National Infrastructure Protection Center CyberNotes

Issue #2000-20 *October 9, 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 September 21 and October 5, 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.**

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Acme[1] Unix	Thttpd 2.16-2.19	A vulnerability exists because SSI does not properly filter certain escape sequences, which could let a malicious user view arbitrary files in known locations anywhere on the web server.	Upgrade to Thttpd 2.20 available at: http://www.acme.com/software/thttpd/thttpd-2.20.tar.gz	Thttpd Arbitrary World-Readable File Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[1] Securiteam, October 5, 2000.

Vendor/ Operating System	**Software Name**	**Vulnerability/ Impact**	**Patches/Workarounds/Alerts**	**Common Name**	**Risk***	**Attacks/Scripts**
Alabanza Corporation[2]	Alabanza Control Panel 3.0 and previous	A vulnerability exists in the automated domain administration software, which could let a remote malicious user add/modify domains in name servers of webhosting companies who are reselling for Alabanza.	A security patch has been applied to remedy the problem. Scripts that had been disabled to prevent this vulnerability have once again been restored to normal status.	Alabanza Control Panel Domain Modification	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
America Online[3] Windows 95/98/NT 4.0/2000	AOL Instant Messenger (AIM) version 4.1.2010	A Denial of Service vulnerability exists when handling file transfers with filenames containing '%s'.	No workaround or patch available at time of publishing.	AOL Instant Messenger Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Apache[4]	Apache versions 1.3.12 and prior	A vulnerability exists if a RewriteRule directive is expressed which could let a malicious user view arbitrary files.	A patch is currently being tested and will be part of the release of Apache 1.3.13. Until then, users should check their configuration files and not use rules that map to a filename.	Apache Rewrite Arbitrary File Disclosure	Medium/ **High** **(High if network security best-practices not in place.)**	Bug discussed in newsgroups and websites.
David Harris[5] Windows 95/98/NT 4.0/2000	Pegasus Mail 3.12	A buffer overflow vulnerability exists in the default configuration setup, which could allow a remote malicious website operator to gain copies of files on the users hard drive.	No workaround or patch available at time of publishing.	Pegasus E-mail File Forwarding	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Extent Technologies[6] Windows 95/98/NT 4.0/2000, Unix	RBS ISP 2.5, 2.63	A directory traversal vulnerability exists which could give a remote malicious user the ability to download files outside the scope of the HTML directory. This includes retrieving credit card details, usernames and passwords, and more.	Patch available at: http://www.extent.com/solutions/down_prod.shtml	RBS Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
GNU[7] Unix	glibc 2.1.3-10	A symlink vulnerability exists in LD_DEBUG_OUTPUT and LD_DEBUG, which could let a malicious user create a symbolic link pointing to a target file.	No workaround or patch available at time of publishing.	Glibc Symlink	Medium	Bug discussed in newsgroups and websites.

[2] Bugtraq, September 24, 2000.
[3] Bugtraq, October 3, 2000.
[4] Securiteam, October 3, 2000.
[5] Bugtraq, October 3, 2000.
[6] Bugtraq, September 21, 2000.
[7] Bugtraq, September 26, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
GNU[8] Unix	GNU Cfengine 1.5x, 1.5.3-4, 1.6a10	Several string format vulnerabilities exist in syslog() calls that could let a malicious user gain root access.	No workaround or patch available at time of publishing.	GNU Cfengine Format String Vulnerabilities	**High**	Bug discussed in newsgroups and websites.
Hewlett-Packard[9] Windows NT 4.x/ 2000, Unix	OpenView Network Node Manager 4.11 HP-UX, Solaris, 5.01 HP-UX, Solaris, 6.1	A buffer overflow vulnerability exists in the Ovalarmsrv Object Manager that could be remotely exploited by a malicious user.	Patch available at: http://ovweb.external.hp.com/cpe/patches/	OpenView Network Node Manager Ovalarmsrv	Low	Bug discussed in newsgroups and websites.
Hewlett-Packard[10] Windows NT 4.0/2000, Unix	OpenView Network Node Manager 6.1	An unchecked buffer overflow vulnerability exists which could allow a malicious user to execute arbitrary code.	HP OpenView Network Node Manager 6.1: http://ovweb.external.hp.com:80/cpe/cgi-bin/saveAs?productName=/home/ftp/pub/cpe/patches/nnm/6.1/	OpenView Node Manager SNMP Denial of Service	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Mandrake Soft[11] Unix	Linux Mandrake 7.0, 7.1	A vulnerability exists in the default X configuration, which could let a malicious user bypass the Xauthority mechanism and connect to any user's X session.	Update available at: http://www.linux-mandrake.com/en/ftp.php3.	Mandrake XSession Local Xauthority Bypass	Medium	Bug discussed in newsgroups and websites.
Microsoft[12] Windows NT 2000	Internet Information Server (IIS) 5.0	A vulnerability exists in the Web Distributed Authoring and Versioning (WebDAV) search implementation, which could let a remote malicious user view the root directory structure and all sub-directories.	Microsoft has released a knowledge base article detailing solutions for this issue available at: http://www.microsoft.com/technet/support/kb.asp?ID=272079	IIS 5.0 Indexed Directory Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[8] Bugtraq, October 2, 2000.

