National Infrastructure Protection Center CyberNotes

Issue #2001-04 *February 26, 2001*

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, malicious scripts, information security 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 6 and February 23, 2001. The table provides the vendor/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. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear as red and/or italic text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Adcycle .com[1]	Windows NT 4.0/2000, Unix	Adcycle 0.77, 0.78b	A vulnerability exists due to the way input commands are handled which could let a malicious user gain access to database resources, elevate privileges, and execute arbitrary commands.	No workaround or patch available at time of publishing.	Adcycle AdLibrary.pm Session Access	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
America OnLine, Inc.[2]	Multiple	AOL 5.0	A buffer overflow vulnerability exists when a long URL is entered into the input box, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	AOL Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[1] Bugtraq, February 19, 2001.

[2] Securiteam, February 13, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Bajie[3]	Multiple	Java HTTP Server 0.78	Two vulnerabilities exist: one allows a remote attacker to execute any CGI script on the file system by using relative paths; and the second allows arbitrary shell commands to be executed if the server is Unix-based.	No workaround or patch available at time of publishing.	Bajie Webserver Remote Command Execution	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
BiblioWeb[4]	Multiple	BiblioWeb Server 2.0	A directory traversal and buffer overflow vulnerability exists which could enable a remote malicious user to crash the server.	No workaround or patch available at time of publishing.	BiblioWeb Server Directory Traversal and Buffer Overflow Vulnerabilities	Low	Bug discussed in newsgroups and websites.
Brightstation[5]	Multiple	Muscat 1.0	A vulnerability exists when an invalid request is sent which could let a malicious user obtain information about the database path.	No workaround or patch available at time of publishing.	Muscat Root Path Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Carey Internet Services[6]	Windows 95/98/NT 4.0/2000	Commerce. cgi 2.0.1	A vulnerability exists when a specially crafted URL is requested which could let a remote malicious user gain read access to directories and files outside the root directory.	A patched version has been released on their website located at: http://www.commerce-cgi.com/	Commerce.cgi Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Caucho Technology Inc.[7]	Windows NT 2000	Resin 1.2	A directory traversal vulnerability exists which could let a remote malicious user gain read access to directories and files outside the root directory.	Upgrade available at: http://www.caucho.com/download/resin -1.2.3.tar.gz	Resin Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
ChiliSoft[8]	Unix	ChiliSoft ASP for Linux 3.0, Linux 3.5	A vulnerability exists under certain configurations, which could allow a local malicious user to execute arbitrary commands with elevated privileges.	No workaround or patch available at time of publishing.	ChiliSoft ASP GID Root Script Execution	**High**	Bug discussed in newsgroups and websites.
FreeBSD[9]	Unix	Elvis 1.08h2_0 korean, Elvis 1.8.4-0 japanese	A buffer overflow vulnerability exists in the elvrec utility, which could let a malicious user gain root privileges.	Upgrade available at: ftp://ftp.FreeBSD.org/pub/FreeBSD/ports	Elvis Local Root Compromise	**High**	Bug discussed in newsgroups and websites.
FreeBSD[10]	Unix	ja-xlock 2.7 and earlier	A buffer overflow vulnerability exists in the Japanese port of xlock, which could let a malicious user gain root privileges.	**Workaround:** Use an alternative, such as xlock or xlockmore, instead of the ja-xlock port.	ja-xlock Local Root Compromise	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.

[3] Bugtraq, February 15, 2001.
[4] Securiteam, February 11, 2001.
[5] UkR Security Team Advisory #6, February 12, 2001.
[6] Securiteam, February 17, 2001.
[7] Securiteam, February 21, 2001.
[8] Bugtraq, February 7, 2001.
[9] FreeBSD Ports Security Advisory, FreeBSD-SA-01:21, February 7, 2001.
[10] FreeBSD Ports Security Advisory: FreeBSD-SA-01:19, February 7, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Hewlett-Packard[11]	Unix	HP9000 Series 700 & 800 HP-UX 11.04 (VVOS) with Virtual Vault A.04.00	Hewlett-Packard VirtualVault with iPlanet is vulnerable to a flaw that may allow a malicious user to cause a Denial of Service.	No workaround or patch available at time of publishing.	VirtualVault iPlanet Denial of Service	Low	Bug discussed in newsgroups and websites.
HIS Software[12]	Windows 95/98/NT 4.0	Auktion 1.62	A directory traversal vulnerability exists which could let a remote malicious user view files outside of the root directory or execute arbitrary code.	No workaround or patch available at time of publishing.	Auktion Directory Traversal	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
IBM[13]	Windows 95/98/NT 4.0/2000, Apple MacOS 9.0	Lotus Notes R5 Client 4.6	A vulnerability exists which could let a remote malicious user embed malicious code in an e-mail message. Opening the e-mail message or viewing it from a preview pane will execute the code.	Unofficial workaround (Bugtraq): Modify the mailbox database properties by disabling 'Store Form in Document' function, and ensure that Execution Control List (ECL) policies are properly configured.	Lotus Notes Remote Code Execution	**High**	Bug discussed in newsgroups and websites.
Internet Software Consor-tium[14, 15] ***BIND exploit script has now been released.[16]***	**Unix**	**BIND 8.2-8.2.2 p7**	**Multiple vulnerabilities exist: a buffer overfl ow in the transaction signature (TSIG) handling code; buffer overflow in nslookupComplain(); an input validation error in NslookupComplain(); and queries to ISC BIND servers may disclose environment variables which could let a remote malicious user gain unauthorized privileged access to the system with superuser privileges, and allow the execution of arbitrary code.**	**Upgrade to BIND version 9.1.0 available at:** **ftp://ftp.isc.org/isc/bind9/9.1.0/bind-9.1.0.tar.gz**	**Bind Multiple Vulnera-bilities** **CVE candidate** **CAN-2001-10** **CAN-2001-11** **CAN-2001-12** **CAN-2001-13**	**Very High** **Very High because the majority of name servers in operation today run BIND, these vulnera-bilities present a serious threat to the Internet infra-structure.**	**Bug discussed in newsgroups and websites. Exploits have been published.** **Vulnerability has appeared in the press and other public media.** ***Remote BIND INFOLEAK and TSIG exploit code released.***

