National Infrastructure Protection Center
CyberNotes

Issue #19-99 *September 15, 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 28 and September 9, 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
Bluestone[1]	Sapphire/Web 5.0	A vulnerability exists that allows the sessions of other clients' to be hijacked. If a malicious user has a username and password and connects with such, the other clients' sessions may be compromised.	Upgrade to version 6.X - Different types of authentication can be selected in this versions. Currently there are no vendor supplied patches that fix version 5.0	Client Hijack Vulnerability	Medium/ Low	Bug discussed in newsgroups and websites. Exploit has been published.

[1] SecurityFocus, September 9, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Caldera[2]	OpenLinux 2.2	Please see entry for Red Hat Vixie Cron 'MAILTO' Sendmail Vulnerability.	Recommend that you upgrade your cron package immediately. ftp://ftp.calderasystems.com/pub/OpenLinux/iupdates/2.2/current/RPMS/vixie-cron-3.0.1-19.i386.rpm	Vixie Cron MAILTO Sendmail Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Debian[3]	GNU/Linux 2.1 alias slink; GNU/Linux pre2.2 alias potato	Please see entry for Red Hat Vixie Cron 'MAILTO' Sendmail Vulnerability.	Recommend that you upgrade your cron package immediately. GNU/Linux 2.1 alias slink: For each architecture select cron_3.0p11-50.2 and the appropriate architecture. http://security/debian/org/dists/stable/updates/binary-alpha/ GNU/Linux pre2.2 alias potato: For each architecture after 'binary-' select the appropriate architecture, then cron_3.0p11-52 and the appropriate architecture. http://security.debian.org/dists/unstable/updates/binary-alpha/	Vixie Cron MAILTO Sendmail Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Debian[4]	GNU/Linux 2.1 alias slink; GNU/Linux pre2.2 alias potato	All versions of epic4 between pre 1.034 (including) and pre2.004-1990718 (excluding) are vulnerable to a buffer overflow which causes the client to crash and possibly display arbitrary characters on the terminal.	It is recommended that you upgrade your epic4 packages immediately. GNU/Linux 2.1 alias slink: Please change 'alpha.deb' to the appropriate architecture for your system. ftp://ftp.debian.org/debian/dists/proposed-updates/epic4_pre2.003-0slink2_alpha.deb ftp://ftp.debian.org/debian/dists/proposed-updates/epic4-dbg__pre2.003-0slink2_alpha.deb GNU/Linux pre2.2 alias potato: Please change 'binary-alpha' to the appropriate architecture for your system. ftp://ftp.debian/org/debian/dists/unstable/main/binary-alpha/net/epic4_pre2.004-19990718-1.deb ftp://ftp.debian.org/debian/dists/unstable/main/binary-alpha/net/epic4-dbg_pre2.004-1990718-1.deb	Epic4 Buffer Overflow Vulnerability	Low	Bug discussed in newsgroups and websites.
Domain Name System (DNS) Servers[5]	Any DNS Server	A generalized exploit has been published that shows a weakness in many vendor's implementations of dynamic DNS Services that allows a Denial of Service Attack.	Check with your DNS vendor to see if your DNS package is Vulnerable.	DDNS Denial of Service Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit script has been published.

[2] SecurityFocus, August 31, 1999.

[3] Debian Security Advisory, August 30, 1999.

[4] Securiteam, August 28, 1999.

[5] Bugtraq, August 30, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
FreeBSD[6]	FreeBSD 3.2-RELEASE & -STABLE; perhaps FreeBSD 3.x.	A Denial of Service attack can be mounted using simple file system functions.	No workaround or patch available at time of publishing.	FreeBSD Denial of Service Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit has been published and is simple to reproduce.