[9] Hewlett-Packard Company Security Bulletin, HPSBUX0009-122, September 27, 2000.

[10] Hewlett-Packard Daily Security Bulletins Digest, #00121, September 25, 2000.

[11] Linux-Mandrake Security Update Advisory, MDKSA-2000:052, October 2, 2000.

[12] @stake, Inc., A100400-1, October 4, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts

Microsoft[13]
Windows 95/98/NT 4.0/2000
	Microsoft Outlook 97.0, 98, 2000;
	Internet Explorer 4.0 for Windows 3.1, 95, 98, NT 3.51, NT 4.0;
	Internet Explorer 5.0 for Windows 95, 98, NT 4.0, 2000, 5.01, 5.5
		A vulnerability exists when viewing web pages or e-mail messages, which could allow a malicious user to execute arbitrary programs.	Unofficial Workaround (Georgi Guninski): Disable any active content in Internet Explorer or Outlook.	Internet Explorer / Outlook Express Com.ms.active X.Active XComponent Arbitrary Program Execution	**High**	Bug discussed in newsgroups and websites. Exploits have been published.
						Vulnerability has appeared in the Press and other public media.

Microsoft[14] Windows 95/98/NT 4.0/2000	Outlook Express 5.0, 5.01, 5.5; Internet Explorer 5.0 for Windows 95, 98, NT 4.0 & 2000, 5.01, 5.5	A vulnerability exists if Active Scripting is enabled, which could let a malicious user read local and UNC files.	No workaround or patch available at time of publishing. Temporary Workaround (Georgi Guninski): Disable Active Scripting.	Internet Explorer / Outlook Express GetObject() File Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[15] Windows 95/98/NT 4.0/2000	Windows Media Player 7	A security vulnerability exists in the method which Media Player 7 handles OCX controls (ActiveX containers) in embedded RTF e-mail messages, which could let a malicious user crash RTF-enabled mail clients such as Microsoft Outlook and Outlook Express.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq00-068.asp	Windows Media Player "OCX Attachment" Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Microsoft[16] Windows NT 2000	Windows NT 2000	A security vulnerability exists in the Simplified Chinese IMEs (Input Method Editor) which could allow a malicious user to gain complete control over an affected machine.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq00-069.asp **Note:** Only the Simplified Chinese version of Windows 2000 is affected by default. Customers running any other language version of Windows 2000 only need to take action if they installed a Simplified Chinese IME during system setup.	Windows NT 2000 Simplified Chinese IME State Recognition	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[13] Georgi Guninski Security Advisory #23, October 5, 2000

[14] Georgi Guninski Security Advisory #22, September 26, 2000.

[15] Microsoft Security Bulletin, MS00-068, September 26, 2000.

[16] Microsoft Security Bulletin, MS00-069, September 29, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft[17] Windows NT 4.0/2000	Windows NT 4.0 Workstation, Server, Enterprise Edition, Terminal Server Edition; Windows 2000 Professional, Server, Advanced Server, Datacenter Server	Several security vulnerabilities exist in the implementations of LPC (Local Procedure Call) and LPC ports ranging from a Denial of Service to privilege elevation.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq00-070.asp	Microsoft Multiple LPC and LPC Ports Vulnerabilities	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[18] Windows 95/98/NT 4.0/2000	Word 97, 2000	A security vulnerability exists in Word 2000 and 97, which could allow a malicious user to run arbitrary code on a victim's computer without their approval. If an Access database is specified as a data source via DDE in a Word mail merge document, macro code can run without the user's approval when the user opens that document.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq00-071.asp	Word Mail Merge	**High**	Bug discussed in newsgroups and websites.
Multiple Vendors[19] Unix	FreeBSD 3.2-3.5, 4.0; NetBSD 1.4-1.4.2; OpenBSD 2.3-2.7	A string format vulnerability in the pw_error() function exists that can allow a local malicious user to gain root privileges.	**FreeBSD:** Upgrade to FreeBSD 4.1. http://www.freebsd.org/support.html#cvs **NetBSD:** A fix should be available soon via anonymous CVS. **OpenBSD:** ftp://ftp.openbsd.org/pub/OpenBSD/patches/2.7/common/025_pw_error.patch	Multiple Vendor BSD Libutil Pw_error() Format String	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Multiple Vendors[20] Unix	Helsinki University of Technology SSH 1.2.14-1.2.27; OpenSSH 1.2, 1.2.3	A vulnerability exists in rcp, which could allow a remote malicious user to overwrite files.	No workaround or patch available at time of publishing.	SSH File Create/ Overwrite	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.

