Software Engineering Institute
Carnegie Mellon University

1994 CERT Advisories

CERT Division

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

http://www.sei.cmu.edu

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

This report was prepared for the

SEI Administrative Agent
AFLCMC/AZS
5 Eglin Street
Hanscom AFB, MA 01731-2100

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM17-0052

Table of Contents

1 CA-1994-01: Ongoing Network Monitoring Attacks

Original issue date: February 3, 1994
Last revised: September 19, 1997
Updated copyright statement

A complete revision history is at the end of this file.

In the week before we originally issued this advisory, the CERT/CC staff observed a dramatic increase in reports of intruders monitoring network traffic. Systems of some service providers have been compromised, and all systems that offer remote access through rlogin, telnet, and FTP are at risk. Intruders have already captured access information for tens of thousands of systems across the Internet.

The current attacks involve a network monitoring tool that uses the promiscuous mode of a specific network interface, /dev/nit, to capture host and user authentication information on all newly opened FTP, telnet, and rlogin sessions.

In the short-term, we recommend that all users on sites that offer remote access change passwords on any network-accessed account. In addition, all sites having systems that support the /dev/nit interface should disable this feature if it is not used and attempt to prevent unauthorized access if the feature is necessary. A procedure for accomplishing this is described in Section III.B.2 below. Systems known to support the interface are SunOS 4.x (Sun3 and Sun4 architectures) and Solbourne systems; there may be others. Sun Solaris systems do not support the /dev/nit interface. If you have a system other than Sun or Solbourne, contact your vendor to find if this interface is supported.

While the attack is specific to /dev/nit, the short-term workaround does not constitute a solution. The best long-term solution currently available for this attack is to reduce or eliminate the transmission of reusable passwords in clear-text over the network.

I. Description

Root-compromised systems that support a promiscuous network interface are being used by intruders to collect host and user authentication information visible on the network.

The intruders first penetrate a system and gain root access through an unpatched vulnerability. Solutions and workarounds for these vulnerabilities have been described in previous CERT advisories, which are available from ftp://ftp.cert.org/pub/cert_advisories.

The intruders then run a network monitoring tool that captures up to the first 128 keystrokes of all newly opened FTP, telnet, and rlogin sessions visible within the compromised system's domain. These keystrokes usually contain host, account, and password information for user accounts on other systems; the intruders log these for later retrieval. The intruders typically install Trojan horse programs to support subsequent access to the compromised system and to hide their network monitoring process.

II. Impact

All connected network sites that use the network to access remote systems are at risk from this attack.

All user account and password information derived from FTP, telnet, and rlogin sessions and passing through the same network as the compromised host could be disclosed.

III. Approach

There are three steps in our recommended approach to the problem:

- Detect if the network monitoring tool is running on any of your hosts that support a promiscuous network interface.
- Protect against this attack either by disabling the network interface for those systems that do not use this feature or by attempting to prevent unauthorized use of the feature on systems where this interface is necessary.
- Scope the extent of the attack and recover in the event that the network monitoring tool is discovered.

A. Detection

The network monitoring tool can be run under a variety of process names and log to a variety of filenames. Thus, the best method for detecting the tool is to look for

1. Trojan horse programs commonly used in conjunction with this attack,
2. any suspect processes running on the system,
3. the unauthorized use of /dev/nit,
4. unexpected ASCII files in the /dev directory, and
5. modifications to /etc/rc* files and /etc/shutdown

1) Trojan horse programs:

The intruders have been found to replace one or more of the following programs with a Trojan horse version in conjunction with this attack:

/usr/etc/in.telnetd
and /bin/login (Used to provide back-door access for the intruders to retrieve information)
/bin/ps (Used to disguise the network monitoring process)
netstat
ifconfig
su
ls
find
du

df
libc
sync
binaries referred in /etc/inetd.conf

Because the intruders install Trojan horse variations of standard UNIX commands, we recommend not using other commands such as the standard UNIX *sum(1)* or *cmp(1)* commands to locate the Trojan horse programs on the system until these programs can be restored from distribution media, run from read-only media (such as a mounted CD-ROM), or verified using cryptographic checksum information.

