# National Infrastructure Protection Center CyberNotes

*Issue #2000-24* *December 4, 2000*

**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 November 17, and November 30, 2000. 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 |
|---|---|---|---|---|---|---|
| Adcycle.com[1] | Adcycle 0.77b | A vulnerability exists if the installation is not completed, which could let a remote malicious user obtain the management username/password. | No workaround or patch available at time of publishing. | Adcycle Password Disclosure | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |

[1] Bugtraq, November 20, 2000.

| Vendor/ Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/Alerts | Common Name | Risk* | Attacks/Scripts |
|---|---|---|---|---|---|---|
| Aladdin Enterprises[2]<br><br>Unix | Ghostscript 4.3, 5.10cl, 5.10.10, 5.10.15, 5.50 | Several vulnerabilities exist: temporary files are created insecurely; and improper LD_RUN_PATH values cause it to search for libraries in the current directory which could let a malicious user elevate their privileges, execute a Denial of Service, or further compromise the target host. | **Caldera:** ftp://ftp.calderasystems.com/pub/updates/OpenLinux/ **Conectiva:** ftp://atualizacoes.conectiva.com.br/ **Debian:** http://security.debian.org/dists/stable/updates/main/ **Linux-Mandrake:** http://www.linux-mandrake.com/en/ftp.php3 **RedHat:** ftp://updates.redhat.com/ | Ghostscript Arbitrary Shared Library Usage and Symlink | Medium | Bug discussed in newsgroups and websites. |
| AT&T[3]<br><br>Windows 95/98/ME/NT 3.5/4.0/2000 | WinVNC 3.3x | A vulnerability exists due to insecure registry permissions on sensitive authentication information stored in the Windows registry, which could let a remote malicious user gain complete access to the system. | Administrators should use Regedit to remove the "Everybody" and "Standard users" permissions from the registry key entry. | WinVNC Remote Desktop Default Configuration | **High** | Bug discussed in newsgroups and websites. Exploit has been published. |
| Balabit[4] | syslog-ng 1.4.8 and prior | A security vulnerability exists in the log message parsing function, which could let a malicious user cause a Denial of Service. | Upgrade to version 1.4.9 or later available at: http://www.balabit.hu/products/syslog-ng/ | Syslog-ng Incomplete Priority String Remote Denial of Service | Low | Bug discussed in newsgroups and websites. Exploit has been published. |
| BSDi[5] | BSD/OS 3.0, 3.1, 4.0, 4.0.1 | A vulnerability exists in rcvtty, which could let a malicious user elevate their system privileges. | No workaround or patch available at time of publishing. | Rcvtty Arbitrary Command Execution | Medium | Bug discussed in newsgroups and websites. Exploit script has been published. |
| Caucho Technology[6]<br><br>Windows NT 4.0 | Resin 1.2 | A vulnerability exists in the source code of a JSP file if a special character is appended to a HTTP GET request, which could let a remote malicious user gain sensitive information. | A new version, 1.2.1, addressed the vulnerability and will be available in the future. | Resin JSP Source Disclosure | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |
| Christopher Heschong[7] | Twig 2.5.1 | A vulnerability exists in the script that checks virtual hosting which could allow a remote malicious user to execute arbitrary code. | No workaround or patch available at time of publishing. | Twig Remote Arbitrary Script Execution | **High** | Bug discussed in newsgroups and websites. Exploit has been published. |

[2] Securiteam, November 29, 2000.
[3] Bugtraq, November 19, 2000.
[4] BalaBit Security Advisory, BB-2000/01, November 22, 2000.
[5] Securiteam, November 28, 2000.
[6] eSecurityOnline.com Free Vulnerability Alert 3182, November 28, 2000.
[7] eSecurityOnline.com Free Vulnerability Alert 3186, November 29, 2000.

| Vendor/ Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/Alerts | Common Name | Risk* | Attacks/Scripts |
|---|---|---|---|---|---|---|
| Cisco[8] | DSL Router 675.0, 677.0 | A remote Denial of Service vulnerability exists in Cisco 675 DSL routers when the Web Administration Interface is enabled. | Unofficial workaround (Securiteam): Disable the Web Based Administration Interface on your 675 until a patch or CBOS revision is made available. | Cisco 675 Web Administration Denial of Service | Low | Bug discussed in newsgroups and websites. Exploit has been published. |
| FreeBSD[9]<br><br>Unix | FreeBSD 3.5, 3.5.1, 4.0, 4.1, 4.1.1-STABLE | A vulnerability exists in the deny_incoming command, which could let a remote malicious user bypass access controls. | Upgrade to 4.1.1-STABLE or 3.5.1-STABLE located at: ftp://ftp.freebsd.org/pub/FreeBSD/ | FreeBSD ppp deny_incoming | Medium | Bug discussed in newsgroups and websites. |
| Hewlett-Packard[10]<br><br>Unix | EMS A.03.00 | A security vulnerability exists in EMS (Event Monitoring System), which may allow malicious users to change any file permissions on the root partition. This affects ServiceGuard OPS edition as well as MC/ServiceGuard. | Hewlett-Packard Company recommends that users of early releases of the Event Monitoring Service migrate to EMS A.03.20. | EMS Arbitrary File Permission Change | **High** | Bug discussed in newsgroups and websites. |
| IBM[11]<br><br>Windows NT 4.0, OS/2, OS/390, OS/400, Unix | Net.Data 7.0 | A vulnerability exists when a specially crafted URL is requested via the CGI application, which could let a malicious user gain server information. Successful exploitation of this vulnerability could assist in further attacks against the victim host. | No workaround or patch available at time of publishing. | Net.Data Path Disclosure | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |
| IBM[12]<br><br>Windows NT, Unix | HTTP Server 1.3.6.3 | A Denial of Service vulnerability exists when a long GET request is sent to the server. | No workaround or patch available at time of publishing. Update to IBM HTTP Server (IHS)1.3.12. | HTTP Server Denial of Service | Low | Bug discussed in newsgroups and websites. |
| Kevin Lindsay[13]<br><br>Unix | Secure Locate 1.4-1.6, 2.0-2.2 | A heap corruption vulnerability exists that could let a malicious user execute arbitrary code. | Upgrade available at: ftp://ftp.mkintraweb.com/pub/linux/slocate/src/slocate-2.3.tar.gz | Secure Locate Heap Corruption | **High** | Bug discussed in newsgroups and websites. Exploit script has been published. |
| Lotus[14] | Lotus Notes Client R5 | A vulnerability exists in the ECL (Execution Control List), which could let a remote malicious user gain sensitive information. | No workaround or patch available at time of publishing. | Lotus Notes Client R5 File Existence Verification | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |

[8] Securiteam, November 30, 2000.
[9] FreeBSD Security Advisory, FreeBSD-SA-00:70, November 14, 2000.
[10] HP-UX Security Advisory, HPSBUX0011-131, November 21, 2000.
[11] Bugtraq, November 28, 2000.
[12] Bugtraq, November 23, 2000.
[13] Bugtraq, November 26, 2000.
[14] Securiteam, November 26, 2000.

| Vendor/ Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/Alerts | Common Name | Risk* | Attacks/Scripts |
|---|---|---|---|---|---|---|
| Markus Triska[15] | CGIForum 1.0 | A vulnerability exists in the 'thesection' parameter, which could let a remote malicious user view files with privileges of the user "nobody." | Update available at: http://www.marcbrinkmann.de/inandonline/netz/CGIForum-1.01.tar.gz | CGIForum Arbitrary File Disclosure | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |
| Microsoft[16]<br><br>Windows NT 2000 | Windows NT 2000 | A Denial of Service vulnerability exists in the Telnet daemon if an initiated session is not reset. | No workaround or patch available at time of publishing. | Windows 2000 Telnet Session Timeout Denial of Service | Low | Bug discussed in newsgroups and websites. Exploit has been published. |
| Microsoft[17]<br><br>Windows NT 2000 | Windows NT 2000 Professional, Server, Advanced Server, Datacenter | A vulnerability exists in the way that NTLM authentication operates which could allow a domain account lockout policy to be bypassed, even if the domain administrator had set such a policy. | Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq00-089.asp | Windows NT Domain Account Lockout | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |
| **Microsoft[18]**<br><br>**Windows NT 4.0/2000**<br><br>***Updated to discuss two newly-discovered variants of the original vulnerability[19]*** | **Internet Information Services 4.0, 5.0** | **A vulnerability exists when IIS receives a specially formed request for an executable file followed by operating system commands, which could let a malicious user read system files and run arbitrary system commands.**<br>***The original variant affected IIS 5.0 in all cases, but only affected IIS 4.0 when a service pack prior to Windows NT 4.0 Service Pack 6a was in use. The new variants affect both IIS 4.0 and IIS 5.0 regardless of the service pack in use.*** | **Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq00-086.asp**<br><br>***Internet Information Server 4.0:***<br>http://www.microsoft.com/ntserver/nts/downloads/critical/q277873<br>***Internet Information Services 5.0:***<br>http://www.microsoft.com/Windows2000/downloads/critical/q277873 | **IIS Web Server File Request Parsing**<br><br>**CVE name CAN-2000-0886** | **High** | **Bug discussed in newsgroups and websites.** |

[15] Bugtraq, November 20, 2000.
[16] Bugtraq, November 29, 2000.
[17] Microsoft Security Bulletin, MS00-089, November 21, 2000.
[18] Microsoft Security Bulletin, MS00-086, updated November 10, 2000.
[19] Microsoft Security Bulletin, MS00-086, updated November 21, 2000.

| Vendor/ Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/Alerts | Common Name | Risk* | Attacks/Scripts |
|---|---|---|---|---|---|---|
| Microsoft[20]<br><br>Windows 95/98/98 SE/98 ME/NT 4.0 | Windows 95, 98, 98 SE, 98 ME, NT 4.0 | A remote Denial of Service vulnerability exists in NetBIOS.<br>**Note:** This vulnerability affects many operating systems aside from Microsoft Windows, however Microsoft is the only vendor so far that has issued a patch and workaround. | Microsoft has released a patch for Windows NT 4.0. For those running Windows 95/98/ME, Microsoft recommends to disable File and Printer Sharing. Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq00-091.asp | Windows Incomplete TCP/IP Packet<br><br>CVE name CAN-2000-1039 | Low | Bug discussed in newsgroups and websites. Exploit has been published. |
| Microsoft[21]<br><br>Windows NT 4.0 | Windows NT 4.0 | A remote Denial of Service vulnerability exists when the registry configuration for "SynAttackProtect" is set to two. | No workaround or patch available at time of publishing. | Windows NT SynAttack Protect Denial of Service | Low | Bug discussed in newsgroups and websites. Exploit has been published. |
| Microsoft[22]<br><br>Windows 95/98/NT 4.0/2000 | Internet Explorer 5.5 | A security vulnerability exists which allows executing arbitrary programs using OBJECT TYPE="text/html" and parsing index.dat by revealing the location of temporary Internet files folder. This may lead to taking full control over user's computer. | Unofficial workaround (Georgi Guninski):<br>Disable Active Scripting and move the location of the Temporary Internet Files Folder to an unpredictable location. | Internet Explorer Index.dat | **High** | Bug discussed in newsgroups and websites. Exploit has been published. |
| Microsoft[23]<br><br>Windows 95/98/NT 4.0/2000 | Media Player 6.4, 7 | Two security vulnerabilities exist in the .ASX and .WMS file formats which could allow a malicious user to execute arbitrary code or create Trojan .ASX files. | Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq00-090.asp<br>**Note**: The ".ASX Buffer Overrun" affects Windows Media Player versions 6.4 and 7. The ".WMS Script Execution" affects only Windows Media Player version 7. The patch installs the correct fix(es) for the particular version of Windows Media Player in use. | Media Player .ASX Buffer Overrun and .WMS Script Execution Vulnerabilities | **High** | Bug discussed in newsgroups and websites. Exploit script has been published. |
| Microsys[24] | CyberPatrol 4.04.003, 4.04.005 | A vulnerability exists in the way credit cards are handled which could let a remote malicious user retrieve credit card information in clear text format. | No workaround or patch available at time of publishing. | CyberPatrol Insecure Registration | Medium | Bug discussed in newsgroups and websites. Exploit script has been published. |

[20] Microsoft Security Bulletin, MS00-091, November 30, 2000.
[21] Bugtraq, November 22, 2000.
[22] Georgi Guninski Security Advisory #29, 2000, November 23, 2000.
[23] Microsoft Security Bulletin, MS00-090, November 22, 2000.
[24] Bugtraq, November 22, 2000.

