National Infrastructure Protection Center
CyberNotes

Issue #18-99 *September 1, 1999*

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, hacker exploit scripts, hacker 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 13 and August 27, 1999. The table provides the hardware/operating system, equipment/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 from previous issues of CyberNotes are listed in bold. New information contained in the update will appear as red and/or italic text.**

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
3Com[1]	HiPer ARC software (4.0 - 4.2.29)	3Com's (Formerly US Robotics') HiPerARC is vulnerable to a Denial of Service attack by a remote user with access to the administrative console.	Workaround can be found on the 3Com Knowledge Base (3KB) at: http://knowledgebase.3com.com/ under document ID: 2.0.2107762.2279004	Denial of Service Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit script has been published.

[1] Bugtraq, August 12, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
AOL[2]	Instant Messenger (AIM)	A buffer overflow in AIM was recently discovered and is allegedly used by AOL to determine whether the client requesting to logon into the AOL system is a genuine AOL Instant Messenger client or any other client (such as Microsoft's MSN Messenger). AOL has denied the allegations.		Buffer Overflow Vulnerability	Medium	Bug discussed in newsgroups and websites. Exploit has been published. Buffer overflow allegedly used by AOL has appeared in the Press.
BSDi[3]	BSDi 4.0.1 Symmetric Multi-processing (SMP)	When a call to fstat is make during high CPU usage, it is possible to cause BSDi to stop responding and 'lock up'.	No workaround or patch available at time of publishing.	SMP Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit is simple to produce and requires no script.
Checkpoint Software[4] ***Update from CheckPoint***[5]	**Firewall 1.3.0 & 1.4.0**	**Firewall-1 can be shutdown by filling its connection table. This is easily done in about 15 minutes with most port scanners. This effectively causes a DoS condition with Firewall-1 defaulting to a 'failed closed' state. Each site should access whether systems protected by Firewall-1 are mission critical.**	**No vendor supplied patch or workaround available at time of publishing.** ***CheckPoint has developed INSPECT code changes that provides a solution for this type of attack, which can be download at:*** http://www.checkpoint.com/techsupport/alerts/ackdos.html	**Table Saturation DoS Vulnerability**	**High (Due to the potential systems affected)**	**Bug discussed in newsgroups and websites. Exploit has been published.**
Debian Linux[6]	GNU/Linux 2.1	An unchecked logging facility to /tmp/log allows deleting arbitrary, root-owned files by any user who has write access to /tmp.	Recommend that you upgrade your smtp-refuser package which can be found at: (Select the smtp patch for your architecture) Debian GNU/Linux alias slink ftp://ftp.debian.org/debian/dists/proposed-updates/ Debian GNU/Linux unstable alias potato ftp://ftp.debian.org/debian/dists/unstable/main/	SMTP-Refuser Vulnerability	**High**	Bug discussed in newsgroups and websites.