[11] eSecurityOnline Free Vulnerability Alert 3395, February 22, 2001.
[12] Securiteam, February 9, 2001.
[13] Bugtraq, February 9, 2001.
[14] CERT® Advisory, CA-2001-02, January 29, 2001.
[15] Network Associates, Inc. COVERT Labs Security Advisory, COVERT-2001-01, January 29, 2001.
[16] Securiteam, February 23, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
ITAfrica[17]	Windows 95/98/NT 4.0/2000	WEBactive 1.0	A directory traversal vulnerability exists which could let a remote malicious user gain access to files and directories residing outside the normal web root.	This product is no longer in production.	WEBactive Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
John Roy[18]	Windows 95/NT 4.0	Pi3Web 1.0.1	A buffer overflow vulnerability exists in the server's internal ISAPI handling procedures, which could let a malicious user execute arbitrary code. The server also reveals the physical path of the web root when a 404 error is encountered.	No workaround or patch available at time of publishing.	Pi3Web Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Kevin Lenzo[19]	Unix	Infobot 0.44.5.3	A vulnerability exists in the way commands are handled by the Fortran math function which could allow a remote malicious user to execute arbitrary commands.	No workaround or patch available at time of publishing.	Infobot Fortran Math Arbitrary Command Execution	**High**	Bug discussed in newsgroups and websites.
LICQ[20]	Unix	LICQ 1.0.1, 1.0.2	A remote Denial of Service vulnerability exists when a rich-text format file (*.rtf) is sent to another client.	No workaround or patch available at time of publishing.	LICQ Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Marconi Corporation[21]	Unix	ForeThought 6.2	A remote Denial of Service vulnerability exists when the ASX switch receives a crafted packet with certain attributes.	No workaround or patch available at time of publishing.	ASX-1000 Administration Denial Of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Martin Stover[22] ***FreeBSD has released patch[23]***	**Unix**	**Mars NWE 0.99pl19**	**A format string vulnerability exists which could allow a remote malicious user to gain superuser privileges from DOS/Windows workstations attached to a Mars server.**	**No workaround or patch available at time of publishing.** ***FreeBSD upgrade available at*:** http://archives.neohapsis.com/archives/freebsd/2001-02/0081.html	**Mars NWE Format String**	**High**	**Bug discussed in newsgroups and websites.**
Merant Micro Focus[24]	Unix	Cobol 4.1	A vulnerability exists if the AppTrack feature is enabled, which could let a malicious user compromise root.	No workaround or patch available at time of publishing.	Cobol Arbitrary Command Execution	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[17] Bugtraq, February 16, 2001.
[18] Securiteam, February 21, 2001.
[19] Bugtraq, February 6, 2001.
[20] Bugtraq, February 10, 2001.
[21] Securiteam, February 21, 2001.
[22] Bugtraq, January 26, 2001.
[23] FreeBSD Ports Security Advisory, FreeBSD-SA-01:20, February 7, 2001.
[24] Bugtraq, February 11, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[25]	Windows	Outlook 98, 2000, Outlook Express 5.01, 5.5	An unchecked buffer overflow vulnerability exists which could let a malicious user execute arbitrary code via e-mail messages containing malformed vCards. When the vCard is opened, a buffer overflow error can cause Outlook to crash, or take any desired action, limited only by the permissions of the recipient on the machine	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/ms01-012.asp	Outlook, Outlook Express VCard Handler Unchecked Buffer CVE name: CAN-2001-0145	**High**	Bug discussed in newsgroups and websites.
Microsoft[26]	Windows	Microsoft Windows Media Player 7	A vulnerability exists that could let a malicious web site embed Java applets in the Media Play Skins package, which then can be called under local system privileges and execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq01-010.asp	Windows Media Player Skins File Download	**High**	Bug discussed in newsgroups and websites.
Microsoft[27]	Windows 2000	Windows 2000 Server, 2000 Advanced Server, 2000 Datacenter Server	A Denial of Service vulnerability exists if a remote malicious user sends a continuous stream of invalid requests to the domain controller.	Patch available at: **Microsoft Windows 2000 Server and Advanced Server:** http://www.microsoft.com/Downloads/Release.asp?ReleaseID=28064 **Microsoft Windows 2000 Datacenter Server:** Patches for Windows 2000 Datacenter Server are hardware-specific and available from the original equipment manufacturer.	Windows Malformed Request to Domain Controller Denial of Service CVE name: CAN-2001-0018	Low	Bug discussed in newsgroups and websites.
