National Infrastructure Protection Center CyberNotes

Issue #8-99 *April 14, 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 March 27 and April 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.**

Hardware/ Operating System	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
HP[1] - UX	Domain Enterprise Server Management System (DESMS)	A number of packages have an extra Domain Management process running in background. Users can gain increase privileges as a result.	Patches and a list of affected programs are available from HP.	HP - UX DESMS extra Domain management process	Medium/ **High**	Bug discussed in newsgroups and Web sites.
HP[2] - UX	Operating System (ServiceGuard and LockManager)	Improper implementation of restricted SAM functionality can lead to users gaining increased privileges.	Patches are available from HP.	HP - UX ServiceGuard and LockManager implementation	Medium/ **High**	Bug discussed in newsgroups and Web sites.

[1] Hewlett-Packard Security Bulletin #095, March 31, 1999.
[2] Hewlett-Packard Daily Security Bulletins Digest, March 31, 1999.

Hardware/ Operating System	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Internet Security Systems, Inc[3]. (ISS)	Internet Scanner (IS)	If IS is configured to use the suid bit to permit "root privileges," an unauthorized user can execute arbitrary commands.	Workaround is to disable the suid bit. The default configuration of IS is not vulnerable to this condition.	IIS Internet Scanner suid bit overflow	Medium/ **High**	Bug discussed in newsgroups and Web sites. Exploit script has been published.
Linux[4] – Debian 2.1	Apache Web server (apache_1.3.3-7.deb)	The current configuration will allow anyone on the Net to discover the exact version of software packages installed.	The maintainer of the Debian Apache package indicated that this configuration is required by the Debian packaging policy and if user wishes a change, the policy must be changed.	Apache on Debian	Low/ Medium **Can provide info for further attacks.**	Bug discussed in newsgroups and Web sites.
Microsoft[5]	Internet Explorer 5.0	Vulnerability in the DHTML edit control allows a remote site to obtain and/or read files on the local machine. Note that this is similar to the "%01 security bug" discovered in January.	Possible workaround is to disable the "allow paste via scripts" option. Note that this workaround has not been tested.	IE 5.0 reading and sending of files (a.k.a. %01 bug again)	Medium/ **High**	Bug discussed in newsgroups and Web sites. Exploit script has been published.
Microsoft[6]	Personal Web Server 4.0 (Windows 95 and Windows 98 versions) and FrontPage Web Server (same editions)	A network user can read files on the server if the file's name is known. A file request with a non-standard URL will bypass the server's normal file access controls.	Patches are available for the Personal Web Server at: http://support.microsoft.com/download/support/mslfiles/Pwssecup.exe Patches are available for the FrontPage Web Server at: http://officeupdate.microsoft.com/downloadDetails/fppws98.htm	Personal Web Server File viewing	Low	Bug discussed in newsgroups and Web sites.
Mirabilis[7]	ICQ99a (build 1700 v2.13)	Turning on the "Activate my home page" option starts web server which allows anything in the "program files\icq\homepage\root\YOUR#\files" to be requested.	This information is provided for awareness.	ICQ web server	Low	Bug discussed in newsgroups and Web sites.

[3] Brazilian Information Security Team, SDI.03-99.iss-scanner.
[4] BUGTRAQ, April 5, 1999.
[5] NTBUGTRAQ, March 30, 1999.
[6] Microsoft Security Bulletin, MS99-010.
[7] BUGTRAQ, March 29, 1999.