[2] Bugtraq, August 16, 1999.
[3] Bugtraq, August 17, 1999.
[4] Bugtraq, July 29, 1999.
[5] Bugtraq, August 5, 1999.
[6] Bugtraq, August 20, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Debian Linux[7]	Debian GNU/Linux 2.1 (other Linux distributions may be affected as well); Mandrake 6.0	Xmonisdn is an X applet that shows the status of the ISDN links. It contains a security hole that could allow execution of applications as root.	Patch available at: http://www.debian.org/security/1999/19990807 Mandrake 6.0: http://www.linux-mandrake.com/en/fupdates.php3	Xmonisdn Vulnerability	**High**	Bug discussed in newsgroups and websites.
Debian Linux[8]	GNU/Linux 2.1 alias slink;	If a malicious user has created a symbolic link to /tmp before upgrading to man2html, system files can be overwritten.	It is recommended that you upgrade your man2html package as soon as possible. Linux 2.1 alias slink: (Select the man2html_1.5-18.1 and the architecture for your system) ftp://ftp.debian.org/debian/dists/proposed-updates/ Linux unstable alias potato: (Select the man2html_1.5-19 and the architecture for your system) ftp://ftp.debian.org/debian/dists/unstable/main/source/doc/	Man2html Vulnerability	Medium / Low	Bug discussed in newsgroups and websites.
Debian Linux[9]	Linux 2.1 alias slink; Linux unstable alias potato	Trn comes with a newsgroups shell script that uses a hardcoded filename in /tmp as temporary storage. This could be exploited to overwrite arbitrary files.	We recommend you upgrade your man2html package as soon as possible. Please select the trn_3.6-9.31 patch for your architecture. Linux 2.1 alias slink ftp://ftp.debian.org/debian/dists/proposed-updates/ Linux unstable alias potato Please select the binary architecture for your system; select 'News'; then select 'Trn_3.6-9.4.deb'. http://security.debian.org/dists/unstable/updates/	Insecure Trn Vulnerability	Medium	Bug discussed in newsgroups and websites.
FreeBSD, FreeBSD 3.2[10] (Same vulnerability as RedHat Linux below)	Window Maker 0.20.1-3, 0.52-2, 0.53, 0.60	A number of buffer overflow vulnerabilities exist in WindowMaker, which could allow arbitrary code to be executed.	No workaround or patch available at time of publishing.	Window Maker Buffer Overflow Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Hughes Technology[11]	Mini SQL 2.0, 2.0.10	A CGI vulnerability exists that allows a malicious attacker to bypass system security settings and read any local file under the Apache HTML tree.	Upgrade to version 2.0.11 located at: http://www.Hughes.com.au/	Mini SQL Vulnerability	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[7] Bugtraq, August 14, 1999.

[8] Securiteam, August 23, 1999.

[9] Bugtraq, August 19, 1999.

[10] Bugtraq, August 22, 1999.

[11] Bugtraq, August 17, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
IBM[12]	IBM's C Set ++ for AIX, Versions 2 & 3	A vulnerability exists in the Source Code Browser, which allows local and remote users to gain root access.	IBM C Set ++ for AIX versions 2 and 3 are no longer supported and no APAR will be issued. IBM is encouraging customers to upgrade to a later compiler version. The pdnsd daemon should be disabled by running the following commands as root: # rmitab browser # chown root.system /usr/lpp/xlC/browser/pdnsd # chmod 0 /usr/lpp/xlC/browser/pdnsd # /usr/lpp/xlC/browser/pdnsdkill	Buffer Overflow Vulnerability	**High**	Bug discussed in newsgroups and websites.
Linux[13]	GNU glibc 2.1.1-6 RedHat Linux 6.0; GNU glibc 2.1	Due to lack of security checks, pt_chown can be easily fooled to gain full control over other user's (root as well) pseudo-terminal.	No workaround or patch available at time of publishing.	Pt_chown Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Linux[14, 15]	Debian GNU/Linux 2.1 alias slink; GNU/Linux alias potato; Red Hat Linux 4.2, 5.2, 6.0 (all architectures)	A buffer overflow in libtermcap's tgetent() function allows a malicious user to execute arbitrary code. Debian is not exploitable by this bug unless you have compiled your own programs using termcap or have installed third party programs that depend on libtermcap and run as root.	Recommend that you upgrade your smtp-refuser package which can be found at: (Select the termcat-compat patch for your architecture) Debian GNU/Linux 2.1 alias slink ftp://ftp.debian.org/debian/dists/slink-proposed-updates/ Debian GNU/Linux unstable alias potato ftp://ftp.debian.org/debian/dists/unstable/main/ RedHat: (select the libtermcap-2.0.8-14.4.2 for your architecture) Linux 4.2: ftp://ftp.redhat.com/redhat/updates/4.2/ Linux 5.2 ftp://ftp.redhat.com/redhat/updates/5.2/ Linux 6.0: ftp://ftp.redhat.com/redhat/updates/6.0/	Buffer Overflow Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.