FreeBSD;
OpenBSD;
BSDI;
Cobalt Linux [7]
	FreeBSD 3.2-RELEASE;
	OpenBSD 2.4 - GENERIC kernel & OpenBSD 2.5;
	BSDI 2.1
	BSDI 3.1
	BSDI 4.0
	BSDI 4.0.1;
	Cobalt Linux (MIPS) - RedHat based
		A Denial of Service attack can be staged on a BSD system, where an unprivileged user can cause a Denial of Service attack.	No workaround or patch available at time of publishing.	Setsockopt() Denial of Service Vulnerability	Low	Bug discussed in newsgroups and websites.
						Exploit has been published.

Hewlett-Packard[8]	HP-9000 Series 700/800 HP-UX releases 10.20, 10.30, 11.00	Buffer overflow vulnerability in the CDE Calendar Manager Service Daemon, rpc.cmsd exists that could allow remote and local users to execute arbitrary code with root privileges.	Install the applicable patch: HP-UX release 10.20 PHSS_19482 HP-UX release 11.00 PHSS_19483 There are significant patch dependencies for both patches. ftp://us-ffs.external.hp.com/export/patches/hp-ux_patch_matrix **Note:** UP-UX release 10.30 was a development releases prior to the release 11.00 and will not be patched.	CDE Calendar Manager Service Vulnerability	**High**	Bug discussed in newsgroups and websites.
IBM[9]	AIX-4 Systems	A list of security-related Authorized Problem Analysis Reports (APARs) for current releases of AIX has been updated August 1999. To facilitate ease of ordering all security related APARs for each release can be ordered using the following packaging APARs: AIX 4.3: IY03152 AIX 4.2: IY03151 AIX 4.1: iy03150	To facilitate ease of ordering all security related APARs for each release can be ordered using the following packaging APARs: AIX 4.3: IY03152 AIX 4.2: IY03151 AIX 4.1: iy03150 APARs can be ordered using FixDist: http://service.software.ibm.com/rs6k/fixes.html	AIX Authorized Problem Analysis Reports		Bug discussed in newsgroups and websites.

[6] Bugtraq, September 2, 1999.

[7] Securiteam, September 4, 1999.

[8] Hewlett-Packard Company Security Bulletin: #00102, 30 August 1999.

[9] AIX Service Mail Server, August 19, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
IBM[10]	GINA for Windows NT 4.0 SP1, SP2, SP3, SP4, SP5	A security hole exists that allows normal users to gain administrator equivalent privileges on Windows NT systems.	Modify the SCLs over the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\ServicesIBMNeTNT\GroupMaping key to: System: Full Administrator: Full Everyone: Read	Privilege Escalation Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Linux[11]	Linux 6.0 (all architectures); Professional FTP ProFTPD 1.2pre1, 1.2pre2, 1.2pre3	A security hole in the ProFTPD exists that enables a remote attacker to gain root privileges. Proftpd is a ftp server that is shipped as part of the Powertools CD collection. If you have switched to proftpd and you are using the version shipped on the Red Hat Powertools 6.0 CD you are at risk.	Site administrators are strongly advised to upgrade to the new packages. Intel: ftp://updates.redhat.com/powertools/6.0/i386/proftpd-1.2.0pre3-6.i386.rpm Alpha: ftp://updates.redhat.com/powertools/6.0/alpha/proftpd-1.2.0pre3-6.alpha.rpm Sparc: ftp://updates.redhat.com/powertools/6.0/sparc/proftpd-1.2.0pre3-6.sparc.rpm Source packages: ftp://updates.redhat.com/powertools/6.0/SRPMS/proftpd-1.2.0pre3-6.src.rpm	Proftpd Buffer Overflow Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published. The vulnerability is being actively exploited on the Internet.
Linux[12, 13] ***Another exploit script has been published for this vulnerability***	**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.**
Martin Stover Mars 0.99[14]	Mars NWE 0.99 (all versions up to and including 0.99)	The Mars NetWare Emulator package contains several buffer overflows, which allow superuser, privileges.	Recommended that you upgrade as soon as possible to the latest version (1.00) that can be found on Mars Netware Emulator's home page: http://www.compu-art.de/mars_nwe/index.html	Mars_new Buffer Overflow Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.