| Vendor/ Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/Alerts | Common Name | Risk* | Attacks/Scripts |
|---|---|---|---|---|---|---|
| Midnight Commander[25]<br><br>Unix | Midnight Commander 4.5.40-4.5.51 | A vulnerability exists in the way directories are handled which may allow a malicious user to execute arbitrary commands. | No workaround or patch available at time of publishing. | Midnight Commander Directory Viewing Command Execution | **High** | Bug discussed in newsgroups and websites. |
| Multiple Vendors[26]<br><br>Unix | Gerald Combs Ethereal 0.8.13 and previous | Multiple buffer overflow vulnerabilities exist in the data parsing routines, which could let a remote malicious user execute arbitrary code. | Upgrade to 0.8.14 available at: http://www.ethereal.com/distribution/ethereal-0.8.14.tar.gz | Ethereal AFS Buffer Overflow Vulnerabilities | **High** | Bug discussed in newsgroups and websites. Exploit script has been published. |
| Multiple Vendors[27]<br><br>Unix | Jan Hubicka Koules 1.4 | A buffer overflow vulnerability exists which could allow a malicious user to elevate their privileges and gain root access. | No workaround or patch available at time of publishing. | Koules Svgalib Buffer Overflow | **High** | Bug discussed in newsgroups and websites. Exploit script has been published. |
| Multiple Vendors[28]<br><br>Unix | BB4 Big Brother Network Monitor 1.5d2 and previous | Numerous vulnerabilities exist which could allow a remote malicious user to view sensitive information and determine users IDs. | Patch the current version or upgrade to 1.5d3 available at: http://bb4.com/ | BB4 Big Brother Multiple CGI Vulnerabilities | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |
| Multiple Vendors[29]<br><br>Unix | Caldera eDesktop 2.4, eServer 2.3, OpenLinux Desktop 2.3; HP HP-UX 11.11; MandrakeSoft Linux Mandrake 6.0, 6.1, 7.0-7.2; RedHat Linux 5.2, 6.0-6.2E sparc, i386, alpha; SuSE Linux 7.0; Sun Solaris 8.0; Wirex Immunix OS 6.2 | A vulnerability exists due to the insecure creation of files in the /tmp directory which could allow a malicious user to create arbitrary files or to overwrite existing ones. | **Caldera eDesktop 2.4:** ftp://ftp.calderasystems.com/pub/updates/<br>**MandrakeSoft:** http://sunsite.ualberta.ca/pub/Mirror/Linux/mandrake/updates/<br>**RedHat Linux:** ftp://updates.redhat.com/<br>**Wirex Immunix OS 6.2:** http://www.immunix.org/ImmunixOS/6.2/updates/RPMS/bash-1.14.7-23.6x_StackGuard.i386.rpm | Multiple Vendor Bash/temp File Symlink | **High** | Bug discussed in newsgroups and websites. Exploit has been published. |

[25] Bugtraq, November 28, 2000.
[26] Securiteam, November 28, 2000.
[27] Securiteam, November 21, 2000.
[28] Fate Research Labs, November 20, 2000.
[29] eSecurityOnline.com Free Vulnerability Alert 3188, November 29, 2000.

| Vendor/ Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/Alerts | Common Name | Risk* | Attacks/Scripts |
|---|---|---|---|---|---|---|
| Multiple Vendors[30]<br><br>Unix | Wirex Immunix OS 6.2, 7.0-Beta; SuSE Linux 6.4, 7.0; RedHat Linux 7.0; MandrakeSoft Linux Mandrake 7.2; Conectiva Linux 5.1;<br><br>(GNU Linux modutils 2.3.11, 2.3.9) | A vulnerability exists in modprobe, which could allow a malicious user to gain root privileges. | **RedHat:** ftp://updates.redhat.com/<br>**Debian:** http://security.debian.org/dists/potato/updates<br>**MandrakeSoft:** http://www.linux-mandrake.com/en/ftp.php3<br>If the version of Linux you are using has not made a patch available for this vulnerability, a temporary workaround is to disable modprobe or remove the setuid bit from ping. | Multiple Vendor Linux modprobe Buffer Overflow | **High** | Bug discussed in newsgroups and websites. Exploit has been published |
| Multiple Vendors[31, 32, 33]<br><br>Unix | Joseph Allen Joe 2.8 | A vulnerability exists when a session abnormally exists which could let a malicious user append the contents of the Joe session to a symbolically linked file, potentially corrupting the linked file. | **RedHat:** ftp://updates.redhat.com/<br>**Linux-Mandrake:** http://www.linux-mandrake.com/en/ftp.php3<br>**Debian:** http://security.debian.org/dists/stable/updates/main/ | Joe Text Editor Symbolic Link | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |
| NetcPlus[34]<br><br>Windows 95/98/NT 4.0/2000 | BrowseGate 2.80.2 | A vulnerability exists that enables an authenticated user to view other users' encrypted passwords, which could let a malicious user obtain the firewall's configuration password. | No workaround or patch available at time of publishing. | BrowseGate Weak Encryption | Medium | Bug discussed in newsgroups and websites. Exploit script has been published. |
| NetcPlus[35]<br><br>Windows 95/98/Nt 4.0/2000 | SmartServer3 3.75 | Remote Denial of Service vulnerabilities exist in the SMTP and POP components of the e-mail server. | No workaround or patch available at time of publishing. | SmartServer3 Denial of Service | Low | Bug discussed in newsgroups and websites. |
| NetcPlus[36]<br><br>Windows 95/98/NT 4.0/2000 | SmartServer3 3.75 | A vulnerability exists which could allow an authenticated malicious user to view user's login information and gain access to passwords. | No workaround or patch available at time of publishing. | SmartServer3 Weak Encryption | Medium | Bug discussed in newsgroups and websites. Exploit script has been published. |

[30] Securiteam, November 22, 2000.
[31] Red Hat Inc. Security Advisory, RHSA-2000:110-06, November 20, 2000.
[32] Linux-Mandrake Security Update Advisory, MDKSA-2000:072, November 20, 2000.
[33] Debian Security Advisory, November 22, 2000.
[34] Bugtraq, November 18, 2000.
[35] eSecurityOnline.com Free Vulnerability Alert 3167, November 20, 2000.
[36] Securiteam, November 21, 2000.

