



National Infrastructure Protection Center CyberNotes

Issue #6-99

March 17, 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 February 27 and March 12, 1999. The table provides the operating system, 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.

Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Bay Networks ¹	Baystack 350T (SW:V1.2.0.10 and SW:V2.0.0.15)	System contains default passwords.	No workarounds or patches known at time of publishing.	Bay Networks default password	High	Default passwords available on Web sites and newsgroups.
CISCO ²	CISCO 700 series routers	Remote attacker can cause CISCO 700 routers to panic and reboot. This attack can be executed continuously. This family of router is commonly used in small businesses with ISDN (BRI).	Users with support contracts can download updates from: http://www.cisco.com/cgi-bin/tablebuild.pl/760 or CISCO Technical assistance Center at tac@cisco.com .	CISCO 700 denial-of-Service	Medium/High	Explanation of exploit available in newsgroups. Exploit script has been published.

¹ Anonymous, February 27, 1999.

² ISS Security Advisory, March 11, 1999.

Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
CISCO ³	CISCO 700 series routers (Clickstart)	Unauthorized remote users may issue certain command to the route and gain information for future attacks via Clickstart.	Users with support contracts can download updates from: http://www.cisco.com/cgi-bin/tablebuild.pl/760 or CISCO Technical assistance Center at tac@cisco.com.	CISCO Clickstart vulnerability	High	Explanation of exploit available in newsgroups.
Efnet ⁴	IRCD	Due to certain character translations, it is possible for a new user to join a channel without current user's knowledge.	Workaround is to edit /src/match.c.	IRCD hidden channel joining	Low	Explanation of exploit available in newsgroups.
IPSWITCH ⁵	Imail	The encrypted password can be easily decrypted allowing an unauthorized individual to gain access to all users mail.	No workarounds or patches known at time of publishing.	IMAIL password recovery	Medium	Explanation of exploit available in newsgroups.
IPSWITCH ⁶	Imail (Imapd)	At login, if two long sets of characters are sent, the imapd service will crash.	No workarounds or patches known at time of publishing.	Imail Imapd crash	Medium	Bug discussed in newsgroups and Web sites.
IPSWITCH ⁷	Imail (LDAP)	Sending over 2,375 characters along with a specific number of "enters" will cause system resourcing to spike and remain at 90%.	No workarounds or patches known at time of publishing.	Imail LDAP resourcing use	Medium	Bug discussed in newsgroups and Web sites.
IPSWITCH ⁸	Imail (Imonitor)	Sending over 2,045 characters along with a specific number of "enters" will cause Imonitor to crash with an overflow.	No workarounds or patches known at time of publishing.	Imail Imonitor crash	Medium	Bug discussed in newsgroups and Web sites.
IPSWITCH ⁹	Imail (Web Service)	Sending over 3,000 characters with "GET" to the Web Service results in a buffer overflow that may be exploitable by unauthorized individual to gain root access.	No workarounds or patches known at time of publishing.	Imail Web Service buffer overflow	High	Bug discussed in newsgroups and Web sites.
IPSWITCH ¹⁰	Imail (Whois32 Daemon)	Sending 1,000 characters when telnetting to port 43 will cause a buffer overflow.	No workarounds or patches known at time of publishing.	Imail Whois32 buffer overflow	Medium/High	Bug discussed in newsgroups and Web sites.
Linux ¹¹	Operating System Below 2.0.36 (TCP)	Unauthorized remote user can pass data to the application layer without an established connection.	Red hat users can obtain an updated kernel at: http://www.redhat.com/support/docs/errata.html	Linux Blind TCP Spoofing	Low/Medium	Explanation of exploit available in newsgroups. Exploit script has been published.

³ Ibid.

⁴ BUGTRAQ, March 7, 1999.

⁵ BUGTRAQ, March 4, 1999.

⁶ eEye Digital Security Team, Advisory Code AD03011999

⁷ eEye Digital Security Team, Advisory Code AD03011999

⁸ eEye Digital Security Team, Advisory Code AD03011999

⁹ eEye Digital Security Team, Advisory Code AD03011999

¹⁰ eEye Digital Security Team, Advisory Code AD03011999

¹¹ Network Associates, Inc., Security Advisory March 9, 1999.

Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Linux ¹²	Xcmail (long subject line with autoquote on)	Buffer overflow condition exists that will allow an unauthorized user to execute code possibly resulting in root compromise.	No workarounds or patches known at time of publishing.	Xcmail buffer overflow	High	Explanation of exploit available in newsgroups. Exploit script has been published.
Linux ¹³ – S.u.S.E.	Operating System (usr/bin/gnuplot)	Buffer overflow condition exists that will allow an unauthorized user to execute code resulting in root compromise.	Workaround is to: Chmod –s /usr/bin/gnuplot	Linux gnuplot buffer overflow	High	Explanation of exploit available in newsgroups. Exploit script has been published.
Macromedia ¹⁴	Shockwave 7	Auto-update feature can transmit password and hard disk information back to Macromedia.	Workaround is to disable Auto-date.	Shockwave 7 data transfer security hole	Medium/High	Bug discussed in newsgroups.
Microsoft Windows ¹⁵ NT 3.51 all, 4.0 SP1, and 5.0 betas	Operating System (Screen saver)	Unauthorized user can gain full system access.	Microsoft Windows NT 4.0 SP 2, 3, and 4 partially correct the problem and prevent the current exploit script from functioning.	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 ¹⁶ NT ¹⁷ (PATCH UPDATE¹⁸)	Operating System (KnownDLL)	All users can read and write to the KnownDLLs list. A user can add malicious DLLs with the same name as system DLLs to gain higher privileges or execute other actions. Vulnerability is restricted to machines that the malicious user is interactively logged onto.	Strong protection is possible if the following is add to the registry key: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SessionManger: Name: ProtectionMode Type: REG_DWORD Value: 1 Patch available at: ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa	Windows NT KnownDLL List Vulnerability	Medium	Bug discussed in newsgroups and Web sites.
Microsoft Windows ¹⁹ NT 4.0 SP4	SAMBA running on NT	Under certain conditions if the Primary Domain Controller (PDC) fails or is reset, the SAMBA server will take over as PDC. In order to bring the original PDC back on-line the SAMBA server must be closed.	No workarounds or patches known at time of publishing.	NT Domain DoS and Security Exploit with SAMBA server	Medium	Bug discussed in newsgroups and Web sites. Exploit script not required for the exploit.

¹² BUGTRAQ, March 2, 1999.

¹³ BUGTRAQ, March 4, 1999.

¹⁴ Lingo programming list, March 11, 1999.

¹⁵ Cybermedia, March 1999.

¹⁶ LOpht Security Advisory, February 18, 1999.

¹⁷ Microsoft Security Bulletin, MS99-006.

¹⁸ Microsoft Security Bulletin, MS99-006 update.

¹⁹ BUGTRAQ, March 2, 1999.

Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Netscape ²⁰	Netscape Communicator 4.5	Hostile site can: browse user directories, read user's cache, read content of HTML page that the users see using JavaScript find() function.	Workaround is to Disable Javascript.	Netscape Communicator 4.5 JavaScript find() vulnerability	Medium	Explanation of exploit available in newsgroups. Exploit script has been published.
Oracle 8.0.3 ²¹ (problem has been reviewed in security posting previously)	Oracle Database Assistant v1.0	A log file is created whenever a database is created. This log file stores the password used to create the database as plaintext. The log file has permissions set so anyone can view it.	No workarounds or patches known at time of publishing.	Oracle plaintext password	Medium/ High	Bug discussed in newsgroups and Web sites. Exploit script not required for the exploit.
Seapine ²²	TestTrack	If an individual telnet's to port 99 and then disconnects without type anything, CPU usage goes to 100% and remains there until the TestTrack server is killed.	No workarounds or patches known at time of publishing.	TestTrack Telnet port 99 Denial-of-Service	Low	Bug discussed in newsgroups and Web sites. Exploit script not required for the exploit.
Seapine ²³	TestTrack	A log file is created in the /scripts directory that contains username and password in plaintext.	No workarounds or patches known at time of publishing.	TestTrack plaintext password log file	Medium	Bug discussed in newsgroups and Web sites.
SeattleLabs ²⁴ (Patch information update)	SLMail 3.1	A DoS and a buffer overflow condition exist. If the "helo" command is sent to port 27 followed by 819 to 849 characters, a potential DoS condition occurs. If 855 to 2,041 characters are sent, a buffer overflow occurs.	SeattleLabs representatives report that they are working on a fix and it will be included in SImail 3.2 maintenance release. Patch is currently undergoing Alpha testing.	SLMail Vulnerabilities	Low/ Medium	Bug discussed in newsgroups. Exploit script not required for the exploit.
Silicon Graphics ²⁵ - IRIX	X server (installed by default on all IRIX machines)	Buffer overflow condition exists that will allow an unauthorized local user to execute code resulting in root compromise.	Patches available at: http://www.sgi.com/Support/security/patches.html	X server font path buffer overflow	High	Explanation of exploit available in newsgroups. Exploit script has been published.
Sun Solaris ²⁶ 2.6	Operating System (noexec_user_stack)	This protection method can be bypassed using a buffer overflow. This will allow an unauthorized user to gain root access.	No workarounds or patches known at time of publishing.	Defeating Solaris Non-Executable Stack Protection	High	Explanation of exploit available in newsgroups. Exploit script has been published.

