



# National Infrastructure Protection Center CyberNotes

Issue #20-99

September 29, 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 September 10 and September 24, 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
Apple <sup>1</sup>  <i>A free utility can be found on the Internet that retrieves the encrypted passwords and breaks their encryption mechanism.</i> <sup>2</sup>	MacOS	Passwords for MacOS are easily cracked.	No vendor supplied patch or workaround available at time of publishing.	MacOS Weak Password Encryption	<b>Medium / High</b>	Bug discussed in newsgroups and websites. Exploit has been published.

<sup>1</sup> Bugtraq, July 9, 1999.

<sup>2</sup> Securiteam, September 19, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
BindView	BindView HackerShield v1.1	HackerShield creates an account during installation, which has local administrator privileges and is created with a password, which is supposed to be randomly generated for each installation. However, due to a programming error the installer creates the same "random" password every time. This information could be used to gain unauthorized access to machines on which HackerShield is installed.	Take one of the following corrective actions: Download and run HackerShield 1.1 - Maintenance Patch 2: <a href="http://www.bindview.com/products/HackerShield/HS_Patch2.zip">http://www.bindview.com/products/HackerShield/HS_Patch2.zip</a> or, You may fix this problem manually by either changing the password to one of your choosing or by deleting the NetectAgentAdmin\$ account and using a different account to provide "log In As" permissions to the HackerShield services or, If you have installed an evaluation copy of 1.0 or 1.1 that is past its evaluation period, uninstaller HackerShield.	AgentAdmin Password Vulnerability	<b>High</b>	Bug discussed in newsgroups and websites. Password has been published.
FreeBSD <sup>3</sup>	FreeBSD 3.0, 3.1, 3.2	A vulnerability exists in the new VFS cache introduced in version 3.0 which allows a local and possibly remote user to force usage of a large quantity of memory creating a Denial of Service condition.	No workaround or patch available at time of publishing.	VFS_Cache Denial of Service Vulnerability	<b>Low</b>	Bug discussed in newsgroups and websites. Exploit script has been published.
FreeBSD <sup>4</sup>	FreeBSD 3.2 & earlier; FreeBSD- current; FreeBSD 3.3 Release	FreeBSD's profiling mechanism, allows an attacker to start execution of the program being profiled in any arbitrary location within the problem, leading potentially to root access.	Apply the patch located at: <a href="ftp://ftp.freebsd.org/pub/FreeBSD/CERT/patches/SA-99:02/">ftp://ftp.freebsd.org/pub/FreeBSD/CERT/patches/SA-99:02/</a>	Profiling Vulnerability	<b>Medium</b>	Bug discussed in newsgroups and websites.
FreeBSD <sup>5</sup>	FreeBSD 3.2 & earlier; FreeBSD- current; FreeBSD 3.2- stable	The FTS library functions contain multiple vulnerabilities which could allow a malicious user to create or overwrite an arbitrary file on the system, leading potentially to root access.	Patch for fts library: <a href="ftp://ftp.freebsd.org/pub/FreeBSD/CERT/patches/SA-99:05/">ftp://ftp.freebsd.org/pub/FreeBSD/CERT/patches/SA-99:05/</a> Patch for coredumps and symbolic links: <a href="ftp://ftp.freebsd.org/pub/FreeBSD/CERT/patches/SA-99:04/">ftp://ftp.freebsd.org/pub/FreeBSD/CERT/patches/SA-99:04/</a>	Multiple FTS Library Vulnerabilities	<b>High</b>	Bug discussed in newsgroups and websites.
FreeBSD <sup>6</sup>	FreeBSD 3.2 (& earlier); FreeBSD- current; FreeBSD 3.2- stable	The amd program contains a vulnerability, which could allow remote users to execute arbitrary code as root.	For patch, please see advisory located at: <a href="ftp://ftp.freebsd.org/pub/FreeBSD/CERT/patches-SA-99:06.amd.asc">ftp://ftp.freebsd.org/pub/FreeBSD/CERT/patches-SA-99:06.amd.asc</a>	Remote AMD Vulnerability	<b>High</b>	Bug discussed in newsgroups and websites. Exploit has been published.

<sup>3</sup> Bugtraq, September 21, 1999.

<sup>4</sup> CIAC Bulletin J-067, September 8, 1999.

<sup>5</sup> FreeBSD Security Advisory SA-99:05.fts, September 16, 1999.

<sup>6</sup> FreeBSD Security Advisory 99:06.amd, September 20, 1999.



Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Linux <sup>10</sup>  <i>ProFTPD 1.2.0pre6 has been found to also contain an exploitable buffer overflow.<sup>11</sup></i>	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. <b>Intel:</b> <a href="http://updates.redhat.com/powertools/6.0/i386/proftpd-1.2.0pre3-6.i386.rpm">http://updates.redhat.com/powertools/6.0/i386/proftpd-1.2.0pre3-6.i386.rpm</a> <b>Alpha:</b> <a href="http://updates.redhat.com/powertools/6.0/alpha/proftpd-1.2.0pre3-6.alpha.rpm">http://updates.redhat.com/powertools/6.0/alpha/proftpd-1.2.0pre3-6.alpha.rpm</a> <b>Sparc:</b> <a href="http://updates.redhat.com/powertools/6.0/sparc/proftpd-1.2.0pre3-6.sparc.rpm">http://updates.redhat.com/powertools/6.0/sparc/proftpd-1.2.0pre3-6.sparc.rpm</a> <b>Source packages:</b> <a href="http://updates.redhat.com/powertools/6.0/SRPMS/proftpd-1.2.0pre3-6.src.rpm">http://updates.redhat.com/powertools/6.0/SRPMS/proftpd-1.2.0pre3-6.src.rpm</a> <i>Upgrade to ProFTPD 1.2.0pre7</i>	Proftpd Buffer Overflow Vulnerability	<b>High</b>	Bug discussed in newsgroups and websites. Exploit scripts have been published. The vulnerability is being actively exploited on the Internet.  <i>Exploit has been released for ProFTPD 1.2.0pre6</i>
Matt Wright WWWBoard <sup>12</sup>	WWWBoard 2.0 Alpha 2	A vulnerability exists in the default installation of the WWWBoard package, which allows remote attackers to steal the encrypted password of the admin account.	Modify the '\$passwd_file' perl variable to point to a password file outside the web document tree.	Password Disclosure Vulnerability	<b>Medium</b>	Bug discussed in newsgroups and websites.
Microsoft <sup>13</sup>	Hotmail (Internet Explorer 5.0 or Netscape Communi- cator 4.x)	There is another security flaw in Hotmail which allows injecting and executing JavaScript code in an email message using the JavaScript protocol. The commands could take various actions on the user's inbox, including: reading e-mail, deleting E-mail, or prompting users to re-enter their password.	Workaround: Disable JavaScript	JavaScript Protocol Vulnerability	<b>High</b>	Bug discussed in newsgroups and websites. Exploit has been published. Vulnerability has appeared in the Press.

<sup>10</sup> RHSA-1999:034, August 31, 1999.

<sup>11</sup> Securiteam, September 20, 1999.

<sup>12</sup> SecurityFocus, September 16, 1999.

<sup>13</sup> Bugtraq, September 13, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft <sup>14</sup>	Microsoft Internet Information Server (IIS) 4.0; NT 4.0; BackOffice 4.5	IIS 4.0 allows an administrator the option to restrict access by specifying a domain or an IP address. Due to a regression error, a user who accesses an FTP site via a browser will be able to download files even if the files are marked "no access." The second problem is that IIS will allow access if it is unable to resolve the IP address of the requestor. This will occur even if the domain of the requestor has been restricted from access. This error only occurs on the first request.	A patch has been released that eliminates two vulnerabilities in IIS 4.0. Patch available at: <a href="ftp://ftp.microsoft.com/bussys/iis/iis-public/fixes/usa/IIS40/hotfixes-postSP6/security/IPRFTP-fix/">ftp://ftp.microsoft.com/bussys/iis/iis-public/fixes/usa/IIS40/hotfixes-postSP6/security/IPRFTP-fix/</a>	IIS 4.0 Domain Resolution Vulnerability	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft <sup>15</sup>	Microsoft Jet 4.0SP1; Microsoft MDAC 2.12.4202.3 (GA); Windows NT 4.0SP3, 4.0SP4	The fixes that Microsoft has made available for the JET/ODBC and RDS vulnerabilities may open the host to exploits via the MDAC RDS exploit.	No workaround or patch available at time of publishing.	Jet/ODBC & RDS Vulnerabilities	High	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft <sup>16</sup>	Microsoft Site Server 3.0, 3.0 Commerce Edition; Microsoft Commercial Internet System (MCIS) 2.0, 2.5	A vulnerability exists which allows a web site visitor to inadvertently access another customer's data, if their Internet gateway caches web pages via a proxy server and the web site authenticates based on a GUID.	Microsoft has released a patch that fixes this issue located at: <a href="ftp://ftp.microsoft.com/bussys/sitesrv/sitesrv-public/fixes/usa/siteserver3/Hotfixes-PostSP2/ProxyCache/">ftp://ftp.microsoft.com/bussys/sitesrv/sitesrv-public/fixes/usa/siteserver3/Hotfixes-PostSP2/ProxyCache/</a>	Set Cookie Header Caching Vulnerability	Medium	Bug discussed in newsgroups and websites.
Microsoft Windows 95, 98, 2000, NT <sup>17</sup>	Internet Explorer 5.0 for Windows 95, 98, 2000, NT 4.0	Vulnerability exists in IE5 that could allow a malicious web site operator to execute arbitrary programs on a victim's machine.	Until a patch is available, disable active scripting.	Import Export Favorites Vulnerability	High	Bug discussed in newsgroups and websites. Exploit has been published.

<sup>14</sup> Microsoft Security Bulletin (MS99-039), September 23, 1999.