| Vendor/ Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/Alerts | Common Name | Risk* | Attacks/Scripts |
|---|---|---|---|---|---|---|
| Netopia[37] | Netopia 650-ST ISDN Router 3.3.2 firmware | A vulnerability exists which could let a remote malicious user read system logs from the telnet prompt without logging into the system. This could lead to a compromise of sensitive information including usernames and passwords. | The PN650-ST with firmware 3.3.2 is no longer supported. Firmware version 4.3.2 for other devices addresses the vulnerability and can be found at: http://www.netopia.com | Netopia ISDN Router Username/ Password Disclosure | Medium | Bug discussed in newsgroups and websites. |
| Network Associates, Inc.[38]<br><br>Windows NT 4.0/2000 | WebShield SMTP 4.5 | Two vulnerabilities exist: the first is a Denial of Service caused by a malicious Web site giving a malformed e-mail address; and the second allows attachments with extended characters to bypass user-defined filters. These vulnerabilities do not affect the effectiveness of viral detection. | No workaround or patch available at time of publishing. | WebShield SMTP Content Filter Bypass And SMTP Invalid Outgoing Recipient Field Denial of Service | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |
| Oracle[39]<br><br>Unix | Oracle8i 8.1.5 | A buffer overflow vulnerability exists in the cmctl (Connection Control Manager) binary that could allow elevation of privileges. | Unofficial workaround (Bugtraq): Remove the setuid and setgid bits from cmctl, though this may limit some functionality for un-privileged users using cmctl. | Oracle cmctl Buffer Overflow | Medium | Bug discussed in newsgroups and websites. Exploit script has been published. |
| Phorum[40] | Phorum 3.1-3.2.7 | Several security vulnerabilities exists which could allow a remote malicious user to gain access to passwords and the source of PHP files. | Upgrade available at: http://www.phorum.org/download.php | Phorum PHP Configuration Disclosure | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |
| Phorum[41] | Phorum 3.1-3.2.8 | A vulnerability exists in the way user input is handled in administrative scripts which could let a malicious user view/read files. | No workaround or patch available at time of publishing. | Phorum Arbitrary File Read | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |
| PTlink Services[42]<br><br>Unix | PTlink IRCd 3.5.3, IRC Services 1.8.1 | Two Denial of Service vulnerabilities exist which could allow a remote malicious user to crash the server. | Upgrades available at: **PTlink IRC Services 1.8.1:** http://download.sourceforge.net/PTlinkSoft/PTlink.Services2.14.3.tar.gz **PTlink IRCd 3.5.3:** http://download.sourceforge.net/ptlinksoft/PTlink5.7.1.tar.gz | PTlink IRCD and Services Denial of Service | Low | Bug discussed in newsgroups and websites. Exploit has been published. |

[37] Bugtraq, November 16, 2000.
[38] Bugtraq, November 22, 2000.
[39] WWW.PLAZASITE.COM System & Security Division, 20001123, November 20, 2000.
[40] Securiteam, November 27, 2000.
[41] Bugtraq, November 23,2 000.
[42] Bugtraq, November 26, 2000.

| Vendor/ Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/Alerts | Common Name | Risk* | Attacks/Scripts |
|---|---|---|---|---|---|---|
| Real Networks[43] | RealServer 5.0, 6.0x, 7.0 | A memory contents disclosure vulnerability exists which could allow a remote malicious user to gain administrative rights and access to server information, authentication credentials, and data. | Upgrade available at: http://docs.real.com/docs/server_703_dos/g2_7_0update2-linux-c6.bin | RealServer Memory Contents Disclosure | **High** | Bug discussed in newsgroups and websites. Exploit has been published. |
| Software602[44]<br><br>Windows 95/98/NT 4.0/2000 | 602Pro LAN SUITE Buffer Overflow | A buffer overflow vulnerability exists in webprox.dll, which could allow a remote malicious user to cause a Denial of Service or execute arbitrary code. | Upgrade to version 2000.0.1.33 available at: http://www.software602.com/products/index.html | 602Pro LAN SUITE Buffer Overflow | **High** | Bug discussed in newsgroups and websites. |
| SonicWALL[45] | SOHO 4.0.0, 5.0.0 | A vulnerability exists which could allow a malicious user to cause a Denial of Service attack against the firewall. | No workaround or patch available at time of publishing. | SOHO Denial of Service | Low/ **High**<br><br>**(High if DDoS best practices not in place).** | Bug discussed in newsgroups and websites. |
| SuSE[46]<br><br>Unix | Linux 6.0-6.4, 7.0 | A buffer overflow vulnerability exists in in.identd, which could let a remote malicious user cause a Denial of Service. | No workaround or patch available at time of publishing. | SuSE in.identd Denial of Service | Low | Bug discussed in newsgroups and websites. |
| Texas Imperial Software[47]<br><br>Windows 95/98/3.1/NT 3.5/4.0/2000 | WFTPD 2.41RC14, 2.41RC14 Pro, 3.0Pro | A vulnerability exists in which could allow a remote malicious user to gain access to systems files, password files, etc. and lead to a complete system compromise. | Upgrade available at: http://www.wftpd.com/downloads/ | Winsock FTPd Directory Transversal | **High** | Bug discussed in newsgroups and websites. Exploit has been published. |
| TransSoft[48]<br><br>Windows 95/98/NT 4.0/2000 | Broker FTP Server 4.7.5.0 | Multiple vulnerabilities exist which could allow a remote malicious user to browse root directories and possibly retrieve account names and passwords. | Upgrade available at:<br>**NT/2000:**<br>http://www.transsoft.com/broker/updates/broker40nt.exe<br>**Windows 95/98:**<br>http://www.transsoft.com/broker/updates/broker40b.exe | Broker FTP Directory Permissions | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |

[43] CORE SDI ADVISORY, CORE-20001116, November 17, 2000.
[44] eSecurityOnline.com Free Vulnerability Alert 3178, November 27, 2000.
[45] Securiteam, November 30, 2000.
[46] Bugtraq, November 29, 2000.
[47] Bugtraq, November 27, 2000.
[48] 403-SECURITY advisory, November 21, 2000.

| Vendor/ Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/Alerts | Common Name | Risk* | Attacks/Scripts |
|---|---|---|---|---|---|---|
| Trend Micro[49]<br><br>Windows NT 4.0 | InterScan VirusWall for Windows NT 3.4 and previous | A vulnerability exists because the installation process assigns the 'Everyone' group 'Full Control' permissions in the Access Control List of the \Interscan directory and all of its contents without notifying the user, which could let a malicious user, execute arbitrary code or implant Trojans. | No workaround or patch available at time of publishing. | InterScan VirusWall Shared Directory | **High** | Bug discussed in newsgroups and websites. Exploit has been published. |
| Unify[50]<br><br>Windows 98/NT 4.0/2000, Unix | eWave ServletExec 3.0, 3.0c | A vulnerability exists that discloses the source code of JSP pages when some special characters are appended to HTTP requests, which could lead to the disclosure of sensitive information. | Workaround:<br>"If they don't have any static pages or images in their web application then they can configure a default servlet by mapping '/' to their default servlet. This will cause their default servlet to be called for any URLs, which don't map to a servlet. In this case their default servlet can just return File Not Found. If they do have static pages or images then they can still do this but they'll need to have their default servlet serve up valid static pages and images." | eWave ServletExec JSP Source Disclosure | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |
| WatchGuard[51]<br><br>Unix | Firebox II 4.1, 4.5 | A Denial of Service vulnerability exists by not freeing resources of its proxy services. | Upgrade to the latest version as it becomes available: https://www.watchguard.com/support | Firebox II Denial of Service | Low/ **High**<br><br>**(High if DDoS best practices not in place).** | 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. 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-

[49] Bugtraq, November 28, 2000.
[50] Bugtraq, November 21, 2000.
[51] Securiteam, November 19, 2000.