[17] Microsoft Security Bulletin, MS00-070, October 3, 2000.
[18] Microsoft Security Bulletin, MS00-071, October 5, 2000.
[19] eSecurityOnline.com, October 4, 2000.
[20] Bugtraq, September 29, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Multiple Vendors[21] Unix	Lawrence Berkeley National Laboratory's traceroute 1.4a5; Debian potato; RedHat 6.0, 6.2; Caldera 2.4; Mandrake 7.0; Conectiva Linux 4.0, 4.0es, 4.1, 4.2, 5.0, 5.1; Solaris 2.5.1	A heap overflow vulnerability exists which could let local malicious users crash the application and possibly execute arbitrary code.	Contact your vendor for upgrade or patch.	Multiple Vendor Traceroute Heap Corruption	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Multiple Vendors[22] Unix	NetBSD 1.4-1.4.2; OpenBSD 2.3-2.7	An eeprom format string vulnerability exists which could let a local malicious user gain root access.	Upgrade to OpenBSD 2.8. http://www.openbsd.org/ NetBSD has patched this vulnerability and the changes/new version of eeprom is available via anonymous CVS. http://cvsweb.netbsd.org/bsdweb.cgi/	Multiple Vendor BSD eeprom Format String	**High**	Bug discussed in newsgroups and websites.
Multiple Vendors[23] Windows 95/98/NT 4.0/2000, Unix	Netscape Communicator 4.0, 4.5, 4.51, 4.6, 4.61, 4.7, 4.72; Microsoft Internet Explorer 5.01, 5.5	A Denial of Service vulnerability exists if a remote malicious user assigns a long string to the argument 'type=password'.	No workaround or patch available at time of publishing.	Multiple Vendor 'Type= password' Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Multiple Vendors[24, 25] Unix	GNOME GnoRPM 0.94 and earlier; Conectiva Linux 4.0, 4.0es, 4.1, 4.2, 5.0, 5.1	A vulnerability exists in the way tmp files are handled which could allow a local malicious user cause an arbitrary file to be overwritten by the root user.	A new release of GnoRPM (0.95.1) is available at: ftp.gnome.org/pub/GNOME/stable/sources/gnorpm/gnorpm-0.95.1.tar.gz **Conectiva:** ftp://atualizacoes.conectiva.com.br/ **MandrakeSoft:** http://www.linux-mandrake.com/cooker/	GnoRPM Arbitrary File Overwrite	**High**	Bug discussed in newsgroups and websites.

