



National Infrastructure Protection Center CyberNotes

Issue #2000-17

August 28, 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 August 9 and August 25, 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" 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
Ashley Montanaro ¹ Unix	Darxite 0.4	An improper bounds checking vulnerability exists when user-supplied data is entered during the login process that could allow a malicious user to supply arbitrary code for execution at the privilege level of the Darxite user.	No workaround or patch available at time of publishing.	Darxite Login Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit script has been published.

¹ Securiteam, August 22, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
BEA Systems ² Windows 98/NT 4.0/2000, Unix	Weblogic Server 3.1.8, 4.0x, 4.5x , 5.1x	Several unchecked buffer overflow vulnerabilities exist within BEA System's Weblogic logic plug-ins, which could allow a remote malicious user to execute arbitrary code on the system running the proxying web server.	Upgrade the proxy plug-in used for third-party Web server integration located at: http://commerce.beasys.com/downloads/weblogic_server.jsp#wls	Weblogic Proxy Multiple Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit has been published.
CGI Script Center ³ Windows NT 4.0/2000, Unix	Account Manager LITE 1.0, Account Manager PRO 1.0	A vulnerability exists which could let a remote malicious user modify the administrative password for CGI Script Center's Account Manager. This would grant the user full administrative privileges.	Upgrade to the latest version available at: Account Manager LITE: http://www.cgiscriptcenter.com/acctlite/ Account Manager PRO: http://www.cgiscriptcenter.com/acctman/	Manager LITE / PRO Administrative Password Alteration	High	Bug discussed in newsgroups and websites. Exploit scripts have been published.
CGI Script Center ⁴ Windows NT 4.0/2000, Unix	Subscribe Me Lite 2.0	A vulnerability exists which could allow a remote malicious user to overwrite the Admin Passwd file, giving him/her Admin access to the Maillist Script.	Upgrade to the latest release which is available at: http://www.cgiscriptcenter.com/subscribe/	Subscribe Me LITE Administrative Password Alteration	Medium	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Computer Associates ⁵ Windows NT 4.0, Unix	eTrust Access Control 4.1, 4.1-SP1, 5.0, 5.0-SP1	A vulnerability exists in the default installation, which could let a malicious user gain root access.	Computer Associates has indicated that the correct solution to this problem is to elect to use strong encryption during the installation. This will cause a key other than the default one to be used, thereby eliminating this problem.	eTrust Access Control Default Encryption Key	High	Bug discussed in newsgroups and websites. Exploit has been published.
Francisco Burzi ⁶ Unix	PHP-Nuke 1.0, 2.5	An access validation error exists, which could let a remote malicious user gain administrative privileges.	Upgrade to PHP-Nuke 3.0 available at: http://www.ncc.org.ve/php-nuke.php?op=download&location=http://download.sourceforge.net/phpnuk e&file=PHP-Nuke-3.0.tar.gz	PHP-Nuke Administrative Privileges	High	Bug discussed in newsgroups and websites. Exploit has been published.
FreeBSD ⁷ Unix	Luca Deri Ntop 1.2a7-9, 1.3.1	A buffer overflow vulnerability exists, which could allow a local/remote malicious user to execute arbitrary code on the local system with increased privileges.	Patch available at: ftp://ftp.FreeBSD.org/pub/FreeBSD/p orts/	Linux Ntop -w Buffer Overflow	High	Bug discussed in newsgroups and websites.

² BEA Systems Inc. Security Advisory, BEA00-05.01, August 14, 2000.

³ Bugtraq, August 23, 2000.

⁴ Bugtraq, August 23, 2000.

⁵ Bugtraq, August 11, 2000.

⁶ Securiteam, August 21, 2000.

⁷ FreeBSD Security Advisory, FreeBSD-SA-00:36, August 14, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Helix Code ⁸ Unix	GNOME Installer 0.2	A vulnerability exists which could allow non-root malicious users to exploit world-writable permissions on /tmp, permitting arbitrarily modified RPM packages to be installed on the system.	Upgrade to Helix GNOME Updater (0.6). A list of supported distributions, platforms and versions can be found at: http://www.helixcode.com/desktop/download.php3 .	Gnome Installer System Config-file Overwrite	High	Bug discussed in newsgroups and websites.
Hewlett-Packard ⁹ Unix	HP-UX 11.0	A vulnerability exists with the cumulative newgrp(1) command, which could allow malicious users additional privileges.	Patch PHCO_22096 available at: http://itrc.hp.com	HPUX Newgrp(1)	Medium	Bug discussed in newsgroups and websites.
Hewlett-Packard ¹⁰ Windows NT 4/0/2000, Unix	OpenView Network Node Manager 6.1	A vulnerability exists which exposes web passwords.	Patch available at: http://ovweb.external.hp.com/cpe/patches/	OpenView Network Node Manager Web Password	Medium	Bug discussed in newsgroups and websites.
IBM ¹¹	OS/2 FTP Server 4.0, 4.2, 4.3	A Denial of Service vulnerability exists in the FTP server that comes with OS/2 Warp 4.5.	IBM has released the following patch for version 4.3 and newer. Users of previous versions should contact IBM support for assistance. IBM OS/2 FTP Server 4.3: ftp://ftp.software.ibm.com/ps/products/tcpip/fixes/v4.3os2/ic27721/	OS/2 FTP Server Login Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Internet Security Systems ¹² Windows NT, Unix	RealSecure 3.2.1, 3.2.2	A vulnerability exists which could allow a malicious user to remotely disable Real Secure.	No workaround or patch available at time of publishing.	RealSecure Fragmented SYN Packets Denial of Service	Low	Bug discussed in newsgroups and websites.
IpSwitch ¹³	Imail 6.00, 6.01, 6.02	A remote Denial of Service vulnerability exists.	Patch available at: http://www.ipswitch.com/support/patches-upgrades.html#IMail	Imail Web Service Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Mandrake Soft ¹⁴ Unix	Linux Mandrake 6.0, 6.2, 7.0, 7.1	A vulnerability exists in the Mandrake Update utility, which may let a local malicious user interfere with downloaded RPMs before installing them.	Upgrade available at: ftp://ftp.linux.tucows.com/pub/distributions/Mandrake/Mandrake/updates	Linux- Mandrake Update Race Condition	Medium	Bug discussed in newsgroups and websites.