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 November 29, 2000 and November 18, 2000, 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, 20 scripts, programs, and net-news messages containing holes or exploits were identified.

| Date of Script (Reverse Chronological Order) | Script Name | Script Description |
|---|---|---|
| November 29, 2000 | Anger-1.33.tgz | Anger v1.33 implements a PPTP challenge/response sniffer. |
| November 29, 2000 | Bsdi_inc.c | Script which exploits the BSDI 3.0 /usr/contrib/mh/bin/inc local root vulnerability. |
| November 29, 2000 | Listsyscalls-1.0.tar.gz | Listsyscalls is a tool for listing contents of the syscall table on a running Solaris kernel. |
| November 29, 2000 | Sendip-1.2.tar.gz | SendIP is a command line tool that sends arbitrary IP packets. It has a large number of command line options to specify the content of every header of a TCP, UDP, ICMP, or raw IP packet and also allows any data to be added to the packet. |
| November 29, 2000 | Sinto.c | An interactive TTY hijacker for Linux. |
| November 29, 2000 | Wap-nmap-1.0.0.tar.gz | Wap-nmap enables an nmap scan from a WAP enabled device and sends the results back to the device. |
| November 29, 2000 | Winupw.zip | The WinU password cracker v0.7b decrypts WinU's stored passwords from the registry. |
| November 28, 2000 | Sbo_ehtereal.c | Script which exploits the Ethereal AFS Buffer Overflow vulnerabilities. |
| November 26, 2000 | Slocate-exp.c | Script which exploits the Secure Locate Heap Corruption vulnerability. |
| November 25, 2000 | Xrcvtty.c | Script which exploits the BSDI rcvtty Arbitrary Command Execution vulnerability. |
| November 24, 2000 | Iplog-2.2.2.tar.gz | A TCP/IP traffic logger capable of logging TCP port scans, TCP null scans, FIN scans, UDP and ICMP "smurf" attacks, bogus TCP flags, TCP SYN scans, TCP "Xmas" scans, ICMP ping floods, UDP scans, and IP fragment attacks. |
| November 24, 2000 | Saint-3.1.1.beta2.tar.gz | An updated version of SATAN. |
| November 22, 2000 | Asx-bufferoverrun.zip | Exploit for the .ASX Buffer Overrun and .WMS Script Execution vulnerabilities. |
| **November 22, 2000** | **Cpetrol.pl** | **Perl script which exploits the Microsys CyberPatrol Insecure Registration vulnerability.** |
| **November 21, 2000** | **Coolz.cpp** | **Script which exploits the Koules v1.4 (Svgalib version) local root vulnerability.** |
| November 21, 2000 | Ethereal-0.8.14.tar.gz | A GTK+-based network protocol analyzer, or sniffer, that lets you capture and interactively browse the contents of network frames. |
| **November 20, 2000** | **Cmctl_start.c** | **Script which exploits the Oracle cmctl Buffer Overflow vulnerability.** |
| **November 18, 2000** | **Browse.c** | **Script which exploits the NetcPlus BrowseGate Weak Encryption vulnerability.** |
| November 18, 2000 | Sbo_ethereal.c | Script which exploits the Ethereal v0.8.13 vulnerability. |
| **November 18, 2000** | **Ss3.c** | **Script which exploits the NetcPlus SmartServer3 Weak Encryption vulnerability.** |

## *Script Analysis*

When available, this section will supply a short description of scripts that have been analyzed by various security professionals and organizations. **We encourage you or your organization to contribute.** If you wish to do so, please send e-mail to nipc@fbi.gov with the subject line "CyberNotes Script Analysis." While space constraints may limit the length of descriptions included in this document, contributors are requested to include a full technical analysis of the script along with release instructions. The release categories are: releasable to anyone; limited releasability (originator-defined list of organizations); or provided for NIPC only. A member of the CyberNotes editorial team will contact you. All contributions will be credited to the contributing individual or organization unless otherwise requested.

*No scripts were submitted during the two-week period covered by this issue of CyberNotes.*

## *Trends*

**DDoS/DoS:**

**The Cert Coordination Center recently issued an alert regarding Denial of Service vulnerabilities in TCP/IP stacks. For more information, please see CERT Advisory CA-2000-21, located at: http://www.cert.org/advisories/CA-2000-21.html.**

**The CERT Coordination Center has recently issued an alert regarding of two serious Denial-of-Service vulnerabilities in the Internet Software Consortium's (ISC) BIND software. For more information, please see CERT Advisory CA-2000-20, located at: http://www.cert.org/advisories/CA-2000-20.html.**

**Probes/Scans:**

**An increase in the number of NETBIOS Session (139/tcp) probes.**

**Intruders are using scripts and toolkits to automate attacks against the input validation problem in rpc.statd and the input validation problems in FTPD, the site exec vulnerability. For more information, see the CERT advisory located at: http://www.cert.org/incident_notes/IN-2000-10.html.**

A number of sites have been compromised by exploiting a vulnerability in the IRIX telnet daemon. Intruders are actively exploiting a vulnerability in telnetd that is resulting in a remote root compromise of victim machines.