[21] Securiteam, October 1, 2000.
[22] OpenBSD Security Advisory, October 4, 2000.
[23] eSecurityOnline.com, October 2, 2000.
[24] eSecurityOnline.com, October 4, 2000.
[25] Conectiva Linux Security Announcement, October 3, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Multiple Vendors[26, 27, 28] Unix	Caldera eDesktop 2.4, eServer 2.3; OpenLinux Desktop 2.3, eBuilder 3.0; RedHat Linux 7.0; NetBSD 1.4-1.4.2; OpenBSD 2.7; Immunix OS 6.2	A format string vulnerability exists in the LPRng printer daemon, which could allow a remote malicious user to obtain root privileges.	**Caldera:** ftp://ftp.calderasystems.com/pub/updates/ **NetBSD:** http://cvsweb.netbsd.org/bsdweb.cgi/basesrc/usr.sbin/lpr/lpd/printjob.c **RedHat:** ftp://updates.redhat.com/7.0/ **ImmunixOS:** http://immunix.org:8080/ImmunixOS/6.2/updates/RPMS/lpr-0.50-7_StackGuard.i386.rpm	Multiple Vendor LPRng User-Supplied Format String	**High**	Bug discussed in newsgroups and websites.
OpenBSD[29] Unix	OpenBSD 2.3-2.7.3	A fstat format string vulnerability exists, which could let a malicious user inherit the privileges of the running fstat program.	OpenBSD 2.8 is not vulnerable. http://www.openbsd.org/	Multiple Vendor BSD fstat Format String	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
OpenBSD[30] Unix	OpenBSD 2.0-2.6	A Denial of Service vulnerability exists due to the lack of limits on the storage of pending ARP requests.	This vulnerability has been fixed in OpenBSD 2.7 available at: http://www.openbsd.org/security.html	OpenBSD Pending ARP Request Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
OpenBSD[31] Unix	OpenBSD 2.3-2.7	A format string vulnerability exists in photurisd, which could let a malicious user execute arbitrary code as root.	This has been corrected in OpenBSD 2.8. http://www.openbsd.org/	OpenBSD photurisd Format String	**High**	Bug discussed in newsgroups and websites.
Palm[32]	Palm OS 3.5.2	A weak encryption implementation vulnerability exists which could let a local malicious user retrieve the password.	No workaround or patch available at time of publishing. Temporary Workaround (@stake, Inc.): Enable the Turn off and Lock Device feature or implement a third party encryption application.	Palm OS Weak Encryption	Medium	Bug discussed in newsgroups and websites. Exploit scripts have been published.
SCO[33] Unix	Unixware 7.0	A vulnerability exists in the search CGI script provided for SCOhelp, which could allow a remote malicious user to execute arbitrary code with privileges of user "nobody."	Workaround supplied by SCO is located at: http://www.core-sdi.com/advisories/scohelp_http_advisory.htm	Unixware SCOhelp HTTP Server Format String	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[26] Caldera Systems, Inc. Security Advisory, CSSA-2000-033.0, September 25, 2000.
[27] Red Hat, Inc. Security Advisory, RHSA-2000:065-04, October 4, 2000.
[28] Bugtraq, September 26, 2000.
[29] Bugtraq, October 4, 2000.
[30] Bugtraq, October 5, 2000.
[31] OpenBSD Security Advisory, October 4, 2000.
[32] @stake, Inc Security Advisory, A092600- 1, September 27, 2000.
[33] CORE SDI Inc, CORE-092700, September 27, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Slashcode[34]	Slashcode 1.0.8 and previous	A default admin password vulnerability exists, which could let a malicious user gain access to an admin account. This could enable him/her to execute arbitrary code by inserting a block as admin, and potentially gain shell access or access to the database.	Upgrade available at: http://slashcode.com/	Slashcode Default Admin Password	**High**	Bug discussed in newsgroups and websites.
SmartWin Technology[35] Windows NT 4.0/2000	CyberOffice Shopping Cart 2.0	A vulnerability exists within the default installations, which could let a malicious user gain access to the database that holds information on customer orders, details and credit card information.	Workaround: 1) Use IIS Management Console to disable the Read permission on the folder (done by ISP). 2) Use FrontPage Explorer to disable the folder from being browsed (done by the Web master). 3) Move the database to /fpdb (the database folder used by newer versions of FrontPage).	CyberOffice Shopping Cart Client Information Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
SmartWin Technology[36] Windows NT 4.0/2000	CyberOffice Shopping Cart 2.0	A vulnerability exists in the order form, which could let a malicious user modify the form with arbitrary values and then resubmit it to the target server.	Workaround provided by SmartWin Technology: Under Global / System Settings of the Shop Manager, you can set Authorized URL(s) to specify the Web sites (folders) where the shopping pages reside.	CyberOffice Shopping Cart Price Modification	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
SuSE[37] Unix	Linux 6.3, 6.4	A vulnerability exists in the Apache configuration that is shipped with SuSE which could let a remote malicious user browse the /doc/ directory.	SuSE recommends making the following changes to your httpd.conf file: <Directory /usr/doc/packages> order deny, allow allow from localhost deny from all Options Indexes FollowSymLinks +Includes AllowOverride None </Directory>	Linux Installed Package Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
TalentSoft[38] Unix	Web+ Application Server (Linux) 4.6	A vulnerability exists when the default example scripts are installed which could let a remote malicious user execute/read any file that the Web+ user has access to.	Vendor is in the process of modifying the Web+Ping example script. Until this is done, TalentSoft recommends disabling the webrun command in the Web+ server administration area.	Web+ Example Script File Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[34] Slashcode SA-00:00, September 29, 2000.
[35] Delphis Consulting Plc Security Team Advisories, DST2K0035, September 22, 2000.
[36] Delphis Consulting Plc Security Team Advisories, DST2K0036, September 22, 2000.
[37] Bugtraq, September 21, 2000.
[38] Delphis Consulting Plc Security Team Advisories, DST2K0042, September 26, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts

TalentSoft[39]
Windows 95/98/NT 4.0, Unix
	Web+ Client 4.6;
	Web+ Monitor 4.6;
	Web+ Server 4.6
		Multiple disclosure vulnerabilities exist which could allow a remote malicious user to gain sensitive information.	Upgrade available at:
			http://www.talentsoft.com
				Web+ Multiple Disclosure Vulnerabilities	Medium	Bug discussed in newsgroups and websites.
						Exploit has been published.