[10] Securiteam, August 28, 1999.

[11] RHSA-1999:034, August 31, 1999.

[12] RHSA-1999:028-01, August 17, 1999.

[13] Bugtraq, August 18, 1999.

[14] SecurityFocus, September 2, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft[15]	Hotmail	A vulnerability exists in Hotmail's webmail service, which enables attackers to easily compromise hotmail accounts and read private e-mail stored on the web server.	Microsoft has fixed the security flaw.	Hotmail Vulnerability	High	Bug discussed in newsgroups and websites. Exploit has been published and used by malicious attackers.
Microsoft[16]	Internet Explorer 4.0, 5.0	Vulnerabilities exist in two ActiveX controls (scriptlet.typlib & eyedog) that could allow a malicious web site operator to take inappropriate actions on the computer of a user who visits their web site.	Patch available at: ftp://ftp.microsoft.com/peropsys/IE/IE-Public/Fixes/usa/Ehyedog-fix	ActiveX Controls Vulnerability	High	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[17] ***This exploit can be e-mailed or mass-mailed.[18]***	**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.**
Microsoft Windows 2000[19]	Windows 2000 (beta version)	A simple Visual Basic script hidden in any HTML document, which can be either posted on a web page, or sent to an Outlook client, can covertly activate a telnet server.	No workaround or patch available at time of publishing.	COM Handler Vulnerability	High	Bug discussed in newsgroups and websites. Exploit has been published.

[15] Securiteam, August 31, 1999.
[16] Microsoft Security Bulletin (MS99-032), August 31, 1999.
[17] Bugtraq, August 21, 1999.
[18] Bugtraq, August 30, 1999.
[19] Securiteam, September 8, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft Windows 95 & 98[20] *Microsoft has released a patch that eliminates a vulnerability in the Telnet client.[21]*	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. *Windows 95:* http://www.microsoft.com/windows95/downloads/contents/WUCritical/Telnet/Default.asp *Windows 98 & 98 2nd edition:* http://www.microsoft.com/windows98/download/contents/WUCritical/Telnet/Default.asp	Heap Overflow Vulnerability	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Microsoft Windows 98/200[22] *Microsoft has released patches that eliminate this vulnerability.[23]*	Operating system	Windows 98 and 2000 TCP/IP stack s were not built to tolerate malformed IGMP headers. Windows will bluescreen when one is received	No workaround or patch available at time of publishing. *Windows 95:* *Patch will be available shortly* *Windows 98:* http://www.microsoft.com/windows98/downloads/corporate.asp *Windows NT Workstation 4.0;* *Windows NT Server 4.0;* *Windows NT Server, Enterprise Edition:* ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP5/IGMP-fix/ *Windows NT Server 4.0, Terminal Server Edition:* ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40TSE/hotfixes-postSP5/IGMP-fix/	Invalid IGMP Header Vulnerability	Low	Bug discussed in newsgroups and websites. Two Exploit scripts have been published.

[20] Bugtraq, August 15, 1999.
[21] Microsoft Security Bulletin (MS99-033), September 9, 1999.
[22] Bugtraq, July 2, 1999.
[23] Microsoft Security Bulletin (MS99-034), September 3, 1999.