**Other:**

**The NIPC has observed that there has recently been an increase in hacker activity specifically targeting U.S. systems associated with e-commerce and other Internet-hosted sites. The majority of the intrusions have occurred on Microsoft Windows NT systems, although Unix based operating systems have been victimized as well. For more information, please see NIPC ADVISORY 00-060 located at: http://www.nipc.gov/warnings/advisories/2000/00-060.htm.**

**Users are strongly advised to avoid suspicious e-mails, particularly during this holiday season. There has been a marked increase in the number of seemingly innocuous holiday e-mails that have malicious content.**

**A continuing increase in reports of computers infected with the QAZ Trojan.**

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

## *Viruses*

**IRC-Worm/Movie.A (IRC Worm):** This is a worm, which is spread through IRC channels and distributed through a file called MOVIE.AVI. When a user whose computer has been infected connects to an IRC channel, the file is sent to everybody connected to the same channel. When one of the users connected to IRC writes the word "qwerty" in the chat channel, this malicious code will then destroy the majority of the files in the WINDOWS directory.

**PE_USSRHYMN.A (Aliases: USSRHYMN.A, W95.Ussrhymn@m) (File Infector Virus):** This direct infector Windows 9x virus infects PE files that include executable files (.EXE) and screen saver files (.SCR) in the current directory, Windows, and Windows System directories. It is also capable of infecting all files on the hard disk as well as network and RAM drives. However, this virus does not infect Dynamic Link Library (DLL) files. If the current system day is 1 and the month is January, the virus plays an old Soviet Republic hymn. The virus also drops a Trojan, TROJ_USSRHYMN.A (See Trojan Section), which resides in memory after the infected computer is re-started.

**VBS/Jean-A (Visual Basic Script Worm):** This virus sends copies of itself to each of the first 50 entries in the Microsoft Outlook addressbook. The message subject is: "News vom Weihnachtsmann." The name of the attached file may vary but is most likely to be xmas.vbs.

**W32/Bymer-A (Aliases: W32/MSINIT.WORM, WORM.RC5) (Win32 Worm):** W32/Bymer-A is a worm that propagates through open file shares. It tries IP addresses at random. If it finds a machine with a share called "C," it will infect the machine by copying files to the Windows and Windows system directories. It may change win.ini or a registry to run the worm on system startup. It will also secretly install a distributed.net program dnetc.exe in the Windows system folder, but note that could also be legitimate software that may have been installed with permission.

**W32/Music-D and W32/Music-E (Alias: W32/Music@m) (Win32 Worm):** This virus has been reported in the wild. When an infected file is executed the worm waits a few minutes before attempting to connect to several Internet websites. It attempts to download an updated version of itself from these websites. The worm then tries to send itself to e-mail addresses found on the infected PC. The e-mail message it sends varies depending on the version of itself it has downloaded from the web, but the message text will probably be similar to:

"Hi, just testing e-mail using Merry Christmas music file, you'll like it."

The worm itself is attached as a file called music.com, music.exe or music.zip. When this file is run the worm attempts to play the first few bars of the song "We wish you a Merry Christmas" and displays a cartoon of Santa Claus with the caption "Music is playing, turn on your speaker if you have one" or "There is error in your sound system, music can't be heard." When it has finished playing the music it will then display "Merry Christmas" and start playing the music again.

**W32/Navidad-B (Windows 32 Executable File Virus):** This virus has been reported in the wild. It is a variant of the W32/Navidad e-mail-aware worm. The worm arrives in an e-mail message with an attachment called EMANUEL.EXE. If the attached program is launched, it displays a dialog box containing the text ;")." It then attempts to read new e-mail messages and to send itself to the senders' addresses. The worm copies itself into the Windows system directory with the filename WINTASK.EXE and changes the registry so that it runs on Windows startup and before any file is run. The worm also installs itself into the system tray. If the user clicks on the icon, it displays a dialog box with the text "Nunca presionar este boton." If the user clicks the button, the worm displays a dialog box with the title "Emmanuel....." and the text "Emmanuel-God is with us! May god bless u. And Ash, Lk and LJ!!." If the user does not press the button but instead attempt to close the message the worm displays a message with the title "Emmanuel....." and the text "May GOd bless u;D;" (See Trojan Section for TROJ_NAVIDAD.E).

**W32/Prolin (Win 32 Worm):** This is a worm which uses Microsoft Outlook to spread. The worm arrives in an e-mail message with the subject "A great Shockwave flash movie." The body of the message contains the text "Check out this new flash movie that I downloaded just now...It's Great, Bye." The attached

filename is CREATIVE.EXE. If the attached file is run, the worm copies itself into C:\CREATIVE.EXE and C:\Windows\Start Menu\Programs\Startup\CREATIVE.EXE and sends itself as an attachment to all contacts from your Outlook address book. It also sends an e-mail with the subject "Job complete" and the text "Got yet another idiot." to an address on the Yahoo.com. The worm then looks for any files with the extension MP3, JPG and ZIP and moves them into the C:\ directory. The moved files remain unchanged but the worm renames them so that the extension is concatenated with the string "change at least now to Linux," (e.g. from "Flowers.jpg" to "Flowers.jpg change at least now to Linux"). In order to restore the files they should be moved back to their default location and renamed so that the concatenated string is removed from the filename. The worm also creates a text file C:\Messageforu.txt that can help to restore the files and a list of previous locations of all renamed files that were moved to C:\.

**W32/Verona-B (Win32 Worm):** This virus has been reported in the wild. It is a variant of W32/Verona. It uses one of 18 SMTP servers to propagate. The subject line may be blank, or made from random lower case letters arranged into 3 or less words, or chosen from the following:

Romeo&Juliet
where is my Juliet ?
where is my Romeo ?
hi
last wish ???
lol :)
,,...
!!!
newborn
merry christmas!
suprise !
Caution: NEW VIRUS !
scandal !
^_^

It copies itself to C:\WINDOWS\SYSRNJ.EXE and creates a new filetype, RNJFILE, in the registry. It then registers the filetypes EXE, JPG, JPEG, JPE, BMP, GIF, AVI, MPG, MPEG, WMF, WMA, WMV, MP3, MP2, VQF, DOC, XLS, ZIP, RAR, LHA, ARJ AND REG, so that explorer will run the virus rather than appropriate program.

***This virus relies on a security vulnerability in Microsoft Outlook and Outlook Express to work. Microsoft has released a patch that eliminates the vulnerability. For further information and to download a patch please read Microsoft Security Bulletin (MS00-046).***

**W97M/Footer.A (Word 97 Macro Virus):** This is a macro virus that infects Microsoft Word 97 documents and the NORMAL.DOT global template the application uses. It also disables the antivirus protection assigned by Word to the macros defined in the documents. W97M/Footer.A does not carry out any destructive action, although it does overwrite the footer in the infected documents.

