2001 | angst-0.4b.tar.gz | An active packet sniffer, based on libpcap and libnet, which creates a file of the payload of all the packets received on the specified ports. |

[34] Debian Security Advisory, DSA-016-3, January 24, 2001.
[35] Bugtraq, January 30, 2001.
[36] Bugtraq, February 2, 2001.

| Date of Script (Reverse Chronological Order) | Script name | Script Description |
|---|---|---|
| February 8, 2001 | SQLExec.zip | A remote exploit for the Microsoft SQL server vulnerability. |
| **February 6, 2001** | **bugtraq.c** | **An exploit for the Bind TSIG vulnerability.** |
| February 5, 2001 | netddemsg.cpp | Script which exploits the Windows NT 2000 Network DDE Agent Request vulnerability. |
| February 5, 2001 | snarp.zip | A tool for NT 4.0 which uses an ARP poison attack to relay traffic between two hosts, allowing sniffing of the data on switched networks. |
| **February 5, 2001** | **Ssh1-log-exp** | **Script which exploits the SSH1 Daemon Logging Failure vulnerability.** |
| February 2, 2001 | bsdfpf.tar.gz | BSD FingerPrintFucker is a Dynamic Kernel Linker (KLD) for FreeBSD, which changes the tcp/ip stack in order to emulate other OS's against tcp/ip fingerprinting. |
| February 2, 2001 | frel-1.0.beta.tgz | A modified version of fragrouter, used to evade NIDS, which can run in partial takeover mode so that the fragmented attack stream seems to be coming from another active machine on the same physical subnet. |
| February 2, 2001 | pkc001.txt | Proof of concept exploit for the Oops proxy server heap overflow vulnerability. |
| February 2, 2001 | pkc002.txt | Proof of concept exploit for the Tinyproxy Heap Overflow vulnerability. |
| February 2, 2001 | pkc003.txt | Proof of concept exploit for the mICQ Remote Buffer Overflow vulnerability. |
| February 2, 2001 | pkc004.txt | Proof of concept exploit for the Icecast Buffer Overflow vulnerability. |
| February 2, 2001 | prodbx.c | Script which exploits the Progress Database Server v8.3b vulnerability. |
| February 2, 2001 | seyon-exploit.pl | Script which exploit the Seyon v2.1rev4b vulnerability. |
| February 2, 2001 | tcpip_lib3.zip | A library for Windows 2000 which allows constructing IP's, IP spoofing, attacks, and more. |
| February 2, 2001 | Xmailx.c | Script which exploits the XMail CTRLServer Buffer Overflow Vulnerabilities. |
| **February 1, 2001** | **bind-tsig.c** | **A Trojan that pretends to be a Bind 8 exploit, but actually attacks dns1.nai.com.** |
| February 1, 2001 | jazip-exploit.pl | Script which exploits the JaZip Buffer Overflow vulnerability. |
| January 31, 2001 | arp-scan.c | Arp-scan is a tool which scans for alive hosts in a subnet with ARP packets. |
| January 31, 2001 | progress-db.txt | Proof of concept exploit for the Progress Database Server buffer overflow vulnerabilities. |
| **January 31, 2001** | **QT.4.1.2J-x.cpp** | **Script which exploits the Apple Quicktime Plugin Remote Overflow vulnerability.** |
| January 31, 2001 | sara-3.3.3.tar.gz | A security analysis tool based on the SATAN model. |
| January 31, 2001 | sw-mitm.tar.gz | A 'Man in the Middle' tool for level2 switches which can redirect traffic between two hosts on a LAN. |
| **January 31, 2001** | **ximp40-ex.c** | **Script which exploits the Solaris ximp40 Library Buffer Overflow vulnerability.** |
| January 28, 2001 | ettercap-0.1.0.beta.tar.gz | A network sniffer/interceptor/logger for switched LANs that uses ARP poisoning and the 'man-in-the-middle' technique to sniff all the connections between two hosts. |
| January 27, 2001 | naptha-1.1.tgz | A Denial of Service attack against many OS's which uses established TCP connections to create a resource starvation attack. |