<sup>15</sup> SecurityFocus, September 23, 1999.

<sup>16</sup> NTBugtraq, September 10, 1999.

<sup>17</sup> Microsoft Security Bulletin (MS99-037), September 10, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft Windows 95, 98, NT <sup>18</sup>	Windows 95.0a, 95.0b, 98.0se; NT Terminal Server, 4.0, 4.0SP1, 4.0SP2, 4.0SP3, 4.0SP4, 4.0SP5	It is possible to pass data through all Windows stacks on systems with two network interfaces which could allow an intruder to obtain information about the remote network while obscuring their origin.	Apply the patch located at: <u>Windows 95, 98, 98 2<sup>nd</sup> edition</u> To be released shortly <u>NT 4.0 Workstation, NT 4.0 Server, Enterprise edition</u> <a href="http://fpl.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/Hotfixes-PostSP5/Spoof-fix">ftp://fpl.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/Hotfixes-PostSP5/Spoof-fix</a> <u>NT 4.0 Server, Terminal Server Edition</u> To be released shortly	IP Source Routing Vulnerability	<b>Medium/ Low</b>	Bug discussed in newsgroups and websites. Exploit script has been published.
Microsoft Windows NT <sup>19</sup>	Microsoft Windows NT 4.0, 4.0SP1, 4.0SP2, 4.0SP3, 4.0SP4, 4.0SP5	An unprivileged network user may gain admin privileges.	No workaround or patch available at time of publishing. Unofficial workaround: Enable Auditing on the HKEY_Local_Machine/SYSTEM/CurrentControlSet/Services/RASMAN key. Look for changes in the ImagePath value.	Privilege Escalation Vulnerability	<b>High</b>	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Microsoft Windows NT <sup>20</sup>	NT 4.0	It is possible for a local user to modify how DCOM servers are run, thereby escalating his/her privilege level.	No workaround or patch available at time of publishing. Unofficial workaround: Restrict write permission to all DCOM registry keys and, using NTFS, service EXEs.	DCOM Server Vulnerability	<b>High</b>	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft Windows NT <sup>21</sup>	NT Workstation 4.0; Server 4.0; Server 4.0 Enterprise Edition; Server 4.0 Terminal Server Edition	Microsoft has released an advisory, informing administrators that it is possible that sensitive information (such as authentication information) used during unintended installs via prewritten scripts is saved in files on the system. It is possible for less privileged users of that system to read this information.	The fix is to delete \$oemsetup\$.inf. For more detailed information, view the FAQ: <a href="http://www.microsoft.com/security/bulletins/MS99-036faq.asp">http://www.microsoft.com/security/bulletins/MS99-036faq.asp</a>	Unattended Installation File Vulnerability	<b>High</b>	Bug discussed in newsgroups and websites. Exploit has been published.
Netplus SmartServer <sup>22</sup>	Work SmartServer 3.3.5.1; Cmail Server; Personal Mail Server; Tiny FTP Daemon; Internet Anywhere; FuseMail; AVirt Mail Server	POP3/SMTP servers from this vendor contain exploitable buffer overflow bugs, which could lead to control of the victim machine remotely.	Currently no workaround or patch available at time of publishing. <u>SmartServer 3.3.51</u> Upgrade to the latest Service Pack available at: <a href="http://www.speedsoft.com/netcplus/public/ss3sp21.exe">http://www.speedsoft.com/netcplus/public/ss3sp21.exe</a>	POP3/SMTP Buffer Overflow Vulnerability	<b>High</b>	Bug discussed in newsgroups and websites. Exploit scripts have been published.

<sup>18</sup> Microsoft Security bulletin (MS99-038), September 20, 1999.

<sup>19</sup> SecurityFocus. September 17, 1999.

<sup>20</sup> SecurityFocus, September 10, 1999.

<sup>21</sup> Microsoft Security Bulletin (MS99-036), September 10, 1999.