Hardware/ Operating System/ Vendor	**Equipment/ Software Name**	**Vulnerability/ Impact**	**Patches/Workarounds/Alerts**	**Common Name**	**Risk***	**Attacks/Scripts**
Microsoft Windows 9X, 2000 and NT[24]	Windows 95, 98, 2000, NT	A potential vulnerability exists in Microsoft's implementation of CryptoAPI (CAPI) that may allow whoever owns or effectively controls the 2nd key the ability to tamper with already running security services, and compromise Windows' security.	No official workaround or patch available at time of publishing. A unofficial patch is available at www.cryptonym.com Users should test all patches prior to implementation on a production network. NOTE: Microsoft has issued a strong denial of allegations of misuse of a second encryption "key" in Windows. "The key is a Microsoft key -- it is not shared with any party including the NSA," said Windows NT security product manager Scott Culp. "We don't leave backdoors in any products."	Cryptographic Backdoor Vulnerability	**Medium**	Bug discussed in newsgroups and websites. Exploit has been published. Vulnerability has appeared in the Press as the "_NSAKEY".
Microsoft Windows NT[25]	Compaq Insight Management Agent for Windows NT v 4.20D, v4.222, v4.23, v4.30, v4.40	PFCUser Account in Compaq Management Agents for Servers for Microsoft Windows NT contains a potential security vulnerability in the account/password.	Compaq and BMC Software are actively working to resolve the potential vulnerability in the next release of Compaq Management Agents. Refer to instructions to determine if your server have these capabilities installed and instructions to modify or remove this potential vulnerability from the server located at: http://www.compaq.com/sysmanage	PFCUser Account Vulnerability	Low	Bug discussed in newsgroups and websites.
Microsoft Windows NT 4.0[26]	Microsoft TCP/IP Stack for NT 4.0 up to and including SP3	Windows NT 4 uses predictable TCP sequence number generating algorithms that could allow an attacker to set up connections to other machines with a spoofed source address of the NT host.	No workaround or patch available at time of publishing.	TCP/IP Sequence Numbering Vulnerability	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[24] Securiteam, September 4, 1999.
[25] NTBugtraq, September 5, 1999.
[26] Securiteam, August 28, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft Windows NT 4.0[27]	NT 4.0SP5; SP4, SP3, SP2, SP1	The Master File Table (MFT) of an NT 4 host may show signs of corruption after it has grown larger than 4 Gig. Corruption may include: presence of formerly deleted files, disappearance of non-deleted files, and warning messages about corruption that recommend running CHKDSK.	Microsoft has issues a post-SP5 hotfix to correct this problem. It can be obtained at: ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/Hotfixes-PostSP5/NTFS-fix	NT Master File Table Corruption Vulnerability	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft Windows NT 4.0; Windows 2000[28]	Internet Explorer 5.0	FTP usernames and passwords for sites accessed via Internet Explorer 5.X are stored (cleartext) in history files. Because the "Bypass Traverse Checking" right is assigned by default to the Everyone group, any user with access to the host can read any other user's index.dat files.	No workaround or patch available at time of publishing.	IE5 FTP Password Storage Vulnerability	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Netscape[29]	Enterprise Server 3,6m 3,6SO2l; FastTrack Server 3.0.1	A malicious user can gain illicit access to the Netscape Enterprise Server and FastTrack server and can remotely upload and execute arbitrary code.	Apply the 3.6 SP 2SSL Handshake fix, available from Netscape at: http://www.iplanet.com/downloads/patches/detail_12_86.html Users of Fastrack 3.0.1 or previous versions should upgrade to Enterprise Server 3.6 then apply the aforementioned patch.	Buffer Overflow Vulnerability	**High**	Bug discussed in newsgroups and websites.
Netscape[30]	Netscape Communicator 4.06, 4.5, 4.5.1, 4.6, 4.61	An unchecked buffer in the code that handles EMBED tags exists. It can be used to execute arbitrary code.	No workaround or patch available at time of publishing.	Embed Buffer Overflow Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published.

