



National Infrastructure Protection Center CyberNotes

Issue #12-99

June 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 May 22 and June 4, 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
Aleph librarian system ver. 3.25 and higher (ExLibris) ¹	Irix 6.2 or high	The setuid root binary midikeys can be used to read or edit any file on the system using its GUI. This vulnerability can be exploited with any text editor.	Temporary solution can be found at: ftp://sgigate.sgi.com/security/19990501-01-A	IRIX midikeys Vulnerability	High	Bug discussed in newsgroups and websites. Exploit script has been published.

¹ Bugtraq, May 25, 1999.

Hardware/ Operating System	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Allaire ² (Updated vulnerability data) ³	ColdFusion Server 2.x, 3.x, 4.0 (all editions)	Vulnerabilities in the server documentation (200 sample code files which are stored in the directory CFDOCS) will permit remote users to view, delete, and upload files to the server. Access to a sample application called the Expression Evaluator is supposed to be restricted to the local machine. However, certain pages may be accessed remotely with the ability to read and delete files anywhere on the system where the application is installed.	A patch to restrict access from all pages of the Evaluator is available at: www.allaire.com . ConFusion 4.0 users should install ColdFusion 4.0.1 maintenance release.	ColdFusion Expression Evaluator Unauthorized Access	High	Bug discussed in newsgroups and websites. Exploit script not required for the exploit. Other related hacker tools can be utilized to gain privileged access.
IBM ⁴	eNetwork Firewall 3.2 for AIX	Any user with shell access to the firewall has the ability to corrupt or possibly modify system files by creating links, pipes, etc. with the same name. AIX contains some poorly written scripts, which create temporary files in /tmp without making any attempt to validate the existence of the file.	Temporary solution: IBM suggests changing the permissions to prevent users from creating symbolic links to sensitive files.	System Files Vulnerability	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Internet Software Consortium ⁵ (Updates to versions affected)	Red Hat Linux 6.0 (version of INN shipped with this software)	By editing the INN.CONF file, or changing the INNCONF environment variable, the 'news' user could execute arbitrary code as root.	Upgrade to new packages found at: http://www.redhat.com/corporate/support/errata/rh60-errata-general.html#inn	INN Config File Vulnerability	High	Bug discussed in newsgroups and websites.

² Allaire Security Bulletin, ASB99-02.

³ Allaire Security Bulletin, ASB99-01.

⁴ Bugtraq, May 26, 1999.

⁵ Red Hat Security Advisory, May 25, 1999.

Hardware/ Operating System	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft Windows NT ⁶	Microsoft Remote Access Service (RAS) Client	The component of the RAS client that processes phonebook entries has an unchecked buffer. The vulnerability could allow a Denial-of-Service attack to be mounted against the client machine or could allow arbitrary code to be executed on it.	Patch available at: ftp://ftp.microsoft.com/bu/sys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP5/RAS-fix/	Malformed Phonebook Entry Vulnerability	High	Bug discussed in newsgroups and websites.
NetBSD-1.3* ⁷	NetBSD-1.3*	Denial of Service or traffic hijacking from local network is possible.	Replace with NetBSD-1.4, and NetBSD-1.4_BETA after 1999-05-05 Patch can be found on the NetBSD ftp server: ftp://ftp.NetBSD.ORG/pub/NetBSD/misc/security/patches/19990505-arp	ARP Table Vulnerability	High	Bug discussed in newsgroups and Web sites. Exploit script has been published.
Sun ⁸	Solaris2.6	Root access can be obtained from setuid buffer overflow.	This is a patch for a similar problem in Solaris 7 and the following patches for Solaris 2.6: <u>RELEASE</u> <u>ARCH</u> <u>PATCH</u> 5.6 i386 105211-06 4.6 sparc 105210-06 Note a new exploit has appeared that defeats the patch.	Solaris libc Vulnerability	High	Bug discussed in newsgroups and Web sites. New exploit script has been published that will defeat the current patch.
Sun ⁹	Solaris 2.6, 7	Problem accessing calendar file /usr/spool/calendar/callog.test: No such file or directory.	This appears to be bug# 4184188 which is fixed in 105566-06 (SPARC) 105567-06 (x86)	sdtcm_convert Overflow Exploits	Low	Bug discussed in newsgroups and Web sites. Exploit script has been published.