In addition to the possibility of having the checksum programs replaced by the intruders, the Trojan horse programs mentioned above may have been engineered to produce the same standard checksum and timestamp as the legitimate version. Because of this, the standard UNIX *sum(1)* command and the timestamps associated with the programs are not sufficient to determine whether the programs have been replaced.

We recommend that you use both the /usr/5bin/sum and /bin/sum commands to compare against the distribution media and assure that the programs have not been replaced. The use of *cmp(1)*, MD5, Tripwire (only if the baseline checksums were created on a distribution system), and other cryptographic checksum tools are also sufficient to detect these Trojan horse programs, provided these programs were not available for modification by the intruder. If the distribution is available on CD-ROM or other read-only device, it may be possible to compare against these volumes or run programs off these media.

2) Suspect processes:

Although the name of the network monitoring tool can vary from attack to attack, it is possible to detect a suspect process running as root using *ps(1)* or other process-listing commands. Until the *ps(1)* command has been verified against distribution media, it should not be relied upon--a Trojan horse version is being used by the intruders to hide the monitoring process. Some process names that have been observed are sendmail, es, and in.netd. The arguments to the process also provide an indication of where the log file is located. If the "-F" flag is set on the process, the filename following indicates the location of the log file used for the collection of authentication information for later retrieval by the intruders.

3) Unauthorized use of /dev/nit:

If the network monitoring tool is currently running on your system, it is possible to detect this by checking for unauthorized use of the /dev/nit interface. We have created a minimal tool, cpm, for this purpose.

We urge you to use the cpm tool on every machine at your site (where applicable). Some sites run this as a cron job at regular intervals, such as every 15 minutes, to report any result that indicates a possible compromise.

cpm (version 1.2) can be obtained from
ftp://ftp.cert.org/pub/tools/cpm/ ftp://ftp.uu.net/pub/security/cpm/.

Below are the MD5 checksums for the tarfiles and the contents of the cpm.1.2 directory, when created.

MD5 (cpm.1.2.tar) = 5f0489e868fbf213c026343cca7ec6ff
MD5 (cpm.1.2.tar.Z) = b76285923ad17d8dbfffd9dd0082ce5b
MD5 (cpm.1.2.tar.gz) = e689ca1c663e4c643887245f41f13a84
MD5 (cpm.1.2/MANIFEST) = ed6ec1ca374113c074547eb0580d9240
MD5 (cpm.1.2/README) = 34713d2be42b434a117165a5002f0a27
MD5 (cpm.1.2/cpm.1) = 84df06d9c6687314599754f3515c461b
MD5 (cpm.1.2/cpm.c) = 3da08fe657b96a75697a41e2700d456e
MD5 (cpm.1.2/cpm.txt) = 5860bfb9c383f519e494a38c682c22fb

This archive contains a readme file, also included as Appendix C of this advisory, containing instructions on installing and using this detection tool.

Note that some sites have reported intruders gaining root access then reinstalling a kernel with /dev/nit functionality.

4) Unexpected ASCII files in /dev

Look for unexpected ASCII files in the /dev directory. Some of the Trojan binaries listed above rely on configuration files, which are often found in /dev.

5) Modifications to /etc/rc* files and /etc/shutdown

Check for modifications to /etc/rc* files and /etc/shutdown. Some intruders have modified /etc/rc files to ensure that the sniffer restarts after a shutdown or reboot. Others have modified the shutdown sequence to remove all traces of compromise.

B. Prevention

There are two actions that are effective in preventing this attack. A long-term solution requires eliminating transmission of clear-text passwords on the network. For this specific attack, however, a short-term workaround exists. Both of these are described below.

1) Long-term prevention:

We recognize that the only effective long-term solution to prevent these attacks is by not transmitting reusable clear-text passwords on the network. We have collected some information on relevant technologies. This information is included as Appendix B in this advisory. Note: These solutions will not protect against transient or remote access transmission of clear-text passwords through the network.

Until everyone connected to your network is using the above technologies, your policy should allow only authorized users and programs access to promiscuous network interfaces. The tool described in Section III.A.3 above may be helpful in verifying this restricted access.

2) Short-term workaround:

Regardless of whether the network monitoring software is detected on your system, we recommend that ALL SITES take action to prevent unauthorized network monitoring on their systems. You can do this either by removing the interface, if it is not used on the system or by attempting to prevent the misuse of this interface.

