



National Infrastructure Protection Center CyberNotes

Issue #7-99

March 31, 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 12 and March 26, 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
Bay Networks ¹ (UPDATED with additional versions affected)	Baystack 350T (SW:V1.2.0.10, SW:V2.0.0.15, SW:V2.02.1, and SW:V1.03) Baystack 350T- HD SW:V2.0.2.1	System contains default passwords.	Partial workaround is to turn off telnet access or limit IP addresses which can telnet in. This can be accomplished in the "TELNET Configuration" menu.	Bay Networks default password	High	Default passwords available on Web sites and newsgroups.

¹ Anonymous, February 27, 1999.

Hardware/ Operating System	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
CISCO Catalyst ² 5XXX and some 29XX switches	Operating System (supervisor software)	A remote user can reload the switches causing a Denial-of-Service condition.	Vendor suggest that customers with contracts update their software through normal channels, and customer without contracts contact CISCO at 1-800-553-2447.	CISCO Catalyst Supervisor Remote Reload	Low/ Medium	Bug discussed in newsgroups and Web sites.
Linux ³ – S.u.S.E with Netscape Communicator	Talkback	Anyone on the system can create/overwrite files of another user if Communicator crashes.	Vendor’s solution is to disable talkback.	S.u.S.E with Netscape communicator talkback failure	Medium	Bug discussed in newsgroups and Web sites.
Linux ⁴ – S.u.S.E. ⁵ (Update to CyberNotes #6-99 Linux¹¹ with new vendor)	Operating System Below 2.0.36 (/dev/kmem)	Unauthorized remote user can pass data to the application layer without an established connection. If other programs contain the vulnerability, this may lead to a root compromise.	Vendor recommends updating to V 2.0.36 or a 2.2.x kernel.	Linux Blind TCP Spoofing	Low/ Medium High (if other programs are not patched)	Explanation of exploit available in newsgroups. Exploit script has been published.
Linux ⁶ – Slackware V 3.6 and prior	Operating System	If installed with the “net.i” or if a network enabled kernel is used to install, an unauthorized user can gain root access during installation. The time period that the system is vulnerable varies and depends on human interactions during log-in.	Vendor solution is to install post v3.6.	Kernel installation root compromise	High (limited time only)	Bug discussed in newsgroups and Web sites.
Lotus ⁷ Notes V4.5, possibly others	Notes Client ⁸	Due to differences in Window and Unix path character “\” vs. “/”, messages sent to the “Sent Mail” folder of a Notes server may be sent unencrypted over the network.	Workaround is to enable “encrypt saved mail” in global preferences.	Lotus Notes saved mail	Low/ Medium	Bug discussed in newsgroups and Web sites.
Lynx ⁹ V2.8.1pre.9	Operating System	A IMG tag longer than 250 characters causes the system to crash due to a buffer overflow.	No workarounds or patches known at time of publishing.	Lynx buffer overflow	Medium	Explanation of exploit available in newsgroups. Exploit script has been published.

² CISCO software bug announcement (CSCdi74333), March 24, 1999.

³ S.u.S.E. Security Announcement, March 18, 1999.

⁴ Network Associates, Inc., Security Advisory, March 9, 1999.

⁵ S.u.S.E. Security Announcement, March 19, 1999.

⁶ ISS Security Advisory, March 17, 1999.

⁷ Martin Bartosch Security Advisory, March 23, 1999.

⁸ BUGTRAQ, March 23, 1999.

⁹ BUGTRAQ, March 16, 1999.