⁶ Microsoft Security Bulletin, MS99-017.

⁷ NetBSD Security Advisory 1999-010, May 25, 1999.

⁸ Bugtraq, May 22, 1999.

⁹ Bugtraq, June 2, 1999.

Hardware/ Operating System	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Windows 95 Linux ¹⁰	Netscape Communicator 4.x (Win 95): 4.07 (Linux)	The way JavaScript code is treated in the title of the document in Netscape Communicator allows the following vulnerabilities: reading user's cache; reading info about the Netscape's configuration. This may allow the reading of user's email. This vulnerability may be exploited using html mail message.	Workaround: Disable JavaScript	JavaScript Vulnerability	Medium	Bug discussed in newsgroups and Web sites. Exploit script has been published.
Windows 9x and FreeBSD 3.0 ¹¹	Red Hat Linux 2.2.x	There is a bug in kernels 2.2.x that causes them to panic when they are sent a large number of specific ICMP packages. When exploited this vulnerability allows remote users to crash the machine running 2.2.x.	Procedure for upgrading the kernel can be found at: http://www.redhat.com/corp/support/docs/kernel-upgrade/kernel-upgrade.html	2.2.x Kernel Vulnerability	Low	Bug discussed in newsgroups and Web sites. Exploit script has been published.
Windows Networks ¹²	Pegasus Mail Client	Weak Encryption on Pegasus Mail allows users to read POP3 passwords. This text file is world read/writable. A user could easily edit the file so messages go to a new directory or choose not to delete POP3 mail from host. But the main problem is the weak encryption on the V2 password.	No workarounds or patches known at time of publishing.	Weak Encryption Vulnerability	Low	Bug discussed in newsgroups and Web sites.

¹⁰ Bugtraq, May 24, 1999.

¹¹ Bugtraq, June 3, 1999.

¹² Bugtraq, May 15, 1999.

Hardware/ Operating System	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Windows NT Novell Netware Servers ¹³	Compaq Insight Manager	The web server included in Compaq Insight Manager could expose sensitive information. Compaq Insight Manager Web Agent's passwords are stored in clear text. This bug gives unrestricted access to the vulnerable server's disk.	Disable the Compaq Insight Manager web server or restrict anonymous access.	Sensitive Information Exposure Vulnerability	High	Bug discussed in newsgroups and Web sites. Exploit script has been published.
Windows NT ¹⁴	Microsoft Jet Database 3.5 (runs Access databases)	A vulnerability exists that allows an individual to embed Visual Basic Application in string expressions, which may allow the individual to run commandline NT commands. This, combined with the flaw of IIS running ODBC commands as system_local allow a remote attacker to have full control of the system.	Repaired in MSJET4.0	Administrator Vulnerability	High	Bug discussed in newsgroups and websites.
Windows NT ¹⁵	CMail 2.3 FTGate 2,1,2,1 NTMail 4.20	Cmail: There are multiple buffer overflows within the various SMTP and POP server functions of Cmail which can be exploited to gain root access. FTGate: Same as Cmail NTMail: NTMail runs as a service by default, therefore an unauthorized user can read files as if they were the user "SYSTEM."	Replace with NTMail 4.3 Fixes Disable the web interfaces where applicable until the vendors release patches.	Mail Vulnerability	Medium/ High	Bug discussed in newsgroups and Web sites. Exploit script has been published.

¹³ Bugtraq, May 26, 1999.

¹⁴ Bugtraq, May 26, 1999.

¹⁵ NTBugtraq, May 26, 1999.

