



National Infrastructure Protection Center CyberNotes

Issue #16-99

August 4, 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 July 16 and July 30, 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. New information contained in the update will appear as red and/or italic text.**

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Axent ¹ <i>Hotfix is now available from Axent²</i>	ESM 5.0	Under specific conditions ESM will copy the user's startup script to the /TMP directory which changes file ownership and permissions to "root." When these files are copied back to the user's directory, the file ownership and permissions remain as root. This prevents the user from executing the startup script.	Vendor recommended solution is to use version 5.01 when available. <i>Axent supplies a hotfix, which solves this problem. For more information, contact support@axent.com</i>	Axent User Profile permission vulnerability	Low/ Medium	Bug discussed in newsgroups and websites. The application causes this denial-of-service condition.
BMC software ³ <i>Vendor has released an upgrade package.⁴</i>	Patrol v3.2 (most Unix platforms)	The out of the box configuration may allow a local user to compromise root. This occurs when snmpagent creates a file. The file is owned by the owner of the parent directory and is potentially world writeable. The local user can specify any file to create including '.rhost'.	No vendor supplied patch or workaround available at time of publishing. <i>Versions 3.2.05 and higher are known not to be vulnerable. You can download the upgrade from the Patrol support web site: http://www.bmc.com/support.html</i>	Patrol SNMP agent file creation/permission vulnerability	High	Bug discussed in newsgroups and websites. The application out of the box causes this problem.
Checkpoint Software ⁵	Firewall 1.3.0 & 1.4.0	Firewall-1 can be shutdown by filling its connection table. This is easily done in about 15 minutes with most port scanners. This effectively causes a DoS condition with Firewall-1 defaulting to a 'failed closed' state. <i>Each site should access whether systems protected by Firewall-1 are mission critical.</i>	No vendor supplied patch or workaround available at time of publishing.	Table Saturation DoS Vulnerability	High <i>(Due to the potential systems affected)</i>	Bug discussed in newsgroups and websites. Exploit has been published.

¹ Bugtraq, July 13, 1999.

² Bugtraq, July 15, 1999.

³ Bugtraq, July 13, 1999.

⁴ Securiteam, July 18, 1999.

⁵ Bugtraq, July 29, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Linux ⁶	AMaViS 0.2.0Pre-4 virus scanner for Linux	The potential exists for malicious users to insert arbitrary commands that AMaViS will run as root.	Co-authors of AMaViS have released a fixed version 0.2.0-pre5 which is available at: http://aachalon.de/AMaViS/	Input Validation Error	High (Insertion of code may introduce additional vulnera- bilities)	Bug discussed in newsgroups and websites. Exploit has been published.
Linux ⁷	Linux 2.2.10	A potential vulnerability in the Linux ipchains firewall implementation exists that makes it possible for an attacker to bypass the packet filter when communicating with machines that allow incoming packets to specific ports. Port information is rewritten in order to gain access to ports that should be blocked by the firewall.	No vendor supplied patch or workaround available at time of publishing.	Packet Filter Bypass Vulnerability	Medium/ High	Bug discussed in newsgroups and websites. Exploit has been published.
Metlab ⁸	GNU Finger Version 1.37	There are two vulnerabilities in the GNU finger package that have to do with proper privilege dropping. The finger daemon runs as root by default and responds to finger queries for information on the system's users, which allows a malicious user to have an arbitrary program run. The second vulnerability allows an attacker to create a symbolic link that fingerd will follow and read.	These vulnerabilities are not new but still remain unfixed.	Access Validation Error	High	Bug discussed in newsgroups and websites. Exploit script has been published.

⁶ Bugtraq, July 16, 1999.

⁷ data protect GmbH - Advisory 2, July 27, 1999.