<sup>22</sup> Securiteam, September 17, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Network Solutions <sup>23</sup>	Dotcomnow Web Site Free Mail Accounts	There is a potential that any user can log into another user's e-mail account.	No workaround or patch available at time of publishing.	Free Web Mail Vulnerability	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Qualcomm <sup>24</sup>	Eudora 3.0x	Systems running Windows 95/98 and NT using Qualcomm's Eudora v3.x with the NAI PGP plug-in have a vulnerability in the manner which Eudora processes the sign and spellcheck commands. If the document is modified after it has been signed, they will have invalidated the PGP signature.	Upgrade to Eudora 4.x or for Eudora 3.x, disable spellchecking upon "send". Manually spellcheck text prior to PGP signing the document.	PGP Spelling Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Red Hat <sup>25</sup>	Linux 6.0 (all architectures); Linux 4.2, 5.2 Intel (mars_nwe was not built for Alpha and Sparc in previous versions of Red Hat Linux.)	Buffer overflows are present in the mars_nwe package. A local root compromise is possible if users create carefully designed directories and/or bindery objects.	<u>Linux 4.2:</u> Intel: <a href="ftp://updates.redhat.com//4.2/i386/mars-nwe-0.99pl17-0.4.2.i386.rpm">ftp://updates.redhat.com//4.2/i386/mars-nwe-0.99pl17-0.4.2.i386.rpm</a> Source packages: <a href="ftp://updates.redhat.com//4.2/SRPMS/mars-nwe-0.99pl17-0.4.2.src.rpm">ftp://updates.redhat.com//4.2/SRPMS/mars-nwe-0.99pl17-0.4.2.src.rpm</a> <u>Linux 5.2:</u> Intel: <a href="ftp://updates.redhat.com//5.2/i386/mars-nwe-0.99pl17-0.5.2.i386.rpm">ftp://updates.redhat.com//5.2/i386/mars-nwe-0.99pl17-0.5.2.i386.rpm</a> Source packages: <a href="ftp://updates.redhat.com//5.2/SRPMS/mars-nwe-0.99pl17-0.5.2.src.rpm">ftp://updates.redhat.com//5.2/SRPMS/mars-nwe-0.99pl17-0.5.2.src.rpm</a> <u>Linux 6.0:</u> Intel: <a href="ftp://updates.redhat.com//6.0/i386/mars-nwe-0.99pl17-4.i386.rpm">ftp://updates.redhat.com//6.0/i386/mars-nwe-0.99pl17-4.i386.rpm</a> Alpha: <a href="ftp://updates.redhat.com//6.0/alpha/mars-nwe-0.99pl17-4.alpha.rpm">ftp://updates.redhat.com//6.0/alpha/mars-nwe-0.99pl17-4.alpha.rpm</a> Sparc: <a href="ftp://updates.redhat.com//6.0/sparc/mars-nwe-0.99pl17-4.sparc.rpm">ftp://updates.redhat.com//6.0/sparc/mars-nwe-0.99pl17-4.sparc.rpm</a> Source packages: <a href="ftp://updates.redhat.com//6.0/SRPMS/mars-nwe-0.99pl17-4.src.rpm">ftp://updates.redhat.com//6.0/SRPMS/mars-nwe-0.99pl17-4.src.rpm</a>	Mars_Nwe Buffer Overflow Vulnerability	High	Bug discussed in newsgroups and websites. Exploit has been published.
SCO <sup>26</sup>  <i>Another security hole has been found.<sup>27</sup></i>	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. <i>A bigger security hole has been discovered that allows local users to execute commands as root.</i>	Change the permissions on /bin/doctor to 700.  <i>SCO is working on fixing the recent vulnerabilities and hopes to release a patch in two weeks.</i>	Doctor Command Execution Vulnerability	High	Bug discussed in newsgroups and websites. Exploit has been published. <i>Exploit script has been published</i>

<sup>23</sup> Securiteam, September 20, 1999.

<sup>24</sup> SecurityFocus, September 18, 1999.

<sup>25</sup> Red Hat Security Advisory RHSA-1999:037-01, September 13, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
SCO <sup>28</sup>  <i>Another script has been released that exploits this vulnerability.</i> <sup>29</sup>	OpenServer 5.0.x XBase package	Almost all the tools that come with this package are vulnerable to buffer overflow problems. Some of these tools are suid root, like scoterm, xterm and xload, and are very easy to exploit.	In newer versions, SCO have patched some holes but not all.	Buffer Overflow Vulnerability	High	Bug discussed in newsgroups and websites. Local root exploit script has been published.
SCO <sup>30</sup>	SCO 5.0.5	Numerous security holes have been found that allows potential root access. The SCOLock utility contains a vulnerability that allows local users to gain root privileges; a buffer overflow vulnerability exists in the 'deliver' daemon that allows root access; the 'Xsco' daemon contains a buffer overflow which allows root privileges; a vulnerability exists in /usr/bin/lpr which allows an unauthorized user rootshell access; and virtually all programs using the Xt library are vulnerability to a local root exploit.	No workaround or patch available at time of publishing. SCO is working on fixing the recent vulnerabilities and hopes to release a patch in two weeks.	Multiple SCO Vulnerabilities	High	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Sun <sup>31</sup>	Solaris 2.6_x86, 2.6	A vulnerability in Solaris TCP/IP stack may allow remote users to panic the system.	For Solaris 2.6 sparc apply patch 105529-07. For Solaris 2.6 x86 apply patch 105530. <a href="ftp://sunsolve.Sun.COM/pub/patches/Solaris2.6_x86.PatchReport">ftp://sunsolve.Sun.COM/pub/patches/Solaris2.6_x86.PatchReport</a>	Recursive Mutex_enter Panic Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Sun <sup>32</sup>	Solaris 2.6_x86, 2.6, 2.5.1_x86, 2.5.1	The dynamic linker ld.so.1 contains vulnerability when profiling dynamic libraries, which allows a malicious user to create world writeable files as root anywhere in the file system.	Solaris patches available from <a href="http://access1.sun.com">http://access1.sun.com</a> Solaris 2.5.1 103627 Solaris 2.5.1x86 103628 Solaris 2.6 105490 Solaris 2.6x86 105491	LD_Profile Vulnerability	High	Bug discussed in newsgroups and websites. Exploit has been published.