**WM97/Afeto-A (Word Macro Worm):** This is a Word macro worm that works in Word 2000 only. The worm spreads via Outlook and sends itself to all but one of the addresses in the Sent box. The file that the worm sends is named after the first entry in the Sent box. The subject and the message body are also taken from items in the Sent box. When the worm is executed within Word, it searches for a .jpg file of 50 KB or less on the C: drive. This .jpg is then embedded in the document before e-mailing takes place.

**WM97/Bobo-H (Word 97 Macro Virus):** This virus is similar to the WM97/Bobo-C Word macro virus. It searches the active document removing any spaces from the text.

**WM97/Ethan-DJ (Word 97 Macro Virus):** This is a variant of the WM97/Ethan Word macro virus. Whenever a document is closed there is a 1 in 3 chance of a File¦Properties¦Summary box appearing on the screen with the title Ethan Frome.

**WM97/Ethan-DO (Word 97 Macro Virus):** This is a variant of WM97/Ethan. Whenever a document is closed there is a 1 in 3 chance of a File¦Properties¦Summary box appearing on the screen with the title Ethan Frome. The method of infection is such that the virus can mix with other viruses to produce a double infection.

**WM97/Metys-F (Word 97 Macro Virus):** This virus has been reported in the wild. It is a minor variant of the WM97/Metys-D Word macro virus. This variant of the virus spreads but does not have a working payload.

**WM97/Metys-J (Word 97 Macro Virus):** This virus is a minor variant of the WM97/Metys-D Word macro virus. This variant of the virus spreads but does not have a working payload.

**WM97/Newhope-F (Word 97 Macro Virus):** This is a self-replicating Word macro virus that infects Microsoft Word Documents.

**WM97/Thus-AD (Word 97 Macro Virus):** This virus is a variant of the WM97/Thus-A Word macro virus.

**X97M.Codemas.B (Excel 97 Macro Virus):** This virus has been reported in the wild. It does not disable macro virus protection inside Excel. Consequently, if macro virus protection is enabled when an infected document is opened, a Microsoft warning dialog box is displayed. The name of the module containing the virus is always 'ThisWorkbook.' To check whether a spreadsheet has been previously infected, the virus looks for the comment 'bum04' at the top of the 'ThisWorkbook' module. If the comment is present, it does not attempt to infect the spreadsheet.

**XM97/Barisada-K (Excel 97 Macro Virus):** This virus is a variant of the XM97/Barisada-A Excel macro Virus which does not have any payload and only replicates.

## *Trojans*

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. The increasing number of Trojans gains added significance due to recent testing conducted to determine the ability of anti-virus software to detect Trojans. According to the test results, a number of popular anti-virus products failed to detect or had limited detection capabilities against current popular Trojans. Testing also indicates that detection of a baseline Trojan does not necessarily mean the anti-virus software can detect a variant. Readers should contact their anti-virus vendors to obtain specific information on Trojans and their variants that their software detects.

The following table provides the reader with a list of Trojans that have received write-ups in CyberNotes. This table includes Trojans discussed in the last six months and will be updated 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. NOTE: At times, Trojans may contain names or content that may be considered offensive.

| Trojan | Version | Issue discussed |
|---|---|---|
| Asylum + Mini | v0.1, 0.1.1, 0.1.2, 0.1.3 + 1.0, 1.1 | CyberNotes 2000-12 |
| Backdoor/Doly.17 | | CyberNotes-2000-16 |
| BackDoor-GZ | | CyberNotes-2000-18 |
| BackDoor-HC | | CyberNotes-2000-18 |
| Backdoor-HD | | CyberNotes-2000-18 |
| BCK/Sub7.Apocalypse | | CyberNotes-2000-23 |
| BioNet | v0.84 - 0.92 +2.2.1 | CyberNotes 2000-12 |

| Trojan | Version | Issue discussed |
|---|---|---|
| Donald Dick 2 | | CyberNotes-2000-15 |
| Erap Estrada | | CyberNotes-2000-18 |
| GIP | | CyberNotes-2000-11 |
| Hooker-E | | CyberNotes-2000-19 |
| ICQ PWS | | CyberNotes-2000-11 |
| Mosaic | v2.00 | CyberNotes-2000-16 |
| Multijoke.B | | CyberNotes-2000-15 |
| Naebi | v2.12 - 2.39, v2.40 | CyberNotes 2000-12 |
| Netbus.153 | | CyberNotes 2000-16 |
| Netbus.170 | | CyberNotes 2000-16 |
| Netsphere.Final | | CyberNotes-2000-15 |
| NoDesk | | CyberNotes-2000-14 |
| Omega | | CyberNotes 2000-12 |
| Palm/Liberty-A | | CyberNotes-2000-18 |
| PALM_VAPOR.A | | CyberNotes-2000-19 |
| PE_MTX.A | | CyberNotes-2000-18 |
| Prosiak | beta - 0.65 – 0.70 b5 | CyberNotes 2000-12 |
| Qaz.A | W32.HLLW.Qaz.A | CyberNotes-2000-20, CyberNotes-2000-16 |
| QDel121 | | CyberNotes-2000-23 |
| Revenger | 1.0-1.5 | CyberNotes 2000-12 |
| Serbian Badman | | CyberNotes 2000-12 |
| Snid | 1-2 | CyberNotes 2000-12 |
| SubSeven | DEFCON8 2.1 Backdoor | CyberNotes-2000-21 |
| Troj/Simpsons | | CyberNotes-2000-13 |
| TROJ_BATMAN | | CyberNotes-2000-20 |
| **TROJ_BLEBLA.A** | | **Current Issue** |
| **TROJ_BLEBLA.B** | | **Current Issue** |
| TROJ_BLOODLUST | | CyberNotes-2000-21 |
| TROJ_BUTANO.KILL | | CyberNotes-2000-19 |
| Troj_Dilber | | CyberNotes-2000-14 |
| **TROJ_ENERGY.A** | | **Current Issue** |
| TROJ_FELIZ | | CyberNotes-2000-22 |
| **TROJ_ICECUBES.A** | | **Current Issue** |
| TROJ_IGMNUKE | | CyberNotes-2000-20 |
| TROJ_KILLME | | CyberNotes-2000-20 |
| TROJ_MSINIT.A | | CyberNotes-2000-21 |
| **TROJ_MUSIC.A** | | **Current Issue** |
| TROJ_MYPICS.F | | CyberNotes-2000-23 |
| TROJ_NAVIDAD.A | | CyberNotes-2000-23 |
| **TROJ_NAVIDAD.E** | | **Current Issue** |
| **TROJ_ORION** | | **Current Issue** |
| TROJ_PERSONAL_ID | | CyberNotes 2000-16 |
| TROJ_POKEY.A | | CyberNotes 2000-16 |
| TROJ_ROCKET | | CyberNotes-2000-22 |
| TROJ_SCOOTER | | CyberNotes-2000-19 |
| **TROJ_SHOCKWAVE.A** | | **Current Issue** |
| TROJ_SONIC | | CyberNotes-2000-22 |
| TROJ_SPAWNMAIL.A | | CyberNotes-2000-18 |
| TROJ_SUB7.214DC8 | | CyberNotes-2000-21 |