Microsoft[28]	Windows NT 4.0	Windows NT Enterprise Server 4.0, NT Server 4.0, NT Terminal Server	A vulnerability exists in the PPTP service that could let a remote malicious user cause a Denial of Service.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq01-009.asp	Windows NT Malformed PPTP Packet Stream	Low	Bug discussed in newsgroups and websites.
Multiple Vendors[29]	Unix	SSH Communications SSH 1.2.24-1.2.31; OpenSSH 1.2.2, 1.2.3, 2.1, 2.1.1, 2.2	Various SSH implementations are vulnerable to a buffer overflow, which could allow a remote malicious user to execute arbitrary code.	Patches available at: **OpenSSH:** ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/openssh-2.3.0.tgz **SSH Communications:** ftp://ftp.ssh.com/pub/ssh/ssh-2.4.0.tar.gz **Debian:** http://security.debian.org/dists/stable/updates/main/	SSH CRC-32 Compensation Attack Detector CVE name: CAN-2001-0144	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[25] Microsoft Security Bulletin, MS01-012, February 22, 2001.
[26] Microsoft Security Bulletin, MS01-010, February 14, 2001.
[27] Microsoft Security Bulletin, MS01-011, February 20, 2001.
[28] Microsoft Security Bulletin, MS01-009, February 17, 2001.
[29] eSecurityOnline Free Vulnerability Alert 3388, February 12, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[30]	Unix	Linux kernel 2.2.18 and previous	A vulnerability exists in the sysctl() call that could allow a malicious user to potentially gain elevated privileges and compromise root.	**Immunix:** http://archives.neohapsis.com /archives/linux/immunix/2001 -q1/0052.html **RedHat:** RedHat RPMs: http://archives.neohapsis.com /archives/linux/redhat/2001-q1/0040.html **Caldera:** http://archives.neohapsis.com /archives/linux/caldera/2001-q1/0009.html	Linux sysctl() Kernel Memory Reading	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Nobreak Techno-logies[31]	Multiple	CrazyWWW Board 2000px, 2000LEpx, 98, 98PE, 3.0.1; CrazySearch 1.0.1 CGIs using qDecoder 4.0 ~ 5.0.8	A buffer overflow vulnerability exists due to insufficient boundary checking in the qDecoder CGI library code which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	CrazyWWW Board Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Novell[32]	Multiple	NetWare 5.0, 5.1	A vulnerability exists due to protocol implementation Problems. A man-in-the-middle attack could allow for password hash recovery, along with a user's RSA private key.	No workaround or patch available at time of publishing.	NetWare Password Hash and RSA Key Recovery	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Novell[33]	Windows 95/98/ME/ NT/2000	Groupwise 5.5	A vulnerability exists because Groupwise does not verify system policies that could let a malicious user view the files system of local or remote drives.	Novell is aware of this issue and recommends contacting Novell GroupWise Support (http://support.novell.com) . This vulnerability will be addressed in sp3, a release date is not yet known.	GroupWise Network Directory Browsing	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Silver Platter[34]	Windows NT 4.0, Unix	WebSPIRS 3.3.1	A vulnerability exists when a specially crafted URL is requested which could let a remote malicious user gain read access to known files outside of the root directory.	No workaround or patch available at time of publishing.	WebSPIRS File Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Soft Lite[35]	Windows 95/98/NT 4.0	ServerWorx 3.0	A directory traversal vulnerability exists which could let a remote malicious user gain read access to directories and files outside the root directory.	No workaround or patch available at time of publishing.	ServerWorx Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[30] Bugtraq, February 10, 2001.
[31] Securiteam, February 10, 2001.
[32] eSecurityOnline Free Vulnerability Alert 3396, February 20, 2001.
[33] Bugtraq, February 10, 2001.
[34] UkR Security Team Advisory #1, February 12, 2001.
[35] Securiteam, February 11, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
SSH Communications[36]	Unix	SSH 1.2.31 and Previous	A vulnerability exists in the key exchange protocol RSA-PKCS1_1.5 that could allow a remote malicious user to gain the session key, and potentially decrypt sensitive traffic.	No workaround or patch available at time of publishing.	SSH1 Session Key Retrieval	Medium	Bug discussed in newsgroups and websites.
Stephen Turner[37]	Unix	Analog 4.90beta2 and previous, Analog 4.15 and previous	A buffer overflow vulnerability exists which could let a malicious user execute arbitrary code.	Upgrade available at: http://www.analog.cx/download.html	Analog ALIAS Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