⁸ Helix Code, Inc. Security Advisory, 08-20-2000-02, August 20, 2000.

⁹ Hewlett-Packard Company Security Bulletin, HPSBUX0008-118, August 9, 2000.

¹⁰ Hewlett-Packard Company Security Bulletin, HPSBUX0008-119, August 9, 2000.

¹¹ Vigilante Security Advisory, VIGILANTE-2000006, August 15, 2000.

¹² Securiteam, August 23, 2000.

¹³ NTBugtraq, August 17, 2000.

¹⁴ Linux-Mandrake Security Update Advisory, MDKSA-2000:034, August 12, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Mediahouse Software ¹⁵ Windows NT 4.0	Statistics Server LiveStats 5.02	A buffer overflow vulnerability exists which could let a local/remote malicious user run arbitrary code with WebServer privileges.	Upgrade available at: http://www.mediahouse.com/statistics/server/download_trial/dist/ss50.exe	Statistics Server LiveStats Buffer Overflow	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft ¹⁶ Windows 95/98/NT 4.0/2000	FrontPage 2000 Server Extensions 1.1	A Denial of Service vulnerability exists which disables all FrontPage operations on a web site. A secondary problem also exists with certain DOS device names that reveal the server's physical path.	Microsoft has eliminated this vulnerability with the release of FrontPage Server Extensions Service Release 1.2. It is available for download at: http://msdn.microsoft.com/workshop/languages/fp/2000/winfpse.asp	FrontPage Server Extensions MS-DOS Device Name Denial of Service	Low (High if DoS best- practices not in place)	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft ¹⁷ Windows 95/98/ NT 4.0/2000	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.	Patch available at: Microsoft IIS 5.0: http://download.microsoft.com/download/win2000pro/Patch/q260347/NT5/EN-US/Q260347_W2K_sp2_x86_en.EXE Microsoft IIS 4.0: http://download.microsoft.com/download/winntsp/Patch/q260347/NT4ALPHA/EN-US/crsscr4a.exe	FrontPage/IIS Cross-Site Scripting	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft ¹⁸ Windows NT 2000	Internet Information Server (IIS) 5.0	A security vulnerability exists which could cause a web server to send the source code of certain types of web files to a visiting user.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq00-058.asp	IIS Specialized Header	Medium	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Microsoft ¹⁹ Windows 95/98/NT 4.0/2000	Microsoft VM (all builds in 2000 series, 3100-3300 series)	A security vulnerability exists when a user is visiting a malicious web site. The web site operator can masquerade as the user, visit other sites using his identity, and relay the information back to the attacker's site.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq00-059.asp	Microsoft Java VM Applet	Medium	Bug discussed in newsgroups and websites.

¹⁵ DeepZone Advisory, August 10, 2000.

¹⁶ Securiteam, August 24, 2000.

¹⁷ Microsoft Security Bulletin, MS00-060, August 25, 2000.

¹⁸ Microsoft Security Bulletin, MS00-058, August 14, 2000.

¹⁹ Microsoft Security Bulletin, MS00-059, August 21, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft ²⁰	Money 2000, 2001	A security vulnerability exists which could allow a malicious user to obtain the password of a Money data file.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq00-061.asp	Microsoft Money Password	Medium	Bug discussed in newsgroups and websites.
Microsoft ²¹ Windows 98/NT 2000	Windows 98, 98SE, NT 2000	Two security vulnerabilities exist: IE 5.x may execute arbitrary programs when visiting a web page, reading HTML based mail with Outlook or simply browsing folders as web pages; and a Local Administrator compromise on default installation of Windows 2000. In both cases a malicious user may take full control over the computer/server.	No workaround or patch available at time of publishing. <u>Unofficial workaround (Georgi Guninski):</u> Disable the "View folders as web pages" option for all users.	Windows 98/2000 Folder.htt	High	Bug discussed in newsgroups and websites. Exploit script has been published. Vulnerability has appeared in the Press and other public media.
Multiple Vendors ²² Unix	XChat 1.3.10- 1.3.13, 1.3.9, 1.4, 1.4.1- 1.4.2, 1.5.x dev	A vulnerability exists in XChat, which passes unchecked URLs as shell commands, which could allow a malicious URL to execute arbitrary shell commands.	Upgrades available at: <u>RedHat:</u> ftp://updates.redhat.com/6.2 <u>Conectiva:</u> ftp://atualizacoes.conectiva.com.br <u>Mandrake:</u> ftp://ftp.linux.tucows.com/pub/distributions/Mandrake/Mandrake/updates	X-Chat Command Execution Via URLs	High	Bug discussed in newsgroups and websites. Exploit has been published.