University of Washington[40] Unix	Pine 4.21	A buffer overflow vulnerability exists when a particularly formed argument is sent in the "From:" e-mail header, which could let a remote malicious user cause a Denial of Service or possibly run arbitrary code.	No workaround or patch available at time of publishing.	Pine "From:" Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
WebTeacher[41] Windows 95/98/NT 4.0, Unix	WebData 2.2 and previous	A vulnerability exists which makes it possible to import any file from the file system to which the Webserver user has access into the WebData database.	Patch available at: http://webteacher.com/webdata/	WebTeacher WebData File Import	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
WinGate[42] Windows NT	WinGate Home/ Standard/Pro 4.0.1	An undetected Denial of Service vulnerability exists when a remote malicious user sends an abnormal string to the Winsock Redirector Service. This could be a potential local Denial of Service.	Upgrade available at: http://wingate.deerfield.com/beta	Winsock Redirector Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
WQuinn[43] Windows NT 4.0/2000	QuotaAdvisor 4.1	Local users can bypass the quotas set by the administrator, and store large files on the local file system.	No workaround or patch available at time of publishing.	WQuinn QuotaAdvisor 4.1 Disk Quota Bypass	Low	Bug discussed in newsgroups and websites. Exploit has been published
XFree86[44] Unix	XFCE 3.5.0-3.5.1	A vulnerability exists within the /etc/X11/xfce/xinitrc file which could let a malicious user gain elevated privileges.	Upgrade to XFCE 3.5.2. available at: http://www.xfce.org/download.html	XFCE Local Xauthority Bypass	Medium	Bug discussed in newsgroups and websites.

[39] Delphis Consulting Plc Security Team Advisories, DST2K0032, September 19, 2000.
[40] eSecurityOnline.com, September 26, 2000.
[41] Delphis Consulting Plc Security Team Advisories, DST2K0039, September 26, 2000.
[42] Blue Panda Vulnerability Announcement, October 2, 2000.
[43] Delphis Consulting Plc Security Team Advisories, DST2K0037, September 28, 2000.
[44] eSecurityOnline.com, October 4, 2000.