Hardware/ Operating System	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft Exchange ¹⁰ V5.5	LDAP ¹¹	Buffer overflow in LDAP Bind can lead to a Denial-of-Service condition or potentially lead to root compromise.	Patch is available from: ftp://ftp.microsoft.com/bussys/exchange/exchange-public/fixes/Eng/Exchg5.5/PostSP2/DIR-fix/PSP2DIRI.EXE	Microsoft Exchange Malformed Bind Request	Medium	Bug discussed in newsgroups and Web sites. Denial-of-Service exploit script has been published.
Microsoft Internet Explorer ¹² V5.XX	Internet Explorer	Any screen saver is disabled during installation. If during the installation the process is aborted, then the screen remains disabled.	No workarounds or patches known at time of publishing.	MSIE screen saver disable problem	Medium	Bug discussed in newsgroups and Web sites.
Microsoft ¹³ Internet Information Service (IIS) v4.0	IIS (SMTP service)	The SMTP service will attempt to resend mail immediately if it receives a 4XX error. The resend will occur regardless of the retry time set on the server. This may result in a Denial-of-Service against the recipient's mail.	Microsoft's SMTP service program manager solution is to have the receiver issue a 5XX code instead of a 4XX code.	IIS SMTP service flooding	Low/ Medium	Bug discussed in newsgroups and Web sites.
Microsoft Windows 95/98/NT	Operating System (time and date)	Using the calendar function from the Control Panel can accidentally change Date/time even if the cancel button is used. This may result in passwords expiring and other certifications expiring.	No workarounds or patches known at time of publishing.	Microsoft Windows time advance problem	Low	Explanation of exploit available in newsgroups.
Microsoft Windows 98	Office 97	Every Word and Excel document contains a unique identifier number. This has led to concerns over privacy.	Vendor has issued a patch and a program designed to remove the numbers. Both are available at: http://officeupdate.microsoft.com/	Office97 privacy concerns	Medium	Issue discussed in newsgroups and press.
Microsoft Windows ¹⁴ 98	RegWiz	A web site may obtain information on a user's computer without the user's knowledge through the hardware identification number (HWID) compiled by RegWiz during product registration with Microsoft.	Microsoft expects to have a utility that that will remove the HWID shortly. Instructions for manually removing the HWID can be found at: http://www.winmag.com/web/regwizoff.htm	Microsoft Windows 98 RegWiz	Low	Bug discussed in newsgroups and Web sites.

¹⁰ ISS Security Advisory, March 15, 1999.

¹¹ Microsoft Security Bulletin, MS99-009.

¹² BUGTRAQ, March 24, 1999.

¹³ BUGTRAQ, March 14, 1999.

¹⁴ Windows Magazine, March 12, 1999.

Hardware/ Operating System	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft Windows ¹⁵ NT	Operating System	It is possible for a user with write permissions to the “/??” Object directory to gain administrator access.	This vulnerability exists on a limited number of configurations. Machines configured with Steve Sutton’s NSA guide consistently block this exploit.	Windows NT Case Sensitivity and Symbolic link problem	Medium/ High (rating due to limited success)	Bug discussed in newsgroups and Web sites.
Microsoft Windows ¹⁶ NT 3.51 all, 4.0 SP1, and 5.0 betas (Vendor patch update ¹⁷)	Operating System (Screen saver)	Unauthorized user can gain full system access.	Patch is available from: ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP4/ScrnSav-fix	Windows NT screen saver system rights problem	Medium/ High	Explanation of exploit available in newsgroups. Exploit script for SP1 machines has been published.
Microsoft Windows ¹⁸ NT	WINMSD.exe	This program functions as intended but supplies information that may be useful to a hacker. On networked NT machines, currently logged-in users’ information including username is provided. This information is useful, as input to other know hacker programs.	This behavior is inherent to the program and represents a misuse of information by hackers.	WINMSD.exe Security exploit	Low	Bug discussed in newsgroups and Web sites. Exploit script not required for the exploit.
OpenSSL project ¹⁹	SSLeay and OpenSSL	Under certain circumstances it is possible for a specially written SSL client to obtain an SSL connection that requires access controls to reuse previous session controls.	Vendor recommended solution is to download OpenSSL v 0.9.2b from: http://www.openssl.org	OpenSSL/ SSLeay session reuse	Medium	Bug discussed in newsgroups and Web sites. No known exploits.
Qualcomm ²⁰	Eudora v4.1	Two long e-mail messages containing the same first 231 characters will cause the system to crash. It may be possible to modify the return address to point to any code the user wishes.	No workarounds or patches known at time of publishing.	Eudora 231 character buffer overflow	Medium/ High	Bug discussed in newsgroups and Web sites. Exploit script not required for the first portion of the exploit.

¹⁵ NTSD Team Alert, March 12, 1999.

¹⁶ Cybermedia, March 1999.

¹⁷ Microsoft Security Bulletin, MS99-008.

¹⁸ NTSECURITY, March 10, 1999.

¹⁹ OpenSSL and SSLeay Security Alert, March 23, 1999.

²⁰ BUGTRAQ, March 20, 1999.

