National Infrastructure Protection Center CyberNotes

Issue #2000-22 *November 6, 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 2, 2000 and October 21, 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
Allaire[1] Windows 95/98/NT 4.0/2000, Unix	JRun 2.3.x	A vulnerability exists when a malformed URI is sent to the server, which could allow browser access to non-webroot resources.	Patch available at: **Windows 95/98/NT/2000 and Windows NT Alpha:** http://download.allaire.com/jrun/jr233p_ASB00_28_29.zip **Unix/Linux:** http://download.allaire.com/jrun/jr233p_ASB00_28_29.tar.gz **Note:** The patch for ASB00-28 and ASB00-29 is identical. If you have already installed the patch for one, you do not need to install it for the other.	JRun File Source Code Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[1] Allaire Security Bulletin, ASB00-28, October 24, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Allaire[2] Windows 95/98/NT 4.0/2000, Unix	JRun 2.3.x	A vulnerability exists which could allow a malicious user to compile and execute JSP code from an arbitrary file on the webserver's filesystem.	Patch available at: **Windows 95/98/NT/2000 and Windows NT Alpha:** http://download.allaire.com/jrun/jr233p_ASB00_28_29.zip **Unix/Linux:** http://download.allaire.com/jrun/jr233p_ASB00_28_29.tar.gz **Note:** The patch for ASB00-28 and ASB00-29 is identical. If you have already installed the patch for one, you do not need to install it for the other.	JRun Arbitrary Code Execution	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Allaire[3] Windows 95/98/NT 4.0/2000, Unix	JRun 3.0	A vulnerability exists which could allow a remote malicious user to view the contents of the WEB-INF directory.	Patch available at: **Windows 95/98/NT/2000 and Windows NT Alpha:** http://download.allaire.com/jrun/jrun3.0/extraslashes.ZIP **Unix/Linux:** http://download.allaire.com/jrun/jrun3.0/extraslashes.tar.gz	JRun Directory Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Avirt[4] Windows 95/98/NT 4.0/2000	Avirt Mail 4.0, 4.2	A Denial of Service vulnerability exists when connecting to port 25 and supplying an unusually long 'From' or 'Recipient' address.	No workaround or patch available at time of publishing.	Avirt Mail 'Mail From:' and 'Rcpt to:' Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Bardon Data Systems[5] **Windows 95/98/NT 4.0/2000** ***Upgrade available[6]***	**WinU 5.1 and previous**	**A built-in emergency password is contained in this tool; however, a number of the passwords are publicly available which could let a malicious user to gain full administrative privileges.**	***Upgrade to WinU 5.2 available at:*** http://www.bardon.com/winudl.htm	**WinU Backdoor Password**	**High**	**Bug discussed in newsgroups and websites. Exploit has been published.**
Carnegie Mellon University[7] Unix	Carnegie Mellon University Cyrus-SASL 1.5.24 with RedHat 7.0	A vulnerability exists in Cyrus-SASL (Simple Authentication and Security Layer) that could allow a malicious user to elevate their privileges.	Upgrade available at: Red Hat Linux 7.0: i386: ftp://updates.redhat.com/7.0/i386/cyrus-sasl-1.5.24-11.i386.rpm sources: ftp://updates.redhat.com/7.0/SRPMS/cyrus-sasl-1.5.24-11.src.rpm	RedHat Cyrus-SASL Authorization	Medium	Bug discussed in newsgroups and websites.
CatSoft[8] Windows 95/98/NT 4.0/2000	Serv-U 2.5x	A security vulnerability exists which could allow a remote malicious user to brute force usernames and passwords.	No workaround or patch available at time of publishing.	Serv-U Bruteforce	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.