²⁰ BUGTRAQ, March 8, 1999.

²¹ NTBUGTRAQ, March 4, 1999.

²² NTBUGTRAQ, March 8, 1999.

²³ NTBUGTRAQ, March 8, 1999.

²⁴ eEye Digital Security Team, Advisory Code AD02041999.

²⁵ Silicon Graphics Inc. Security Advisory 19990301-01-PX.

²⁶ BUGTRAQ, March 3, 1999.

Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Sun Solaris ²⁷ All versions	Operating System (cancel)	All versions contain this buffer overflow, but version 2.6 is setuid root when the overflow occurs. On both the SPARC and i386 versions 2.6 an unauthorized user can gain root access.	No workarounds or patches known at time of publishing. Sun indicates that a patch should be available in 4 weeks.	Sun Solaris cancel buffer overflow	Medium (most versions) High (version 2.6)	Explanation of exploit available in newsgroups. Exploit script has been published for both SPARC and i386 versions.
Sun Solaris ²⁸ 2.7, 2.6, and 2.6 x86	Operating System (/usr/bin/write)	Buffer overflow condition exists that will allow an unauthorized user to execute code with sgid TTY. Further exploit may be possible.	No workarounds or patches known at time of publishing.	Solaris "/usr/bin/write" bug	Low/ Medium	Explanation of exploit available in newsgroups. Exploit script has been published.
Unix – Santa Cruz Operations ²⁹ (SCO) 5.0.4	Operating System	It is possible to erase/overwrite file using startup scripts.	No workarounds or patches known at time of publishing.	Startup script problem	Medium/ High	Explanation of exploit available in newsgroups. 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, 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 - Any 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.

²⁷ BUGTRAQ, March 5, 1999.

²⁸ BUGTRAQ, March 8, 1999.

²⁹ BUGTRAQ, March 7, 1999.

Recent Exploit Scripts

The table below contains a representative sample of exploit scripts, identified between February 27 and March 12, 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, 41 scripts, programs, and net-news messages containing holes or exploits were identified.

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
Mar 10, 1999	Mtr-033.tar.gz	A traceroute and ping program that provides link information on all machines between the host and destination computers.	
Mar 10, 1999	Lin35.c	Exploit program for the Linux TCP Blind Spoofing vulnerability. See "Bugs, Holes & Patches" (Linux¹¹).	
Mar 10, 1999	Winfreeze-sparc.c	The Winfreeze program ported to Solaris. See Winfreez.c (Mar 8, 1999).	
Mar 10, 1999	Receive.c	Exploit program for the Linux TCP Blind Spoofing vulnerability. See "Bugs, Holes & Patches" (Linux¹¹).	
Mar 10, 1999	Solaris.7.procfs	Local Denial-of-service attack against Solaris 7.	
Mar 10, 1999	ScrnSave.zip	Exploit program that allows local user to add themselves to the admin group using the Windows NT screen saver system rights problem. See "Bugs, Holes & Patches" (Microsoft Windows ¹⁵).	
Mar 10, 1999	BEADMIN.zip	Exploit program that allows local user to add themselves to the admin group using the Windows NT screen saver system rights problem. See "Bugs, Holes & Patches" (Microsoft Windows ¹⁵).	
Mar 10, 1999	Cancelex.c	Exploit program for the Sun Solaris cancel buffer overflow vulnerability. See "Bugs, Holes & Patches" (Sun Solaris²⁷).	
Mar 9, 1999	Mtr-032.tar.gz	See Mar 10, 1999.	
Mar 9, 1999	Miffo-check-1.3.1.c	Port scanner that scans class B or Class C IP ranges.	
Mar 8, 1999	NTSweep v1.0	Brute force password cracker that gathers a list of network users. Does not require access to the registry or SAM database.	
Mar 8, 1999	Sco-filewiper.sh	Shell script that will allow non-privileges user to erase any file on SCO OpenServer.	
Mar 8, 1999	Winfreez.c	Program that sends a storm of ICMP/redirect packets that cause Microsoft Windows 9x/NT machines to freeze.	
Mar 8, 1999	Bitch.x	Exploit script that allows a user to join mIRC channel without other users knowledge and spy on the channel.	
Mar 4, 1999	xnec_plot.c	Exploit script for a buffer overflow in Linux gnuplot. See "Bugs, Holes & Patches" (Linux¹³).	
Mar 5, 1999	Miffo-check-1.3.c	See Mar 9, 1999.	
Mar 5, 1999	Iemail.sh	Script to decrypt Iemail server user passwords.	
Mar 5, 1999	InetdDoS-spewfing.tgz	Denial-of-Service exploit script against inetd.	
Mar 5, 1999	Scanpromisc.c	Remote promiscuous mode Ethernet detector.	