²⁰ Microsoft Security Bulletin, MS00-061, August 25, 2000.

²¹ Georgi Guninski Security Advisory #18, August 14, 2000.

²² Securiteam, August 25, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Multiple Vendors ^{23 24, 25,} ²⁶ Unix	Zope 1.10.3, 2.1.x, 2.1.1, 2.1.7, 2.2 beta1	A vulnerability exists which gives any user the ability to edit the DTML package to take on additional roles (or modify roles) without authorization.	RedHat: Zope packages from 6.2 are located at: ftp://ftp.redhat.com/pub/redhat/powertools/6.2/ Debian: http://security.debian.org/dists/frozen/updates/main/ FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/ports Conectiva: ftp://atualizacoes.conectiva.com.br	Zope Unauthorized Role Modification	Medium	Bug discussed in newsgroups and websites.
Multiple Vendors ^{27, 28} Unix	David Bagley xlock 4.16, 4.16.1	A format string vulnerability exists, which could let a malicious user gain read access to the shadow file.	Debian: http://security.debian.org/dists/slink/updates/ Conectiva: ftp://atualizacoes.conectiva.com.br	Xlockmore User Supplied Format String	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Multisoft ²⁹ Unix	FlagShip 4.4	Some binaries are installed with world-writable permissions, which could allow a malicious user to alter a binary and cause other users to execute arbitrary code.	No workaround or patch available at time of publishing. Unofficial workaround (Bugtraq): Executing 'chmod 755' on the following binaries: /usr/bin/FSserial /usr/bin/FlagShip_c /usr/bin/FlagShip_p	FlagShip Installation Permission	High	Bug discussed in newsgroups and websites. Exploit has been published.
Netscape ³⁰ Windows 95/98/NT 4.0/2000, Unix <i>New patches released³¹</i>	Communi- cator 4.05-4.08, 4.0, 4.5-4.51, 4.6-4.61, 4.72-4.74	A pair of new capabilities in Java, one residing in the Java core and the other in Netscape's Java distribution, allows creating of a remote management tool that can be used to compromise a remote system. The first allows Java to open a local server that can be accessed by arbitrary clients. The second allows Java to access arbitrary URLs, including local files.	Workaround: Until a fix becomes available, Java should be disabled in the browser. Red Hat Linux 6.2 (6.1, 6.0): ftp://updates.redhat.com/6.2/ Conectiva: ftp://atualizacoes.conectiva.com.br/4.0 Netscape (patch download, non- RPM): http://www.netscape.com/computing/download/index.html Linux-Mandrake: ftp://ftp.linux.tucows.com/pub/distributions/Mandrake/Mandrake/updates Caldera: ftp://ftp.calderasystems.com/pub/updates/OpenLinux/	Netscape URL File Read and Listening Socket Vulnera- bilities	Medium/ High	Bug discussed in newsgroups and websites. Exploit script has been published. Vulnerability has appeared in the Press and other public media.

²³ Red Hat, Inc. Security Advisory, RHSA-2000:052-02, August 11, 2000.

²⁴ Debian Security Advisory, August 18, 2000.

²⁵ FreeBSD Ports Security Advisory, FreeBSD-SA-00:38, August 14, 2000.

²⁶ Conectiva Linux Security Announcement, August 15, 2000.

²⁷ Debian Security Advisory, August 16, 2000.

²⁸ Conectiva Linux Security Announcement, August 17, 2000.

²⁹ Bugtraq, August 10, 2000.

³⁰ Securiteam, August 7, 2000.

³¹ Securiteam, August 23, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Netscape ³² <i>Upgrade packages released</i> ^{33, 34, 35}	Communi- cator 4.05- 4.08, 4.0, 4.5, 4.5BETA, 4.51, 4.6, 4.61, 4.7-4.73; Mozilla Browser M15	The way JPEG images are handled in Netscape Communicator may lead to buffer overflow problems and malicious users running their own code on targeted machines. The browser, mail, and newsreaders are all vulnerable to this.	Upgrade to Netscape 4.74 or Mozilla M16, or newer. <i>Conectiva:</i> ftp://atualizacoes.conectiva.com.br <i>NetBSD:</i> <i>For more information on how to rebuild a package from source for your architecture, see</i> ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/README <i>SuSE:</i> ftp://ftp.gwdg.de/pub/linux/suse/	Netscape Communica- tor JPEG- Comment Heap Overwrite	High	Bug discussed in newsgroups and websites. Exploit script has been published.
NetWin ³⁶ Windows 95/NT 4.0, MacOS 9.0, Unix	Netauth 4.2 and previous	A directory traversal vulnerability exists, which could let a remote malicious user gain read access to any known file residing on the host.	Upgrade to Netauth 4.2f available at: http://netwinsite.com/netauth/download.htm	Netwin Netauth Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Network Associates ³⁷ Windows 95/98/NT 4.0/2000	PGP 5.5.3x-6.5.3i	An implementation vulnerability allows unsigned ADKs (Additional Decryption Keys), which have been maliciously added to a certificate to be used for encryption. For more information, see CERT http://www.cert.org/advisories/CA-2000-18.html	Network Associates has produced a new version of PGP 6.5 which corrects this vulnerability by requiring that the ADK be included in the signed portion of the certificate.	PGP ADK Insertion	Medium/ High	Bug discussed in newsgroups and websites. Vulnerability has appeared in the Press and other public media.
Pragma Systems ³⁸ Windows NT 2000	TelnetServer 2000	A buffer overflow memory vulnerability exists in the 'rpc' module.	No workaround or patch available at time of publishing.	TelnetServer Rexec Buffer Overflow	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
RapidStream ³⁹	RapidStream 2000, 4000, 6000, 8000	A vulnerability exists which could let a malicious user append arbitrary commands to the SSH string when connecting to the SSH server on the remote VPN.	RapidStream is reportedly correcting the modified sshd in their product. Workaround (Securiteam): 1) Disable SSHD, or restrict it to internal hosts. 2) Deny access to port TCP/22 (SSHD).	RapidStream Unauthenti- cated Remote Command Execution	High	Bug discussed in newsgroups and websites. Exploit has been published.