# *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:**

**Based upon investigations and information from other sources, the "Anna Kournikova" mass-mailing worm/virus is spreading rapidly throughout the Internet. For more information, see NIPC ASSESSMENT 01-001, "Anna Kournikova," located at: http://www.nipc.gov/warnings/assessments/2001/01-001.htm.**

**The CERT/CC has recently learned of four vulnerabilities spanning multiple versions of the Internet Software Consortium's (IS C) 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.**

PC/Internet users should be on alert for possible malicious e-mail messages harboring dangerous Valentine computer viruses.

# *Viruses* *(NOTE: At times, viruses may contain names or content that may be considered offensive.)*

**VBS_KALAMAR.A (Aliases: Anna Kournikova, SST, Kalamar, VBS/VBSWG.J, VBS/Onthefly.A, Lee) (Visual Basic Script Worm):** There have been several reports of this virus in the wild. It is an email-aware Visual Basic Script worm that propagates via MS Outlook as an attachment, "ANNAKOURNIKOVA.JPG.VBS." The worm arrives in an e-mail with the following characteristics:

Subject line: Here you have, ;0)
Message text: Hi:
Check This!
File attachment: AnnaKournikova.jpg.vbs

The virus lures users into activating it by pretending to be a jpeg graphic of Russian tennis player Anna Kournikova. The first time the attached file is executed it mails itself to everybody in your Outlook address book. The worm makes changes to the Registry, creating an entry called HKCU\software\OnTheFly. On the 26th of January the worm attempts to connect to a website in the Netherlands, www.dynabyte.nl. For more detailed information, please see NIPC ASSESSMENT 01-001, "Anna Kournikova," located at: http://www.nipc.gov/warnings/assessments/2001/01-001.htm, or CERT® Advisory CA-2001-03, located at: http://www.cert.org/advisories/CA-2001-03.html.

**VBS/LoveLet-CD (Visual Basic Script Worm):** This is a variant of the VBS/LoveLet-A worm (also known as the Love Bug) and is currently spreading in Europe (commonly referred to as the Italian Love Bug virus). The worm copies itself to the Windows system directory as CARTOLINA.VBS and then attempts to e-mail this file as an attachment to a message with the following characteristics:

Subject: "una cartolina per te!"
Body text: "Ciao, un tuo amico ti ha spedito una cartolina
virtuale... mooolto particolare!"

The worm tries to send this e-mail to addresses in the infected user's Outlook address book.

**W32/Hybris-Drop (Dropper Virus):** This virus has been reported in the wild. It is a Windows 32 executable file that drops the W32/Hybris worm. Files carrying W32/Hybris-Drop are created by W32/Hybris using one of its upgradeable components.

**W97M_DIGMA.A (Aliases: DIGMA.A, W97M/DIGMA, Macro.W97M.Digma, W97M/DIGMA.A) (Word 97 Macro Virus):** When an infected document is closed, this macro virus infects active Word documents and document templates. It carries a destructive payload of changing all letters "a" and "o" with the word "FUCK." It also inserts the text "DIGITAL MADMAN" on the first line of the document. The supposed trigger date for this payload to execute is on the 13th of any month but it does not happen because there are errors in this release of the virus code.

**W97M_FS.O (Aliases: F.O, W97M/Fly.gen, Macro.Word97.FS.O, W97M/FS.V:Tw) (Word 97 Macro Virus):** This macro virus infects Word documents and document templates when an infected document is closed. It is also a password-stealing virus that sends password files of an infected user's computer via File Transfer Protocol (FTP) to a remote virus author. It does not carry a destructive payload.