[2] Allaire Security Bulletin, ASB00-29, October 23, 2000.
[3] Allaire Security Bulletin, ASB00-27, October 23, 2000.
[4] Bugtraq, October 24, 2000.
[5] Securiteam, October 16, 2000.
[6] SecurityFocus, October 27, 2000.
[7] Red Hat, Inc. Security Advisory, RHSA-2000:094-01, October 26, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
CGI Script Center[9]	News Update 1.1	A vulnerability exists in the password changing implementation, which could let a remote malicious user gain administrative access to the system.	No workaround or patch available at time of publishing.	News Update Password Changing	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Cisco[10]	Cisco Catalyst 3500 XL	A vulnerability exists in the configuration interface with the webserver, which could let an anonymous malicious user execute arbitrary commands. This could lead to a complete compromise of the host.	Unofficial workaround (Defcom Labs): Disable the web configuration interface completely.	Cisco Catalyst Remote Arbitrary Command Execution	**High**	Bug discussed in newsgroups and websites.
Cisco[11]	Cisco IOS versions 12.0-12.1	A Denial of Service vulnerability exists that will cause a Cisco router or switch to halt and reload if the IOS HTTP service is enabled.	Upgrade available at: http://www.cisco.com/	Cisco IOS "?/" HTTP Request Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Cisco[12]	Cisco IOS 12.1(4)	A vulnerability exists in the way access control lists are enforced, which could allow a malicious user to access vulnerable network services thought to be protected by the access control lists.	No workaround or patch available at time of publishing.	Cisco IOS Extended Access List Failure	Medium	Bug discussed in newsgroups and websites.
Cisco[13]	Virtual Central Office 4000 (VCO/4K) 5.1.3 and earlier	A vulnerability exists which could let remote malicious users obtain login and password credentials and gain access with administrator privileges.	Upgrade to software version 5.1.4. available at: www.cisco.com	Cisco CVCO/4k Remote Username and Password Retrieval	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Element N.V[14] Windows NT 4.0	Element InstantShop 1.0	An input validation vulnerability exists in the hidden field portion of the order form, which could let a malicious user modify unit item prices with arbitrary values.	The vendor has been informed, but until an official patch is released, it is recommend using non-real-time transactions (i.e. manual authorization).	Element InstantShop Price Modification	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[8] eSecurityOnline.com, Vulnerability Alert 3092, November 2, 2000.
[9] Securiteam, October 30, 2000.
[10] Defcom Labs Advisory, def-2000-02, October 26, 2000.
[11] Cisco Security Advisory, CI-00.09, October 25, 2000.
[12] Bugtraq, October 22, 2000.
[13] @stake, Inc. Security Advisory, A102600-1, October 26, 2000.
[14] Securiteam, October 25, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
FreeBSD[15] Unix	FreeBSD 3.5x, 4.0, 4.0 alpha, 4.1, 4.1.1, 4.1.1-STABLE, RELEASE	A format string vulnerability exists which could let a malicious user corrupt stack variables and execute arbitrary code.	Patch available at: ftp://ftp.freebsd.org/pub/FreeBSD/CERT/patches/SA-00:62/top.patch	FreeBSD top Format String	**High**	Bug discussed in newsgroups and websites.
FreeBSD[16] Unix	FreeBSD 4.0, 4.0 alpha, 4.1, 4.1.1, 4.1.1-RELEASE	A vulnerability exists in the implementation function, which could lead to a remote Denial of Service.	Patch available at: ftp://ftp.freebsd.org/pub/FreeBSD/CERT/patches/SA-00:63/getnameinfo.patch	FreeBSD getnameinfo() Denial of Service	Low	Bug discussed in newsgroups and websites.
FreeBSD[17] Unix	FreeBSD 2.2.8, 3.3, 4.0, 4.1	A vulnerability exists in the cron command-scheduling package, which could allow malicious users to read certain system files without attaining root or file ownership privileges.	No workaround or patch available at time of publishing.	FreeBSD Crontab/tmp File	Medium	Bug discussed in newsgroups and websites.
Hewlett-Packard[18] Unix	VirtualVault 3.50, 4.0	A Denial of Service vulnerability exists in Netscape Server Application Programming Interface (NSAPI) plugin.	Apply the appropriate patch: HP-UX release 10.24: PHSS_22187 HP-UX release 11.04: PHSS_22296	VirtualVault Denial of Service	Low	Bug discussed in newsgroups and websites.
Hewlett-Packard[19] Unix	HP-UX 10.20, 11.00	A vulnerabiltiy exists in the way temporary files are handled in crontab that could allow a local malicious user to read portions of any file on a system.	Workaround: Disable crontab access for any unauthorized user.	HP-UX Crontab/tmp File	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Inktomi Search Software[20] Windows NT4.0, Unix	Inktomi Search Software 3.x	A vulnerability exists when connecting to the search engine that could let a malicious user pass a malformed URL to the engine, which will cause the process to stop responding to valid requests.	Upgrade to 4.0 available at: HP-UX platform: ftp://ftp.ultraseek.com/pub/InktomiSearch/4.0.0/InktomiSearch-hpux-4.0.0.tar.gz Linux platform: ftp://ftp.ultraseek.com/pub/InktomiSearch/4.0.0/InktomiSearch-linux-4.0.0.tar.gz Windows NT platform: ftp://ftp.ultraseek.com/pub/InktomiSearch/4.0.0/InktomiSearch-winnt-4.0.0.exe Sun Solaris: ftp://ftp.ultraseek.com/pub/InktomiSearch/4.0.0/InktomiSearch-solaris-4.0.0.tar.Z	Inktomi Search Software Denial of Service	Low	Bug discussed in newsgroups and websites.