Sun Mircosystems, Inc.[38]	Windows, Unix	SDK & JRE 1.2.2_005 or earlier, 1.2.1_003 or earlier;
		JDK & JRE 1.1.8_003 or earlier, 1.1.7B_005 or earlier, 1.1.6_007 or earlier;
		Solaris Production Releases SDK & JRE 1.2.2_05a or earlier, 1.2.1;
		JDK & JRE 1.1.8_10 or earlier, 1.1.7B, 1.1.6;
		Linux Production Release SDK & JRE 1.2.2_005 or earlier
			A vulnerability exists which could allow a malicious user to use malicious Java code to execute unauthorized commands.	Update available at:
				Windows Production & Solaris Reference Releases:
				http://java.sun.com/products/jdk/
				Solaris Production Releases:
				http://www.sun.com/software/solaris/java/
					Sun Java Runtime Environment Unauthorized Command Execution	**High**	Bug discussed in newsgroups and websites.
							Vulnerability has appeared in the Press and other public media.

Symantec[39]	Windows 98 SE	pcAnywhere 9.0	A buffer overflow vulnerability exists when a large stream of data is sent which could cause a Denial of Service. It may also be possible to execute arbitrary code.	Upgrade to Symantec pcAnywhere version 9.01	PcAnywhere Denial of Service	Low/ **High**	Bug discussed in newsgroups and websites. Exploit has been published.

[36] CORE SDI S.A. Security Advisory, CORE-20010116, February 7, 2001.
[37] Securiteam, February 18, 2001.
[38] Sun Microsystems, Inc. Security Bulletin Security Bulletin Number, #00201, February 22, 2001.
[39] eSecurityOnline Free Vulnerability Alert 3399, February 22, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Thinking Arts[40]	Unix	ES.One 1.0	A directory traversal vulnerability exists which could let a remote malicious user gain read access to directories and files outside the root directory.	No workaround or patch available at time of publishing.	ES.One Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Van Dyke Technologies[41]	Windows NT 4.0/2000	VShell 1.0, 1.0.1	Two vulnerabilities exist: a buffer overflow in the handling of username validation which could let a remote malicious user execute arbitrary code; and a vulnerability in the port forwarding rule which could let a remote malicious user gain privileged access and network access.	Upgrade available at: http://www.vandyke.com/download/vshell	VShell Buffer Overflow and Default Port Forwarding vulnerabilities CVE name: CAN-2001-0155, CAN-2001-0156	**High**	Bug discussed in newsgroups and websites.
Watch Guard[42]	Unix	Firebox II 4.5	A remote Denial of Service vulnerability exists when malformed PPTP packets are sent via a Telnet connection.	Patch available at: http://www.watchguard.com/support	Firebox ll PPTP Denial of Service	Low	Bug discussed in newsgroups and websites.
Working Resources Inc.[43]	Windows 95/98/NT 4.0/2000	BadBlue 1.2.7	A Denial of Service vulnerability exists if a remote malicious user requests a specially crafted URL. Also, when a specially crafted URL is requested, it discloses the physical path to the root directory.	Upgrade available at: http://www.badblue.com/down.htm	BadBlue Denial of Service And Path Disclosure	Low/ Medium	Bug discussed in newsgroups and websites. Exploit 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 and/or the intruder can execute or alter arbitrary system files. 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.