[12] IBM-ERS Security Vulnerability Alert, August 17,1999.
[13] Bugtraq, August 24, 1999.
[14] RHSA-1999-028-01, August 17, 1999.
[15] Bugtraq, August 18, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Lotus Development Corporation[16, 17]	LotusNotes Domino Server 4.6 Oracle 8 for Windows NT is not affected by these vulnerabilities	There is an overflow vulnerability in the Notes LDAP Service (NLDAP), which could crash the Lotus Notes Domino server, and stop e-mail and other services that Domino provides. Additional vulnerabilities in superuser owned executables that may allow local root compromise have also been discovered.	Upgrade to Maintenance release 4.6.6 or 5.0. A patch is also available at: http://technet.oracle.com/misc/agent/section.htm Oracle has provided information to answer any questions concerning these vulnerabilities at: http://technet.oracle.com/misc/agent/faq.htm	LDAP Service Overflow Vulnerability	Low	Bug discussed in newsgroups and websites

Microsoft[18]
Microsoft has released a patch that addresses this vulnerability.[19]
	**Commercial Internet System 2.0, 2.5;
	IIS 4.0;
	Site Server 3.0 Commerce Edition;
	Site Server 3.0**
		Microsoft IIS and all products that use the IIS web engine have a vulnerability whereby a flood of specially formed HTTP request headers will make IIS consume all available memory on the server and then hand. IIS activity will be halted until the flood ceases or the service is stooped and restarted.	**Microsoft released a patch for this vulnerability on August 11th (MS99-028). However, on August 12, they retracted it due to an error that made IIS hang whenever the logfile was an exact multiple of 64KB. A new patch will be released shortly. (See Microsoft Security Bulletin (MS99-029) located at: www.microsoft.com/security/bulletin/MS99-029.asp**
			Microsoft re-released the bulletin on August 16, 1999. The new patches are available at: ftp://ftp.microsoft.com/bussys/iis/iis-public/fixes/usa/security/JDBRK-fix/
				Malformed HTTP Request Header Vulnerability	**Low**	**Bug discussed in newsgroups and websites.**
						Exploit has been published. Vulnerability has appeared in the Press.

Microsoft[20]	Internet Explorer 5.0 (Windows 95, 98, NT4.0)	A vulnerability exists in the ActiveX Control that allows executing arbitrary programs on the local machine by creating and overwriting local files and putting content in them.	No vendor supplied patch available at time of publishing. Recommend you disable Active scripting or disable run ActiveX Controls and plug-ins.	ActiveX Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit has been published. Vulnerability has appeared in the Press.

[16] ISS Security Advisory, August 23, 1999.
[17] Bugtraq, August 25, 1999.
[18] Security-Focus, August 11, 1999.
[19] Security Focus, August 17, 1999.
[20] Bugtraq, August 21, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft[21] ***Microsoft has re-released the patch for this vulnerability.***[22]	**Internet Information Server (IIS) 3.0, 4.0**	**If the server's default language is set to Chinese, Japanese, or Korean, IIS could allow a web site visitor to view the source code for selected files on the server.**	**Apply the patch corresponding to the language version of IIS, rather than the current default language on the server.** **English:** **ftp://ftp.microsoft.com/bussys/iis/iis-public/fixes/usa/security/fesrc-fix** **Simplified Chinese:** **ftp://ftp.microsoft.com/bussys/iis/iis-public/fixes/chs/security/fesrc-fix** **Traditional Chinese:** **ftp://ftp.microsoft.com/bussys/iis/iis-public/fixes/cht/security/fesrc-fix** **Japanese:** **ftp://ftp.microsoft.com/bussys/iis/iis-public/fixes/jpn/security/fesruc-fix** **Korean:** **ftp://ftp.microsoft.com/bussys/iis/iis-public/fixes/kor/security/fesrc-fix** ***A regression error in the IIS 4.0 version of the previously released patch has been identified. The corrected patch has been re-released, and updated security bulletin is available at:*** http://www.microsoft.com/security/bulletins/ms99-0322.asp ***The re-released patches for this vulnerability are time stamped August 17, 1999.***	**Double Byte Code Page Vulnerability**	**Medium**	**Bug discussed in newsgroups and websites.**
Microsoft[23]	Visual Studio 6.0 (NT 4.0); Internet Explorer 4.0 (Windows 95, 98 NT 4.0); Internet Explorer 4.1 (Windows 95, NT 4.0); Internet Explorer 5.0 (Windows 95, 95 NT 4.0)	A security vulnerability exists that could allow a Java applet to operate outside the bounds set by the sandbox and take any desired action on the user's computer. If such an applet were hosted on a web site, it could act against the computer of any user who visited the site.	Microsoft has released a patch that eliminates this vulnerability which can be found at: http://www.microsoft.com/java/vm/dl_vm32.htm Frequently asked questions regarding this vulnerability can be found at: http://www.microsoft.com/security/bulletins/MS99-31faq.asp/	Virtual Machine Sandbox Vulnerability	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the Press.