<sup>26</sup> Securiteam, September 9, 1999.

<sup>27</sup> Securiteam, September 16, 1999.

<sup>28</sup> Bugtraq, June 14, 1999.

<sup>29</sup> Securiteam, September 20, 1999.

<sup>30</sup> Securiteam, September 17, 1999.

<sup>31</sup> SecurityFocus, September 24, 1999.

<sup>32</sup> SecurityFocus, September 22, 1999.



Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Unix <sup>39</sup>	Cfingerd 1.4.2 and earlier	A buffer overflow exists in cfingerd that will allow arbitrary code execution with root (or nobody) privileges. The attacker must carefully set GECOS.	No workaround or patch available at time of publishing.	Cfingerd Buffer Overflow Vulnerability	<b>High</b>	Bug discussed in newsgroups and websites. Exploit script has been published.
Unix <sup>40</sup>	Multiple Unix Vendors: Compaq (Digital), IBM, Solaris, Open Group	A buffer overflow vulnerability exists in the dtsession program that can lead to local root compromise.	<u>Compaq Computer Corporation:</u> A patch for this problem has been made available for Tru64 UNIX V4.0D, V4.0E, V4.0F and V5.0 at: <a href="http://www.service.digital.com/patches">http://www.service.digital.com/patches</a> <u>IBM Corporation:</u> For customers that require the CDE desktop functionality, a temporary fix is available via anonymous ftp from: <a href="ftp://aix.software.ibm.com/aix/efixes/security/cdecert.tar.Z">ftp://aix.software.ibm.com/aix/efixes/security/cdecert.tar.Z</a>	CDE TT_SESSION Buffer Overflow Vulnerability	<b>High</b>	Bug discussed in newsgroups and websites. Exploit script has been published.
Unix <sup>41</sup>	Multiple Unix Vendors: HP, Compaq (Digital), IBM, Novell, Sun Solaris	It is possible for local/remote users to falsely identify themselves to the system due to the way authentication is conducted in the dtsession program.	<u>Compaq Computer Corporation:</u> A patch for this problem has been made available for Tru64 UNIX V4.0D, V4.0E, V4.0F and V5.0 at: <a href="http://www.service.digital.com/patches">http://www.service.digital.com/patches</a> <u>IBM Corporation:</u> For customers that require the CDE desktop functionality, a temporary fix is available via anonymous ftp from: <a href="ftp://aix.software.ibm.com/aix/efixes/security/cdecert.tar.Z">ftp://aix.software.ibm.com/aix/efixes/security/cdecert.tar.Z</a> <u>Sun Microsystems:</u> The use of DES authentication is recommended to resolve this issue. To set the authentication mechanism to DES, use the ttsession command with the '-a' option and specify 'des' as the argument (see ttsession(1) for more information). DES authentication also requires that the system use Secure NFS, NIS+, or keylogin. See the System Administration Guide, Volume II. <u>HP-UX:</u> Install the applicable patch: HP-UX release 10.10 In progress; HP-UX release 10.20 PHSS_19747; HP-UX release 10.24 PHSS_19819; HP-UX release 11.00 PHSS_19748	CDE Ttsession Authentication Vulnerability	<b>High</b>	Bug discussed in newsgroups and websites. Exploit script has been published.

<sup>39</sup> Bugtraq, September 21, 1999.

<sup>40</sup> SecurityFocus, September 15, 1999.

<sup>41</sup> SecurityFocus, September 15, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Unix <sup>42</sup>	Solaris 2.5.1, 2.6, 7	The CDE subprocess daemon /usr/dt/bin/dtspcd contains insufficient checking on client credentials which can lead to a local root compromise.	No workaround or patch available at time of publishing.	CDE DTSPCD Root Compromise Vulnerability	<b>High</b>	Bug discussed in newsgroups and websites. Exploit script has been published.
Unix <sup>43</sup>	Solaris 2.5.1, 2.6, 7; Digital Unix	A buffer overflow vulnerability exists which could lead to local root compromise.	Digital Unix patch found at: <a href="http://ftp.service.digital.com/public/Digital_UNIX/">http://ftp.service.digital.com/public/Digital_UNIX/</a> NOTE: The patch has a major omission in the instructions, it does not tell the administrator to remove the setuid root off the original file, to do so use the following command: #chmod 0100 /usr/dt/bin/dtaction.orig No workaround or patch available at time of publishing for Solaris.	CDE Dtaction Vulnerability	<b>High</b>	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Unix <sup>44</sup>	Solaris 2.7	A possible buffer overflow vulnerability exists in the sgid mail/usr/bin/mail, which allows execution of any command a malicious user wants.	No workaround or patch available at time of publishing.	Usr/bin/mail Security Vulnerability	<b>Medium</b>	Bug discussed in newsgroups and websites. Exploit has been published.
Unix <sup>45</sup>	SuSE 6.2	Several holes exist in the way SuSE suid root is set by default that could be used by local users to access protected files.	No workaround or patch available at time of publishing.	Configuration File Vulnerability	<b>Medium</b>	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.