*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 September 22 and October 5, 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, 44 scripts, programs, and net-news messages containing holes or exploits were identified.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
October 5, 2000	33_su.c	Script which exploits the Immunix OS stackguard glibc + su + msgfmt vulnerability.
October 5, 2000	Exiscan-0.6.tar.gz	An e-mail virus scanner which works together with the Exim MTA and McAffee's uvscan or Trend Micro's vscan.
October 5, 2000	Obsd_fun.c	Denial of Service exploit script for OpenBSD 2.6.
October 5, 2000	Xlockx.C	Script that exploits the OpenBSD 2.6 and 2.7 xlock local root format string vulnerability.
October 4, 2000	Bsdchpass-exp.c	Script which exploits the Multiple Vendor BSD Libutil Pw_error() Format String vulnerability.
October 4, 2000	Cached_feed.cgi.txt	Exploit URL for the cached_Feed.cgi v1.0 from moreover.com vulnerability.
October 4, 2000	Easy-adv-exploit.pl	Perl script which exploits the Easy Advertiser v. 2.04 Remote vulnerability.
October 4, 2000	k2-caddis-fstat.c	Script which exploits the Multiple Vendor BSD Fstat Format String vulnerability.
October 4, 2000	Obsd_fstat.c	Exploit script for the OpenBSD 2.7 local root /usr/bin/fstat + libutil vulnerability.
October 4, 2000	Scp.hole.txt	Proof of concept exploit for the Scp replacement vulnerability.
October 4, 2000	Thttpd-219.txt	Exploit example for the Thttpd 2.19 Arbitrary World-Readable File Disclosure vulnerability.
October 3, 2000	Bsd_chpass.c	Exploit for the /usr/bin/chpass local EDITOR variable format string vulnerability.
October 3, 2000	Inebriation.c	Script which exploits Linux/x86 /bin/su + locale libc vulnerability.
October 3, 2000	Openssh.reverse.tgz	Openssh-Reverse is a patched OpenSSH which goes in reverse, allowing outside users to connect to machines behind NAT firewalls.
October 3, 2000	Sara-3.2.2.tar.gz	A security analysis tool based on the SATAN model.
October 2, 2000	Saint-3.0.beta2.tar.gz	A security assessment tool based on SATAN.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
October 2, 2000	Wgate401.pl	Perl script for the Wingate Redirecter Service String vulnerability.
September 30, 2000	Bfbtester-2.0b-20000709.Tar.Gz	A utility for doing quick, proactive security checks of binary programs by performing checks of single and multiple argument command line and environment variable overflows.
September 30, 2000	Siden-0.1.0.tar.gz	A distributed network discovery tool that allows you to simulate coordinated/distributed network probes by a group of malicious users against one or many target machines.
September 29, 2000	**Tpi.pl**	**Perl script which exploits the SSH File Create/ Overwrite vulnerability.**
September 28, 2000	12250.c	Exploit script for the IMAPrev1 12.2xx lsub vulnerability.
September 28, 2000	Axur.c	Script which exploits the Q-POP 2.53 Remote Overflow vulnerability.
September 28, 2000	Cxterm.c	Local exploit for the cxterm 5.1 vulnerability.
September 28, 2000	Ezbounce.c	Ezbounce version (0.85.2 and probably others) remote overflow exploit for RedHat 6.0.
September 28, 2000	Fi.sh	Exploit script for FlagShip /usr/bin/FS serial vulnerability.
September 28, 2000	Innd.c	Script which exploits the INND/NNRP remote root overflow vulnerability.
September 28, 2000	**Linstatex.c**	**Remote root overflow for Linux rpc.statd SM_UNMON_ALL vulnerability.**
September 28, 2000	Qpop3b.c	Script which exploits the QPOP 3.0beta AUTH remote root stack overflow vulnerability.
September 28, 2000	Sco-httpx.c	Script which exploits the SCO Unix httpd Remote Exploit vulnerability.
September 28, 2000	Tsql.c	Script which exploits the MSQL local overflow vulnerability.
September 28, 2000	**Wu30.c**	**Remote root exploit script for wu-ftpd on SCO Unix.**
September 28, 2000	**Wu-lnx.c**	**Script which exploit the Linux wu-ftpd - 2.6.0(1) vulnerability.**
September 28, 2000	Xloadx.c	Script which exploits the SCO 5.0.4 local overflow vulnerability.
September 28, 2000	Xsunsploit.c	Script which exploits the Solaris 7 Xsun(suid) local overflow vulnerability.
September 27, 2000	Brwgate-dos.c	Denial of Service exploit script for the NetcPlus BrowseGate vulnerability.
September 27, 2000	**Notsync.zip**	**Script which exploits the Palm OS Weak Encryption vulnerability.**
September 27, 2000	**Palmcrypt.zip**	**Script which exploits the Palm OS Weak Encryption vulnerability.**
September 27, 2000	Pine421.txt	Proof of Concept exploit for the Pine 4.21 C-client Denial of Service vulnerability.
September 27, 2000	Smurftools.tar.gz	An ICMP Source Address spoofing utility.
September 27, 2000	Sqlpoke.zip	An NT based tool that locates MSSQL servers and tries to connect with the default 'sa' account. A list of SQL commands is executed if the connection is successful.
September 27, 2000	Tcpip_lib2.zip	A library for Windows 2000 which allows arbitrary packet creation.
September 26, 2000	**Pinebuf.c**	**Script which exploits the Pine "From:" Buffer Overflow vulnerability.**
September 26, 2000	wmpoutlook.zip	Exploit for the Windows Media Player "OCX Attachment" vulnerability.
September 23, 2000	Cisco.tar.gz	Denial of service exploit for the CiscoSecure ACS 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:

- **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."**
- A DDoS agent named "trinity v3 by self" was installed on about 20 Linux machines on a university network via an rpc.statd exploit.
- 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.
- 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.
- An increase in scans on port 21 (when WuFTPD 2.5.0 was shown vulnerable).
- 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:

- **Multiple vulnerabilities have been published concerning OpenBSD.**
- **The CERT Coordination Center has issued a new policy with respect to the disclosure of vulnerability information. For more information please see advisory at: http://www.cert.org/faq/vuldisclosurepolicy.html.**
- Mobile Operating Systems have become the latest target of virus writers and hackers.
- 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.

Viruses

PE_CRAZYPC.30030 (Aliases: CRAZYPC.30030, CRAZYPC, Win32.Hllo.Zmk.30030, Win32.HLLO.ZMK.b) (File Infector Virus): This destructive Windows executable virus overwrites all .exe files found in the Windows directory with its own codes. It has seven different triggers and payloads. If the current system minute is 30, a bitmap is displayed on the active window. If the day of the week is Monday/Wednesday/Fri, the computer reboots, if MS Outlook is launched. If the day of the week is Sunday/Tuesday/Thursday/Saturday, the computer reboots if Internet Explorer is launched. If Norton Antivirus is launched, the system reboots. If that day of the week is Friday and the date is 13, the virus adds a line to the AUTOEXEC.BAT, which causes the C:\ drive to be formatted and the system reboots. If the day, the hour, the minute, and the second are 13, a message box is displayed. Every hour the CD-ROM drive is opened and the audio sound is turned off.