Hardware/ Operating System	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Windows NT Microsoft Information Server (IIS) ¹⁶	Frontpage 97	Frontpage 97 server extensions vulnerabilities associated with Microsoft IIS installed from NT Option pack and Frontpage server extensions may be exploited to modify web pages.	Vendor recommends that system using frontpage obtain the Server extension 98 from: www.microsoft.com/frontpage	Server Extension Vulnerability	Medium	Bug discussed in newsgroups and websites.
Winframe, Windows NT Server Terminal Edition ¹⁷	Citrix Winframe client for Linux 2.x, 3.x	Files created by Windows on such client-mapped drive appear to be world-writable. Any user on the system can overwrite configuration data.	Workaround (for platforms supporting dynamic linking). Compile following "module" as a shared object and make run-time linker preload it (by setting LD_PRELOAD on Linux and Solaris and <code>RLDLIST+\${ICAROOT}/chmod.so:DEFAULT</code> on IRIX) <code>Int chmod() {return 0;}</code>	Configuration File Vulnerability	High	Bug discussed in newsgroups and websites. Exploit script 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.

Recent Exploit Scripts

The table below contains a representative sample of exploit scripts, identified between May 22 and June 4, 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, 29 scripts, programs, and net-news messages containing holes or exploits were identified.

¹⁶ NAVCIRT ADVISORY 99-025. May 19, 1999.

¹⁷ Bugtraq, May 28, 1999.

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
June 3, 1999	Ex_sdtcm_convert86.c	Intel (x86) version of the Solaris sdtcm_convert buffer overflow exploit that leads to root compromise.	
June 3, 1999	Linux.2.2.x.icmp.dos.c	Denial of Service exploit code for ICMP vulnerability.	
June 3, 1999	Nsdadv.c	IRIX 6.5 nsd virtual filesystem vulnerability allows remote attacker to mount filesystem and retrieve privileged data, such as shadowed password files, monitor filesystem for changes and execute Denial-of-Service attacks.	
June 3, 1999	SDI-pop2.c	Exploit code for remote ipop2D security vulnerability that gives attacker a shell as user 'nobody'.	
May 30, 1999	ADMsniff.tgz	A libpcap-based sniffer.	
May 30, 1999	Cgichk.r	CGI vulnerability scanner that checks for over 60 common CGI security holes on remote web servers.	
May 30, 1999	Packet Sniffer Construction, Part II	The second installment of the "packet Sniffer Construction" services of whitepapers. Includes good code and detailed descriptions.	
May 30, 1999	Zlip.tar.gz	Three examples of exploit code for the weaknesses in DNS label decoding.	
May 28, 1999	Cgi-check99.r	CGI vulnerability scanner that checks for 69 CGI-based web server security holes.	
May 28, 1999	Ex_admintool-2.c	Exploit for the Solaris 2.7 and 7 admin tool buffer overflow that results in local root compromise.	
May 28, 1999	Insecurity by Design	A whitepaper, "The Unforeseen Consequences of Login Scripts," that details security problems commonly found in most Windows and NetWare login scripts.	
May 28, 1999	Relayck.pl	Perl script that scans a list of SMTP servers to find servers that will relay email.	
May 28, 1999	Windog-dtk.zip	Windows deception toolkit contains fake telnet and sendmail daemons coded in Perl and runs on Windows.	
May 24, 1999	Ex_lobc-2.c	Modified version of the exploit code for Solaris 2.6, 2.7 (sparc) libc/LC_MESSAGES buffer overflow that results in root compromise.	
May 24, 1999	Jscan.tar.gx	Java-based vulnerability scanner.	
May 24, 1999	Mswinhlp.exploit.txt	Exploit code and detailed analysis of the Winhlp32.exe buffer overrun. Source code for Windows NT exploit program included.	
May 24, 1999	Netscape.title.tag.about.txt	JavaScript <TITLE> tag security vulnerability. This security hole can be exploited via HTML email messages and by malicious web masters. Exploit code included.	
May 24, 1999	Tmp-racer	Shell script that exploits programs that make insecure uses of /tmp.	