⁸ Bugtraq, July 21, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft ⁹	Internet Explorer 4, 5; Outlook 98, 2000	There is a security hole that allows an introduction of a virus by simply looking at a web page or reading an e-mail message. This vulnerability takes advantage of a problem in Word 97.	For complete details, plus the downloadable patch, go to: http://officeupdate.microsoft.com/downloadDetails/wd97sp.htm	Word 97 Virus Vulnerability	Medium	Bug discussed in newsgroups and websites. Vulnerability has appeared in the Press.
Microsoft ¹⁰	Microsoft's MSN Messenger	Numerous vulnerabilities exist: Password (which is the same as your Hotmail e-mail password) and Contact list are stored in the Registry (HKEY_CURRENT_USER\Identities); The instant messages are sent unencrypted in MIME format; and the program is using Hotmail as its user base. You must have a Hotmail account, which is terminated after 120 days of inactivity.	No vendor supplied patch or workaround available at time of publishing.	MSN Messenger Vulnerabilities	Medium	Bug discussed in newsgroups and websites.
Red Hat ¹¹ <i>This is a new Samba 2.0.5a software package release that addresses vulnerabilities identified in previous CyberNotes.</i>	New Samba packages for Red Hat Linux 4.2, 5.2, 6.0	Samba 2.0.5a has been released which addresses the following security vulnerabilities: - A DoS attack could be performed against the netbios name daemon (nmbd). - a buffer overflow was present in the message service in smbd - a race condition in smbmnt allowed users to mount at arbitrary points of the file system if submnt is setuid	Upgrade to the new version of Samba which can be downloaded from: http://www.samba.org	Various Security Vulnerabilities	Low/ Medium/ High (Multiple vulnerabilities addressed)	Bug discussed in newsgroups and websites.

⁹ PC Computing E-Letter, July 14, 1999.

¹⁰ Bugtraq, July 22, 1999.

¹¹ RHSA-1999:022-02, July 22, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Red Hat ¹²	Red Hat 5.0, 5.1, 5.2	A bug exists in early anti-relay rulesets that makes it possible to bypass any relaying rules. This leaves the server open to be used as a relaying agent	No vendor supplied patch or workaround available at time of publishing.	Mail Relay Vulnerability	Medium/ High	Bug discussed in newsgroups and websites. Exploit has been published
Sun ¹³ <i>Hotspot has fixed this vulnerability¹⁴</i>	Java Hotspot with Microsoft Internet Information Server (IIS)	A specific URL will cause a system crash when IIS and Java HotSpot Performance engine are running together.	No vendor supplied patch or workaround available at time of publishing. <i>The latest version of hotspot has fixed this vulnerability. This version can be downloaded from: http://java.sun.com/products/hotspot/</i>	Java HotSpot Denial-of-Service vulnerability	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Sun Solaris ¹⁵ - Multiple versions <i>Patches that fix this vulnerability have been released.¹⁶</i>	Rpc.cmsd (Operating System)	Remote unauthorized user can execute a buffer overflow in the calendar manager that may result in root access.	No vendor supplied patch or workaround available at time of publishing. <i>The following patches have now been released:</i> <i>Solaris 7/Sparc:</i> <i>107022-03 CDE 1.3</i> <i>Solaris 7/x86:</i> <i>107023-03 CDE 1.3_x86</i> <i>Solaris 2.6:</i> <i>105567-08 CDE 1.2_x86</i> <i>Solaris 2.5.1:</i> <i>104976-04 OW 3.5.1</i> <i>Solaris 2.4 patches will be Released at a later date.</i> <i>Systems may still be running the old, vulnerable daemon after installing the patch unless the Rpc.cmsd process is killed *after* the patch has been installed.</i>	Solaris Rpc.cmsd Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit has been published.
Unix ¹⁷	Joe 2.8 (text editor)	Creates a file that is world-readable/writable. This file may be left in normally restricted directories allowing an unauthorized user to gain access.	No vendor supplied patch or workaround available at time of publishing.	Text Editor Vulnerability	High	Bug discussed in newsgroups and websites. Exploit has been published.

¹² Bugtraq, July 16, 1999.

¹³ NTBugtraq, July 6, 1999.

¹⁴ Securiteam, July 23, 1999.

¹⁵ Bugtraq, July 9, 1999.

¹⁶ Bugtraq, July 15, 1999.