[27] SecurityFocus, August 30, 1999.
[28] SecurityFocus, August 30, 1999.
[29] SecurityFocus, September 2, 1999.
[30] Bugtraq, September 2, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Red Hat[31]	Linux 4.2, 5.0, 5.1, 5.2, 6.0 (all architectures)	An exploitable buffer overflow vulnerability that existed in the amd daemon has been fixed. This problem is being actively exploited on the Internet and can be used to gain root access on machines running amd.	Upgrade to the fixed versions immediately. Intel: ftp://updates.redhat.com/6.0/i386/am-utils-6.01s11-1.6.0.i386.rpm ftp://updates.redhat.com/5.2/i386/am-utils-6.0.1s11-1.5.2.i386.rpm ftp://updates.redhat.com/4.2/i386/am-utils-6.01s11-1.4.2.i386.rpm Alpha: ftp://updates.redhat.com/6.0/alpha/am-utils-6.01s11-1.6.0.alpha.rpm ftp://updates.redhat.com/5.2/alpha/am-utils-6.0.1s11-1.5.2.alpha.rpm ftp://updates.redhat.com/4.2/alpha/am-utils-6.01s11-1.4.2.alpha.rpm Sparc: ftp://updates.redhat.com/6.0/sparc/am-utils-6.01s11-1.6.0.sparc.rpm ftp://updates.redhat.com/5.2/sparc/am-utils-6.0.1s11-1.5.2.sparc.rpm ftp://updates.redhat.com/4.2/sparc/am-utils-6.01s11-1.4.2.sparc.rpm Source Packages: ftp://updates.redhat.com/6.0/SRPMS/am-utils-6.01s11-1.6.0.src.rpm ftp://updates.redhat.com/5.2/SRPMS/am-utils-6.0.1s11-1.5.2.src.rpm ftp://updates.redhat.com/4.2/SRPMS/am-utils-6.01s11-1.4.2.src.rpm	Buffer Overflow Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published. A buffer overflow exploit that came from Korea has a channel to send information back, ostensibly, to the writer of the exploit.
Red Hat[32] **The Crond buffer overflow vulnerability was covered in issue 18-99 but Red Hat has updated their advisory to include another vulnerability and also acknowledge that exploit scripts now exist.**	Linux 4.2, 5.2, 6.0 (all architectures)	The additional vulnerability found make it possible for local users to gain root access by creating a crontab that runs with a specially formatted 'MAILTO' environment variable. Also it was possible to use specially formatted 'MAILTO' environment variables to send commands to sendmail.	**Red Hat 4.2** Intel: ftp://ftp.redhat.com/redhat/updates/4.2/i386/vixie-cron-3.0.1-37.4.2.i386.rpm Alpha: ftp://ftp.redhat.com/redhat/updates/4.2/alpha/vixie-cron.3.0.1-37.4.2.alpha.rpm Sparc: ftp://ftp.redhat.com/redhat/updates/4.2/aparc/vixie-cron.3.0.1-37.4.2.sparc.rpm Source packages: ftp://ftp.redhat.com/redhat/updates/4.2/SRPMS/vixie-cron-3.0.1-37.4.2.src.rpm **Red Hat 5.2** Use the same addresses above, replacing 4.2 with 5.2. **Red Hat 6.0** Intel: ftp://ftp.redhat.com/redhat/updates/6.0/i386/vixie-cron-3.0.1-38.6.0.i386.rpm Alpha: ftp://ftp.redhat.com/redhat/updates/6.0/alpha/vixie-cron-3.0.1-38.6.0.alpha.rpm Sparc: ftp://ftp.redhat.com/redhat/updates/6.0/sparc/vixie-cron-3.0.1-38.6.0.sparc.rpm Source packages: ftp://ftp.redhat.com/redhat/updates/6.0/SRPMS/vixie-cron-3.0.1-38.6.0.src.rpm	Vixie Cron 'MAILTO' Sendmail Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published.

[31] RHSA-1999:032-01, August 30, 1999.
[32] RHSA-1999:030-02, August 27, 1999.