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
May 24, 1999	Whlpbo.htm	Exploit code and detailed analysis of the Winhlp32.exe buffer overrun. Source code for Windows NT exploit program included.	
May 24, 1999	Alibaba.2.0.genkey.txt	Security hole in Alibaba 2.0 web server software for Windows NT does not properly implement cryptographic functions, resulting in absolutely no secure sockets at all.	
May 24, 1999	Winhlpadd.exe	Exploit code for Windows NT Winhlp32.exe buffers overrun condition.	
May 22, 1999	Ex_lobc.c	See entry for May 24, 1999.	
May 22, 1999	Fraqrouter-1.1.tar.gz	Network intrusion detection evasion toolkit.	
May 22, 1999	Saint-1.3.9.tar.gz	Security Administrator's Integrated Network Tool that gathers as much information about remote hosts and networks as possible by examining all network services and potential security flaws.	
May 22, 1999	Lamescan-1.402b.tar.gz	Multi-threaded portscanner that supports scanning domains, class A,B,C nets, random scan, scanning hostnames as they are typed on stdin, ANSI, identlookups(buggy), sending a "user lalala" string to any open port, output to a filename and delaying between each connect() call.	
May 22, 1999	Ntbufferoverruns.txt	Paper that details how to exploit Windows NT buffer overflows. Proof of concept exploit code and step-by-step exploit instructions included.	
May 22, 1999	Procfs.solaris.time.c	Exploit code that demonstrates how the time() system call can be faked via procfs on Solaris.	
May 22, 1999	Sun-snmplib.txt	Whitepaper that details security vulnerabilities in Sun's implementation of SNMP with exploit descriptions included.	
May 22, 1999	Warscan-0.7.2.tar.gz	An Internet Scanner Dispatch that is a vehicle for automating any text exploit in an efficient, timely, and large-scale manner. Anyone with a security exploit can automate their exploit over large numbers of hosts in a short amount of time.	

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. Computer virus activity has picked up in the last three months, including an increase in the use of older, known viruses.
2. Hackers are currently testing methods to defeat detection systems. These include experimentation with timing thresholds and scanning methodologies.
3. Probes to port 1800 and 1945 continue.
4. An increased number of reports of SYN and IP Spoofing attacks that result in a Denial-of-Service.
5. Probes looking for Cold Fusion and IIS sites continue.
6. Probes continue to look for machines with Back Orifice installed.

Viruses

Emperor: This new clone of the Chernobyl virus named Emperor carries even more deadly capacity and promises to infect more computers. The Emperor virus has additional technology to infect more systems by copying itself to more areas of the computer and has the possibility to travel further. It infects DOS (16-bit) COM and EXE programs and overwrites the Master Boot Record of the hard drive and boot sector on floppy diskettes. This virus uses many anti-debugging tricks, Stealth functions and a very complex algorithm to intercept and bypass the built-in anti-virus protection that is installed in many computers. This virus also has the lethal destruction routine contained in the Chernobyl virus. It can erase the data on the hard drive and corrupts the Flash BIOS thus rendering the PC unusable.

BackDoor-G & Armageddon: Back Orifice-like Trojan Horse hack tool called BackDoor-G is being distributed like spam e-mail to users in the disguise of a new screensaver, a game update and other misdirection. Once installed, the program will provide an individual with surreptitious access to the client system. BackDoor-G is difficult to detect because it is able to change its filename and therefore hide from some traditional virus eradication methods. A similar Trojan horse is also currently spreading through France under the name Armageddon and may spread to the United States as well.

PrettyPark.Worm: This worm program behaves similar to Happy99 Worm. The program is spread by email spamming from a French email address. When the attached program called PreppyPark.EXE is executed, it may display the 3D pipe screen saver. It will also create a file called FILES32.VXD in the Windows/System directory and modify the following registry entry value from “%1” %* to

FILES#@>VXD “%1” %* without your knowledge:
HKEY_LOCAL_MACHINE\Software\Classes\exefile\shell\open\command

Once the worm program is executed, it will try to email itself automatically every 30 minutes (or 30 minutes after it is loaded) to email addresses registered in your Internet address book. It will also try to connect to an IRC server every 30 seconds and connect to a specific IRC channel. This connection can potentially be used maliciously.