¹⁷ Bugtraq, July 17, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Windows 2000 ¹⁸	Windows 2000 Encrypting File System (EFS)	A whitepaper has been released entitled "Windows 2000 Encrypting File System (EFS) Vulnerability detailing purported vulnerabilities in the EFS that will ship as part of Microsoft Windows 2000.	More information on Windows 2000 security and the EFS is available at: http://www.microsoft.com/windows/server/Technical/security/default.asp Http://www.microsoft.com/windows/server/Technical/security/encrypt.asp http://www.microsoft.com/security/default.asp	Encrypting File System Vulnerability	Risk not yet determined	Bug discussed in newsgroups and websites. Exploit has been published in a whitepaper.
Windows 3.1, 95, 98, NT 4.0, NT 2000 ¹⁹	WS-FTP Pro and LE versions	The FTP site configuration information, including the username and password for that site is stored in an INI file, encrypted by a very weak encryption algorithm.	No vendor supplied patch or workaround available at time of publishing.	Weak Password Encryption	Medium/High	Bug discussed in newsgroups and websites. Exploit script has been published.
Windows NT ²⁰	Microsoft Windows NT Workstation 4.0; Windows NT Server 4.0; Microsoft Windows NT Server 4.0, Enterprise Edition; Microsoft Windows NT Server 4.0, Terminal Server Edition	Dialer has a potential buffer overflow in the dialer.ini file that maybe exploited by a local user to gain increased privilege. This buffer overflow could be used to run arbitrary code via a classic buffer overrun technique.	Patch can be downloaded at: NT ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP5/Dialer-fix/ NT Terminal Server ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40tse/hotfixes-postSP4/Dialer-fix/	Malicious Dialer Entries Elevate Privileges Vulnerability	High	Bug discussed in newsgroups and websites. Exploit script has been published. This vulnerability has received a great deal of attention in the Hacker community.
Windows NT ²¹	WinGate 3.0	WinGate 3.0 has three vulnerabilities: The ability to read any file on the remote system; a DoS attack against the WinGate service; and the ability to decrypt WinGate passwords.	No vendor supplied patch or workaround available at time of publishing.	Multiple WinGate Vulnerabilities	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.

¹⁸ NTSecurity, July 25, 1999.

¹⁹ NTBugtraq, July 29, 1999.

²⁰ Microsoft Security Bulletin (MS99-026), July 29, 1999.

²¹ NT Security, July 20, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Windows NT 4.0 ²²	Internet Information Server (IIS) 3.0 or 4.0 that have or have had Microsoft Data Access Components (MDAC) 1.5 installed on it. NOTE: MDAC 1.5 is installed during a default installation of the Windows NT 4.0 Option Pack	This vulnerability gives complete access to the box as SYSTEM. An unauthorized user can add users, modify the registry, open up things that are closed, put files, take files, delete files, etc. All versions of MDAC are vulnerable, if sample pages of RDS are installed. Many of the Internet's largest sites are at potential risk.	Newer versions of MDAC (2.0, 2.1) resolve these known vulnerabilities. A system that had MDAC 1.5 installed on it, and then upgraded to MDAC 2.0/2.1 must still take actions to disable the DataFactory object. Current versions of MDAC can be downloaded from: http://www.microsoft.com/data/download.htm If you downloaded HANDUNSF.REG and used it to automatically change the registry, you should download the corrected file (HANDSAFE.REG) and run it on all affected systems. FAQs regarding this vulnerability and updating systems to protect against it can be found at: http://www.microsoft.com/security/bulletins/MS99-025faq.asp If you do not complete all steps, unauthorized access may still be possible.	IIS RDS Vulnerability	High	The hole was originally announced on July 17, 1998. Microsoft re- released the advisory after several large companies failed to fix the bug. Bug discussed in newsgroups, websites, and the Press. This hole can be exploited with a mere six lines of code and is so easy to exploit that people with little technical knowledge would have no problem cracking an affected site.
Windows NT, 95, 98 ²³	Jet 3.51 driver (ODBCJT32. DLL) shipped with the Office 97 software suite	A vulnerability in Microsoft Office 97 can allow malicious code contained in an Excel 97 worksheet hidden in a web page or sent in e-mail to take control of online computers without the victims' being aware	Upgrade to Jet 4.0 driver. This driver is delivered as part of MDAC 2.1 which can be downloaded at: http://www.microsoft.com/data/	MS Office Driver Vulnerability	High	Bug discussed in newsgroups and websites.