PE_ILUVBRITNEY (Aliases: ILUVBRITNEY, WIN32.ILOVEBRITNEY, ILOVEBRITNEY) (File Infector Virus): This virus mimics a freeware software, IloveBritney. It is a direct-action infector that overwrites .exe files upon execution and modifies the registry so that it is executed at every start up. The virus also modifies the start page of Internet Explorer and is capable of propagating via MAPI by using contacts in the address book of the infected user. If the virus is unable to propagate via MAPI, it displays a message box and deletes all files in the root directory of drive C:\. If certain trigger conditions are met, the virus displays certain message boxes and for some shuts down Windows.

PE_MORIDIN.A (Aliases: MORIDIN.A) (Polymorphic Virus): This polymorphic direct infector Windows virus, infects EXE and SCR files in the current directory. It contains a VB Script worm (VBS_ MORIDIN.A), an IRC worm (IRC_ MORIDIN.A), and a back Trojan (TROJ_ MORIDIN.A).

Spanska.4250 (Polymorphic, Encrypted Virus): This virus uses stealth techniques and infects certain .exe and .com files. When an infected program is run, the virus becomes memory resident and the "Spanska 97" appears on the screen of the infected computer.

VBS_Tune.E (Aliases: TUNE.E, VBS/Cod.C) (Visual Basic Script Worm): This worm spreads via e-mail and mIRC. It sends a copy of itself to all lists in the infected user's address book. The worm also sends a copy of itself to the users in mIRC disguised as "A List of Hacked Porno site passwords.” If the current system date is April 20 or December 25, the worm deletes all files and subdirectories in the current directory.

W32/Apology-B (Aliases: W32/MTX@MM, I-Worm.MTX, W32/MTX) (Win 32 Executable File Virus): This virus has been reported in the wild and it is a variant of the W32/Apology virus which behaves in the same way.

W32/Msinit (Internet Worm): This worm spreads through open network shares like the VBS/Netlog worm. It scans random IP address over NetBIOS for computers that have shares named "C" and a Windows folder called "Windows.” When it finds one, it copies itself and the files "dnetc.exe" and "dnetc.ini" to the "C:\windows\system" folder of the remote computer. The file "dnetc.exe" is an encryption-cracking program from www.distributed.net. When the virus finds a computer with an open share, it copies itself directly to the unprotected computer, and modifying the registry/win.ini so the worm and encryption-cracking program runs without any user intervention.

W95/Luna.2724 (Word 95 Macro Virus): This virus infects executable files in Windows 95. On the 15th of every odd month (January, March etc.) the virus changes the case of all letters in all '.txt' files opened. Every time the file is opened, the letters will be changed again. W95/Luna.2724 does not infect files beginning with 'AV', 'av' 'DR', 'dr', 'F-', 'f-', 'AN', 'an', 'CE', 'ce', 'PI', 'pi', 'TB', or 'tb' that are part of antivirus programs.

W97/Arbind2000 (Word 97 Macro Virus): This virus disables the macro virus protection in Word documents and a warning feature Word displays when NORMAL.DOT global template is saved or when users attempt to convert a document.

W97M/Chameleon.A (Word 97 Macro Virus): This polymorphic Word 97/2000 macro virus contains the module "ThisDocument." When the virus is run, it performs the following tasks:

- Writes the key "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\MVP" = "Enabled by Total Konfuzion"
- Checks for the presence of this key value and tries to infect if absent
- Disables Microsoft's macro virus protection
- Disables save prompt for the Normal.DOT template
- Disables the confirm older version conversion prompt
- Writes the virus code source to "C:\Windows\System\Chameleon.dll" and uses this file as a reference to insert the code into other files
- Write "C:\Windows\Start Menu\Programs\Startup\Chameleon.vbs" which displays the following message in a dialog box entitled:
  "W97M/Chameleon:"
  "Greetz from Chameleon :)"

W97M/CronoMessage (Word 97 Macro Virus): This virus infects Microsoft Word 97 documents and the NORMAL.DOT global template used by this program. It disables the 'macro' option in the 'Tools' menu and also displays a dialog box (chosen at random from 15 different possibilities) when closing an infected document provided that the system date stamp shows a date after April 22, 2000. A macro called 'Document_Close' is executed every time the user closes an infected document.

WM97/Metys-F (Word 97 Macro Virus): This virus has been reported in the wild. It is a minor variant of the WM97/Metys-D Word macro virus that spreads but has no payload.

W97M/Steroid.B (Word 97 Macro Virus): When this virus is activated it prevents access to the features 'macro' 'templates' and 'options' in the Tools menu. When the user tries to access 'About' in the Help menu, different dialog boxes appear.

W97MWalker.E (Word 97 Macro Virus): This virus disables the macro virus protection in Word documents. It also disables a warning feature Word displays when the NORMAL.DOT global template is saved or when users attempt to convert a document.