[21] Microsoft Security Bulletin (MS99-022), June 24, 1999.
[22] Microsoft Product Security, August 20, 1999.
[23] SecurityFocus, August 26, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft Windows 3.1, 95, 98; Windows NT 4.0[24]	Cat Soft Serv-U 2.5, 2.51; Imatix Xitami for Windows 2.4d2; Netscape Enterprise Server 3.1; Netscape FastTrack Server 2.0.1, 3.01; VqSoft vqServer for Windows 1.9	32bit Windows operating systems support long filenames, but also offer a means of compatibility with the older 8.3 filenames required by previous versions of DOS and Windows. This leads to problems with programs that have their own internal file security mechanisms.	Workaround: Using only 8.3 filenames in the web and ftp file hierarchies will avoid this issue. Also for NTFS filesystems, 8.3 filenames can be disabled. Netscape Enterprise and FastTrack Servers have released patches for their servers. Contact Netscape for more information	Multiple Vendor 8.3 Filename Vulnerability	Medium/ Low	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft Windows 9.x/NT[25] ***Exploit script has been published and vulnerability has appeared in the Press.[26]***	**Microsoft Internet Explorer 5.0**	**HTML Applications (HTAs) are fully trusted and have read/write access to the system registry, can run embedded ActiveX controls and Java applets, and zone security is off. All operations subject to security zone options are permitted, which opens up a wide range of security holes.**	**No workarounds or patches known at time of publishing.** ***Solution: Disable file downloads or disassociate .HTA files from MSHTA.exe.***	**HTML Applications Security Hole**	**High**	**Bug discussed in newsgroups and websites.** ***Exploit script has been published.*** ***Vulnerability has appeared in the Press.***
Microsoft Windows 95 & 98[27]	Telnet (which ships as part of Windows 95 & 98) Internet Explorer 4.0 & 5.0	A heap overrun vulnerability exists in the Telnet application that allows an attacker to execute arbitrary code. **This can be used by any web site since telnet is a default 'helper application' for certain protocols under Internet Explorer.**	The vulnerability is fixed in IE 5.0b, which ships as part of Windows 98 Second Edition. It also is eliminated by the patch for the "Malformed Favorites Icon" vulnerability, which was released in May. http://www.microsoft.com/security/bulletins/ms99-018.asp The vulnerability is present in IE 4.0 as well, at time of publishing Microsoft hadn't released a patch to fix it.	Heap Overflow Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.

[24] SecurityFocus, August 18, 1999.
[25] NTBugtraq, June 8, 1999.
[26] Securiteam, August 25, 1999.
[27] Bugtraq, August 15, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft Windows NT, 95, 98[28] ***Exploit for this vulnerability has been published.***[29] ***Office 2000 is also contains this vulnerability.***[30]	**Jet 3.51 driver (ODBCJT32. DLL) shipped with the Office 97 software suite** ***Office 2000 suite, Access 2000, Excel 2000***	**Vulnerability in Microsoft Office 97 can allow malicious code hidden in a web page or sent in e-mail to take control of online computers without the victims' knowledge. This vulnerability was first reported in Excel 97 but other Office applications can be used to hide the code.**	**Upgrade to Jet 4.0 driver. This driver is delivered as part of MDAC 2.1 which can be downloaded at: http://www.microsoft.com/data/** ***Additional information and frequently asked questions regarding this vulnerability can be found at:*** http://www.microsoft.com/security/bulletins/MS99-030faq.asp ***Patch available at:*** http://officeupdate.microsoft.com/articles/mdac_typ.htm	**MS Office Driver Vulnerability**	**High**	**Bug discussed in newsgroups and websites.** ***Exploit has been published.*** ***Vulnerability has also appeared in the Press.***
Nullsoft (Unix)[31]	SHOUTcase audio system by Nullsoft	A vulnerability exists in this product that stores the administrative password of the server insecurely on Unix-based systems.	No workaround or patch available at time of publishing.	Insecure Password Vulnerability	Medium	Bug discussed in newsgroups and websites.
Oce[32]	9400 Plotter	The OCE 9400 plotter is a network printer/plotter that allows telnet login access. By default the "root" user has no password, which could allow a malicious user to log into the plotter, where he or she can change plotter settings as well as telnet back out to other machines.	Minimum recommended workaround is to apply a password to the root user were possible. No patch available at time of publishing.	Password Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
OpenBSD NetBSD[33]	OpenBSD 2.3; NetBSD 1.3.2.	Buffer overflow vulnerability exists in routines of the procfs and fdescfs filesystems.	OpenBSD patch available at: http://www.openbsd.org/errata.html#miscfs	Buffer Overflow Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Persits Software[34]	AspUpload 1.4	Denial of Service attack affects IIS web servers when a buffer overflow event is created in the filename box of your browser.	AspUpload component has been fixed in version 1.4.0.2, which is available to registered users upon request. For more information: http://www.AspUpload.com	Buffer Overflow Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit has been published.