³² Bugtraq, July 24, 2000.

³³ Conectiva Linux Security Announcement, August 10, 2000.

³⁴ NetBSD Security Advisory 2000-011, August 10, 2000.

³⁵ SuSE Security Announcement, August 23, 2000.

³⁶ Bugtraq, August 17, 2000.

³⁷ CERT Advisory CA-2000-18, August 24, 2000.

³⁸ USSR Labs Advisory Code, USSR-2000051, August 24, 2000.

³⁹ Securiteam, August 19, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
SGI ⁴⁰	Omron WorldView	A buffer overflow vulnerability exists, which could let a malicious user execute arbitrary code on the system and could lead to root compromise.	No workaround or patch available at time of publishing.	Omron Worldview Root Compromise	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Silicon Graphics, Inc. ⁴¹ Unix	IRIX 5.2, 5.3, 5.3XFS, 6.0, 6.0.1, 6.0.1XFS, 6.1-6.5, 6.5.1, 6.5.2m, 6.5.3, 6.5.3f, 6.5.3m, 6.5.4-6.5.8	A vulnerability exists in the telnet daemon, which could let a remote malicious user execute arbitrary commands with root privileges.	Workaround available at: ftp://sgigate.sgi.com/security/20000801-01-A	IRIX Telnetd Environment Variable Format String	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Slackware ⁴² Unix	Linux 7.0.0 and 7.1.0.	Multiple buffer overflow vulnerabilities exist in the utility top program, included with the procps package.	A patch for the most current version of procps (procps-2.0.6) is available at: http://www.slackware.com/	Linux Multiple Buffer Overflow Vulnerabilities	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Software Composition Group ⁴³ Unix	Oscar Nierstrasz Htgrep	A vulnerability exists which could allow a remote malicious user to view arbitrary files on the system with the privileges of the web user.	No workaround or patch available at time of publishing.	Htgrep CGI Arbitrary File Viewing	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Sun Microsystems, Inc. ⁴⁴ Windows NT 4.0, Unix	Sun Java Web Server 1.1.3, 2.0	Using Sun's Java Web Server's administration module configuration and the Bulletin Board example application supplied with Java Web Server, it is possible to remotely execute arbitrary commands on the target system despite existing vendor recommendations for hardening.	Patch available at: Sun Java Web Server 2.0: http://java.sun.com/products/java-server/jws20patch3.html Sun Java Web Server 1.1.3: http://java.sun.com/products/java-server/jws113patch3.html	Sun Java Web Server Web Admin / Bulletin Board	High	Bug discussed in newsgroups and websites. Exploit has been published.
Trustix ⁴⁵ Unix	Trustix Secure Linux 1.1	Due to a typo in the rpm spec file for Apache-ssl, a local malicious user can obtain root access.	Patch available at: ftp://ftp.trustix.com/pub/Trustix/updates/1.1	Trustix Apache-SSL RPM Permissions	High	Bug discussed in newsgroups and websites.

⁴⁰ SGI Security Advisory, 20000803-01-A, August 17, 2000.

⁴¹ SGI Security Advisory, 20000801-01-A, August 14, 2000.

⁴² Bugtraq, August 15, 2000.

⁴³ Bugtraq, August 17, 2000.

⁴⁴ Foundstone, Inc. Security Advisory, FS-082200-11-JWS, August 22, 2000.

⁴⁵ Securiteam, August 16, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
University of Minnesota ⁴⁶ Unix	Gopherd 2.3.1p0 and previous	An unchecked buffer exists in the 'halidate' function which could allow a malicious user to either execute arbitrary code or crash a remote system.	No workaround or patch available at time of publishing.	UMN Gopherd 'Halidate' Function Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit has been published.
University of Minnesota ⁴⁷ Unix	University of Minnesota gopherd 2.3, 2.3.1	The program uses a flawed implementation of Data Encryption Standard for authentication, which can be exploited to gain root access.	Patch available at: ftp://boombox.micro.umn.edu/pub/gopher/Unix/gopher2_3.1.tar.gz	Gopherd Remote Root Buffer Overflow	High	Bug discussed in newsgroups and websites.
WatchGuard ⁴⁸ Unix	Firebox II	A Denial of Service vulnerability exists when a malformed URL is sent to the authentication service running on TCP port 4100.	Patch available at: http://www.watchguard.com/support	Firebox II Denial of Service	Low	Bug discussed in newsgroups and websites.