Hardware/ Operating System	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Ramp Networks[8]	WebRamp Internet access device	Two Denial-of-Service vulnerabilities have been discovered. An attacker can (1) send a specific string of characters to the HTTP causing the device to hang, or (2) send a specific UDP pack to port 5353 changing the local IP address.	Firmware upgrades can be obtained at: http://www.rampnet.com/upgrades	WebRamp Denial-of-Service	Medium	Bug discussed in newsgroups and Web sites. Exploit script has been published.
Sun Java[9]	JDK 1.1, 1.1.X, 1.2 and 2 (multiple platforms) Netscape 4.5 (FreeBSD and NT) Netscape 4.05 (NT) Netscape 4.02 (Solaris) Netscape 4.07 (Linux) Symantec Visual Café V 3	Hostile Web site can gain full control of the user's machine.	Patch available at: Http:/www.sun.com	Java 2 byte code verifier	**High**	Bug discussed in newsgroups and Web sites. Exploit script has been tested in University Labs.
Sun Solaris[10] V 7	Operating System (ff.core)	It is possible for a user to overwrite arbitrary files include "/etc/shadow" using a bug in ff.core.	No workarounds or patches known at time of publishing. Patches on Solaris 2.6 and 2.5.1 exist for this vulnerability.	Solaris 7 ff.core bug	Medium/ **High**	Bug discussed in newsgroups and Web sites. Exploit scripts for earlier versions of the operating system have been published.
Symantec[11]	PCAnywhere V8.0 upgrade B	This upgrade will disable the NT Screensaver even if SP 4 is reinstalled after the PCAnywhere upgrade.	No workarounds or patches known at time of publishing.	PCAnywhere V8.0 and NT Screensaver	Low/ Medium/ **High** (security policy issue)	Bug discussed in newsgroups and Web sites.
Unix[12] - Multiple systems	Xfree86 V3.3.3-5 (X11-unix)	If an unauthorized user creates a symlink with the name ".X11-unix" and point it to any directory (e.g., root), the permissions of the directory are set to 777. This vulnerability occurs a result of a flaw in the way the program handles the "/tmp" directory.	Vendor recommends upgrading to latest version of Xfree86.	Xf86 directory permissions	Medium/ **High**	Explanation of exploit available in newsgroups. Exploit script has been published.

[8] Internet Security System Security Advisory - WebRamp Denial of Service Attacks, March 31, 1999.
[9] BUGTRAQ, April 5, 1999.
[10] BUGTRAQ, April 7, 1999.
[11] NTSECURITY, March 30, 1999.
[12] S.u.S.E. Security Announcment, March 28, 1999.

Hardware/ Operating System	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Unix[13] – Multiple Systems	rsync	The permissions of your home directory may be changed to the permissions of the directory you are transferring to, if you transfer an empty directory into a non-existent directory.	Patches available at: ftp://rsync.samba.org/pub/rsync	Rsync ghost directory	Medium	Bug discussed in newsgroups and Web sites.
Unix[14] – Multiple Systems	Xfree86 (Xfs)	If an unauthorized user creates a symlink with the name ".font-unix" and point it to "/etc/shadow" the permissions of "/etc/shadow" are set to 777. This vulnerability occurs a result of a flaw in the way the program handles the "/tmp" directory.	Various non-vendor patches are available but not tested.	Xfree86 xfs bug	**High**	Bug discussed in newsgroups and Web sites. Exploit script has been published.
Xylan OmniSwitch [15]	Operating System 3.1.8 and 3.1.9	Denial-of-Service condition results if an unauthorized user telnets to the interface and uses any username and the password "<ctrl> d."	Vendor recommends upgrading to later version. Later versions have been tested and are not affected by this attack.	OmniSwitch telnet "<ctrl> d" problem	Low	Bug discussed in newsgroups and Web sites.

*Risk is defined in the following manner:

High - A vulnerability that will allow an intruder to immediately gain privileged access (e.g., sysadmin, 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.

[13] BUGTRAQ, April 7, 1999.
[14] BUGTRAQ, March 30, 1999.
[15] BUGTRAQ, March 31, 1999.

Recent Exploit Scripts

The table below contains a representative sample of exploit scripts, identified between March 27 and April 9, 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, 30 scripts, programs, and net-news messages containing holes or exploits were identified.