[28] Bugtraq, July 29, 1999.
[29] NTBugtraq, August 11, 1999.
[30] Microsoft Security Bulletin (MS99-030), August 20, 1999.
[31] Bugtraq, August 23, 1999.
[32] Bugtraq, August 19, 1999.
[33] Bugtraq, August 13, 1999.
[34] Bugtraq, August 17, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
QMS CrownNet Unix utilities for 2060[35]	QMS 2060 Network Printer	Root access to the printer can be gained without root's password. By gaining this access privilege, any attacker can gain full control of the printer.	No workaround or patch available at time of publishing.	Pinter Password Root Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Red Hat[36]	Linux 4.2, 5.2, 6.0	The in.telnetd telnet daemon attempts to negotiate a compatible terminal type between the local and remote host. By setting the TERM environment variable before connecting, a remote user could cause the system telnet daemon to open files it should not. Depending on the TERM setting used, this could lead to Denial of Service attacks.	Recommend you upgrade your In.telnetd package as soon as possible. Please select the architecture patch for your system; then select 'NetKit-B-0.09-11' and the appropriate architecture. Red Hat Linux 4.2: ftp://ftp.redhat.com/redhat/updates/4.2/ Red Hat Linux 5.2: ftp://ftp.redhat.com/redhat/updates/5.2/ Red Hat Linux 6.0: ftp://ftp.redhat.com/redhat/updates/6.0/	In.telnetd Dos Vulnerability	Low	Bug discussed in newsgroups and websites.
Red Hat[37]	Linux 6.0	A buffer overflow exists in crond, which could allow local users to gain root privileges.	Patch available at: Intel: ftp://updates.redhat.com/6.0/i386 Alpha: ftp://updates.redhat.com/6.0/alpha Sparc: ftp://updates.redhat.com/6.0/sparc Source: ftp://updates.redhat.com/6.0/SRPMS Architecture neutral: ftp://updates.redhat.com/6.0/noarch	Crond Buffer Overflow Vulnerability	**High**	Bug discussed in newsgroups and websites.
Red Hat[38] (New wu-ftp available to correct all currently known problems)	Linux 6.0 (all architectures)	New packages of wu-ftpd are available for all Red Hat platforms which includes a security fix for all known problems in wu-ftpd.	Patch available at: (Select the architecture for your system) ftp://updates.redhat.com/6.0/	Wu-Ftpd Vulnerability	Low	Bug discussed in newsgroups and websites.
Red Hat [39]	Linux	There is a Trojan being spread that exploits portmap on Red Hat boxes This Trojan adds rootshell to your inetd.conf file and e-mails other info like your IP address to a hotmail account: goat187@hotmail.com.	Newgroup suggested workaround is, if your firewall can block outgoing mail according to e-mail address, to block this address. Log should be check for this e-mail as it indicates one of your systems has been potentially exploit.	Portmap Trojan	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.