[40] Bugtraq, February 16, 2001.
[41] @stake Security Advisory, A021601-1, February 16, 2001.
[42] Defcom Labs Advisory def-2001-07, February 14, 2001.
[43] Strumpf Noir Society Advisories, February 17, 2001.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between February 10 and February 23, 2001, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing**. During this period, 22 scripts, programs, and net-news messages containing holes or exploits were identified. NOTE: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
February 23, 2001	**BIND_TSIG_exploit_source.txt**	**Script which exploits the INFOLEAK and TSIG BIND vulnerabilities.**
February 21, 2001	**Asxswitch.c**	**Script which exploits the Marconi ASX-1000 Administration Denial Of Service vulnerability.**
February 21, 2001	**Exklock.c**	**Script which exploits the ja-xlock Local Root Compromise vulnerability.**
February 21, 2001	Sqlping.zip	A tool which sends a specially crafted UDP packet to port 1434 on a SQL Server 2000 that will return useful information including SQL version and service pack information. Also includes the ability to send broadcast queries.
February 21, 2001	Ssh1.crc32.txt	Exploit for the SSH CRC-32 Compensation Attack Detector vulnerability.
February 20, 2001	Ettercap-0.2.0.tar.gz	A network sniffer/interceptor/logger for switched LANs, which uses ARP poisoning and the man-in-the-middle technique to sniff all the connections between two hosts.
February 20, 2001	Lpdfp.tar.gz	A Perl script that sends a malformed query to TCP port 515 in an attempt to determine the remote OS.
February 20, 2001	Nmap-2.54BETA19.tgz	A utility for port scanning large networks.
February 20, 2001	Osdetect-lpd.txt	Proof of concept code that contains a database of Line Printer Daemons (LPD) listening on TCP port 515 that gives away information about which OS is running.
February 20, 2001	Scanssh-1.4.tar.gz	Scanner that scans a list of addresses and networks for running SSH servers and their version numbers that supports random selection of IP addresses from large network ranges.
February 20, 2001	Twwwscan12.zip	A Windows based WWW vulnerability scanner, which looks for 400 WWW/cgi vulnerabilities.
February 19, 2001	**Ad-cycle.pl**	**Script which exploits the Adcycle AdLibrary.pm Session Access vulnerability.**
February 13, 2001	Dc20exp.c	Script which exploits the FreeBSD getenv() vulnerability.
February 13, 2001	Sc.txt	Proof of concept exploits for the Sun Clustering v2.x tempfile vulnerabilities.
February 13, 2001	Scanssh-1.3a.tar.gz	Scanner that scans a list of addresses and networks for running SSH servers and their version numbers that supports random selection of IP addresses from large network ranges.
February 13, 2001	Urdls.c	A directory lister for listing files in directories on the local machine without having permission to do so.
February 11, 2001	Dkbf-0.1.1b.tar.gz	A Distributed, Keyboard, Brute-Force program, for Linux clusters that attacks Windows NT using the Message Passing Interface (MPI) to distribute the program.
February 11, 2001	Nessus-1.0.7a.tar.gz	Remote security scanner for Linux, BSD, Solaris and some other systems which is multithreaded, plugin-based, and currently performs over 531 remote security checks.
February 11, 2001	Sara-3.3.4.tar.gz	A security analysis tool based on the SATAN model.

Date of Script (Reverse Chronological Order)	**Script Name**	**Script Description**
February 10, 2001	**Crazy.pl**	**Perl script which exploits the CrazyWWW Board Buffer Overflow vulnerability.**
February 10, 2001	**Licqkill.c**	**Script which exploits the LICQ Denial of Service vulnerability.**
February 10, 2001	Sysctl_exp.c	Script which exploits the Linux sysctl() Kernel Memory Reading vulnerability.

Trends

Probes/Scans:

There has been an increase in the number of suspicious probes and scans designed to find vulnerable domain name servers on corporate networks.

Backdoor-G and NetBus Trojan scans have increased in number.

Other:

A script that exploits the BIND INFOLEAK and TSIG vulnerability has been released. Please update your BIND server if you haven't already done so.

The CERT/CC has recently learned of four vulnerabilities spanning multiple versions of the Internet Software Consortium's (ISC) Berkeley Internet Name Domain (BIND) server. Because the majority of name servers in operation today run BIND, these vulnerabilities present a serious threat to the Internet infrastructure. For more information, please see CERT® Advisory CA-2001-02 located at: http://www.cert.org/advisories/CA-2001-02.html.

Viruses

A list of viruses infecting two or more sites as reported to various anti-virus vendors and virus incident reporting organizations has been categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. 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 soon as updates become available**. The table list the viruses by: ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported during the latest three months), and approximate date first found. During this month, a number of anti-virus vendors have included information on Trojan Horses and Worms. These types of malicious code will also now be included in the table. Following this table are write-ups of new viruses and updated versions discovered in the last two weeks. NOTE: At times, viruses may contain names or content that may be considered offensive.

Note: Virus reporting may be weeks behind the first discovery of infection. A total of **230** distinct viruses are currently considered “in the wild” by anti-virus experts, with another **620** viruses suspected. “In the wild” viruses have been reported to anti-virus vendors by their clients and have infected user machines. The additional suspected number is derived from reports by a single source.

Ranking	Common Name	Type of Code	Trends	Date
1	W32/Hybris	Worm	Slight increase	November 2000
2	PE_MTX.A	File Infector, Trojan	Slight increase	September 2000
3	VBS/Kakworm	Script	Slight decrease	December 1999
4	W32/Navidad	File, Worm	Slight increase	November 2000
5	VBS/LoveLetter	Script	Slight decrease	March 2000
6	VBS/SST	Script, Worm	New to table	February 2001
7	W32/SKA	File	Increase	March 1999
8	W95/CIH	File	Return to table	July 1998
9	W32/FunLove	File	Return to table	November 1999
10	W32/Bymer	Worm	New to table	October 2000

VBS/LoveLet-I (Visual Basic Script Worm): This is a minor variant of the VBS/LoveLet-A worm (also known as the Love Bug).