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
April 8, 1999	**Subseven 1.3**	**Trojan Horse program that is similar to netbus/Back Orifice.**	
April 8, 1999	**Nlog-15.3.tar.gz**	**A set of Perl scripts that assist in the databasing and report generation of Nmap logs.**	
April 8, 1999	NetBus Pro v2.01	**Trojan horse program with a Graphical User Interface (GUI), proxy support, file manager, web-cam capture, registry manager, hosts scheduler, application redirect, chat and many other features.**	
April 8, 1999	**Gspot121.tar.gz**	**Control panel for Back Orifice that uses GTK+ widget set and provides cut-and-paste and more descriptive list of the commands.**	
April 8, 1999	Crackpipe.c	Code designed to allow users to tunnel IP's over "normal TCP/UDP connections" in an effort to go around firewalls.	
April 7, 1999	Proc.c	Sample exploit code for the procmail vulnerability that allows local user to dump contents of any file to the screen.	
April 7, 1999	Nessus-alpha2-fix2.tgz	Network security auditing tool that checks for 208 vulnerabilities, detects remote services, portscans and more.	
April 7, 1999	**Gspot.patch**	**See entry for (Gspot121.tar.gz) April 8, 1999.**	
April 6, 1999	Wingate.3.0.txt	Explanation of exploit against WinGate 3.0.	
April 6, 1999	Smdos.c	Denial-of-Service exploit against sendmail (up to version 8.9.3) using queue filling.	
April 6, 1999	**SDI-iss.c**	**Sample exploit code for the ISS Internet Scanner buffer overflow. See "Bugs, Holes & Patches" (CyberNotes - April 14, 1999, Internet Security Systems, Inc[16]).**	
April 6, 1999	**Rat20.exe**	**Remote administration tool similar to but less powerful than Back Orifice. Can receive commands from the net via UDP. This version can be used with netcat and IRC.**	
April 6, 1999	Nessus-alpha2-fix1.tgz	See entry for April 7, 1999.	
April 5, 1999	Shmkill.c	Local Denial-of-Service exploit code for Linux 2.X IPC and mmap vulnerabilities.	

[16] Brazilian Information Security Team, SDI.03-99.iss-scanner.

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
April 5, 1999	**Nmap-2.12.tgz**	**Network-scanning tool that has a variety of scanning modes, including stealth, Xmas, and Null stealth. This release adds more operating system fingerprinting and several bug fixes. Note: This tool continues to be used by hackers. A number of systems become unstable when scanned if patches are not applied.**	
April 5, 1999	Lock-exploit.c	Denial-of-Service exploit against Washington.EDU ipop3d 4.xx using the lock vulnerability.	
April 4, 1999	Nessus-alpha2.tgz	See entry for April 7, 1999.	
April 3, 1999	Wipe-0.58.3.tar.bz2	Program to overwrite hard disk making recovery of data difficult/impossible.	
April 3, 1999	Nmap-2.11.tgz	See entry for April 5, 1999.	
April 2, 1999	Net-RawIP-0.06c.tar.gz	**Perl module that manipulates raw Internet Protocol (IP) packets and Ethernet headers. Also includes the oshare script that cause Microsoft Windows to stop functioning.**	
April 2, 1999	Nessus-alpha2-pre1.tzg	See entry for April 7, 1999.	
April 1, 1999	xfsx.sh	Shell script that exploits the xfs security hole. See "Bugs, Holes & Patches" (CyberNotes April 14, 1999, Xfree86 xfs bug).	
April 1, 1999	Vengine.zip	Program that allows any user to create Microsoft Word polymorphic macro viruses. Melissa and Poyssa viruses' code are included in the sample.	
April 1, 1999	Msie5.0.local	Exploit script that allows a remote user to read and grab files on Microsoft Internet Explorer 5.0.	
April 1, 1999	Insmod	Exploit script that allows a local attacker to gain root access.	
April 1, 1999	Imp211-auto.exe	Self-extracting file that contains a NetWare password cracking utility with a Microsoft Windows GUI.	
March 31, 1999	Ftpscan.c	Ftp port scanner.	
March 30, 1999	Smbgrinder.zip	Program that removes duplication from sniffer dumps and facilitates the targeting of a specific user for L0phtcrack.	
March 30, 1999	Tobbv1.zip	Claims to bind Trojan horse or virus programs to any file specified. This is done in an effort to defeat anti-virus programs.	
March 30, 1999	Fortrv1r.exe	Allows an attacker to obtain the passwords for Fortres v4.0.	