Hardware/ Operating System/ Vendor	**Equipment/ Software Name**	**Vulnerability/ Impact**	**Patches/Workarounds/Alerts**	**Common Name**	**Risk***	**Attacks/Scripts**
SCO[33]	Open Server 5.0.4, 5.0.5	A local root compromise vulnerability exists in /bin/doctor 2w.0.0.32 and probably other versions as well.	Change the permissions on /bin/doctor to 700.	Doctor Command Execution Vulnerability	High	Bug discussed in newsgroups and websites. Exploit has been published.
Sun Solaris[34] - Multiple versions ***Patches that fix this vulnerability have been released.[35]*** ***Sun releases final rpc.cmsd patches*** ***Sun has released the final rpc.cmsd patches for the following versions of Solaris/SunOS SunOS 5.7, 5.7_x86, 5.6, 5.6_x86, 5.5.1, 5.5.1_x86, 5.5, 5.5_x86, 5.4, 5.4_x86, 5.3, 4.1.4, and 4.1.3_U1[36]***	**Rpc.cmsd (Operating System)**	**Remote unauthorized user can execute a buffer overflow in the calendar manager that may result in root access.**	**No vendor supplied patch or workaround available at time of publishing.** ***The following patches have now been released: Solaris 7/Sparc:*** ***107022-03 CDE 1.3*** ***Solaris 7/x86:*** ***107023-03 CDE 1.3_x86*** ***Solaris 2.6:*** ***105567-08 CDE 1.2_x86*** ***Solaris 2.5.1:*** ***104976-04 OW 3.5.1*** ***Solaris 2.4 patches will be Released at a later date.*** ***Systems may still be running the old, vulnerable daemon after installing the patch unless the Rpc.cmsd process is killed *after* the patch has been installed.*** ***Sun gives recommended patch routes and matrices in their advisory: http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-license&nav=***	**Solaris Rpc.cmsd Buffer Overflow**	**High**	**Bug discussed in newsgroups and websites. Exploit has been published.**
Sybase[37]	Power Dynamo 3.0.652	The Sybase power Dynamo personal webserver will service HTTP GET requests, allowing access to the entire drive that contains any web-published document.	No workaround or patch available at time of publishing.	Atomicity Error	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[33] Securiteam, September 9, 1999.
[34] Bugtraq, July 9, 1999.
[35] Bugtraq, July 15, 1999.
[36] Securiteam, August 28, 1999.
[37] SecurityFocus, September 6, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Tenfour[38]	TFS Gateway 4.0; TFS SMTP 3.2	Gateway 4.0 is vulnerable to a remote Denial of Service attack. TFS SMTP 3.2 allows a malicious user to use a misconfigured TFS SMTP for spamming and can remotely crash the TFS SMTP Gateway	TenFour has made a fixed version available at: http://www.tenfour.se	Denial of Service Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit has been published.
WU-FTPD Development Group[39]	All platforms using: wu-ftpd-2.4.2-beta-18-vr4 through beta-1j8-vr15; wu-ftpd-2.4.2-vr16, vr17; wu-ftpd-2.5.0; BeroFTPD, all present versions; other derivatives of wu-ftpd may be effected	A vulnerability exists in wu-ftpd that may allow local and remote users to gain root privileges.	The Wu-FTPD Development Group has made the following patch available for wu-ftpd 2.5.0: ftp://ftp.wu-ftpd.org/pub/wu-ftpd/quickfixes/apply_to_2.5.0 Users of BeroFTPD 1.3.4 can apply the same patch.	Wu-FTPD Buffer Overflow Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

*Risk is defined in the following manner:

High - A vulnerability that will allow an intruder to immediately gain privileged access (e.g., sysadmin, and root) to the system. An example of this would be a vulnerability in which a sequence of instructions is sent to a machine by an unauthorized user and the machine responds with a command prompt.

Medium - A vulnerability that will allow an intruder immediate access to the system that is not privileged access. This allows the intruder the opportunity to continue the attempt to gain root access. An example would be a configuration error that allows an intruder to capture the password file.

Low - A vulnerability that provides information to an intruder that could lead to further compromise attempts or a Denial-of-Service (DoS) attack. The reader should note that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered as a "High" threat.

[38] SecurityFocus, August 31, 1999.
[39] SecurityFocus, August 31, 1999.

