National Infrastructure Protection Center CyberNotes

Issue #14-99 *July 7, 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 June 21 and July 2, 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.**

Hardware/ Operating System	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
BSD, Linux, IRIX, AIX, SCO, SunOS[1]	Pine MUA (up to & including v4.10)	A security hole exists that allows a malicious remote attacker to potentially execute arbitrary code, resulting in a possibility of a root compromise.	Pine 4.10 patch is available for download at: http://hhp.hemp.net/	Charset Vulnerability	High	Bug discussed in newsgroups and websites. Exploit script has been published.

[1] Bugtraq, June 22, 1999.

Hardware/ Operating System	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Hewlett-Packard [2]	HP-UX Series 700, release 10.20	HP Visualize Conference is a T-120 conference solution for HP-UX Workstations. The ftp capability allows a conference participant to push a file to all other participants, which could result in a possible DoS attack or unauthorized access.	Apply PHSS_17168 available at: ftp://us-ffx.external.hp.com	HP Visualize Conference Vulnerability	Medium	Bug discussed in newsgroups and websites.
Internet Software Consortium[3]	Red Hat Linux 6.0 shipped with PHP 3.0.7.	This release of PHP had some problems with glibc 2.1. **A later errata release corrected those problems, but it had problems with postgresql, which it intended to support.**	Upgrade to the new PHP 3.0.9 RPMs. **Intel:** ftp://updates.redhat.com/6.0/i386/ **Alpha:** ftp://updates.redhat.com/6.0/alpha/ **Sparc:** ftp://updates.redhat.com/6.0/sparc	PHP RPM Vulnerability	Low	Bug discussed in newsgroups and websites.
Internet Software Consortium[4]	Red Hat Linux 6.0 net tools	A change to 32 bit UID_t's within glibc 2.0.x opened a potential buffer overrun vulnerability.	Buffer Overruns have been corrected within the net-tools package which can be found 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	Net Tools Buffer Overruns Vulnerability	Low	Bug discussed in newsgroups and websites.
Internet Software Consortium[5]	Red Hat Linux 5.2 (all architectures)	A change to 33 bituid-t's within glibc 2.0x has opened a potential hole in root squashing.	Updates can be found at: **Intel:** ftp://updates.redhat.com/5.2/i386 **Alpha:** ftp://updates.redhat.com/5.2/alpha **Sparc:** ftp://updates.redhat.com/5.2/sparc	NFS-Server Vulnerability	Medium	Bug discussed in newsgroups and websites.

[2] HPSBUX9906-099, June 28, 1999.
[3] RHEA-1999:010-01, June 21, 1999.
[4] RHSA-1999:017-01, June 24, 1999.
[5] RHSA 199:016-01, June 24, 1999.

Hardware/ Operating System	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Internet Software Consortium[6]	Red Hat Linux 6.0 XFree86 RPMs	Numerous vulnerabilities exist on the XFree86 package which include: the font server is hardcoded not to accept TCPconnections; a race condition leads to slow startups on X servers which is entirely cached in memory; there are some problems with inputting ISO-8859-1 characters with an ISO-8859-2 language in use; by default, the directory /etc/X11/xdm/authdir does not exist, which causes the X server to fall back to no authentication at all; and users who did not use Xkb keyboard extension had problems with backspace and Motif applications.	You should upgrade at least the core XFree86 package, the font server (xfs) package, the libraries, and the server for your video card. More detailed instructions on installing XFree86 are available from: `http://www.redhat.com/corp/support/docs/XFree86-upgrade/XFree86-upgrade.html` Also upgrade your xinit package: rpm-Uvh xinitrc-2.4-1.noarch.rpm	XFree86 Vulnerabilities	Medium	Bug discussed in newsgroups and websites.
Microsoft[7]	PGP v 2.x	Microsoft Exchange has a feature that tries to interpret PGP encrypted messages sent in ACSII RASDIX-64 format, which compromises communications to the point that messages cannot be decrypted and must be re-sent by other means.	No patch or workaround available at time of publishing.	PGP Encryption Vulnerability	Low	Bug discussed in newsgroups and websites.
Microsoft[8]	MS Outlook 97/98/2000	A DoS attack against Microsoft Outlook clients because Outlook looks for unique uidl's for each message and if there are duplicates it will hang prior to downloading any mail.	No patch or workaround available at time of publishing.	MS Outlook Mail Vulnerability	Low	Bug discussed in newsgroups and websites.
Microsoft[9]	Windows 98/2000	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.	Invalid IGMP Header Vulnerability	Low	Bug discussed in newsgroups and websites. Two Exploit scripts have been published.