[15] FreeBSD Security Advisory, FreeBSD-SA-00:62, November 1, 2000.
[16] FreeBSD Security Advisory, FreeBSD-SA-00:63, November 2, 2000.
[17] Bugtraq, October 21, 2000.
[18] SecurityFocus, October 27, 2000.
[19] eSecurityOnline.com Vulnerability Alert 3071, October 24, 2000.
[20] USSR Advisory Code, USSR-2000056, October 30, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Intel Corporation[21]	InBusiness eMail Station 1.4.87	A buffer overflow vulnerability exists which could allow a remote malicious user cause a Denial of Service and possibly execute arbitrary code.	No workaround or patch available at time of publishing.	Intel InBusiness eMail Station Denial of Service	Low/ **High**	Bug discussed in newsgroups and websites. Exploit has been published. Vulnerability has appeared in the Press and other public media.
Kootenay Web Inc.[22] Unix	whois 1.0	A vulnerability exists because user-supplied input isn't properly checked, which could let a remote malicious user execute arbitrary commands and gain root access.	No workaround or patch available at time of publishing.	Whois Remote Command Execution	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Lawrence Berkeley Laboratory[23] Unix	tcpdump 3.4, 3.5, 3.5 alpha	Several buffer overflow vulnerabilities exist which could let a malicious user gain root access.	Patch available at: ftp://ftp.freebsd.org/pub/FreeBSD/CERT/patches/SA-00:61/tcpdump-3.x.patch	tcpdump Packet Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Microsoft[24] Windows NT 2000	Indexing Services for Windows 2000	A security vulnerability exists which could let a malicious web site operator misuse another web site as a means of attacking users.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq00-084.asp	Microsoft Indexing Services Cross Site Scripting	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[25] Windows NT 2000	Microsoft Windows NT 2000	A security vulnerability exists which could let a malicious user potentially run code on another user's machine.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq00-085.asp	Microsoft ActiveX Parameter Validation	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[21] Securiteam, October 21, 2000.
[22] Bugtraq, October 29, 2000.
[23] FreeBSD Security Advisory, FreeBSD-SA-00:61, October 30, 2000.
[24] Microsoft Security Bulletin, MS00-084, November 2, 2000.
[25] Microsoft Security Bulletin, MS00-085, November 2, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft[26] **Windows 95/98/ NT 4.0/2000** ***New variant of vulnerability and new patch[27].***	**Internet Information Server (IIS) 4.0, 5.0; FrontPage 2000 Server Extensions 1.2**	**A vulnerability exists when FrontPage Extensions 1.2 is installed on an IIS, which may return content specified by a malicious third party back to a client through the use of specially formed links. This becomes an issue especially if the server specified in the hostile URL is a trusted site, as content from that site may then be granted a higher privilege level than usual.** ***An additional variant of this vulnerability has been identified.***	***Updated patch available at:*** ***Internet Information Server 4.0:*** http://www.microsoft.com/Downloads/Release.asp?ReleaseID=25534 ***Internet Information Server 5.0:*** http://www.microsoft.com/Downloads/Release.asp?ReleaseID=25533	**FrontPage/IIS Cross-Site Scripting**	**Medium**	**Bug discussed in newsgroups and websites. Exploit has been published.**
Microsoft[28] Windows NT 4.0/2000	Internet Information Server 4.0, 5.0	A security vulnerability exists which could allow a malicious user to "hijack" another user's secure web session, under a very restricted set of circumstances.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq00-080.asp	Microsoft IIS Session ID Cookie Marking	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[29] **Windows 95/98/NT 4.0/2000** ***Patch now available[30]***	**Microsoft Outlook Express 4.0, 5.0, 5.01, 5.5; Outlook 97, 98, 2000; Internet Explorer 4.0.1, 4.1, 5.0, 5.01, 5.5**	**A security vulnerability exists which could allow a malicious user to read local files, arbitrary URLs, and local directory structure after viewing a web page or reading a HTML message.** ***A new variant of the vulnerability exists that originally was discussed in Microsoft Security Bulletin MS00-011.***	***Frequently asked questions regarding this vulnerability and the patch can be found at:*** ***http://www.microsoft.com/technet/security/bulletin/fq00-081.asp***	***Microsoft VM File Reading***	**Medium**	**Bug discussed in newsgroups and websites. Exploit script has been published.**
Microsoft[31] Windows NT 4.0	Windows NT 4.0	A vulnerability exists due to weak default permissions on a registry key that handles the Microsoft Installer Service (MSIEXEC), which could allow a malicious user to elevate his/her privileges.	Unofficial workaround (Bugtraq): Verify that only Administrators are able to set registry key values under HKLM\Software\Clsid.	Microsoft Windows NT 4.0 MSIEXEC Registry Permissions	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[26] Microsoft Security Bulletin, MS00-060, August 25, 2000.
[27] Microsoft Security Bulletin, MS00-060, Re-release, November 2, 2000.
[28] Microsoft Security Bulletin, MS00-080, October 23, 2000.
[29] Georgi Guninski Security Advisory #24, October 18, 2000.
[30] Microsoft Security Bulletin, MS00-081, October 25, 2000.
[31] Bugtraq, October 23, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft[32] Windows NT 4.0	Microsoft Exchange Server 5.5	A security vulnerability exists which could let a malicious user cause an Exchange server to fail.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq00-082.asp	Malformed MIME Header	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[33] Windows NT 4.0	Windows NT 3.5. 3.5.1, 4.0, 2000, Terminal Server; Microsoft Systems Management Server 1.2, 2.0	Multiple buffer overflow vulnerabilities exist which could let a remote malicious user execute arbitrary code or deny administrators the ability to view capture files.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq00-083.asp	Microsoft Netmon Protocol Parsing CVE name CAN-2000-0885	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Multiple Vendors[34] Windows NT 4.0	Sun - Netscape Alliance iPlanet Certificate, Management System 4.2 for Windows NT 4.0, Netscape Directory Server 4.12	Two vulnerabilities exist: due to the storage of the administrative password in plaintext, a malicious user could gain administrative control over the application; and a directory traversal vulnerability which could let a malicious user gain access to known files outside of the web root.	Patches for both iPlanet Certificate Management System and Netscape Directory Server can be found at: http://www.iplanet.com/downloads/patches/index.html	iPlanet CMS/Netscape Directory Server Plaintext Administrative Password And Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploits have been published.
Multiple Vendors[35] Unix	Max-Wilhelm Bruker bftpd 1.0.11	A buffer overflow vulnerability exists when entering the USER command that could cause a Denial of Service.	Upgrade available at: http://c.codercity.de/bruksoft/bftpd/src/bftpd-1.0.12.tar.gz	bftpd Buffer Overflow	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Multiple Vendors[36] Unix	Luca Deri ntop 1.1pre3, 1.2a10, 1.2a7-9, 1.3.1, 1.3.2	A format string vulnerability exists which could let local malicious users execute arbitrary code.	Unofficial workaround (eSecurityOnline.com): Remove the setuid/setgid flags from the program with the following command: *chmod -s ntop*	Multiple Vendor Ntop -i Local Format String	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
NetBSD[37] Unix	Shigio Yamaguchi Global 3.55	A vulnerability exists in the CGI interface, which could allow a remote malicious user to execute arbitrary commands.	Upgrade available at: ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/devel/global/README.html	NetBSD Global Port Package CGI	**High**	Bug discussed in newsgroups and websites.