[35] NTBugtraq, August 18, 1999.
[36] RHSA-1999:029-01, August 19, 1999.
[37] RHSA-1999:030-01, August 25, 1999.
[38] RHSA-100:031-01, August 25, 1999.
[39] Bugtraq, August 20, 1999,

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
RedHat Linux 5.2, 6.0[40] (Same vulnerability in FreeBSD above)	Window Maker 0.20.1-3, 0.52-2, 0.53, 0.60	A number of buffer overflow vulnerabilities exist in WindowMaker, which could allow arbitrary code to be executed.	No workaround or patch available at time of publishing.	Window Maker Buffer Overflow Vulnerability	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Sun[41] ***Fix for Solaris 7 [42]***	**Solaris2.6**	**Root access can be obtained from setuid buffer overflow.**	**There is not a patch for a similar problem in Solaris 7. However, the following patches for Solaris 2.6:** **RELEASE ARCH PATCH** **5.6 i386 105211-06** **5.6 sparc 105210-06** **Note a new exploit has appeared that defeats the patch.** ***The fix for Solaris 7 will be included in the following three patches. These patches have not yet been released officially, however if you have a service contract, you can get a pre-release version from Sun.*** ***106541-06 Solaris 7 Kernel Update*** ***106793-03 ufsdump and ufsrestore patch*** ***107972-01 /usr/sbin/static/rcp patch***	**Solaris libc Vulnerability**	**High**	**Bug discussed in newsgroups and Web sites. New exploit script has been published that will defeat the current patch.**
SuSE[43]	Linux 4.4, 4.4.1, 5.0, 5.1, 5.2, 5.3, 6.0, 6.1	A remote malicious attacker can mount a Denial of Service attack by starting a large number of ident requests in a short period of time.	No workaround or patch available at time of publishing.	Identd DoS Vulnerability	Low	Bug discussed in newsgroups and websites
Unix[44]	CiscoSecure Access Control Server for Unix Remote Admin. Ver. 1.0 through 2.3.2	The database access protocol could permit unauthorized remote users to read and write the server database without authentication, remove accounts, add accounts and change passwords or privileges in the user database, including implementing an administrative account that would give them control of the server.	Either a CiscoSecure configuration change, or network configuration change can eliminate this vulnerability. Cisco has provided a new release located at http://www.cisco.com	Database Access Protocol Vulnerability	High	Bug discussed in newsgroups and websites.

[40] Bugtraq, August 22, 1999.
[41] Bugtraq, May 22, 1999.
[42] Bugtraq, August 17, 1999.
[43] Bugtraq, August 14, 1999.
[44] Cisco Security Notice, August 19, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Unix[45]	Oracle7 7.3.3; Oracle 8 8.0.5.3, 8.0.4, 8.0.5, 8.0.5.1, 8.15	Oracle installations with the 'Oracle Intelligent Agent' contain vulnerabilities in super-user owned executables that may allow local root compromise.	Patch available at: http://technet.oracle.com/misc/agent/section.htm	Oracle Intelligence Agent Vulnerability	**High**	Bug discussed in newsgroups and websites.
Unix; Linux[46]	Digital Unix 4.0E; SuSE Linux 6.1; RedHat Linux 6.0; Solaris; HP/UX; Irix	Default Xaccess file allows XDMCP connections from any host. This can be used to get a login screen on any host and therefore get around access control mechanisms and root login restrictions to the console.	No workaround or patch available at time of published.	XDM Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Washington University[47]	Wu-ftpd 2.5.2 (beta 18) VR9; 2.4.2 (beta 18) VR10; 2.5	An overflow vulnerability in mapped_path exists.	No workaround or patch available at time of published.	Wu-Ftpd Overflow Vulnerability	Low	Bug discussed in newsgroups and websites. It is rumored that there is an exploit in use and in circulation among hackers.

*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.

[45] SecurityFocus, August 16, 1999,
[46] Bugtraq, August 18, 1999.
[47] SecurityFocus, August 24, 1999.

Recent Exploit Scripts

The table below contains a representative sample of exploit scripts, identified between August 13 and August 27, 1999, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that hackers/crackers are utilizing**. During this period, 8 scripts, programs, and net-news messages containing holes or exploits were identified.