[6] RHSA-1999:013-01, June 14, 1999.
[7] Bugtraq, June 22, 1999.
[8] Bugtraq, June 25, 1999.
[9] Bugtraq, July 2, 1999.

Hardware/ Operating System	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft[10]	Internet Information Server 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	Double Byte Code Page Vulnerability	Medium	Bug discussed in newsgroups and websites.
Microsoft[11]	IIS 4.0 Peer Web Services	An attacker can do a search on Alta Vista for "Microsoft Peer Web Services", then get a complete list of NT Workstations running this service. The user will then be prompted for a UserID and password and if successful authentication takes place where they are given access to sensitive server information.	No workaround or patch available at time of publishing.	Microsoft Peer Web Services Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft NT Server[12]	Cognos PowerPlay Web Edition	Executions of the PowerPlay CGI pulls cube data into files in an unprotected temporary directory, which could result in a brute force attack.	No patch or workaround available at time of publishing.	PowerPlay Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit has been published.
SCO[13]	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.

[10] Microsoft Security Bulletin (MS99-022), June 24, 1999.
[11] Bugtraq, June 17, 1999.
[12] Bugtraq, June 28, 1999.
[13] Bugtraq, June 14, 1999.

Hardware/ Operating System	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Solaris[14]	Cabletron Spectrum Enterprise Manager 5.0.1	Directory permissions situation can be exploited by an unprivileged shell user, which causes a component of Spectrum to run any executable as root.	No patch or workaround available at time of publishing.	Unprivileged User Vulnerability	**High**	Bug discussed in newsgroups and websites.
Sun[15]	Solaris 7.0	The Solaris useradd binary has a bug, which can possibly allow users who are supposed to be expired by a certain time to login. The problem with useradd is the interpretation of the value passed after the paramater -e (expire). The consequence of this vulnerability is having expired users having access to the vulnerable host.	Workaround supplied by Sun.	Useradd Program Expiration Date Vulnerability	**If expiration dates are critical, you have a real problem**	Bug discussed in newsgroups and websites. Exploit script has been published.
Unix[16] **Several security holes have been closed, and other bugs noted in the original RPMs have been corrected.[17]**	**KDE's K-Mail 1.1**	**When K-Mail receives an e-mail with attachments, it creates a directory to store the attachments. K-Mail does not verify that the directory already exists and will follow symbolic links, allowing local attackers to create files with the contents they choose in any directory writable by the user executing K-Mail. If K-Mail is run as root, unauthorized superuser access may be obtained.**	**Patch available at:** **ftp://ftp.kde.org/pub/kde/security_patches/kmail-security-patch.diff** **Upgrade to KDE 1.1.1 final, which fixes a number of bugs present in the previous release and contains additional patches to correct security holes in kmail and kvt. For each RPM for your particular architecture, run:** **rpm -Uvh <filename>** **where filename is the name of the RPM.**	**K-Mail File Creation Vulnerability**	**High**	**Bug discussed in newsgroups and websites.**
Unix[18]	Debian GNU/Linux	A bug in LRPng server (when installed with default settings) allows a malicious user to take control over the printing queues on LPRng server.	No workaround or patch available at time of publishing.	Print Queue Vulnerability	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.

[14] Bugtraq, June 23, 1999.
[15] Bugtraq, June 10, 1999.
[16] ISS Security Advisory, June 9, 1999.
[17] RHSA-1999:015-01, June 21, 1999.
[18] Bugtraq, July 2, 1999.

Hardware/ Operating System	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Unix, Linux, FreeBSD, Solaris/x86, SCO[19]	Xi Graphics, Inc.'s Accelerated-X Server 4.x, 5.x (and possibly earlier versions)	Local users can gain administrative privileges by exploiting multiple buffer overflows (stack overwrites).	**AccelX 5.x**: ftp://ftp.xig.com/pub/updates **AccelX 4.x**: Patch will be made available shortly. An interim solution is to use an X-server wrapper, or to limit access to the Xaccel binary via a special group.	Accelx Buffer Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
VMware, Inc.[20]	Linux 1.0.1 & all previous versions	VMware for Linux is vulnerable to a buffer overflow attack which results in unprivileged root access.	Upgrade to VMware v1.0.2. Upgrade can be found at: http://www.vmware.com/dowload/downloadlinux.html	Buffer Overrun Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Voice Mail[21]	Pagoo Internet voice MailBox	The password to the specified PagooID is vulnerable when you connect to your UpdateForm through signup.asp.	No workaround or patch available at time of publishing.	Voice Mail Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Windows 98[22]	Netscape 4.6	Communicator will open up an email message and start inserting hundreds of recipients into the header part, effectively shutting down until this process is complete.	No workaround or patch available at time of publishing.	Netscape 4.6 Mail Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Windows NT[23]	NT4	A race condition exists which allows users with access to the root directory of the boot partition to plant Trojans that will be executed at logged-on user privileges.	No workarounds or patches available at time of publishing.	Race Condition Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Windows NT[24]	Eastman Software's Work Management 3.21	Passwords are stored in cleartext in the COMMON and LOCATOR keys.	No workaround or patch available at time of publishing.	Password Cleartext Vulnerability	Medium	Bug discussed in newsgroups and websites.