[32] Microsoft Security Bulletin, MS00-082, October 31, 2000.
[33] Microsoft Security Bulletin, MS00-083, November 1, 2000.
[34] CORE SDI ADVISORY, CORE-2000-10-26, October 26, 2000.
[35] Bugtraq, October 27, 2000.
[36] eSecurityOnline.com, Vulnerability Alert 3079, October 27, 2000.
[37] NetBSD Security Advisory, 2000-014, October 26, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Netscape[38] Windows NT 4.0	Netscape Certificate Management System 4.2; Netscape Directory Server 4.12	A heap buffer overflow vulnerability exists which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing	Netscape Servers Suite Heap Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Netscape[39] Windows NT 4.0	Netscape Certificate Server 4.2; Netscape Directory Server 4.12	A vulnerability exists in several components, which could allow a malicious user to conduct a Denial of Service.	No workaround or patch available at time of publishing	Netscape Servers Suite Denial of Service	Low	Bug discussed in newsgroups and websites.
Oracle[40]	Oracle Listener 7.3.4, 8.0.6, 8.1.6	An input validation vulnerability exists that could let unauthorized clients connect to and send certain commands to the listener, which could lead to a compromise of root privileges on the host.	Upgrade available at: http://metalink.oracle.com	Oracle Listener Input Validation CVE name CAN-2000-0818	**High**	Bug discussed in newsgroups and websites.
Oracle[41] Unix	Oracle Oracle8i 8.1.6; Oracle Internet Directory 2.0.6	A buffer overflow vulnerability exists which could let local malicious users elevate their privileges and access sensitive information such as credit card numbers, e-mail address, etc.	Upgrade available at: **Oracle Internet Directory 2.0.6:** http://technet.oracle.com/software/products/oracle8i/software_index.htm **Oracle Oracle8i 8.1.6:** http://technet.oracle.com/software/products/oracle8i/software_index.htm	Oracle Internet Directory Oidldap	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Padl Software[42] Unix	nss_ldap Build 105, 113, 85	A Denial of Service vulnerability exists when nss_ldap is in use with nscd (name service caching daemon).	Upgrade available at: ftp://updates.redhat.com/	nss_ldap Local Denial of Service	Low	Bug discussed in newsgroups and websites.
RedHat[43] Unix	Dump 0.4b15-1	A vulnerability exists in the dump package that allows suid root execution of other executables. Successful exploitation of this vulnerability results in root compromise.	Upgrade available at: http://www.securityfocus.com/external/ftp://updates.redhat.com/	RedHat dump Insecure Environment Variables	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
RedHat[44] Unix	RedHat Linux 6.2 sparc, i386, alpha BSD lpr 0.54-4	A vulnerability exists in the lpr package that could allow a malicious user to execute arbitrary commands with the privileges of group 'lp'.	Unofficial workaround (Bugtraq): Disable lpr.	RedHat Lpr Arbitrary Command Execution	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[38] CORE SDI Security Advisory, CORE-2000103101, October 31, 2000.
[39] CORE SDI Security Advisory, CORE-2000103102, October 31, 2000.
[40] Internet Security Systems Security Advisory, October 25, 2000.
[41] Securiteam, October 19, 2000.
[42] Red Hat, Inc. Security Advisory, RHSA-2000:024-02, October 27, 2000.
[43] Red Hat, Inc. Security Advisory, RHSA-2000:100-02, November 2, 2000.
[44] Bugtraq, October 20, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Samba[45] Unix	Samba 2.0.7	A vulnerability exists which could let a malicious user bruteforce the username and password and leverage root access.	No workaround or patch available at time of publishing.	SAMBA SWAT Logging Failure and Symlink	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
SourceForge[46] Unix	Pam_mysql 0.1-0.4	An authentication input vulnerability exists that could lead to local and remote compromise.	Upgrade to version 0.4.7 available at: http://download.sourceforge.net/pam-mysql/pam_mysql-0.4.7.tar.g	Pam_mysql Authentication Input Validation	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Sun Microsystems, Inc.[47] Windows 95/98/NT 4.0/2000, Unix	Netscape Communi-cator 4.75; Microsoft Internet Explorer 5.0.1 for Windows 98, NT 4.0	A potential compromise of two specific security certificates exists that could let a malicious user run code signed by the compromised certificates. Any such code would appear to be from Sun Microsystems, thus creating a misleading sense of trust. These certificates had limited distribution and have the following serial numbers: Internet Explorer: 3181 B12D C422 5DAC A340 CF86 2710 ABE6; and Netscape: 1705 FB13 A22F 9AF3 C130 F562 6E12 504C.	Sun has issued instructions available at: http://sunsolve.sun.com/securitypatch	Sun Compromised Browser Certificates	**High**	Bug discussed in newsgroups and websites.
Sun Microsystems, Inc.[48] Windows 98/NT 4.0, MacOS 8.0, Unix	HotJava Browser 3.0	A security vulnerability exists which could allow a malicious user to access the DOM of arbitrary URLs. Among other things, this allows stealing cookies from other visited websites.	Unofficial workaround (Georgi Guninski): Disable JavaScript "Sun's current plan is that the HotJava Browser may not be included in a future Solaris release. However, this plan is subject to change at Sun's sole discretion."	Sun HotJava Browser Arbitrary DOM Access	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Sun-Netscape Alliance[49] Windows NT 4.0, Unix	iPlanet Web Server 4.x	A buffer overflow vulnerability exists which could lead to a Denial of Service or execution or arbitrary code.	Temporary Workaround (Securiteam): Disable server side parsing of HTML pages.	iPlanet Webserver .shtml Buffer Overflow	Low/ **High**	Bug discussed in newsgroups and websites.