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. Large numbers of scans and attacks continue to be directed at machines running the Linux or Sun Solaris operating systems.
2. Increased scanning for Internet Message Access Protocol (IMAP) (143), POP (110), Telnet (23) and Domain Name Servers (DNS) (53). Please note that this activity has increased dramatically.
3. Scans have also been reported against the following in decreasing order: Echo (7), WWW (80), Sun RPC (111), and Finger (79).
4. Viruses continue to being written to capture and transmit information or spam other Internet sites.
5. Large numbers of SMTP servers are being scanned for common user names, most likely in an effort to obtain names for spam attacks.[17]
6. A company (Network ICE) has reported observing three "Internet-wide" scans from the same site. Two of the scans were for Back Orifice and one was an SNMP "public" scan.

Viruses

False Positive – Recently, Network Associates Incorporated (NAI) McAfee Anti-Virus product with data file 4.0.4017 has reported that Adobe Reader contains the NetBus Trojan horse. Adobe has indicated that this is a false positive with this data file and NAI corrected this with data file 4.0.4019.

W95.CIH - In the last few weeks a number of anti-virus vendors have issued alerts regarding CIH and its variants. Many of the variants are programmed to execute their payload on **April 26**. Versions of this virus attempt to overwrite the MBR and Boot sector and write to FLASH BIOS on some chip sets. All major anti-virus vendors identify most versions of CIH. Anti-virus vendors recommend that users update their virus definitions at least every two weeks. IBM has issued a warning that several thousand Aptivas manufactured between March 5-17, 1999 and sold in the US may have the virus.

W97M.Melissa – The first reported discovery of this virus occurred on Friday, March 26, 1999. Since the discovery, hundreds of sites have been infected including several Fortune 50 companies. One company reported over 60,000 machines infected with this virus. Most infections have occurred via e-mail. The e-mail contains the subject line: "Important Message from (user name)" and the Message body contains: "Here is the document you asked for … don't show anyone else ;-)." The user must open the document to become infected. If macro warnings are enabled in Microsoft Word 97, the user will reeive a warning when he/she attempts to open the infected document. If the infected machine uses Microsoft Outlook®, then the virus will execute a number of Visual Basic instructions to read the user's personal address book and send e-mail to 50 recipients in the address book. Individuals can check for infection by looking in the registry (HKEY_CURRENT_USER\Software\Microsoft\Office) for the term "Melissa?" which indicates the presence of the virus. If the key has a value of "Kwyjibo," then the machine has already mailed the virus out. It should be noted that several variants have started to appear and readers should contact their anti-virus vendors for an update. Most anti-virus vendors have isssued updates that will detect and remove this virus.

X97M.PAPA.B – This worm is a working version of the PAPA virus originally discovered on March 29, 1999. The worm is similar to the Melissa virus and is considered by some anti-virus vendors to be a "copy-cat" of Melissa. This worm affects Excel spreadsheet and is transmitted via Microsoft Outlook. The worm sends e-mail to 60 recipients in the address book. The e-mail contains the subject: "Fwd: Workbook from all.net and Fred Cohen" and the message body: "Urgent info inside. Disregard macro warning." The workbook is currently named pass.xls. The payload executes a shell, which executes ping.exe and attempts to ping two IP addresses. Readers should contact their anti-virus vendors for an update.

---

[17] A number of states have enacted legislation making spamming illegal.