<sup>42</sup> Technotronic, September 14, 1999.

<sup>43</sup> Technotronic, September 14, 1999.

<sup>44</sup> Securiteam, September 16, 1999.

<sup>45</sup> Bugtraq, September 16, 1999.

## Recent Exploit Scripts

The table below contains a representative sample of exploit scripts, identified between September 10 and September 24, 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, 52 scripts, programs, and net-news messages containing holes or exploits were identified.

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
September 24, 1999	Irixlp.c	Scans for default logins on IRIX boxes.	
September 24, 1999	Pippa.pl	A small network datapipe that redirects a network connection from one site to another, hiding the identity of the real connection originator and exposing just the host where the datapipe is running.	
<b>September 24, 1999</b>	<b>Sccw.sh</b>	<b>SuSE exploit script for the sscw home environment variable buffer overflow vulnerability</b>	
September 24, 1999	Targa2.c	Remote DoS attack against 11 different IP stack holes on various operating systems.	
<b>September 24, 1999</b>	<b>Webscan.c</b>	<b>Multithreaded high speed scanner that records the versions of web servers and scans for 65 different CGIs.</b>	
September 23, 1999	Crypt7.zip	Cryptographic utility using private key random salting DoS binary.	
September 23, 1999	ExploitExpress.zip	This is an engine that will parse scripts written in its own scripting language and submit information to CGI scripts.	
September 23, 1999	Gateway.tgz	Password protected remote shell daemon that integrates a Syn flooder, bounce/gateway, port scanner, and remote root exploits.	
September 23, 1999	Leapfrog 1.0	The Leapfrog utility will anonymize and redirect any port. It can be used to work around firewall configuration and other issues requiring a port redirect.	
September 23, 1999	Lscan2.c	Multithreaded high speed scanner than scans for six different daemons and records the version of every daemon for analysis.	
September 23, 1999	Mw06.tgz	Unix internet worm.	
September 23, 1999	Nscan.c	An iquery request and a version query are performed and if both succeed, the host will be logged in a file.	
September 23, 1999	Obsidian.tgz	A unix virus (ELF infector).	
September 23, 1999	Phantom.tgz	Linux promiscuous Ethernet sniffer that sends sniffed traffic to remote logging daemon.	

<b>Date of Script (Reverse Chronological Order)</b>	<b>Script Name</b>	<b>Script Description</b>	<b>Comments</b>
September 23, 1999	Pipefakeps.c	Modified version of datapipe, where you can specify a name that will displayed instead of the process' name.	
September 23, 1999	Pot.tgz	Ping observation tool that is a high-speed tool to sweep for smurf broadcast amplifiers.	
September 23, 1999	Rfscan.zip	A program to scan for Cold Fusion vulnerabilities by feeding it a list of domains and it will let you know if any are vulnerable.	
September 23, 1999	Tfn.tgz	Flood network client/server that can be installed on a large number of hosts and used to hit a target with high bandwidth simultaneously.	
<b>September 23, 1999</b>	<b>Tgiscan.c</b>	<b>Phf, CGI, htmlscript, view-source, wrap, campas, pfdisplay, webdist, aglimpse, php, nph-test-cgi scanner.</b>	
September 23, 1999	Vetescan09-22-1999.tar.gz	Unix/Windows remote vulnerability exploit scanner with fixes for vulnerabilities.	
<b>September 23, 1999</b>	<b>Vfs_cache.c</b>	<b>A Denial of Service exploit script for the VFS cache vulnerability.</b>	
September 22, 1999	Dnsabuser.c	Exploit code for a DoS attack using DNS.	
September 22, 1999	DoS_frontpage.pl	Perl exploit code to crash Front Page remotely.	
<b>September 22, 1999</b>	<b>Scosessionx.c</b>	<b>Scosession local bin exploit script.</b>	
<b>September 22, 1999</b>	<b>Scotermx.c</b>	<b>Scoterm local root exploit script.</b>	
September 22, 1999	Smashdu.c	Digital Unix exploit script for the dtaction vulnerability.	
September 22, 1999	Wtkill.pl	Exploit script for remote DoS of Webtrends Enterprise reporting server.	
<b>September 21, 1999</b>	<b>Cfingerd.c</b>	<b>GECOS buffer overflow vulnerability exploit script.</b>	
<b>September 21, 1999</b>	<b>Fragrouter-1.6.tar.gz</b>	<b>IP source routing attack script.</b>	
September 20, 1999	Xloadx.c	Local root exploit script for SCO OpenServer 5.0.4 xlock vulnerability.	
<b>September 20, 1999</b>	<b>Xtermx.c</b>	<b>Local root exploit script for SCO OpenServer 5.0.4</b>	
<b>September 19, 1999</b>	<b>Deliverx.c</b>	<b>SCO local root exploit script.</b>	
<b>September 19, 1999</b>	<b>Scolockx.c</b>	<b>Local exploit script that gives you an auth group suid shell for the SCOLock vulnerability.</b>	