[45] Bugtraq, October 30, 2000.
[46] Secure Reality Pty Ltd. Security Advisory #4, October 27, 2000.
[47] Sun Microsystems, Inc. Security Bulletin, #00198, October 24, 2000.
[48] Georgi Guninski Security Advisory #25, October 25, 2000.
[49] Securiteam, October 30, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Symantec[50] Windows ME	Norton AntiVirus for Windows ME 2001	A vulnerability exists if a virus or Trojan is placed in the C:_RESTORE folder, because the scanning software bypasses this folder.	No workaround or patch available at time of publishing	Norton AntiVirus 2001 _Restore Directory Virus Detection Bypass	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
T.C.X DataKonsult[51]	MySQL 3.20.x, 3.21.x, 3.22.x, 3.23.x	A vulnerability exists because the authentication mechanism is not cryptographically strong which could allow a malicious user to recover the user's password. This could lead to a compromise of data integrity depending on the access of the account compromised.	The vendor is aware of the problems described and suggests encrypting the traffic between client and server to prevent exploitation. For further details refer to: http://www.mysql.com/documentation/mysql/commented/manual.php?section=Security	MySQL Authentication Algorithm	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
TIS[52]	Internet Firewall Toolkit 2.1	A format vulnerability exists in the x-gw (X Windows gateway) component, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Firewall Toolkit Format String	**High**	Bug discussed in newsgroups and websites.
Unify[53] Windows 98/NT 4.0/2000, Unix	eWave ServletExec 3.0c	A Denial of Service vulnerability exists if a URL invoking the ServletExec servlet is preceded by "/servlet."	Upgrade to ServletExec version 3.0E, available at: http://www.servletexec.com/downloads/	eWave ServletExec Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Unify[54] Windows 98/NT 4.0/2000, Unix	eWave ServletExec 3.0c	A vulnerability exists when a specially formed HTTP or 'GET' request is requested, which could let a remote malicious user, upload an arbitrary file to any directory on the server.	Upgrade to ServletExec version 3.0E, available at: http://www.servletexec.com/downloads/	Unify eWave ServletExec File Upload	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Valve Software[55] **Unix** ***Upgrade available[56]***	**Half-Life Dedicated Server 3.1 and previous**	**A buffer overflow vulnerability exists in the changelevel rcon command, which could let a remote malicious user execute arbitrary code.**	***Upgrade available at:*** http://www.fileplanet.com/index.asp?file=51283	**Half-Life Dedicated Server**	**High**	**Bug discussed in newsgroups and websites.**

[50] Bugtraq, October 22, 2000.
[51] CORE SDI Security Advisory, CORE-20001023, October 23, 2000.
[52] Geekgang Security Advisory, gsa2000-01, October 26, 2000.
[53] Foundstone, Inc. Security Advisory, FS-103000-15-SRVX, October 30, 2000.
[54] Foundstone, Inc. Security Advisory, FS-103100-16-SRVX, October 31, 2000.
[55] Bugtraq, October 16, 2000.
[56] Bugtraq, October 25, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Valve Software[57] Unix	Half-Life Dedicated Server 3.1 and previous	A format string vulnerability exists in the RCON command, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	Half-Life Format String	**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. 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 November 2, 2000 and October 23, 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, 27 scripts, programs, and net-news messages containing holes or exploits were identified.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
November 2, 2000	**Dump.sh**	**Proof of concept exploit for the RedHat Lpr Arbitrary Command Execution vulnerability.**
November 2, 2000	**Dump-0.4b15x.c**	**Script which exploits the RedHat Lpr Arbitrary Command Execution vulnerability.**
November 2, 2000	**Netftpbrute.java**	**Exploit for the CatSoft FTP Serv-U Brute-Force vulnerability.**
November 1, 2000	Saint-3.1.tar.gz	A security assessment tool based on SATAN.
October 30, 2000	**Flyswatter.c**	**Script which exploits the SAMBA SWAT Logging Failure and Symlink vulnerability.**
October 30, 2000	**Newsexp.tgz**	**Script which exploits the CGI Script Center News Update Password Changing vulnerability.**
October 30, 2000	Sscan2k-pre6.HWA.tar.gz	A remote auditing tool which scans for more than 200 remote known vulnerabilities.
October 28, 2000	Formnow-exploit.pl	Perl script that exploits the FormNow CGI script v1.0 remote insecure sendmail call vulnerability.

[57] Tamandua Sekure Labs, Sekure-2000-01, October 25, 2000.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
October 28, 2000	**Hl-advisory.asc**	**Exploit for the Linux Half-life Dedicated Server vulnerability.**
October 28, 2000	Hostexp.c	Script which exploits the host command remote buffer overflow vulnerability.
October 28, 2000	Listmail-exploit.pl	Perl script which exploits the Listmail v112 insecure open call vulnerability.
October 28, 2000	Mimedefang-0.5.tar.gz	Flexible MIME e-mail scanner designed to protect Windows clients from viruses and other harmful executables.
October 28, 2000	Newsexp.tar.gz	Remote exploit which allows changing the passwords for the CGI program without knowing the former password, allowing malicious users to modify your news-page.
October 28, 2000	Unicodexecute2.pl	Perl script to execute commands on vulnerable IIS servers w/ Unicode.
October 28, 2000	Utilmind-maillist-exploit.pl	Perl script which exploits the Mailing List & News Version 1.7 vulnerability.
October 27, 2000	Ethereal-0.8.13.tar.gz	A GTK+-based network protocol analyzer, or sniffer, that lets you capture and interactively browse the contents of network frames.
October 27, 2000	**Ntop-1.1-1-ex.c**	**Script which exploits the Ntop -i Local Format String vulnerability.**
October 27, 2000	Ntop-src-Oct-26-2000.tar.gz	Unix / Windows network sniffing tool that shows the network usage.
October 27, 2000	**Ntop-w-exp.c**	**Ntop -w v1.2a1 remote stack overflow exploit.**
October 25, 2000	**Hl-recon.c**	**Script which exploits the Half-Life Format String vulnerability.**
October 24, 2000	**Avirtdos.c**	**Script which exploits the Avirt Mail 'Mail From:' and 'Rcpt to:' Denial of Service vulnerability.**
October 24, 2000	Crontab.sh	Script which exploits the HP-UX crontab /tmp File vulnerability.
October 23, 2000	Hp-ux.crontab.sh	Local shell script exploit for the HP/UX crontab /tmp File vulnerability.
October 23, 2000	Password.c	Script which exploits the MySQL Authentication Algorithm vulnerability.
October 23, 2000	Pqwak2.zip	Exploits a flaw in the share level password authentication of MS windows 95/98/ME in its CIFS protocol to find the password of a given share on one of these machines.
October 23, 2000	Sendip-1.1.tar.gz	A command-line tool that can send 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.
October 23, 2000	Whisker-1.4+SSL.tar.gz	A 'next generation' CGI scanner which scans for over 200 vulnerabilities.