Hardware/ Operating System	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Sun Solaris ²¹ 7	Operating System	Non-privileged user can cause the system to crash by entering in the command “/usr/xpg4/bin/more” while in “/proc/self/psinfo”.	Vendor is currently working on a patch.	Solaris procs bug	Low	Bug discussed in newsgroups and Web sites. Exploit script not required for the exploit.
Unix ²² – HP-UX V10.20	Operating System (hpterm)	PHSS_13560 introduced an access problem into hpterm. Users can increase privileges on the system.	Vendor solution is to install patch PHSS_17830	HP-UX hpterm privilege increase	Medium/ High	Bug discussed in newsgroups and Web sites.
Unix ²³ - NetBSD	Operating System (noexec mount flag)	A user is able to execute binaries in a sub-tree even if the “noexec” option is on.	Patch is available at: ftp://ftp.NetBSD.ORG/pub/NetBSD/misc/security/patches/19990317-mount	NetBSD noexec mount problem	Medium	Bug discussed in newsgroups and Web sites. Exploit script not required for the exploit.
Unix ²⁴ – NetBSD V1.3.3 and prior	Operating System (umapfs)	Due to insufficient checking a local user can change their user id to root.	Patch is available at: ftp://ftp.NetBSD.ORG/pub/NetBSD/misc/security/patches/19990311-umapfs	NetBSD umpafs privilege increase	High	Bug discussed in newsgroups and Web sites.
Unix ²⁵ – NetBSD	Operating System (doscmd)	Buffer overflow exists in the program. This overflow occurs after permissions have been reset to the user’s permission.	No workarounds or patches known at time of publishing.	NetBSD doscmd buffer overflow	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.

²¹ BUGTRAQ, March 10, 1999.

²² HP Security Bulletin #00093, March 18, 1999.

²³ NetBSD Security Advisory 1999-007.

²⁴ BUGTRAQ, March 18, 1999.

²⁵ BUGTRAQ, March 17, 1999.

Recent Exploit Scripts

The table below contains a representative sample of exploit scripts, identified between March 13 and March 26, 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, 28 scripts, programs, and net-news messages containing holes or exploits were identified.

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
March 25, 1999	MSIE5.dntml	Script allows public access to the clipboard on Microsoft Internet Explorer 5.	
March 25, 1999	Quick Hacks & Tricks	Compilation of many simple hacks into one package.	
March 25, 1999	Sesquipedalian.c	Denial-of-Service against Linux 2.1.89-2.2.3 using the zero length fragment bug.	
March 25, 1999	Yahoo.c	Code that attempts to discover the userid/password of yahoo accounts.	
March 23, 1999	Httpptunnel-2.0.tar.gz	Allows a user to tunnel through a restrictive firewall that has an HTTP proxy.	
March 22, 1999	Gammaprog152.tgz	Bruteforce password cracker for web based e-mail systems and Post Office Protocol (POP) 3 servers. Latest version includes a configurable CGI cracking program and targets angelfire.com and yahoo.com.	
March 22, 1999	Novell95.zip	Trojan horse log-in program that erases the original log-in program.	
March 22, 1999	Wu-2.4.2-academ[BETA-18].c	Exploit code for the FTPD vulnerability.	
March 21, 1999	Eudora.bof.c	Denial-of-Service code for the Eudora program.	
March 21, 1999	Httpdtype-0.05.tar.gz	Utility that attempts to identify what type of web server a remote host is running.	
March 21, 1999	Promail.1.21.trojan	Shareware mail program that e-mails userid/password and server to hacker address.	
March 19, 1999	Forhack.exe	Program that changes the Fortress password and bypasses security.	
March 18, 1999	Cgichk-11b.c	CGI exploit scanner.	
March 18, 1999	Domtools1.4.0.tar.gz	Tool that automates traversing DNS domain hierarchies, lists all Domains, converts host names to IP addresses and more.	
March 18, 1999	Httpptunnel-1.102.tar.gz	See entry for March 23, 1999.	
March 17, 1999	Httpptunnel-1.101.tar.gz	See entry for March 23, 1999.	
March 17, 1999	Netbsd.umapfs.txt	Explanation of the umapfs vulnerability. See See "Bugs, Holes & Patches" (CyberNotes - March 31, 1999, Unix ²⁴).	
March 16, 1999	Httpptunnel-1.99.tar.gz	See entry for March 23, 1999.	
March 15, 1999	Califax.tar.gz	MS-DOS/Linux virus that is placed in every program that is compiled with gcc.	