<b>Date of Script</b> (Reverse Chronological Order)	<b>Script Name</b>	<b>Script Description</b>	<b>Comments</b>
September 17, 1999	BertzHole.exe	This program will change the binary path name of the service to be executed by the RasMan Service.	
September 17, 1999	BertzSvc.exe	An executable that modifies the RASMAN/ImagePath key and a sample Trojan service that may be run.	
<b>September 17, 1999</b>	<b>Sco_lpr.c</b>	<b>Buffer overflow exploit script that exploits the /usr/remote/lpd/lp vulnerability and gives you rootshell.</b>	
September 16, 1999	Netcplus.c	Buffer overflow exploit script for Work SmartServer3 that may allow an intruder to execute arbitrary code on the target server.	
<b>September 16, 1999</b>	<b>Solx86.c</b>	<b>Solaris 2.7 exploit script, which allows execution of any command you wish.</b>	
September 16, 1999	Ultra Password Crackers	This three password-cracking components: Word 97 Password Cracker; Excel 97 Password Cracker; and Zip Password Cracker.	
<b>September 15, 1999</b>	<b>Ovsession.c</b>	<b>Exploit script for the CDE TT_Session buffer overflow vulnerability.</b>	
<b>September 15, 1999</b>	<b>Ttsession.c</b>	<b>Exploit script for the CDE Ttsession authentication vulnerability.</b>	
<b>September 14, 1999</b>	<b>Dtaction_ov.c</b>	<b>Exploit script for the dtaction vulnerability for Solaris</b>	
<b>September 14, 1999</b>	<b>Dtspaced.c</b>	<b>Exploit script for the local root hole vulnerability with dtspcd.</b>	
<b>September 14, 1999</b>	<b>Sco_xt.c</b>	<b>SCO XT library overflow exploit script.</b>	
<b>September 12, 1999</b>	<b>Cmail_Server.c</b>	<b>Cmail Server 2.3 SP2 exploit for Windows 98 buffer overflow vulnerability.</b>	
<b>September 12, 1999</b>	<b>FuseMail.c</b>	<b>FuseMail Version 2.7 exploit for Windows 98 buffer overflow vulnerability.</b>	
<b>September 12, 1999</b>	<b>Personal_Mail_Prog1.c</b>	<b>Personal Mail Serer Version 3.072-3.09 exploit for Windows 98 buffer overflow vulnerability that sends the small client program which executes a Trojan after translation from the other host.</b>	
<b>September 12, 1999</b>	<b>Personal_Mail_Server_Prog2.c</b>	<b>Personal Mail Server Version 3.072-3.09 exploit for Windows 98 buffer overflow vulnerability program translation server which is used by Program 1 described above.</b>	
September 12, 1999	Work_SmartServer3.c	NecPlus SmartServer3 exploit for windows 98 buffer overflow vulnerability.	
September 3, 1999	Solaris_LCmessages.txt	Exploit code to utilize the LC_MESSAGES bug in Solaris 2.7 to gain root.	
<b>September 3, 1999</b>	<b>St2.c</b>	<b>SCO exploit script that gives you root access.</b>	

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
September 3, 1999	Xserverx.c	Exploit script that gives you root access in SCO.	

## 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](mailto: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:

- Intrusion detection systems ranging from home computers with cable modems to high-end government facilities have been reporting a large number of probes to TCP port 3128.
- 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 web pages and turn off logging.
- 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.

## Viruses/Trojans

**Suppl.doc:** This is a new virus that is quietly replicating itself using some of the same techniques as Worm.ExploreZip. This virus waits 163 hours from infection before it starts rendering files unusable.

SUPPL.DOC has macro code which makes use of two routines found in the DLL files, LZ32.DLL and KERNEL32.DLL. When the document is opened, if Word's macro warning feature is enabled, a warning appears.

The virus will write three files to the Windows directory -- WININIT.INI, DLL.LZH, and ANTHRAX.INI -- then automatically expand the compressed file DLL.LZH to DLL.TMP. The file DLL.TMP is a replacement WSOCK32.DLL file. The contents of the new WININIT.INI file instructs the operating system to replace the current WSOCK32.DLL file by first renaming it to WSOCK33.DLL, then renaming DLL.TMP to WSOCK32.DLL.

The new WSOCK32.DLL includes the instructions to both monitor outbound email and to begin nulling files. If a recipient opens the attachment, they will see only a blank screen while the system is infected. Approximately 163 hours after infection, the virus will begin "nulling," or setting the file's length to zero

bytes rendering data inaccessible. The Suppl.doc is both a Trojan horse and a virus, with the potential to render useless files with the extensions, .doc, .xls, .txt, .rtf, .dbf, .zip, .arj and .rar on a victim's hard-drive by setting those document's file lengths to zero.