*Risk is defined in the following manner:

High - A vulnerability that will allow an intruder to immediately gain privileged access (e.g., sysadmin, and root) to the system. 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 August 12 and August 24, 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, 48 scripts, programs, and net-news messages containing holes or exploits were identified.

⁴⁶ Securiteam, August 25, 2000.

⁴⁷ Guardent Security Advisory, A0208102000, August 10, 2000.

⁴⁸ Vigilante Advisory, VIGILANTE-2000005, August 15, 2000.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
August 24, 2000	Halidate.c	Script which exploits the UMN Gopherd 2.x Halidate Function Buffer Overflow vulnerability.
August 24, 2000	Labs51.txt	Shell code for the remote Denial of Service buffer overflow in Pragma TelnetServer 2000 for Windows.
August 24, 2000	Telnetserverdos.pl	Perl script which exploits the TelnetServer 2000 rexec Buffer Overflow vulnerability.
August 23, 2000	Amlite-xploit.pl	Exploit for the CGI Script Center Account Manager LITE / PRO Administrative Password Alteration vulnerability.
August 23, 2000	Cgiamsploit.htm	Exploit for the CGI Script Center Account Manager LITE / PRO Administrative Password Alteration vulnerability.
August 23, 2000	Cgisubme.html	Script that exploits the CGI Script Center Subscribe Me LITE Administrative Password Alteration vulnerability.
August 23, 2000	Sms.197.java	Code which exploits the Sun Java Web Server vulnerability.
August 23, 2000	Sploit.zip	Script that exploits the CGI Script Center Subscribe Me LITE Administrative Password Alteration vulnerability.
August 23, 2000	Sublite-xploit.pl	Perl script that exploits the CGI Script Center Subscribe Me LITE Administrative Password Alteration vulnerability.
August 22, 2000	Darxite.tar.gz	Exploit script for the Darxite 0.4 Login Buffer Overflow vulnerability.
August 22, 2000	Fpipe_2.01	A TCP source port forwarder/redirector that can be used to force a TCP stream to always connect using a specific source port. This tool can be used to get around firewalls that only accept traffic originating from common source ports.
August 22, 2000	Windump203.zip	Network capture program for Windows NT 4.0 / Win95, which consists of an executable (the windump main program) with a network capture driver.
August 22, 2000	Xslrnpull.c	Script which exploits a local buffer overflow vulnerability in slrnpull version 0.9.6.2.
August 21, 2000	Htgrep.c	Script which exploits the Htgrep vulnerability that allows a remote user to read arbitrary files on the system with the privilege of the user running the program.
August 21, 2000	Parasite-0.5.tar.gz	THC-Parasite allows you to sniff traffic on a switched network by using either ARP Spoofing or MAC Flooding. The algorithms are designed to bypass basic switch security.
August 21, 2000	PHP-Nuke.c	Script that exploits the vulnerability in the way PHP-Nuke authenticates administrative accounts.
August 21, 2000	Rnmap_0.2-beta.tar.gz	A python client/server package which allows many clients to connect to a centralized nmap server to do port scanning.
August 21, 2000	Winfingerprint-227.zip	Advanced remote Windows OS detection.
August 18, 2000	Pdump-0.777.tar.gz	A sniffer written in Perl that dumps, greps, monitors, creates, and modifies traffic on a network.
August 17, 2000	Anomy-sanitizer-1.25.tar.gz	The Anomy mail sanitizer is a filter designed to block e-mail based attacks such as Trojans, viruses, and hostile Java.
August 17, 2000	Ldistfp-0.1.2.tar.gz	Ldistfp is an identd fingerprinting tool, which works well with all Linux and most BSD hosts that have their auth service running.
August 17, 2000	Rnmap_01-beta.tar.gz	A python client/server package which allows many clients to connect to a centralized nmap server to do their port scanning.
August 17, 2000	Srcgrab.pl.txt	Exploit for the Translate:f vulnerability in the Microsoft IIS Specialized Header vulnerability.
August 17, 2000	Threadcrashmail.zip	Exploit for the Imail Web Service remote Denial of Service vulnerability.
August 16, 2000	Crackncftp.c	The ncftp client uses an easily decrypted scheme to save passwords to remote FTP sites in a bookmark file.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
August 16, 2000	Stateful.firewall-1.txt	A Stateful Inspection of FireWall-1 advisory which summarizes the finding from BlackHat 2000.
August 15, 2000	IE5-msn.exec.txt	Proof of concept HTML code for two Microsoft vulnerabilities.
August 15, 2000	Linsql.c	A command-line client for the MS SQL server which can execute arbitrary SQL queries and OS commands on an MS-SQL hosts that uses a blank 'sa' password, a common default configuration.
August 15, 2000	Saint-2.1.3.tar.gz	A security assessment tool based on SATAN.
August 15, 2000	Topoff.c	Script which exploits the Linux Multiple Buffer Overflow vulnerabilities.
August 14, 2000	Ac.zip	Exploit for the Microsoft Windows 98/2000 Folder.htt vulnerability.
August 14, 2000	Bktrpibdc.c	A network tool for ARP redirection which implements a man-in-the-middle attack.
August 14, 2000	Bktsplibdc.c	BKtsplibdc.c allows sniffing on switched networks by flooding the switch with TCP & IP & ARP requests containing spoofed MAC addresses.
August 14, 2000	Cgichk-2.42.tar.gz	A web vulnerability scanner which automatically searches for a series of interesting directories and files on a given site.
August 14, 2000	Fakegina.zip	FakeGINA intercepts the communication between Winlogon and the normal GINA, and while doing this it captures all successful logins (domain, username, and password) and writes them to a text file.
August 14, 2000	Irix.telnetd.txt	Proof of concept exploit for the IRIX telnetd Environment Variable Format String vulnerability.
August 14, 2000	Irx_telnetd.c	Script which exploits the IRIX telnetd Environment Variable Format String vulnerability.
August 14, 2000	Nmap-2.54BETA3.tgz	A utility for port scanning large networks.
August 14, 2000	Sara-3.1.7a.tar.gz	A security analysis tool based on SATAN.
August 14, 2000	Srcgrab.pl	Perl script which exploits the Microsoft Internet Information Server Specialized Header vulnerability.
August 14, 2000	Trans.pl.	Perl script which exploits the Microsoft Internet Information Server Specialized Header vulnerability.
August 14, 2000	Vlad-0.7.1.tgz	A freeware, open-source scanner that checks for the common security problems referenced in the SANS Top Ten list of common security problems.
August 14, 2000	Wais.pl.advisory.txt	Exploit for Linux/x86 for the Waisq buffer overflow vulnerabilities.
August 13, 2000	Ssexploit502x.pl	Perl script which exploits the Statistics Server 5.02x vulnerability.
August 13, 2000	Wcgoph.c	Remote exploit script for the Gopher+ v2.3.1p0 vulnerability.
August 12, 2000	Xgopher.c	Gopher+ daemon v2.3 remote root buffer overflow exploit script.
August 11, 2000	Sploit502x.pl	Perl script which exploits the Mediahouse Statistics Server LiveStats Buffer Overflow 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:

- **A DDoS agent named "trinity v3 by self" was installed on about 20 Linux machines on a university network via an rpc.statd exploit.**
- A new backdoor exploit program called "Brown Orifice" takes advantage of vulnerabilities in Netscape and Java. For more information, please see NIPC System Assessment 00-0521, which is available at <http://www.nipc.gov/warnings/assessments/2000/assess00-052.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 address.
- The "Trinoo" DDoS program has attacked over 250 Korean Networks.
- A simple exploit/DoS tool named "octo" or "octopus" has the ability to shut down services remotely.
- A steady number of reports of intruders using nameservers to execute packet-flooding Denial of Service attacks.

Probes/Scans:

- An increase in rpc.statd program scanning.
- An increase in linuxconf scanning.
- An increase in scanning for the Bind vulnerability.
- An increase in scans on port 21 (when WuFTP 2.5.0 was shown vulnerable).
- A continuation of scans to port 109 (pop2 exploit).
- A continuation of probes to UDP Port 137 (NetBIOS Name Service).
- Increasing reports of scans to known Trojan ports. System administrators should consult their intrusion detection system and firewall logs for unusual port scans.

Other:

- **Mobile Operating Systems have become the latest target of virus writers and hackers.**
- **A new e-mail virus which attacks UBS PIN software has been released.**
- Chat clients and Internet Relay Chat (IRC) networks pose a serious security risk due to recent viruses like the 'I Love You' and 'Life-Stages' bugs. Both were programmed to take advantage of flaws in instant messaging software and chat client software to spread themselves rapidly across computers and could be easily exploited by malicious users to plant and launch malicious code in corporate networks. Users could be also tricked into communicating sensitive information or downloading files containing malicious code via chat clients.
- An increase in sites being probed or root compromised related to input validation vulnerabilities in many FTP databases.
- A steady number of reports of intruders exploiting unprotected Windows networking shares.
- Reports indicate domain name registration information continues to be maliciously altered, including point of contact information for domain names, IP address delegations, and autonomous system numbers.

Viruses

A list of viruses infecting two or more sites as reported to various anti-virus vendors has been categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. **To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available.** The tables list the viruses by: ranking (number of sites affected), common virus name, type of virus (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported during the latest three months), and approximate date first found. During this month, a number of anti-virus vendors have included information on Trojan Horses and Worms. These types of malicious code will now be included in the table where appropriate. Following this table are write-ups of new viruses and updated versions discovered in the last two weeks. At times, viruses may contain names or content that may be considered offensive.

Note: Virus reporting may be weeks behind the first discovery of infection. A total of **215** distinct viruses are currently considered “in the wild” by anti-virus experts, with another **565** viruses suspected. “In the wild” viruses have been reported to anti-virus vendors by their clients and have infected user machines. The additional suspected number is derived from reports by a single source.

Ranking	Common Name	Type of Code	Trends	Date
1	W32/SKA	File	Slight increase	March 1999
2	VBS/LoveLetter	Script	Increase	March 2000
3	VBS/Kakworm	Script	Slight decrease	December 1999
4	W97M/Ethan.A	Macro	Increase	February 1999
5	W32/PrettyPark	File	Increase	June 1999
6	VBS/Stages	Script	Decrease	June 2000
7	W97M/Marker	Macro	Decrease	August 1998
8	W95/CIH	File	Slight decrease	April 1999
9	SubSeven	Trojan	New to table	March 2000
10	W97M/Melissa.A-BG	Macro	Slight decrease	April 1999

OF97/Shiver-N (Office 97 Macro Virus): This virus is a variant of the OF97/Shiver Microsoft Office macro virus, which infects Microsoft Word documents and Excel spreadsheets. The virus displays multiple message boxes containing the words 'Shiver[DDE] by ALT-F11' on Microsoft Excel spreadsheets.