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:

A new variant of the SubSeven Trojan Horse has been discovered in the wild. For more information please see NIPC ADVISORY 00-056 located at:
http://www.nipc.gov/warnings/advisories/2000/00-056.htm.
New Variants of the Trinity and Stacheldraht Distributed Denial of Service tools have been reported in the wild. The new versions of Stacheldraht include "Stacheldraht 1.666+antigl+yps" and "Stacheldraht 1.666+smurf+yps," and the new version of Trinity is "entitee." For more information please see NIPC ADVISORY 00-055 located at:
http://www.nipc.gov/warnings/advisories/2000/00-055.htm**.**
Numerous sites that still run an old version of Apache have been victimized by a Windows-based DDoS attack originating from over 500 different IP addresses.
A steady number of reports of intruders using nameservers to execute packet-flooding Denial of Service attacks.

Probes/Scans:

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 CERT advisory located at: http://www.cert.org/incident_notes/IN-2000-10.html.
Intruders are actively exploiting a vulnerability in telnetd that is resulting in a remote root compromise of victim machines.

Other:

There has been a compromise of two SUN security certificates on any system whose web browser has accepted SUN certificates with the following numbers: 3181 B12D C422 5DAC A340 CF86 2710 ABE6 (Internet Explorer), and 17:05:FB:13:A2:2F:9A:F3:C1:30:F5:62:6E:12:50:4C (Netscape). For more information, see CERT Advisory, CA-2000-19 Revocation of Sun Microsystems Browser Certificates, located at: http://www.cert.org/advisories/CA-2000-19.html.
There has been an increased level of cyber activity against web sites related to Israel and pro-Palestinian organizations. For more information, please see NIPC ASSESSMENT 00-057 located at: http://www.nipc.gov/warnings/assessments/2000/00-057.htm.
The "I Love You" virus is still turning out destructive mutants.

Viruses

JS_Logo.A (Aliases: Logo.A, JS/Logo) (JavaScript Virus): The virus executes its payload on the next boot up after infection. At this time, the virus adds some entries in the Favorites folder.

Malatinec.3737 (MS-DOS Encrypted Virus): When the virus is run it goes memory resident, and proceeds to infect the following files: COMMAND, AFD, CHKDSK, DOS4G, HIEW, KRNL, SCANDISK, WIN, ADINF, AIDS, ANTI, ASTA, AUTHOR, AVAST, AVG, AVP, AVSCAN, BAIT, CERT, CLEAN, CPAV, CRC, DRWEB, F-, FINDVIR, FV86, FV386, GOAT, GUARD, IBMAV, ICE, IV, MKS, MSAV, NAV, NOD, PAS, QCV, QMS, SCAN, TB, TKUTIL, TOOLKIT, V-, VAC, VDS, VIR, VIVERIFY, VPCSCAN, WEB. It inserts the virus code in every one of these files that it infects, which increases the size. However, it falsifies the results, so that the user does not notice the increase. Finally, depending on the current system time, Malatinec.3737 displays a text message.

PE_Greenday (Alias: Greenday) (File Infector Virus): The virus infects EXE files in the current directory by overwriting the files with its own code. When an infected EXE file is executed, the virus is run instead of the original EXE file.

VBS/777-B (Visual Basic Script Worm): This virus has been reported in the wild. It is a variant of the VBS/777 worm. Although the original VBS/777 worm had a non-working payload, this variant has had VBS/LoveLet code added into it. The worm arrives as an e-mail with the subject line "I HATE YOU." The body of the e-mail message says "kindly check the attached GOODBYE NEWSGROUPS coming from me." The attachment is called "MY-FAREWELL-2- NEWSGROUPS.TXT.VBS," which has a double-extension. Mailers which suppress well-known extensions such as vbs may present this file as "MY-FAREWELL-2-NEWSGROUPS.TXT," which appears more innocent.

VBS_LOVELETTR.AS (Aliases: LOVELETTR.AS, LOVELETTER.AS, VBS_COLOMBIA, COLOMBIA, PRESIDENT AND FBI SECRETS,) (Visual Basic Script Worm): This destructive Visual Basic Script virus propagates via MS Outlook. Once executed, it sends itself as an attachment to all lists in the infected user's address book. If the current system date is November 7, the virus removes all connected network drives from the system.

VBS_LOVELETTR.BH (Aliases: LOVELETTR.BH, Loveletter.variant) (Visual Basic Script Worm): This is another variant of the VBS_LOVELETTER.A virus. It propagates via e-mail like its predecessor, however it has a unique characteristic. This variant creates 62 registry entries. Most of these registry entries are harmless, such as changing the Internet Explorer Window title, but others like deactivating Internet Explorer security, may be harmful.

VBS_PLACID (Aliases: VBS/Loveletter.AR) (Visual Basic Script Worm): The virus is a new destructive Visual Basic Script worm, which arrives via e-mail. Once executed, VBS_PLACID replaces the Windows Startup screen with the Windows Shutdown screen and then writes virus code to C:\AUTOEXEC.BAT. Upon reboot, VBS_PLACID attempts to delete all files in the A:\ drive and then uses the "FDISK" command to replace the Master Boot Record with a new one. VBS_PLACID also attempts to spam itself via e-mail and Internet Relay Chat (IRC). It does this by e-mailing the file "PLACID.TXT.VBS" to other users.