[19] KSR[T] Advisory 011, June 25, 1999.
[20] Bugtraq, June 25, 1999.
[21] Bugtraq, June 22, 1999.
[22] Bugtraq, June 30, 1999.
[23] Securiteam, July 2, 1999.
[24] NTBugtraq, June 24, 1999.

Hardware/ Operating System	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Windows NT[25] **(Microsoft has issued patch)[26]**	**Windows Terminal Server 4.0**	**The bug occurs when a thread changes its priority. NT changes the thread's priority, but also gives it a new execution quantum. By repeating this process, a single thread can monopolize a CPU.**	**No workaround or patch available at time of publishing.** **Patch available at:** **ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/Hotfixes-PostSP5/CSRSS-fix**	**Never Ending Quantum Vulnerability**	**Low**	**Bug discussed in newsgroups and websites. Exploit script has been published.**
Windows NT.[27]	Microsoft Windows NT 4.0 Workstation; 4.0 Server; 4.0 Server Terminal Edition 4.0	A remote attacker can crash systems running Windows NT Local Security Authority (LSA).	Patch available at: ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP5/LSA3-fix	Malformed LSA Request Vulnerability	**High**	Bug discussed in newsgroups and websites.
Windows NT[28]	Microsoft Windows NT 4.0 Workstation; 4.0 Server; 4.0 Server Terminal Edition 4.0	If an executable file with a specially malformed image header is executed, it will cause a system failure. The affected machine will need to be rebooted in order to place it back in service.	Patch available at: **Windows NT Server and Workstation 4.0:** ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/Hotfixes-PostSP4/Kernel-fix/ **Windows NT Server 4.0, Terminal Server Edition:** ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40tse/Hotfixes-PostSP4/Kernel-fix/	Malformed Image Header Vulnerability	Low	Bug discussed in newsgroups and websites.
Windows, Unix[29]	Session Directory (SDR earlier than version 2.6.3)	A serious security problem has been discovered with SDR which will allow remote intruders to execute arbitrary code with the privileges of the SDR user. This problem exists in all recent versions of SDR and affects both unix and windows versions.	This problem has been fixed in SDR 2.6.3.	SDR Vulnerability	**High**	Bug discussed in newsgroups and websites.

*Risk is defined in the following manner:

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

[25] Bugtraq, June 9, 1999.
[26] Microsoft Security Bulletin (MS99-021), June 23, 1999.
[27] Microsoft Security Bulletin (MS99-020), June 23, 1999.
[28] Microsoft Security Bulletin (MS99-023), June 30, 1999.
[29] Bugtraq, June 21, 1999.

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

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

Recent Exploit Scripts

The table below contains a representative sample of exploit scripts, identified between June 21 and July 2, 1999, listed by date of script, script name, 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, 20 scripts, programs, and net-news messages containing holes or exploits were identified.