VBS/San-A (Visual Basic Script Worm): The worm exploits the Scriptlet Typelib and Eyedog vulnerability in some versions of Microsoft Outlook Express and Microsoft Internet Explorer to automatically execute when the e-mail message is viewed. This is a similar attack as that used by the commonly encountered VBS/Kakworm virus. It is recommended that users apply the patch available from Microsoft to close this vulnerability. **Please view Microsoft Security Bulletin MS99-032 for more details at: http://www.microsoft.com/technet/security/bulletin/ms99-032.asp**.

The worm can initially infect using two infection paths: either by the user visiting a web page with embedded worm code or opening an infected e-mail message, previewed in a browser or e-mail client without the security patch installed. When the viral code runs, it drops a file LOVEDAY14-B.HTA into the Windows StartUp folder. When the computer is rebooted, the dropped HTA file is run. It first changes the Internet Explorer homepage so that it points to a page that contains a dropper for VBS/Valentin-A worm (this webpage has now been shut down) and then drops a file called MAIN.HTML into the Windows System directory. The worm then uses Microsoft Outlook to send the worm to all contacts from the each user's address book. The message comes without a subject and embedding its script code into each message sends the worm, so that the message has no attachments. The worm also attempts to send ten SMS text messages to randomly chosen numbers on a Spanish mobile phone network. The subject of the message is:

"Feliz san valentin" (Happy St.Valentine's day)

and the message text is:

"Feliz san valentin. Por favor visita htpp://www.terra.es/personal/ acaymo."

The URL mentioned in the message contains the embedded virus dropper. The worm also searches all fixed and network drives for MIRC32.exe or MLINK32.EXE and if any of them is found, the worm drops a mIRC (Internet Relay Chat) script which attempts to send the worm to other mIRC users. If any files with a URL extension are found, the worm replaces them with a new one, which points to http://www.terra.es/personal2/jackis. On 8th, 14th, 23rd, or 29th day of the month, the worm attempts to overwrite all files on the local hard drive and shared network drives with Spanish text. When a file is overwritten, it is renamed so that it has a double extension with the .TXT extension added to the original one (e.g., Notepad.exe becomes Notepad.exe.txt).

VBS/SST-B (Visual Basic Script Worm): This is a variant of the VBS/SST-A worm (also known as Anna Kournikova). Because the worm transmits itself using German language it is unlikely to spread widely in non-German speaking communities. The VBS/SST-B worm copies itself to the Windows directory as a file called Neue Tarife.txt.vbs. Users may think the file is an innocent text file, but in fact it is a Visual Basic Script worm. The worm can make changes to the Registry as follows:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\T-Online
HKCU\software\\mailed
HKCU\software\\mirqued
HKCU\software\\pirched

The worm will attempt to spread via the Microsoft Outlook e-mail client, mIRC and Pirch. When the worm arrives via e-mail it has the following characteristics:

Subject: Neues von Ihrem Internetdienstleister - Robert T.
Online informiert

VBS_VALENTIN.A (Aliases: VALENTIN.A, VBS/Valentin@MM) (Visual Basic Script Worm): This worm is encrypted in an HTML file. This worm comes embedded in an e-mail message that has no subject, message body or attachment. It propagates via MS Outlook and also sends messages to mobile phones. If the current system date is 8, 14, 23, or 29, this worm renames all files in the C:\ drive by adding a .TXT extension to all. Then it overwrites the contents of the renamed files with some text in Spanish. This worm may also use mIRC.

WM97/Bleck-A (Word 97 Macro Virus): On August 31 this virus overwrites the contents of the current document with:

"A CURSE FROM BLACKROSE TO SOMEONE HE HATES. HIJADIPUTA KANG HAYUP KA! BURAY MO, SAKA BURAY NI INA MO! HAYUP KA! SAYANG KA, HAYUP KA! HAYUP KA TALAGA! WORD97/BLACKCURSE VIRGOBLACKROSE Virus Development Libmanan Camarines Sur."

WM97/Eight941-H (Word 97 Macro Virus): This is a minor variant of the Eight941 family of viruses. It is a macro virus which only replicates and contains no malicious payload.

WM97/InAdd-E (Word 97 Macro Virus): This is a minor variant of the WM97/InAdd-D Word macro virus.

WM97/Marker-GJ (Word 97 Macro Virus): Whenever a document is closed there is a 1 in 3 chance of a File Summary box appearing on the screen with the author name set to Ethan Frome.

WM97/Nsi-F (Word 97 Macro Virus): WM97/Nsi-F is a Word macro virus which only replicates and contains no malicious payload.