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
Mar 5, 1999	Ego_21.tar.gz	Wordlist Generator that can be customized and invoked with command-line arguments.	
Mar 5, 1999	picky_10.tar.gz	Program that compares wordlist and creates a master list without duplicates.	
Mar 5, 1999	Nlog-1.5.1.tar.gz	A set of Perl scripts that assist in the databasing and report generation of Nmap logs.	
Mar 4, 1999	Count.cgi.l.c	Exploit script for count.cgi.	
Mar 3, 1999	Lpstatex.c	Buffer overflow exploit against Solaris 2.6 lpstat. See "Bugs, Holes & Patches" (CyberNotes - March 3, 1999, Sun Solaris ²⁹).	
Mar 3, 1999	Rdistex.c	Buffer overflow exploit against Solaris 2.6 rdist. See Bugs, Holes & Patches (December 10, 1998, Sun Solaris ¹⁸). Note: Bugs, Holes & Patches was the name of this publication before January 1999.	
Mar 3, 1999	Dexpand.zip	Program to expand wordlists by adding plurals and possessive versions. It will also create verb endings.	
Mar 3, 1999	Samgrab.zip	Newest version of a tool that extracts SAM databases from NTFS volumes and is effective against server and workstations.	
Mar 3, 1999	Dmerge.zip	Program that merges two wordlists deletes duplicates and outputs result in a list separated by CRLF.	
Mar 3, 1999	Hintcrack.zip	Program that attempts to crack hotmail hints.	
Mar 3, 1999	Httpdtype-0.22.tar.gz	Program that attempts to identify the type of web server running on a remote host.	
Mar 3, 1999	Nlog-1.5.tgz	See Mar 5, 1999.	
Mar 3, 1999	P3psn.tar.gz	Program that identifies the PIII serial number.	
Mar 3, 1999	Pgpcrack99.tgz	Program that attempts to brute force decrypt a file encrypted by PGP.	
Mar 3, 1999	winscan.zip	Searches a Class C IP range and identifies Wingate proxies.	
Mar 3, 1999	Xcmail_exp.c	Explanation and exploit script for xcmail vulnerability. See "Bugs, Holes & Patches" (Linux ¹²).	
Mar 2, 1999	Httpservertype-0.01.tar.gz	See Httpdtype-0.22.tar.gz (Mar 3, 1999).	
Mar 2, 1999	Net::Nessus::Client Perl module v0.05	Perl-based application that can be used as a non-GUI replacement for other Nessus clients.	
Mar 2, 1999	Net-RawIP v0.06b.tar.gz	The latest version ported to Perl 5.005 and BSD, and including the oshare script (causes Microsoft Windows 98 machines to lock) with additional bug fixes from version 0.06.	
Mar 2, 1999	Sbouncer004b.c	Latest version of program that can bounce using wingate and socks proxies.	
Mar 1, 1999	Gammprog151.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.	
Mar 1, 1999	Spike.sh	Shell script front-end for a number of Denial-of-Service attacks.	

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 include all the trends two weeks ago and several additional trends.

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 operating system.
3. Scanning for Internet Message Access Protocol (IMAP), POP and Domain Name Servers (DNS) continues.
4. Significant increase in reports of NetBus and Back Orifice scanning.
5. For the quarter the following are the ports targeted by hackers in decreasing order: IMAP (143), DNS (53), Echo (7), POP (110), WWW (80), Sun RPC (111), Finger (79) and Telnet (23) .
6. Viruses are now being written to capture and transmit information.
7. Large numbers of SMTP servers are being scanned for common user names, most likely in an effort to obtain names for spam attacks³⁰.

Viruses

Anti-virus vendors recommend that their users update the anti-virus definition packages on a regular basis (every two weeks or sooner).

WM97.Marker – This virus collects information on the user from Word including the user's name, address, and date/time of infection. On the first of the month, this information is transmitted via ftp to the site codebreakers.org. The virus will only upload the information once. This is accomplished by tracking the success of the upload using a registry key. The key is "HKEY_CURRENT-USER\Software\Microsoft\MS Setup (ACME)\User Info" with the addition of "Logfile". If "Logfile" is TRUE then the virus has upload the information. It also randomly names a temporary text file while infecting. This file is named "HSFxxxx.SYS" where xxxx is a randomly generated number. Because of this, the virus is also called WM97.HSFX. There are currently 4 known variants of this virus.

WM97.Sattelite(sic)– This virus encrypts and decrypts itself on-the-fly in an effort to make detection more difficult. The current version modifies the registered owner of Microsoft Windows95/98 to "The wEiRd GeNiUs." This virus is reported as being widespread in Northern Europe.

³⁰ A number of states have enacted legislation making spamming illegal.