Date of Script **(Reverse Chronological Order)**	**Script Name**	**Script Description**	**Comments**
July 2, 1999	SKIaccelX.c	Exploit script for a vulnerability found in the Accelerate-X Xserver (Versions 5.0 and earlier).	
July 2, 1999	**Kox.c**	**Windows 98 and Windows 2000 TCP/IP stacks malformed IGMP header exploit.**	
July 2, 1999	**Kod.c**	**Malformed IGMP header exploit which will bluescreen windows and kill TCP stack. Exploit works on BSD/Linux/*nix/Windows 98/2000**	
July 2, 1999	Uzip.tgz	BSD UFS Secure Level 1 Vulnerability exploit.	
June 30, 1999	Sunexp	Latest Solaris 7.0 local exploit script for the useradd binary vulnerability that allows users who are supposed to be expired by a certain time to login.	
June 29, 1999	Vmware.c	Exploit script that allows a buffer overrun attack, which results in unprivileged root access to a machine..	
June 28, 1999	Cable.modem.ip.hihack.txt	Detailed description of how to exploit cable modem security flaws and effectively hijack IP addresses.	
June 28, 1999	NULL session weaknesses	Detailed paper describing how to programmatically connect to NT Server NULL Sessions and extract the name of the true administrator account.	
June 27, 1999	Propecia.c	A fast class C domain scanner than scans for a specified open port.	
June 27, 1999	IsOf.c	Isof 4.40 exploit local root compromise.	
June 27, 1999	Ipop2d.txt	Exploit for ipop2 maemons shipped with the imap-4.4 package, remote attackers can spawn a shell with uid of user "nobody".	
June 27, 1999	Netscape.js.table.dos.txt	HTMO parsing bug in all versions of Netscape Communicator 4.x allows malicious web master to crash your browser using JavaScript.	
June 27, 1999	Killmod-0.69.tar.gx	Killmod.php3 is a pho front end that calls a simple shell script (killmod.sh) that allows you to use the +++ath0 bug to hand up older modems.	

Date of Script **(Reverse Chronological Order)**	**Script Name**	**Script Description**	**Comments**
June 26, 1999	NTOScanne126.exe	TCP/IP port scanner for Windows NT platforms. The scanner has been clocked scanning 5,000 ports in 8 seconds and all 65K in 3:30 minutes.	
June 26, 1999	SDIaccelX.c	This script will exploit a vulnerability in the Accelerate-X Xserver.	
June 25, 1999	**Lpcontrol.c**	**LPRng Print Queue Control vulnerability exploit which allows a malicious user to take control over the printing queues on LPRng server.**	
June 22, 1999	Hhp.pine.exploit.txt	The Pine MUA up to and including v4.10 contains a security hold that allows a malicious remote attacker to potentially execute arbitrary code, resulting in a possibility of root compromise.	
June 22, 1999	**Xterm.c**	**Local root exploit for SCO Openserver Xbase tools which include suid root, like scoterm, xterm and xload.**	
June 22, 1999	**Hhp-pagoo.pl**	**Exploit will extract the password to the specified PagooID (voice mail) you specify.**	
June 21, 1999	**Ms.outlook.DoS.txt**	**Microsoft Outlook (all versions) does not properly handle X-UIDL: headers in email, resulting in the potential for dental of service attacks against MS outlook users.**	

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:

1. Well-known security holes for which patches were previously available are being used by crackers to break into web sites.
2. Security holes in CGI scripts are currently being exploited.
3. Virus and worm attacks on information systems have increased significantly this year.
4. FTP and FRAG attack combinations have escalated recently.
5. Denials of Service attacks are becoming of increasing concern.
6. An increased number of reports of SYN and IP Spoofing attacks that result in a Denial-of-Service.

Viruses/Trojans

July Killer: The July Killer virus is a Microsoft Word macro that spreads as users exchange Word files and carries with it a political message. Despite the potentially catastrophic results of the virus, it has been hardly noticed. “It’s not a big problem,” Vivian Chung, Trend Micro’s general manager for Hong Kong and China, told Newsbytes. “We found it in May and very quickly developed a cure. In Hong Kong, we haven’t received any reports about it.” Ironically, the chaos caused by the CIH virus in China has helped minimize the impact of July Killer. “On April 26 the CIH virus caused major damage in China so many corporations bought good anti-virus software. As we knew about July Killer in May, most of the software included filters for the virus,” said Chung.

W97M/Heathen.A (June 25, 1999): This is a multipartite virus that uses two types of classes, a ‘.exe’ portion and a ‘.doc’ portion for its infection. The virus was originally spread from a news group and replicates itself across Microsoft Word 97 files, but does not destroy data. It is delivered if someone receives an e-mail with a Word 97 infected document or they access any server file that is infected. It doesn’t carry a particular payload except for dropping a patch into the Windows 95/98 shell.. The macro drops three system files, named heathen.vex, heathen.vdl, and heathen.vdo into a systems C:/Windows subdirectory. When the system is rebooted the heathen.vex file will be renamed exploer.exe.

BO2K (July 4, 1999): BO2K has evolved from Back Orifice released by cDc at Defcon VI last year. It has had over 300,000 downloads from its primary and secondary mirror sites. BO2K has basically the same underlying concepts as the previous version. BO2K is a powerful application and is promoted as a remote administration tool for Microsoft products. However, it has been widely used as a Trojan, in order to cause damage and gain access to unauthorized data. Windows NT support in BO2K can extend the danger of a powerful Trojan to NT networks.

.