Recent Exploit Scripts

The table below contains a representative sample of exploit scripts, identified between August 28 and September 9, 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, 21 scripts, programs, and net-news messages containing holes or exploits were identified.

Date of Script **(Reverse Chronological Order)**	**Script Name**	**Script Description**	**Comments**
September 6, 1999	Sdlamd.c	Buffer overflow exploit script that allows root access on machines running amd.	
September 6, 1999	Slurpie	A Unix password cracker that can run in a distributed environment.	
September 4, 1999	Xploit.zip	Exploit script that crashed Netscape 4.6.	
September 3, 1999	Ftpd-ex.c	Wu-ftpd exploit code for x86 Linux that allows a remote user to gain root access.	
September 3, 1999	**Mountd-ex.c**	**Mountd exploit code for x86 Linux where a remote user can gain root access.**	
September 3, 1999	Mutt-ex.c	An exploit script that allows local user to gain mail group access for X86 Linux 5.0	
September 3, 1999	Smbd-ex.c	SMBD exploit code for x86 Linux where a remote user can gain root access.	
September 3, 1999	Xterm-ex.c	Xterm exploit code for x86 Linux 4.0 that allows a local user to gain root access.	
September 2, 1999	Amdex.tgz	Buffer overflow exploit script that allows root access on machines running amd.	
September 2, 1999	Amd-exploit.c	Buffer overflow exploit script that allows root access on machines running amd.	
September 2, 1999	Mars.c	Buffer overflow script that allows local root compromise.	
September 2, 1999	**Nc4ex_ex.c**	**Exploit script for the EMBED buffer overflow vulnerability in Netscape for Windows 98.**	
September 2, 1999	**Nc4x_ex.cgi**	**Exploit script for the EMBED buffer overflow vulnerability in Netscape which executes welcome.exe.**	
September 2, 1999	**Nc4x_ex2.cgi**	**Exploit script for the EMBED buffer overflow vulnerability in Netscape which executes notepad.exe.**	
September 2, 1999	**Nfsexp.c**	**FreeBSD Exploit**	
August 31, 1999	Babacia.c	ProFTPD remote root exploit script.	
August 31, 1999	Crontab_exploit.c	Crond exploit script that allows root access.	
August 31, 1999	Pro.c	Script that exploits the proftpd remote buffer overflow vulnerability.	
August 31, 1999	W00w00crond.c	VixieCron 3.0 proof of concept exploit script.	
August 30, 1999	**Ddns.tar.gz**	**Exploit script that can be used for update spoofing.**	
August 30, 1999	Libtermcap.c	Exploit code that takes advantage of the libtermcap buffer overflow.	

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:

- **Weak passwords continue to be the number one cause of system compromise.**
- University computers continue to be main focus points for the hacking community.
- A recently publicized vulnerability is being used to modify opening web page, and subsequently turn off logging.
- Probe continues against well-known services and a variety of registered and unregistered service ports.
- Reports of intruders exploiting three different RPC service vulnerabilities to compromise UNIX systems continue.
- Analysis indicates that Hostile Active Code is now the hacker's weapon of choice.
- Infrastructure attacks continue to be directed against corporate e-mail systems.
- Systems connect to the Internet via cable modems and DSL lines are now reporting an average of two or more probes a day.

Viruses/Trojans

Cholera Worm Virus Warning: This is a new combined worm and virus threat. Cholera is similar to Worm.ExploreZip because it unleashes a worm-like attack and will automatically send itself to any e-mail address it finds on an e-mail system. The bug therefore supports the potential to shut down e-mail servers.

Cholera is not platform-dependent and can operate on any e-mail system. The bug also contains a virus aspect, dropping a virus file called W32/CTX, once it infects a new computer.

In its present form, Cholera sends itself to a recipient with a "smiley" face in the text and an attachment titled Setup.exe, which has the appearance of a self-extracting setup program.