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
March 15, 1999	Dip2.c	Buffer overflow in dip-33.3.7 that gives local user root access.	
March 15, 1999	Module.c	Virus source code that infects Linux kernels.	
March 15, 1999	My_login.c	Trojan horse that captures userid/password combinations.	
March 15, 1999	VLP_I.c	Demonstration virus that infects ELF-executables.	
March 15, 1999	Vsrc.tar.gz	Unix/Linux demonstration virus.	
March 14, 1999	Humpdee2.tar.gz	Exploit for Linux rpc.mountd vulnerability that spoofs the udp packet address of the attacker.	
March 13, 1999	BeSysAdm.zip	Exploit code for the Microsoft Windows NT Case Sensitivity and Symbolic link problem. See See "Bugs, Holes & Patches" (CyberNotes - March 31, 1999, Microsoft ¹⁵).	
March 13, 1999	Guideonv1.exe	Program the removes the Globally Unique Identifier (GUID) in Microsoft Office applications or allows the user to insert any string in the GUID*.	
March 13, 1999	Httpunnel-1.97.tar.gz	See entry for March 23, 1999.	

* Note this may call into question the ability to solely rely on the GUID as a basis for identification. This method has been suggested as a potential means for identifying malicious code writer in recent press reports.

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. Several hackers/hacker groups appear to be using coordinated scans and probes from different sites.
2. Large numbers of scans and attacks continue to be directed at machines running the Linux or Sun Solaris operating systems.
3. 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.
4. Scans have also been reported against the following in decreasing order: Echo (7), WWW (80), Sun RPC (111), and Finger (79).
5. Viruses are now being written to capture and transmit information or spam other Internet sites.
6. Large numbers of SMTP servers are being scanned for common user names, most likely in an effort to obtain names for spam attacks.²⁶

²⁶ A number of states have enacted legislation making spamming illegal.

7. Large number of ICMP packets are being sent to source ports just above 1024. The source of these packets are normal dialup accounts or shell accounts.

Viruses

A list of the top ten viruses infecting two or more sites as reported to various anti-virus vendors has been categorized into the two tables below. The first table list macro viruses, and the second table lists other viruses. Macro viruses have, historically, spread fastest due to their ability to be transferred by e-mail.

For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. The tables list the viruses by: ranking (number of sites affected), common virus name, type of virus (i.e., boot, file, macro, multi-partite), trends (based on number of infections during the last three months reported), and approximate date first found.

Note: Virus reporting is normally 6 to 8 weeks behind the first discovery of infection. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages, as updates become available.

The viruses listed in the virus table infected over 1800 machines in January, which represents an increase in the number of reported infections from the last prevalence table. The number 1 ranked virus for February/March accounted for 450 infections, and the last virus listed in the tables infected 22. A total of 465 distinct viruses were reported this month, infecting over 2,000 sites. **Readers should note that CyberNotes has changed the way it keeps statistics on virus infections. Infections rates are now based on number of machines infected, not number of sites.** This change reflects the way statistics are being gathered and reported by a number of anti-virus vendors.

Table 1 – Macro viruses:

Ranking	Common Virus Name	Type of Virus	Trends	Date First Reported
1	CAP	Macro	Steady	April 1997
2	Class	Macro	Increasing	September 1998
3	Marker	Macro	Increasing	February 1999
4	ColdApe	Macro	Increasing	December 1998
5	Laroux	Macro	Increasing	July 1997
6	Temple	Macro	Increasing	December 1998
7	Npad	Macro	Steady	December 1996
8	Concept	Macro	Steady	December 1996
9	Munch	Macro	Increasing	October 1998
10	Wazzu	Macro	Steady	December 1996

Table 2 – Other viruses:

Ranking	Common Virus Name	Type of Virus	Trends	Date First Reported
1	Form	Boot	Steady	September 1991
2	W95/CIH	File	Increasing	July 1998
3	Parity_Boot	Boot	Steady	September 1993
4	AntiEXE	Boot	Steady	September 1994
5	Sampo	Boot	Increasing	January 1995
6	Stat	Boot	Increasing	February 1998
7	AntiCMOS	Boot	Steady	October 1995
8	Ripper	Boot	Steady	March 1994
9	Empire.Monkey	Boot	Steady	July 1994
10	DelCMOS.B	Boot	Increasing	January 1999

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 receive 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 issued updates that will detect and remove this virus.

X97M.PAPA – This worm has been reported in the wild as of 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.