PE_BUGFIX.A (Aliases: BUGFIX.A, PE_ADRENALINE, VBS_BUGFIX.A, IRC_BUGFIX.A) (File Infector Virus): This is a non-destructive virus, which tries to spread itself via e-mail and Internet Relay Chat (IRC) to other users. It usually arrives in an e-mail with the attachment "BUGFIX.EXE". Once executed, it infects files in the Windows directory and also displays a DOS window with the text “Adrenaline.” The message box is displayed each time an infected file is executed. Another payload attempts to e-mail an infected attachment to users in the Microsoft Outlook address book and users on IRC.

VBS_Loveletter.bd (Worm): This virus was recently reported in the wild and is a variant of the VBS_Loveletter virus, which was originally found in May, 2000. Once an infected file is executed, VBS_LOVELETTER.BD attempts to e-mail itself (as resume.txt.vbs) to all users in the Microsoft Outlook address book. The subject of the e-mail is: “Resume.” VBS_LOVELETTER.BD also attempts to

download and run a backdoor Trojan, "TROJ_PSW.HOOK.B", which captures network password information and sensitive PIN information stored in the registry related to UBS online banking software. For more information, please see NIPC Alert: Alert 00-053 Loveletter.bd, which can be found at: <http://www.nipc.gov/warnings/alerts/2000/alert00-053.htm>

VBS/Lovelet-BE (Visual Basic Script Worm): This is a variant of the VBS/Lovelet worm. The virus tries to spread itself in several ways. Most commonly, it sends itself as an attachment to an e-mail. Infected e-mails have the following characteristics:

Subject: fwd: Joke
Message text: None
Attached file: JOKE.vbs

Because the virus arrives in a VBS file, it requires the Windows Scripting Host (WSH) in order to work. If you disable WSH, the viral attachment will be rendered harmless. The virus attempts to drop an HTM file. The virus also checks the Internet Explorer Download directory for the presence of the file WinFAT32.exe. If that file does not exist, the virus randomly picks one of four websites and changes the registry to set it as the Start Page for Internet Explorer. The websites point to an EXE file, WIN-BUGSFIX.exe, which is then downloaded and the registry is modified to run the file on reboot. The virus copies itself to two places in the system directory where they are executed each time the computer reboots.

W32/Bugfix and VBS/Bugfix (Win 32 Executable File Virus and Visual Basic Script Worm):

This virus arrives in an empty e-mail with the subject "Microsoft Windows latest bugfix" as a file attachment called "bugfix.exe". On execution, it will infect all files in the Windows directory. A DOS box with the word "Adrenaline" may be visible for a short time. If mIRC is installed it will also infect the files in the mIRC download directory and drop a mIRC script to send the virus over IRC. If Microsoft Outlook is installed it drops and executes a VBS script (detected as VBS/Bugfix) which sends infected files to addresses in the Windows address book.

W32/Sysid (Win 32 Executable File Worm): This is an e-mail worm that is sent as an executable file attached to an e-mail with no subject or text. The attachment can have any of 99 different names.

If the attachment is run, the worm copies itself to:

C:\WINNT\SYSTEM32\SYSID.EXE
C:\WINNT\SYSID.EXE
C:\WINDOWS\SYSTEM\SYSID.EXE
C:\WINDOWS\SYSID.EXE

It also modifies the registry so that it is run whenever the PC is restarted. The worm creates, runs and then deletes a Visual Basic Script:

C:\WINDOWS\SYSTEM\WINVER.VBS

This script uses Outlook Express to send the worm to e-mail addresses picked randomly from the address book.

WM97/Doeii-A (Word Macro Virus): This is a Word macro virus that contains the following hidden comments:

'(c) 2000 by LiFEwiRE... writt3n 4g4inst my phucking 3x-sk3wl...
i c4n c0de ring0 p0ly P3 1nf3ct0rs, but w0rd is 4 b3tt3r
't4rg3t in w97... I kn0w this c0d3 w0n't spr34d Outzide sk3wl,
wh0 cares? Th3 b3tt3r!

There is a one in a hundred chance that upon infection the virus will either display a message box saying:

'w97.LAME by LiFEwiRE [www.shadowvx.org]
'...:LiFEwiRE:...'

or replace the document contents with:

'LiFEwiRE2000 - www.shadowvx.org'

and set the document password to:

'pietje'

WM97/Myna-X (Word 97 Macro Virus): This virus is a variant of the WM97/Myna-N Word macro virus. The replicating code contains the string "MYNAMEISVIRUS". The virus uses this string as a flag to tell whether it has already infected the document. If it is not present it will infect the document. The virus also turns off Microsoft's Word virus protection warning.

W97M/Marker.C (Word Macro Virus): This a macro virus designed to infect Microsoft Word 97 documents and templates. The global Word template (normal.dot) is infected after closing an infected document, and allows the virus to subsequently infect other clean Word documents. The virus overrides the macro warning system shipped with Word 97 in order to prevent users from disabling potentially infected macros.

WM97/Marker-FF (Word 97 Macro Virus): This is a variant of the WM97/Marker Word macro virus, which will cause compile errors upon replication. This should dramatically reduce its chances of successfully spreading. Whenever a document is closed there is a 1 in 3 chance of a File Summary box appearing on the screen with the author name set to Ethan Frome.