**W97M_HOPE.AA (Aliases: HOPE.AA, W97M/CLASS, W97M.CLASS, WM97/HOPE-AA) (Word 97 Macro Virus):** This semi-polymorphic macro virus infects when an infected document is opened or closed and when the ToolsMacro menu is accessed. It overwrites the ThisDocument module so that it infects the normal template and active documents. It attempts to drop an Internet Relay Chat script and configures the mIRC client to propagate the virus. It carries a payload that executes when the system day equals the 14th of any month from July through December.

**W97M_MEDIA.A (Aliases: MEDIA.A, W97M/MEDIA, W97M.Ping.A) (Word 97 Macro Virus):** When an infected document is opened, this Word macro virus infects the document template and active documents. It does not have a destructive payload and it only displays a message box when a random condition is satisfied.

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

Title: "Creap school"
Author: "fpschoolanarchist"
Keywords: "fpanarchist"

**WM97/FF-H (Word 97 Macro Virus):** The virus was created as a result of two existing viruses (WM97/Class-D and WM97/FF-A) interacting with each other.

**WM97/Footer-W (Word 97 Macro Virus):** The virus is a Class type infector that bypasses the protection built into Microsoft Office SR1.

**WM97/Marker-GF (Word 97 Macro Virus):** Whenever an infected document is closed, there is a 1 in 3 chance of a File Summary box appearing on the screen with the author name set to Ethan Frome.

**WM97/Myna-AF (Word 97 Macro Virus):** This is a Word macro virus that does little more than replicate. The replicating code contains the phrase MYNAMEISVIRUS, which is used as a flag to check for its presence.

**WM97/Surround-C (Word 97 Macro Virus):** When the virus infects other Word documents, it attempts to "clean" them of other virus infections and user defined macros.

**WM97/Titch-H (Word 97 Macro Virus):** This virus is a variant of the WM97/Titch virus. It is a simple Word macro virus. The virus code includes the following text, which does not get displayed: "If you had looked you could have found and deleted it but… You probably never knew it was here!"

**WM97/Wrench-I (Word 97 Macro Virus):** WM97/Wrench-I is a Word macro virus. When you try to access the Visual Basic Editor the virus displays the Office Assistant, as though you had asked for Help, and then runs the infection routine.

**XM97/Reten-B (Excel 97 Macro Virus):** This is an Excel macro virus which on the 26th of any month displays a message box containing the text:
"Microsoft Excel has Protected your system. This product registered to: <username>"

## *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 | N/A | CyberNotes-2001-02 |
| BAT_EXITWIN.A | N/A | CyberNotes-2001-01 |
| Flor | N/A | CyberNotes-2001-02 |
| PHP/Sysbat | N/A | CyberNotes-2001-02 |
| PIF_LYS | N/A | CyberNotes-2001-02 |
| Troj/KillCMOS-E | N/A | CyberNotes-2001-01 |
| TROJ_AOL_EPEX | N/A | CyberNotes-2001-01 |
| TROJ_AOLWAR.B | N/A | CyberNotes-2001-01 |
| TROJ_AOLWAR.C | N/A | CyberNotes-2001-01 |
| **TROJ_APS.216576** | **N/A** | **Current Issue** |
| TROJ_AZPR | N/A | CyberNotes-2001-01 |
| TROJ_BAT2EXEC | N/A | CyberNotes-2001-01 |
| TROJ_BKDOOR.GQ | N/A | CyberNotes-2001-01 |
| **TROJ_DARKFTP** | **N/A** | **Current Issue** |
| **TROJ_FIX.36864** | **N/A** | **Current Issue** |
| TROJ_GLACE.A | N/A | CyberNotes-2001-01 |
| **TROJ_GOBLIN.A** | **N/A** | **Current Issue** |
| TROJ_GTMINESXF.A | N/A | CyberNotes-2001-02 |
| **TROJ_HERMES** | **N/A** | **Current Issue** |
| **TROJ_HFN** | **N/A** | **Current Issue** |
| TROJ_ICQCRASH | N/A | CyberNotes-2001-02 |
| TROJ_JOINER.15 | N/A | CyberNotes-2001-02 |
| TROJ_NAVIDAD.E | N/A | CyberNotes-2001-01 |
| **TROJ_PORTSCAN** | **N/A** | **Current Issue** |
| TROJ_QZAP.1026 | N/A | CyberNotes-2001-01 |
| **TROJ_RUNNER.B** | **N/A** | **Current Issue** |
| **TROJ_RUX.30** | **N/A** | **Current Issue** |
| TROJ_SUB7.401315 | N/A | CyberNotes-2001-01 |
| TROJ_SUB7.MUIE | N/A | CyberNotes-2001-01 |
| TROJ_SUB7.V20 | N/A | CyberNotes-2001-02 |
| TROJ_SUB7DRPR.B | N/A | CyberNotes-2001-01 |
| **TROJ_SUB7DRPR.C** | **N/A** | **Current Issue** |
| TROJ_TWEAK | N/A | CyberNotes-2001-02 |
| TROJ_WEBCRACK | N/A | CyberNotes-2001-02 |