*Risk is defined in the following manner:

High - A vulnerability that will allow an intruder to immediately gain privileged access (e.g., sysadmin, and root) to the system. An example of this would be a vulnerability in which a sequence of instructions is sent to a machine by an unauthorized user and the machine responds with a command prompt.

²² Re-released Microsoft Security Bulletin (MS99-25), July 19, 1999.

²³ Bugtraq, July 29, 1999.

Medium - A vulnerability that will allow an intruder immediate access to the system that is not privileged access. This allows the intruder the opportunity to continue the attempt to gain root access. An example would be a configuration error that allows an intruder to capture the password file.

Low - A vulnerability that provides information to an intruder that could lead to further compromise attempts or a Denial-of-Service (DoS) attack. The reader should note that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered as a "High" threat.

Recent Exploit Scripts

The table below contains a representative sample of exploit scripts, identified between July 16 and July 30, 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, 6 scripts, programs, and net-news messages containing holes or exploits were identified.

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
July 28, 1999	Cracking Win2000 EFS Whitepaper*	A Whitepaper which describes various attacks against a stand-alone machine and considers cases in which the EFS recovery agent has been left as the default or has been delegated to another user.	
July 28, 1999	Msadc.pl	Exploit script that looks for a common file to exploit in the RDS DataFactory object.	
July 28, 1999	IC Pass 2.1	AppleScript exploit that finds an encrypted password in the Internet Preferences file in the Preferences folder using a resource editor	
July 16, 1999	Segment-bug.c	Exploit script that takes advantage of the division of the address space between a user process and the kernel.	
July 16, 1999	Vm-dos.c	Denial of service exploit.	
July 16, 1999	NMRC Pandora v4 beta	The recently released NMRC Pandora v4 Beta includes the exploit for gaining admin privileges on machines running Novell.	
July 15, 1999	Saint 1.4 Beta 3	Web-based vulnerability scanner that updates SATAN.	

Script Analysis

* This Whitepaper has been included to provide the reader with an alert/warning that the "Hacker Community" is investigating Windows 2000 vulnerabilities prior to the official release of the product.

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.

Back Orifice 2000

Back Orifice 2000 is a powerful hacker tool designed to remotely control computers installed with Windows 95, 98, and NT. The tool can be installed on the victim machine without the knowledge of the user and can cause serious damage. Back Orifice 2000, (BO2K) is an upgrade to the original Back Orifice hacker tool. Members of the hacker group "Cult of the Dead Cow" authored both programs. The program is freely available over the Internet. The prominent new features of BO2K are:

- It runs on Windows NT. When the BO2k server portion, (The piece that runs on the victim machine) is installed, it runs as a service with full administrator privileges. The previous version only ran on Windows 9.x.
- The product has been released under the terms of the GNU license, which means that the source code is freely available. Modifications made to the source code may alter the signature of the tool and make it more difficult to detect.

The program uses client server architecture to control victim machines:

- BO2K client: The BO2K client is installed on the hacker's machine and is used to configure, generate and eventually control the server portion. The server is generated using an intuitive GUI and a "wizard" is also available further simplifying the process. Once the server has been generated, it can be emailed as an attachment to the victims' machine. Once the attachment has been "double-clicked" the BO2K server installs itself without the knowledge of the user.
- BO2K server: The portions of BO2K that runs on the victim machine and allows the client complete administrative control of the PC where the server is installed.

BO2K Features:

The new version includes support for 3DES. This allows communication between BO2K client and server to be encrypted. The program has a modular architecture that allows for the creation of "plug-ins". The program comes with a plug-in called BOPEEP that allows a remote hacker to lock the local keyboard and mouse while maintaining remote control over these devices.