W32/Sonic-B (Aliases: W32/Sonic.worm, Sonic) (Windows 32 Executable File Virus): The virus has been reported in the wild. It is a multi-part virus with backdoor Trojan characteristics. For additional details, please see the write-up in the Trojan Section under "TROJ_SONIC."

W97M_CHAMELEON.B (Aliases: CHAMELEON.B) (Word 97 Macro Virus): This macro virus infects MS Word documents and document templates. If the current system day is greater than 26, the virus replaces the word "the" in the active document with a text string and also adds a text string in the infected document. It also changes the caption of the infected document.

W97M_CHAMELEON.C (Aliases: CHAMELEON.C) (Word 97 Macro Virus): This macro virus infects MS Word documents and document templates. It disables some document command bars such as: TOOLS|MACROTOOLS|TEMPLATES and ADD-INS.FORMAT|STYLE GALLERY.

W97M_CUENTA.A (Word 97 Macro Virus): The macro virus infects when a document is opened. It only infects templates in a specific folder. When the virus reaches 50 infections within a system, it modifies AUTOEXEC.BAT and deletes several directories.

W97M_MARKER.EI (Aliases: MARKER.EI, W97M/Marker.gen, Macro.Word97.Marker-based, W97M.Marker.Q, W97M/Marker.EI) (Word 97 Macro Virus): This non-polymorphic Word macro virus infects NORMAL.DOT (Word document template) and every other document used thereafter. It is mostly non-destructive but it deletes some submenus in the FILE menu in Word if the current system day is 15.

W97M_PASSBOX.R (Aliases: W97M_PASSBOX.R, PASSBOX.R, PASSBOX, Macro.Word97. Passbox.e, W97M.DWMVCK1/ZMK.gen) (Word 97 Marco Virus): The virus avoids detection by disabling the notification that is displayed when the virus code is saved. It also disables the activation of Visual Basic for application program where the virus code can be found. If a document is successfully infected, the formatted string "Star Ude" replaces the currently selected text. The characters typed after that are also formatted.

W97M/Pinky (Word 97 Macro Virus): The virus belongs to the W00M group that infects Microsoft Word 2000 documents and the global template used by the program. When a user closes, prints, or saves a Word document, the virus checks the date, and if it coincides with 3 July, it deletes the content of the document and replaces it with a given text. Once this change has been made, or if the date does not coincide with 3 July, the document is automatically closed, saved, or printed.

WM97/Blaster-D (Word 97 Macro Virus): The virus is a Word macro virus, which will attempt to hide the desktop icons and the taskbar on the 27th of any month.

WM97/Class-FB (Word 97 Macro Virus): The virus is a Word macro virus which has been created by merging the WM97/Class-B and WM97/Panther Word macro viruses.

WM97/Marker-FQ (Word 97 Macro Virus): This is a variant of the WM97/Marker Word macro virus. There is a 1 in 3 chance that the virus will change the file properties of the infected document to include:

Title = Ethan Frome
Author = EW/KN/CB
Keywords = Ethan

WM97/Thus-BP (Word 97 Macro Virus): This is a variant of WM97/Thus-A. On the 13th and 26th of any month the virus may display a dialog box with the title "Matrix" and the text "Attention! Do everything, your computer tells you!" It then displays an input box with the title "Matrix" and the phrase "Enter your name, User." When the user enters a response the virus will display another dialog box containing the message "Do you know, you're the greatest stupid lamer? If no please call WWW.MICROSOFT.COM." If the date is September 13th, December 13th, or December 26th, the virus then attempts to exit Windows.

XM97/Barisada-G (Excel 97 Macro Virus): This is a variant of the XM97/Barisada-A Excel macro virus. On April 24th between 2 and 3pm the virus displays a message box with the text: "Question: What is the Sword Which Karl Styner(=Gray Scavenger) used? Answer: Barisada." If the user presses the "No" button, the virus displays a message box saying: "Good! You're Authorized now!!" If the user chooses "Yes" the message box displays "I will give you one more Chance. Be careful!!" The next message box displayed says "Summoning Xavier is the Ultimate Magic, Right?" If the user chooses the "Yes" button the virus displays the message box "ok, i will forgive you." If the user chooses "No," the virus displays the message box "Wrong Answer, Your file will be deleted!" and deletes data from every worksheet of the infected workbook.

XM97/Divi-W (Excel 97 Macro Virus): This is a variant of the XM97/Divi-A Excel macro virus which creates a file called ODR.XLS in the XLSTART subdirectory.

XM97/Divi-Y (Excel 97 Macro Virus): This is a minor variant of the XM97/Divi-A Excel macro virus.