| Trojan | Version | Issue discussed |
|---|---|---|
| TROJ_SUB7.382883 | | CyberNotes-2000-21 |
| **TROJ_USSRHYMN.A** | | **Current Issue** |
| TROJ_VBSWG | | CyberNotes-2000-16 |
| Trojan/Anything | | CyberNotes-2000-23 |
| Trojan/ICQ | | CyberNotes-2000-20 |
| Trojan/Parkinson | | CyberNotes-2000-21 |
| Trojan/PSW.StealthD | | CyberNotes-2000-19 |
| **Trojan/Ring0.B** | | **Current Issue** |
| **Trojan/Twinshoe** | | **Current Issue** |
| Trojan/Varo31 | | CyberNotes-2000-19 |
| Trojan/Win32 | | CyberNotes-2000-21 |
| VBS_MAILPEEP | | CyberNotes-2000-22 |
| W32.Nuker.C | | CyberNotes-2000-14 |
| Win.Unabomber | | CyberNotes-2000-14 |
| WinCrash | Beta | CyberNotes-2000-12 |
| Winkiller | | CyberNotes 2000-12 |

**TROJ_BLEBLA.A (Alias: BLEBLA.A):** This Trojan horse propagates by sending a copy of itself to all addresses included in the user address book. It comes in an HTML-type e-mail and executes as soon as it is opened. It drops a file named MYJULIET.CHM (detected as CHM_BLEBLA.A) in the Windows TEMP directory. This file initiates the propagation of the Trojan to other users.

**TROJ_BLEBLA.B (Alias: BLEBLA.B):** This is a destructive Windows Trojan that propagates by sending copies of itself to all addresses found in the infected users' Microsoft Outlook address book. This Trojan will arrive as an attachment in an HTML e-mail, and executes as soon as it is opened. Using Outlook Express, the Trojan will automatically execute in Preview Mode.

**TROJ_ENERGY.A (Aliases: ENERGY WORM, ENERGY.A):** This Trojan worm spreads via e-mail as an attachment. Unlike other worms, it spreads via a RAR compressed file. It monitors MAPI e-mails for messages with a RAR file attachment and inserts itself on that compressed RAR file.

**TROJ_ICECUBES.A (Aliases: W32.Icecubes.Worm, ICECUBES.A):** This Windows Trojan propagates by monitoring all outgoing e-mail messages and then sending another e-mail to the same address with itself as an attachment. The attached filename is "ICECUBES.EXE" and the subject of the e-mail is "Windows Icecubes!"

**TROJ_MUSIC.A:** This is a network-enabled Trojan that is disguised as a simple program that displays graphics and plays a tune. The graphic is that of Santa Claus and the tune played is the Christmas carol "We Wish You a Merry Christmas." Upon execution, it modifies the Windows registry and drops files to propagate via e-mail. A sample of the e-mail is as follows:

Subject: Testing to send file
Message Body: Hi, just testing e-mail using Merry Christmas music file, not bad music.
Or
Hi, just testing e-mail using Merry Christmas music file, you'll like it.
Attachment: MUSIC.COM or MUSIC.EXE or MUSIC.ZIP Although the samples received so far are non-destructive, this Trojan has the capability to download upgrades from the Internet, which may be more malicious.

**TROJ_NAVIDAD.E (Aliases: NAVIDAD.E, NAVIDAD.B, EMMANUEL, TROJ_EMMANUEL):** This malicious Internet worm propagates via e-mail. It uses Microsoft Messaging API to send a copy of itself as an e-mail attachment to all lists in the address book of the infected user. A variant of TROJ_NAVIDAD.A, this Trojan differs in the icon used, the messages used and the file that it spreads. Upon execution, it displays an errors message box and prevents users from execution EXE programs.

**TROJ_ORION (Aliases: BackDoor-IF.svr, ORION, Backdoor.Dynod, Backdoor.Trojan):** This Trojan is disguised as a serial generator for FRUITYLOOPSPRO. Upon execution, it drops a copy of itself in the Windows System directory. This dropped file is a server program that allows a remote user running the client program to access the infected computer.

**Trojan/Ring0.B:** This is a Trojan that uses two files in order to get into other IT systems remotely. One of them is 5682 bytes in size and is called RING0.VXD. The second file has different names -amongst which are WINDLL32.EXE and MSRUNSRV.EXE- and it occupies a little more than 47Kb. In order not to arouse suspicion amongst users, both files seem to be related to common applications. Furthermore, once these files have been installed, Trojan/Ring0.B enters a key in the Windows Registry.

**TROJ_SHOCKWAVE.A (Aliases: CREATIVE, TROJ_PROLIN.A):** This Windows Trojan propagates via Microsoft Outlook. Upon execution, this Trojan sends itself twice as an attachment to every address listed in the address book of the infected user. The subject of this e-mail is " A great Shockwave flash movie" and the attachment is "CREATIVE.EXE." After this, the Trojan sends an e-mail to a Yahoo e-mail address, which maybe the author of the virus. This Trojan also changes the filenames of all JPG and ZIP files and then moves the files to the C:\ root directory.

**Trojan/Twinshoe:** This Trojan gets into the system it wants to infect through a file that occupies 481699 bytes. As with most Trojans, Trojan/Twinshoe copies itself to the WINDOWS directory, giving this file a different name every time which makes it difficult to detect. This malicious code changes various Registry keys and system files.

**TROJ_USSRHYMN.A (Aliases: USSRHYMN.A, W95.Ussrhymn@m):** This is the Trojan part of the PE virus, PE_USSRHYMN.A. The Trojan programs resides in memory and checks whether a debugger is present. If a debugger is found, the Trojan restarts the computer. If the current system date is January 1, an old Soviet Republic hymn is played. This Trojan may cause system instability on computers that have debuggers installed, such as SoftIce. It is also reported that it alters some antivirus programs.