XM97/Barisada-O (Excel 97 Macro Virus): This is a minor variant of the XM97/Barisada-B Excel macro virus. It stores its virus macros in the file RMC.XLS. On April 24, between 2pm and 3pm, the virus displays a series of dialog boxes asking the user questions which appear to be related to a fantasy role-playing game. The first dialog box has the title '1st Question' and the text 'Question: What is the Sword Which Karl Styner (=Grey Scavenger) used? Answer: Barisada'. If you press 'No', a dialog box with the title 'Right Answer' and the message 'Good! You're Authorized now!' is displayed. If you press 'Yes', then a dialog box with the title 'Wrong Answer' and the text 'I will give you one more Chance. Be careful!!' is displayed. The next dialog box has the title 'Wrong Answer may cause The Serious Problem!' and the text 'Summoning Xavier is the Ultimate Magic. Right?'. If you press 'Yes' a dialog box with the title 'Right Answer' and the message 'ok, i will forgive you' appears. If you press 'No' a dialog box with the title 'You shall Die' and the message 'Wrong Answer, Your file will be deleted!' appears. The virus then clears all the cells in all the open sheets.

XM97/Barisada-P (Excel 97 Macro Virus): This is a variant of the XM97/Barisada-N Excel macro virus. The virus's trigger conditions have been removed which means that the virus will do little more than replicate.

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table starts with Trojans discussed in CyberNotes #2001-01, and items will be added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on Trojans and Trojan variants that anti-virus software detects. NOTE: At times, Trojans may contain names or content that may be considered offensive.

Trojan	Version	CyberNotes Issue #
Backdoor.Acropolis	**N/A**	**Current Issue**
Backdoor.Netbus.444051	**N/A**	**Current Issue**
Backdoor-JZ	N/A	CyberNotes-2001-02
BAT.Install.Trojan	**N/A**	**Current Issue**
BAT_EXITWIN.A	N/A	CyberNotes-2001-01
Flor	N/A	CyberNotes-2001-02
HardLock.618	**N/A**	**Current Issue**
PHP/Sysbat	N/A	CyberNotes-2001-02
PIF_LYS	N/A	CyberNotes-2001-02
PWSteal.Coced240b.Tro	**N/A**	**Current Issue**
Troj/KillCMOS-E	N/A	CyberNotes-2001-01
TROJ_AOL_EPEX	N/A	CyberNotes-2001-01
TROJ_AOLWAR.B	N/A	CyberNotes-2001-01
TROJ_AOLWAR.C	N/A	CyberNotes-2001-01
TROJ_APS.216576	N/A	CyberNotes-2001-03
TROJ_AZPR	N/A	CyberNotes-2001-01
TROJ_BAT2EXEC	N/A	CyberNotes-2001-01
TROJ_BKDOOR.GQ	N/A	CyberNotes-2001-01
TROJ_BUSTERS	**N/A**	**Current Issue**
TROJ_DARKFTP	N/A	CyberNotes-2001-03
TROJ_DUNPWS.CL	**N/A**	**Current Issue**
TROJ_FIX.36864	N/A	CyberNotes-2001-03
TROJ_GLACE.A	N/A	CyberNotes-2001-01
TROJ_GOBLIN.A	N/A	CyberNotes-2001-03
TROJ_GTMINESXF.A	N/A	CyberNotes-2001-02
TROJ_HERMES	N/A	CyberNotes-2001-03
TROJ_HFN	N/A	CyberNotes-2001-03
TROJ_ICQCRASH	N/A	CyberNotes-2001-02
TROJ_JOINER.15	N/A	CyberNotes-2001-02
TROJ_MOONPIE	**N/A**	**Current Issue**
TROJ_NAVIDAD.E	N/A	CyberNotes-2001-01
TROJ_PORTSCAN	N/A	CyberNotes-2001-03
TROJ_QZAP.1026	N/A	CyberNotes-2001-01
TROJ_RUNNER.B	N/A	CyberNotes-2001-03
TROJ_RUX.30	N/A	CyberNotes-2001-03
TROJ_SUB7.401315	N/A	CyberNotes-2001-01
TROJ_SUB7.MUIE	N/A	CyberNotes-2001-01
TROJ_SUB7.V20	N/A	CyberNotes-2001-02
TROJ_SUB7DRPR.B	N/A	CyberNotes-2001-01
TROJ_SUB7DRPR.C	N/A	CyberNotes-2001-03
TROJ_TWEAK	N/A	CyberNotes-2001-02
TROJ_WEBCRACK	N/A	CyberNotes-2001-02
Trojan.MircAbuser	**N/A**	**Current Issue**
VBS.Delete.Trojan	**N/A**	**Current Issue**
VBS.Trojan.Noob	**N/A**	**Current Issue**
W32.BatmanTroj	**N/A**	**Current Issue**

Backdoor.Acropolis: This Trojan horse permits a remote operator to control an infected system. When launched, the Trojan horse opens a network connection on ports 32791 and 45673. This gives a remote operator the capability to use your computer to send messages using mIRC. These messages may contain attached files. It is possible, but not confirmed, that the Trojan horse could also be used to control e-mail programs.