Date of Script (Reverse Chronological Order)	**Script Name**	**Script Description**	**Comments**
August 28, 1999	**Xtcptrace.c**	**A tcpdump "wrapper" to decode X KeyCodes exploit script.**	
August 24, 1999	**Ftpd.c**	**Remote root compromise script that exploits the wt-ftpd vulnerability.**	
August 24, 1999	**Potfory.c**	**Automated exploit script for Linux pt_chown vulnerability.**	
August 23, 1999	Smashcap.c	Exploit code that takes advantage of the libtermcap buffer overflow.	
August 22, 1999	**Wdefualts.c**	**Script which exploits the buffer overflow in WindowMaker.**	
August 20, 1999	**Portmap.c**	**A trojaned version of the portmap vulnerability.**	
August 19, 1999	IE5telx.c	Exploit script, which downloads and runs an arbitrary file exploiting the heap overflow in Windows 95/98.	
August 12, 1999	Hiperbomb2.c	An exploit script that will let an attacker remotely reboot all HiperARC software.	

Script Analysis

This section will supply a short description of scripts that have been analyzed by various security professionals and organizations. If you or your organization wish to contribute, please send e-mail to nipc@fbi.gov with the subject line “CyberNotes Script Analysis.” While this section will list only short descriptions, 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. If you would like to receive a copy of the full technical analysis version of any summarized analysis, please send an e-mail listing the script name and requesting the full technical analysis. A member of the CyberNotes editorial team will contact you. All contributions will be credited to the contributing individual or organization unless otherwise requested.

Trends

Trends for this two week period:

- Trivial FTP (TFTP) is one of the commands most targeted by intruders.
- Servers are being penetrated using the RDO exploits.
- IIS vulnerabilities are still being exploited.

- Infrastructure attacks against corporate e-mail.
- Weak passwords are becoming a security nightmare for large organizations.
- Security holes in CGI scripts are currently being exploited.
- Hackers have taken a greater interest in cable modems and DSL lines. Individual report receiving two probes per day against their machines using cable modems or DSL lines.

Viruses/Trojans

Toadie: Toadie.exe is written in high level language, ASIC, and attaches itself to email messages waiting to be sent. This virus is being actively distributed in the guise of a program for cloning cell-phones as well as a program designed to generate adult site passwords. This is a relocating virus. It is encrypted and non-memory resident.

This virus was posted to several newsgroups as a cell phone cloning application on 15th of August 1999. The virus was in CELLCRK.ZIP file. When the CELLCRK.EXE program that was inside that ZIP is run it displays a rhyme and a copyright string of Symantec.

The virus writes 7800 bytes of its code, which is a DOS, program (with EXE header) itself to infected file beginning thus converting any Windows program to DOS format. When any infected DOS or Windows program is run, virus code gets control first, infects more EXE files on hard disk(s) and then passes control to the original file code.

The virus has an ability to spread itself through IRC networks. On infected system the virus modifies settings of IRC client (mIRC) and creates TOADIE.EXE file. This file is sent [DCC] by an infected user to anyone who is joining any IRC channel the user is on at the moment.

Christmas' Virus: A nasty new virus discovered by researchers promises to do even more damage to victims than the Chernobyl virus. It has the ability not only to erase files, but also to render a PC useless by destroying its flash BIOS.

The good news is it won't execute until Dec. 25; the bad news is PC users without anti-virus programs may have a very bad Christmas Day.

Inside the virus is a text string with a poem full of expletives criticizing those who preach religion: "I don't wanna hear it, coz I know none of it's true," the author writes, according to anti-virus research firm Kaspersky Lab.

Victims of the virus -- who can be anyone using Windows 95, Windows 98 or Windows NT -- can expect a load of trouble. The virus kills the CMOS memory, overwrites data in all files on all available drives, and then destroys the flash BIOS by using the same routine that was found in the "Win95_CIH" virus, also known as Chernobyl.

Kriz Virus: Another variant of the infamous Chernobyl virus was discovered recently. This virus, called Win32Kriz will destroy the Flash BIOS memory and all available hard drives. It infects .EXE files, .SCR files, and the kernel32.dll file. It runs and replicates under Windows 95, 98 and NT. On December 29th, this virus will erase the CMOS memory, overwrite data in all available drives and trash the Flash BIOS memory using the routine used in the original CIH Virus. This virus is memory resident and once it infects kernel32.dll it will remain resident for the entire Windows session.