WM97/Checkup-A (Word 97 Macro Virus): This is a simple macro virus that has no payload.

WM97/Plant-A (Word 97 Macro Virus): On January 1st, this virus will display the message:
"Happy NewYear ! You are infected by Plant.Virus. Don't panic, i'm KILL you."

WM97/Thus-AM (Word 97 Macro Virus): This is a macro virus which may attempt to delete all the files from drive C: on December 13th.

WM97/Thus-BG (Word 97 Macro Virus): This virus is a variant of the WM97/Thus-A Word macro virus. However, this variant does not contain a data-damaging payload.

W97M/Title (Word 97 Macro Virus): This virus propagates by infecting Word Documents in Microsoft Word 97/2000. It consists of the module "ThisDocument." When an infected document is opened the following events take place:

- Microsoft's macro virus protection is turned off
- When the document is closed, the virus code is written to the global "Normal.DOT" template
- On May 3, June 6, and July 30, the document becomes password protected with a randomly generated password

XM97/Ready-A (Excel 97 Macro Virus): This is an Excel macro virus which changes the Excel Status bar to read "XM97.ReadyZ," and attempts to delete files from certain anti-virus products. It drops the infected file PERSONAL.XLS into the XLSTART directory to ensure that the virus is run every time Excel is opened.

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
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

Trojan	Version	Issue discussed
Netbus.153		CyberNotes 2000-16
Netbus.170		CyberNotes 2000-16
NetSphere	v1.0 - 1.31337	CyberNotes-2000-09
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**	**Current Issue** 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		**Current Issue**
TROJ_BUTANO.KILL		CyberNotes-2000-19
Troj_Dilber		CyberNotes-2000-14
TROJ_IGMNUKE		**Current Issue**
TROJ_KILLME		**Current Issue**
TROJ_PERSONAL_ID		CyberNotes 2000-16
TROJ_POKEY.A		CyberNotes 2000-16
TROJ_SCOOTER		CyberNotes-2000-19
TROJ_SPAWNMAIL.A		CyberNotes-2000-18
TROJ_VBSWG		CyberNotes-2000-16
Trojan/ICQ		**Current Issue**
Trojan/PSW.StealthD		CyberNotes-2000-19
Trojan/Varo31		CyberNotes-2000-19
W32.Nuker.C		CyberNotes-2000-14
Win.Unabomber		CyberNotes-2000-14
WinCrash	Beta	CyberNotes-2000-12
Winkiller		CyberNotes 2000-12

TROJ_BATMAN: This is a non-polymorphic, non-memory resident Windows executable Trojan which is capable of destroying data on the hard disk when it is run on Windows 9x. When run on Windows 2000, the Trojan displays a message box.
Trojan/ICQ: This a Win 32 Trojan which establishes a remote connection from one computer (attacker) to another (victim). In order to this it opens a port and waits for a connection to be made. The main symptom of the presence of this Trojan is the change of name of the file 'ICQ.EXE' to 'ICQ2.EXE'.

TROJ_IGMNUKE (Aliases: IGMNUKE, Nuker.IGMNuke): This Trojan sends packets of data to any remote location. It can be used to flood a specific network and produce network traffic.

TROJ_KILLME (Aliases: KILLME): This Trojan is a tool that can be used to flood a specified IP address.

W32.HLLW.Qaz.A (Aliases: Troj/Qaz, W32/QAZ.worm, Qaz.Worm, W32.HLLW.Qaz (gen)): W32.HLLW.Qaz.A was renamed from Qaz.Trojan on August 10, 2000. As of September 14, there are at least four variants of the original virus. The Trojan has been reported in the wild. It is a companion virus that can spread over the network and also has a backdoor that lets a remote malicious user connect to and control the computer via port 7597.

When the virus is launched it searches available network drives for copies of notepad.exe and renames them to note.com. It then copies itself (virus code) across the network to the infected computers as notepad.exe. Each time notepad.exe is executed it runs the virus code and the original notepad (renamed to note.com) to avoid being noticed. It also modifies the following system registry entry to execute itself every time the system is started:

```
HKLM\Software\Microsoft\Windows\CurrentVersion\Run
"StartIE"="C:\WINDOWS\NOTEPAD.EXE qazwsx.hsq"
```

W32.HLLW.Qaz.A enumerates through the network neighborhood to find computers to infect. When it finds a computer, it infects it by searching for notepad.exe and making the same modifications (renaming notepad.exe to note.com). It does not require any mapped drives to infect other computers. Once the computer is infected, the computer's IP address is e-mailed to the virus author automatically. The backdoor payload in the virus uses WinSock and awaits connections. This lets a malicious user connect to the infected computer and gain access to the computer.