When accessing a remote BO2K system, an attacker can access files, directories, and network shares with administrator privileges. These files and directories can be retrieved, deleted or renamed on the target machine. On Windows NT systems, processes and services can be monitored and stopped by the remote attacker. Keystrokes can be recorded and viewed. The remote machine can be locked or rebooted. The program has its own compression utility so files can be quickly transferred to and from the target machine. DNS queries can be launched from the target machine. The registry, (a windows database of system and user settings) can be modified. Multimedia devices attached to a victim's machine, including

video cameras can be operated remotely, giving the attacker the ability to “listen in”. Finally, the BO2K server itself can be remotely stopped restarted and completely removed.

Detection of BO2K

Host based Detection

At the present time there are configurations of the BO2K server that cannot be detected by antivirus programs. It is imperative that users obtain the latest virus signature from their vendors.

When installed in the default configuration BO2K creates registry entries under HKEY_LOCAL_MACHINE > SYSTEM > CURRENTCONTROLSET > SERVICES. The actual service name depends on the BO2K server configuration. The default name of the BO2K server is “remote administration service”. If this key is deleted it will disable BO2K functionality. As always, only an experienced NT administrator should make registry changes. If the server was configured with the defaults, a file name UMGR32.EXE will reside in the WINNT\SYSTEM32 directory. Deletion of this file will complete the removal of BO2K. One should assume that an unauthorized user/intruder is aware of the default file detection method and will configure the BO2K server to install files under different names. This increases the difficulty in removing BO2K.

Network based Detection

BO2K can operate under “insidious” mode where client server communications appear as ICMP traffic. This will make network detection of BO2K difficult.

Precautions

It is recommended that users do not execute email attachments from unknown sources and keep virus signatures up to date. Users should secure computers when not in use to prevent manual installation of the BO2K server.

Trends

Trends for this two week period:

1. Infrastructure attacks against corporate e-mail.
2. Attacks have increased that exploit software that manages appointment calendar programs shipped with Unix operating systems.
3. Weak passwords are becoming a security nightmare for large organizations.
4. Crackers to break into web sites are using well-known security holes for which patches were previously available.
5. Security holes in CGI scripts are currently being exploited.
6. An increased number of reports of SYN and IP Spoofing attacks that result in a Denial-of-Service.
7. Web hacks using Cold fusion vulnerabilities continues.
8. Hackers have taken a greater interest in cable modems and DSL lines. Individual report receiving two probes per day against their machines using cable modems or DSL lines.

Viruses/Trojans

Back Orifice for Macintosh - TakeDown Suite 2.5:

This is a backdoor program similar to the original Back Orifice. Once installed the application allows someone to remotely administer the machine. This is similar functionality to Back Orifice, which only works under Windows. TakeDown Suite operates by installing an invisible extension into the system folder, when the machine next reboots it is vulnerable. When you double click the server, it installs an extension called 'Takedown Server Suite' in the extensions. This item is invisible, so you will need a program like ResEdit to change the visible/invisible flag.

Anti-virus scan may damage Excel files:

Your Excel files may be damaged after you scan and clean your Excel workbooks with an anti-virus software program. When you attempt to open, close or save a workbook, you may receive an error message similar to: "EXCEL caused an invalid page fault in module KERNEL32.DLL at 0137:3001b693" or "EXCEL caused an invalid page fault in module EXCEL.EXE at 0137:3001b963." Then Excel quits when you click Close. If you can open the workbook, your troubles are not over: It may contain two worksheets named ***** (five asterisks) with the visible property set to xlveryhidden. This problem may occur in Excel 97 for Windows, Excel for Windows 95 7.0, Excel for Windows 5.0 and Excel for Windows 5.0c. If you can open the damaged workbook, Microsoft suggests these steps to recover your data:

- 1) Open a new workbook.
- 2) Select the cells that contain data and click Copy in the first worksheet in the damaged workbook.
- 3) In the new workbook, paste the data into a worksheet.
- 4) Repeat these steps for each worksheet.
- 5) Save the new workbook as a new file.