Backdoor.Netbus.444051: This is a variant of the well-known backdoor Trojan, Netbus. The Trojan contains a registry file that modifies the Windows registry. This was done because NetBus Pro version 2.1 has been redesigned so that, by default, it is not hidden. This allows NetBus Pro version 2.1 to be used as a legitimate remote-control tool. When this variant is run, it modifies the Windows registry so that NetBus runs in stealth mode. To further hide its malicious actions, this backdoor Trojan attempts to trick you into believing it is a picture. When the file has been executed, after performing all the malicious actions, this backdoor Trojan will display a picture. By default, this variant of Netbus will open port 20034.

BAT.Install.Trojan: This is a batch file Trojan horse that creates many folders in the root of drive C. After creating the folders, it copies itself to many locations, and in doing so, overwrites necessary Windows files. The original file name is "Install.bat."

HardLock.618 (Aliases: Trojan Dood, Mutha Trojan): This is a boot Trojan. It does not infect or delete files. When this Trojan is executed, it changes a single byte of the MBR of the first hard drive on the computer (normally drive C). This change prevents the computer from booting. Following the failure to start, the Trojan displays the following message:

Hardlock Completed Sucessfully

PWSteal.Coced240b.Tro (Aliases: Trojan.PWS.Coced.240.b, PWS.gen, NAEBI.240B.Trojan): The password stealer appears as an attachment named 26705-i386-update.exe. It claims to be a vulnerability patch that is mailed from support@microsoft.com. The Trojan sends confidential password information to an e-mail address. Microsoft has posted information regarding bogus files such as this at: http://www.microsoft.com/technet/security/bogus.asp.

TROJ_BUSTERS (Alias: BUSTERS): This is the server side of a hacking tool, which gives a remote malicious user running the client side of this hacking tool access to an infected computer. Similar to the Back Orifice Trojan, it compromises network security since administrative privileges are granted to a remote user. Upon execution, this Trojan makes itself active in memory and executes upon boot-up. The Trojan resides in memory, listens to port 39507, and waits for commands from the client side of this hacking tool.

TROJ_DUNPWS.CL (Aliases: DUNpws.cl, Trojan.PSW.TFC, HackTool.PWSteal, Troj/Zorro): This Trojan does not infect any file and does not replicate. It is a hacking tool that attempts to crack Dial-Up networking passwords and then save them in a file. This Trojan may be used for malicious purposes, therefore it is considered destructive. It creates a named "~TF43C.TMP" text file which contains the following information:

Account: <Account>
Username: <Username>
Password: <password

TROJ_MOONPIE (Alias: MOONPIE): This client side of a hacking tool enables a remote hacker access to a computer running the server side. It is similar to the Back Orifice Trojan that compromises network security. It gives system administrator privileges to a remote user.

Trojan.MircAbuser: Trojan.MircAbuser is installed on the computer by an executable file, named "CD-R Doubler.exe," that is detected as Trojan.MircAbuser.dr. When executed, this file appears to install a useful tool such as a CD speed doubler; however, this program:

Installs Mirc32 in the C:\Mirc folder.

Creates a copy of Mirc32.exe in the C:\Program Files folder. The file name of this copy is Schd.exe, but it is just a renamed Mirc32.exe file.

Creates a shortcut to the copy in C:\Windows\Start Menu\Programs\StartUp so that the computer is connected to mIRC as much as possible.

Trojan.MircAbuser generally consists of three hidden .ini script files that are used by the Mirc32 copy that is installed along with this Trojan horse. These hidden files are installed in the C:\Program Files folder and allow a hacker to access the affected system and use it for a Denial of Service attack. One indication that the installer file has been launched is that a small envelope icon appears in the system tray.

VBS.Trojan.Noob: This Trojan uses animation to disguise its actions. Once executed, it searches for mIRC, and if found, it will attempt to modify mIRC settings to allow unauthorized access to the infected computer.

VBS.Delete.Trojan: This is a Trojan horse that tries to remove the \Windows and \Program Files folders, including their contents. It is 373 bytes long. After trying to remove these folders, it displays a message box with the following text: http:/ /www.Webtool.com. The message box has the title "ERROR."

W32.BatmanTroj: This is a destructive Trojan horse that deletes files. It deletes all files from the root of C:, including Autoexec.bat, Command.com and Config.sys. From the C:\Windows folder, it deletes:

Himem.sys
Win.ini
System.ini
Protocol.ini

From the C:\Windows\System folder, it deletes El90x???.sys (this is apparently a backup file). Because this effectively deletes the operating system, Windows will not load.