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-2000-10, CyberNotes 2000-12
AttackFTP		CyberNotes-2000-10
Backdoor/Doly.17		CyberNotes-2000-16
BackDoor-GZ		CyberNotes-2000-18
BackDoor-HC		CyberNotes-2000-18
Backdoor-HD		CyberNotes-2000-18
BF Evolution	v5.3.12	CyberNotes-2000-10
BioNet	v0.84 - 0.92 +2.2.1	CyberNotes-2000-09, CyberNotes 2000-12
Bla	1.0-5.02, v1.0-5.03	CyberNotes 2000-09
Bobo	v1.0 - 2.0	CyberNotes-2000-09
Donald Dick 2		CyberNotes-2000-15
Drat	v1.0 - 3.0b	CyberNotes-2000-09
Erap Estrada		CyberNotes-2000-18
GIP		CyberNotes-2000-11
Golden Retreiver	v1.1b	CyberNotes-2000-10
Hooker-E		CyberNotes-2000-19
ICQ PWS		CyberNotes-2000-11
InCommand	1.0-1.4, 1.5	CyberNotes-2000-09
Infector	v1.0 - 1.42, v1.3	CyberNotes-2000-09
iniKiller	v1.2 - 3.2, 3.2 Pro	CyberNotes-2000-09, CyberNotes-2000-10
JS_SEEKER.B		**Current Issue**
Kaos	v1.1 - 1.3	CyberNotes-2000-10
Khe Sanh	v2.0	CyberNotes-2000-10
Magic Horse		CyberNotes-2000-10
Matrix	1.4-2.0, 1.0-2.0	CyberNotes-2000-09
Mosaic	v2.00	CyberNotes-2000-16
Multijoke.B		CyberNotes-2000-15
Naebi	v2.12 - 2.39, v2.40	CyberNotes-2000-09, CyberNotes 2000-12
Netbus.153		CyberNotes 2000-16
Netbus.170		CyberNotes 2000-16
NetSphere	v1.0 - 1.31337	CyberNotes-2000-09

Trojan	Version	Issue discussed
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
Phaze Zero	v1.0b + 1.1	CyberNotes-2000-09
Prayer	v1.2 - 1.5	CyberNotes-2000-09
Prosiak	beta - 0.65 – 0.70 b5	CyberNotes-2000-09, CyberNotes 2000-12
Qaz.A	W32.HLLW.Qaz.A	CyberNotes-2000-20, CyberNotes-2000-16
Revenger	1.0-1.5	CyberNotes 2000-12
Serbian Badman		CyberNotes 2000-12
ShitHeap		CyberNotes-2000-09
Snid	1-2	CyberNotes 2000-12
Troj/Simpsons		CyberNotes-2000-13
TROJ_BATMAN		CyberNotes-2000-20
TROJ_BLOODLUST		CyberNotes-2000-21
TROJ_BUTANO.KILL		CyberNotes-2000-19
Troj_Dilber		CyberNotes-2000-14
TROJ_FELIZ		**Current Issue**
TROJ_IGMNUKE		CyberNotes-2000-20
TROJ_KILLME		CyberNotes-2000-20
TROJ_MSINIT.A		CyberNotes-2000-21
TROJ_PERSONAL_ID		CyberNotes 2000-16
TROJ_POKEY.A		CyberNotes 2000-16
TROJ_ROCKET		**Current Issue**
TROJ_SCOOTER		CyberNotes-2000-19
TROJ_SONIC		**Current Issue**
TROJ_SPAWNMAIL.A		CyberNotes-2000-18
TROJ_SUB7.214DC8		CyberNotes-2000-21
TROJ_SUB7.382883		CyberNotes-2000-21
TROJ_VBSWG		CyberNotes-2000-16
Trojan/ICQ		CyberNotes-2000-20
Trojan/Parkinson		CyberNotes-2000-21
Trojan/PSW.StealthD		CyberNotes-2000-19
Trojan/Varo31		CyberNotes-2000-19
Trojan/Win32		CyberNotes-2000-21
VBS_MAILPEEP		**Current Issue**
W32.Nuker.C		CyberNotes-2000-14
Win.Unabomber		CyberNotes-2000-14
WinCrash	Beta	CyberNotes-2000-12
Winkiller		CyberNotes 2000-12

JS_SEEKER.B (Aliases: SEEKER.B, JS.Trojan.Seeker.b, JS/Seeker.B): This encrypted JavaScript Trojan sets the default and home page of Internet Explorer to http://www.JetHomePage.com. The program is encrypted using Microsoft's Windows script encoder, which allows HTML pages, ASP Pages, and Windows Script Host files to be encrypted so that the infected user cannot read the code.

TROJ_FELIZ: This is a new destructive Trojan that tries to delete vital system files in Windows (9x and NT). Once the Trojan is executed, it displays several message boxes and suggests the user restart Windows. However, at the same time, TROJ_FELIZ also deletes many important system files, leaving the system unable to boot into the Windows GUI.

VBS_MAILPEEP (Aliases: MAILPEEP): This non-destructive VB Script Trojan does not infect files. It just makes a copy of the infected user's e-mail, and sends them via MS Outlook to a Hotmail account. Attached to the e-mail sent are files with FF. Extensions: DAT, UIN, CHT. This Trojan only affects MS Outlook.

TROJ_ROCKET (Aliases: ROCKET): This is a destructive Trojan that deletes all files with the extensions DLL or VXD in the Windows System directory. The Trojan also deletes c:\COMMAND.COM when found. When executed, it displays a window with a check box and a button. When the option "Rocket Launcher" is checked and the "Install Standby" button is clicked, the virus executes its payload. The extent of the damage of this Trojan is limited since most DLLs and VXDs in the C:\Windows\System are being loaded upon boot-up, which means that the files cannot be deleted by this Trojan.

TROJ_SONIC.B (Aliases: SONIC.B, I-Worm.Sonic.B, TROJ_SONIC.27, TROJ_SONIC.28, TROJ_SONIC.29, TROJ_SONIC.40, TROJ_SONIC.A): This multi-component Internet worm, and Backdoor tool spreads itself via e-mail. It disguises itself as a Windows native executable GDI32.EXE and comes via e-mail as a UPX compressed file. When executed, this Trojan connects to a predetermined host, and downloads its main component into the infected computer. Upon execution of the main component, the Trojan searches for Windows Address Book files (*.WAB) and uses the e-mail addresses found there to spread. It sends an e-mail to all addresses found with itself as an attachment, LOVERS.EXE. This e-mail has the subject: “I'm your poison.” The main component of this Trojan is saved in the Windows directory with the same name as the loader. The backdoor component of this Trojan is very dangerous, since it allows a remote user to have full access to the infected computer, similar to B0`2K.