WM97/Nagem-A (Word 97 Macro Virus): This macro virus infects the global template and all documents opened thereafter. If the day of the month is greater than the 20th the virus will password protect infected documents with the word 'password'. It also randomly attempts to restart the computer when a document is closed. If the user tries to access Tools|Macro|Macros, a message box is displayed.

W97M/Thus.B (Word 97 Macro Virus): This is a macro virus that infects Word 97 documents and templates. The virus disables the macro warning system included with Word 97 and triggers its payload on December 13. This extremely destructive payload consists of deleting all the files stored in drive C of infected computers.

WM97/Tpro-A (Word 97 Macro Virus): This is a Word macro virus with no malicious payload.

WM97/Vmpck1-DV (Word 97 Macro Virus): This is a macro virus that attempts to set the label of drive C: to 'suca'. The virus has a 1 in 10 chance of replacing the text 'il' in Word documents with 'il cazzo duro.'

X97M_JAL.A (Excel 97 Macro Virus): This macro virus infects MS Excel files when infected documents are opened. It traps the macro AutoOpen to infect the system. If the system is not infected, it drops a file in XlStart folder (location may vary) named PJDAPKIR.XLS. It does not delete or destroy other files. When trigger conditions are met, the virus displays messages with Indonesian text.

X97M_LAROUX.EK (Aliases: LAROUX.EK, X97M/Laroux.EI) (Excel 97 Macro Virus): This non-destructive macro virus infects MS Excel 97 files. It is a variant of the Laroux family of viruses and the upper portion of the variant's virus module is composed of codes that appear to be user-created macros. However, the virus does not use these codes.

X97M_VCODE.A (Excel 97 Macro Virus): This Excel 97 macro virus infects the "ThisWorkbook" module every time the user opens a workbook or switches to another Window. A system infected with this virus prompts the user to save a file even when it is not modified.

XM97/Barisada-D (Excel 97 Macro Virus): This virus has been reported in the wild. It is a variant of the XM97/Barisada-C Excel macro virus, but does not contain the same payload of displaying message boxes. The virus stores its viral macros in the file KHM.XLS

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, starting with CyberNotes #2000-07, 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
Acid Shiver + Imacid	v1.0 + 1.0Mod	CyberNotes-2000-07
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
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
GIP		CyberNotes-2000-11
Golden Retriever	v1.1b	CyberNotes-2000-10
ICQ PWS		CyberNotes-2000-11
ik97	v1.2	CyberNotes-2000-07
InCommand	1.0-1.4, 1.5	CyberNotes-2000-09
Infector	v1.0 - 1.42, v1.3	CyberNotes-2000-07, CyberNotes-2000-09
iniKiller	v1.2 - 3.2, 3.2 Pro	CyberNotes-2000-09, CyberNotes-2000-10
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		Current Issue
Netbus.170		Current Issue
NetController	v1.08	CyberNotes-2000-07
NetSphere	v1.0 - 1.31337	CyberNotes-2000-09
Netsphere.Final		CyberNotes-2000-15
Nirvana / VisualKiller	v1.94 - 1.95	CyberNotes-2000-07
NoDesk		CyberNotes-2000-14
Omega		CyberNotes 2000-12

Trojan	Version	Issue discussed
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		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
SubSeven	V1.0-1.9b, v2.1+SubStealth, v2.2b1	CyberNotes-2000-07
Troj/Simpsons		CyberNotes-2000-13
Troj_Dilber		CyberNotes-2000-14
TROJ_PERSONAL_ID		Current Issue
TROJ_POKEY.A		Current Issue
TROJ_VBSWG		CyberNotes-2000-16
W32.Nuker.C		CyberNotes-2000-14
Win.Unabomber		CyberNotes-2000-14
WinCrash	Beta	CyberNotes-2000-12
Winkiller		CyberNotes 2000-12

Netbus.153: This is a Trojan horse that makes it possible to control an infected computer from a remote machine through an IP connection. Like other Trojans of this kind, Trojan/Netbus.153 is made up two separate programs: a server, which is run on the infected system, and a client, which runs on the malicious user's computer. The use of this Trojan allows a malicious user to perform a number of actions on the targeted computer, which include opening/closing the CD-ROM tray, changing mouse button functions, running programs, sending messages, keylogging, and removing confidential user information and file data.

Netbus.170: This Trojan works in basically the same way as Netbus.153 and offers malicious users identical possibilities.

TROJ_PERSONAL_ID: This a Windows Trojan, which attempts to e-mail documents from the "C:\My Documents " folder to other users. Once an infected file is executed, the Trojan displays a "Personal ID Number" generator. However, at the same time, the Trojan also drops infected copies of itself (filename: SYSID.EXE) into several directories. Once a system is rebooted, the Trojan activates and spams itself to other recipients in the Microsoft Outlook address book of the infected user.

TROJ_POKEY.A (Aliases: POKEY.A, Pokey, WIN32/Pikachu.32768.Worm, I-Worm.Pikachu): This is an Internet worm, which uses MAPI to propagate. It arrives as an executable with an icon like the Pokemon character, Pikachu. Once executed, it modifies Autoexec.bat such that files in certain directories are deleted when the computer is rebooted. It also sends out unsolicited e-mail messages to all addresses in the infected user's MS Outlook address book.