**TROJ_APS.216576 (Aliases: APS.216576, AOL Trojan):** This is an AOL Trojan virus that works as an AOL password stealer. Although it is considered non-destructive, it stays in your Windows memory and monitors all of your AOL logon account information.

**TROJ_DARKFTP**: This Win32 network enabled Trojan gives remote users access to an infected system. It uses File Transfer Protocol (FTP) and Internet Relay Chat (mIRC) connections.

**TROJ_FIX.36864 (Aliases: FIX.36864, Mw32/Fix@M.36864, Trojan.PSW.Atomic, W95/Fix.36864):** This destructive Trojan enables a malicious user to access a user's computer from a remote location, therefore compromising network security. It propagates via e-mail.

**TROJ_GOBLIN.A (Alias: GOBLIN.A):** This destructive Windows Trojan is written in Visual Basic 6.0. Upon execution, it displays messages before it deletes files and directories of an infected computer's C:\ drive.

**TROJ_HERMES (Aliases: W32/Hermes@MM, HERMES, I-Worm.Hermes):** This Win32 worm spreads itself via e-mail. It sends itself twice to all entries in the infected user's address book and also tries to copy itself in the root directory of the infected user's hard disk drive.

**TROJ_HFN (Alias: HFN):** This Win32 Trojan installs a number of Trojan horse programs on an infected user's system. It does not have a destructive payload but it can be used to hack remote computers from a remote area.

**TROJ_PORTSCAN (Alias: PORTSCAN):** This Win32 hacking tool is used to look for an open port in a remote computer. It infects by opening certain ports so that other Trojan hacking programs can easily tap into the infected user's computer.

**TROJ_RUNNER.B (Aliases: RUNNER.B, MultiDropper, Trojan.Win32.TrojanRunner.a):** This is a server-side backdoor Trojan that compromises network security. It allows a remote user to obtain system administrator privileges to an infected user's computer.

**TROJ_RUX.30 (Aliases: Backdoor.RUX.30, RUX.30):** This remote-access and password-stealing Trojan is written in Visual Basic 5.0 and compromises network security. It executes only when MSWINSCK.OCX is installed on the infected user's system. Otherwise an error message is displayed and its execution is stopped. This Trojan allows a malicious user to have access to vital information on the infected user's computer.

**TROJ_SUB7DRPR.C (Aliases: SUB7DRPR.C, Multidropper.z, Trojan.Win32.Trojan Runner.RSP.a):** This is a Trojan dropper program for TROJ_SUB7.401315. It arrives as a Standard Video File (MPEG) of a pornographic clip. When this Trojan executes, it plays the MPEG file "LOLITA0.MPEG," while it drops the Trojan program IEXPLORER.EXE.