Once resident, the worm installs itself by adding keys to WIN.INI on Win9x and registry on WinNT and tries to copy itself to any shared drives currently connected, then proceeds to infect executable files in the directory with a virus named W32/CTX.

The worm remains invisible to the user and becomes an auto-start application by writing a RUN entry to the Win.ini file (Windows 9x) or to the registry (Windows NT) and then deletes itself after resending itself as e-mail, leaving the virus resident.

Anti-virus vendors warn that even though no reports of infection "in the wild" have yet been received, there is a strong potential that virus writers might create and launch "copy-cat" versions of the bug.

CAP: A complex Word macro virus originally from Venezuela. It's complex because it consists of several encrypted macros, with names like CAP, AutoOpen, FileSaveAs, FileClose, FileOpen, and others. In addition, CAP deletes any existing macros from documents it infects, then removes the Tools/Macro and Tools/Customize menus to protect itself by staying hidden from view.

Despite its complexity, CAP has become one of the most commonly reported viruses in the world, because it was designed to fool users. Regardless of the format the user selects to save a document, CAP saves all files in Word's DOC format. For example, if a user saves a document as an RTF file, the result will actually be a DOC file (with the virus), even though the document will have an RTF extension. Since a true RTF file doesn't contain macros at all and thus can't spread macro viruses, users assume they're safe, and many antivirus scanners ignore them.

TROJ_Cain.15 (September 1, 1999): This Trojan program is a password recovery tool for Windows 95/98 operating systems. It is able to recover passwords like logon passwords, share passwords (both local and remote), screen saver passwords, dialup passwords, link passwords and any other application defined ones that are cached in your system or external. With this Trojan these passwords can be modified quickly.

Boobs Trojan Horse (August 1999): The Trojan creates some Registry entries including the one, which will enable it to run during all next Windows sessions. Unlike other password stealing Trojans the PSW.Boobs doesn't copy itself to \Windows\ or \Windows\System\ directory and is always started from the same location it was run first time. After activation the Trojan displays a dialog with a picture of a nude girl and a message 'Click Here'. When the picture is clicked the Trojan animates it. At the same time the Trojan scans all directory trees of the first hard drive and creates a log file WSTMP.$$$ where locations of all DOC files are listed. The Trojan uses this file as a 'flag' and doesn't show its dialog box again during further activations if this file already exists. The Trojan also creates an empty TMP.$$$ file in root directory of drive C:. After reboot the Trojan gets control and looks for a valid Internet connection. When it is acquired the Trojan sends all DOC files listed in WSTMP.$$$ to an e-mail address in Zaire <pearcem@sacs.co.za>. The subject line of the message is 'NBS As Requested'. The Trojan doesn't use any e-mail browser to send out messages, so data leak might be difficult to discovered.

Naebi v2.12-2.32 (August 31, 1999): The main function of this Trojan is a password logger and has basic file manipulation commands. This Trojan attaches to the IRQ preferences in your registry, running when ICG would.

Eclypse v 1.0 (August 30, 1999): The Trojan allows a hacker to open an FTP server to your harddrive, giving them full access to read, write, delete, or change, any file on your computer.

MBK (August 30, 1999): This is an e-mail bomber, designed to be placed on many computers, and each PC infected email bombs a single victim. Each Trojan sends one email bomb every ten seconds. While usually harmless to the infected PC, its devastating to the victims email account as well as the network it is on.

Progenic Password Thief / Keylogger v 1.0 (August 30, 1999): This one is a simple key logger that can be accessed remotely over the Internet. Its main use is to log passwords typed to be sent back to the person that installed it.

Retrieve v1.3 (August 30, 1999): This program gets and unencrypts passwords from applications to send back to its installed.

Spirit 2000 Beta v1.2 (August 7, 1999): The beta of this Trojan boasts the following features: can upload and download files from your harddrive, can grab ICQ and other passwords, as well as a special feature called “Burn Monitor”, which will constantly resets the screen resolution.