**Y2K Countdown or Polyglot Trojan:** A new Trojan horse has surfaced that is searching for login, username and password information. The malicious code has been distributed as an attachment called Y2KCOUNT.EXE in e-mail claiming to be from Microsoft Corp. It spoofs the return address "support@microsoft.com" and uses the subject "Microsoft Announcement." **Microsoft has warned users to delete the message without opening it.**

The text of the message "announces" something it calls the Microsoft Year 2000 Counter and urges users to run the software attachment. Once the file is executed, a WinZip self-extracting dialog box and fake message box appear, containing this line: Password protection error or invalid CRC32!.

The Trojan horse then places four files -- PROCLIB.DLL, PROCLIB.EXE, PROCLIB16.DLL and SVSRV.DLL -- into the Windows System directory of an infected machine and overwrites the contents of WSOCK32.DLL.

The altered software affects files that control communications with the Internet, and searches for the words "password," "login" and "username" in incoming and outgoing mail..

**W32/Fix2001:** The W32/Fix2001 worm normally arrives in an email claiming (in both Spanish and English) to be a fix for a Y2K Internet bug. If the attached file is executed, the virus copies itself to the Windows System folder and changes setting in the Registry. It then displays the message "Your Internet Connection is already Y2K, you don't need to upgrade it."

After rebooting the computer, all outgoing mail will be followed by another message with this virus as an attachment. The E-mail has the subject: "Internet problem year 2000." and appears to be from "Administrator". The message includes the following text:

"Internet Customer:

We will be glad if you verify your Operative System(s) before Year 2000 to avoid problems with your Internet Connections. If you are a Windows 95 / 98 user, you can check your system using the Fix2001 application that is attached to this e-mail or downloading it from Microsoft (C) WEB Site: [HTTP://WWW.MICROSOFT.COM](http://WWW.MICROSOFT.COM) if you are using another Operative System, please don't wait until Year 2000, ask your OS Technical Support.

Thanks. Administrator."

**W2KM\_IRCJACK.A:** This is a macro virus that infects Microsoft Word 97 and 2000 templates and documents. It disables the menu Tools/Macro, Tools/Customize, View/Toolbars and View/Status Bar in infected documents. . This virus is currently being spread as a document file "Storyu.doc" via MIRC.

Upon execution, this macro virus copies the original MIRC if it exists, to c:/windows/script1.ini, and reloads the modified c:/mirc/script.ini to the system.

The virus also sends text e-mail in a random manner to the following e-mail addresses and sites:

Mirc.com, georgecarlin.com, carrottop.com, anvdesign.net, Symantec.com, drsolomon.com, www.bocklags.wisc.edu, ebay.com, evrt@avp.com, samples@datafellows.com, virus\_research@nai.com and tech\_support@mai.com.

The e-mail may contain the following text: Jack-In-The-Box Has Popped Up Again

**Bobo (24 September 1999):** Another Trojan, basically a small subset of commands from BackOrifice, with much the same interface as the BackOrifice GUI. This Trojan has no registry editor commands or plugin support.

**Depththroat updated to include 3.1 (final ?) (24 September 1999):** This Trojan adds a registry line not only when its run, but when its shutdown. Some small changes to the application.. author claims it is the final version

**Doly updated to include version 1.6 (24 September 1999):** Doly is a destructive Trojan, which is difficult to get rid of. Some of the features of this Trojan are:

- Trojan comes in setup.exe installer form pretending to be a memory manager.
- Single button 'format harddisk' command.
- FTP server of harddrive.
- Can change 'owner name' shown in System control panel.
- Change window names, close, move, and etc windows.
- Change most monitor settings

**Matrix updated to include 1.5 (24 September 1999):** This is a Trojan based on the sourcecode to Girlfriend Trojan. Its main features seems to be an FTP like file server, and the ability to update the Trojan exe on a victims computer to a newer version with one button click.

**Donald Dick v 1.52 (24 September 1999):** A new remote administration tool, similar to Bo2K or NetBus. Runs on 95, 98 and NT 4.0. Allows full access to the File system, Processes and threads, the Registry, system information and a lot more.

**Eclipse2000 (24 September 1999):** A lot of features of NetBus, tries to add in multiple places in registry to make it harder to remove, but no features that are outstanding.

**InCommand v1.0 (24 September 1999):** Seems to have the standard file transfer, program control and registry editing ability. But does have potential to be damaging.

**NetSphere v1.0 – 1.31337 (24 September 1999):** This Trojan has all the features you see in NetBus, plus a few extras such as Kill CPU, add to the ICQ, see the open ports on target, IP scan, view ALL hidden windows processes, etc.

**SubSeven v1.0 – 2.0 (Updated 23 September 1999):** The SubSeven Trojan has the exact same feature list as NetBus, with one original feature: The server can send the hacker your IP when you connect to the Internet by either e-mail and/or ICQ.