For systems other than Sun and Solbourne, contact your vendor to find out if promiscuous mode network access is supported and, if so, what is the recommended method to disable or monitor this feature.

For SunOS 4.x and Solbourne systems, the promiscuous interface to the network can be eliminated by removing the /dev/nit capability from the kernel. The procedure for doing so is outlined below (see your system manuals for more details). Once the procedure is complete, you may remove the device file /dev/nit since it is no longer functional.

Procedure for removing /dev/nit from the kernel:

```
1.  Become root on the system.
2.  Apply "method 1" as outlined in the System and Network Administration manual, in
    the section, "Sun System Administration Procedures," Chapter 9, "Reconfiguring the
    System Kernel." Excerpts from the method are reproduced below:
3.           # cd /usr/kvm/sys/sun[3,3x,4,4c]/conf
4.           # cp CONFIG_FILE SYS_NAME
5.           [Note that at this step, you should replace the CONFIG_FILE
6.           with your system specific configuration file if one exists.]
7.           # chmod +w SYS_NAME
8.           # vi SYS_NAME
9.              #
10.             # The following are for streams NIT support.  NIT is used by
11.             # etherfind, traffic, rarpd, and ndbootd.  As a rule of thumb,
12.             # NIT is almost always needed on a server and almost never
13.             # needed on a diskless client.
14.             #
15.             pseudo-device   snit            # streams NIT
16.             pseudo-device   pf              # packet filter
17.             pseudo-device   nbuf            # NIT buffering module
18.          [Comment out the preceding three lines; save and exit the
19.          editor before proceeding.]
20.          # config SYS_NAME
21.          # cd ../SYS_NAME
22.          # make
23.          # mv /vmunix /vmunix.old
24.          # cp vmunix /vmunix
25.          # /etc/halt
26.          < b
```

[This step will reboot the system with the new kernel.]

[NOTE that even after the new kernel is installed, you need to take care to ensure that the previous vmunix.old , or other kernel, is not used to reboot the system.]

C. Scope and recovery

If you detect the network monitoring software at your site, we recommend following three steps to successfully determine the scope of the problem and to recover from this attack.

1. Restore the system that was subjected to the networkmonitoring software.

The systems on which the network monitoring and/or Trojan horse programs are found have been compromised at the root level; your system configuration may have been altered. See Appendix A of this advisory for help with recovery.

2. Consider changing router, server, and privileged account passwords due to the widespread nature of these attacks.

Since this threat involves monitoring remote connections, take care to change these passwords using some mechanism other than remote telnet, rlogin, or FTP access.

3. Urge users to change passwords on local and remote accounts.

Users who access accounts using telnet, rlogin, or FTP either to or from systems within the compromised domain should change their passwords after the intruder's network monitor has been disabled.

4. Notify remote sites connected from or through the local domain of the network compromise.

Encourage the remote sites to check their systems for unauthorized activity. Be aware that if your site routes network traffic between external domains, both of these domains may have been compromised by the network monitoring software.

Appendix A: RECOVERING FROM A UNIX ROOT COMPROMISE

A. Immediate recovery technique

1. Disconnect from the network or operate the system in single- user mode during the recovery. This will keep users and intruders from accessing the system.
2. Verify system binaries and configuration files against the vendor's media (do not rely on timestamp information to provide an indication of modification). Do not trust any verification tool such as *cmp(1)* located on the compromised system as it, too, may have been modified by the intruder. In addition, do not trust the results of the standard UNIX *sum(1)* program as we have seen intruders modify system files in such a way that the checksums remain the same. Replace any modified files from the vendor's media, not from backups.

   -- or --

   Reload your system from the vendor's media.

3. Search the system for new or modified setuid root files.

```
4. find / -user root -perm -4000 -print
```

   If you are using NFS or AFS file systems, use ncheck to search the local file systems.

```
ncheck -s /dev/sd0a
```

5. Change the password on all accounts.
6. Don't trust your backups for reloading any file used by root. You do not want to re-introduce files altered by an intruder.

More detailed advice can be found in ftp://ftp.cert.org/pub/tech_tips/root_compromise.

B. Improving the security of your system

1. CERT Security Technical Tips
   The CERT/CC staff has developed technical tips and checklists based on information gained from computer security incidents reported to us. These tips are available from

   ftp://ftp.cert.org/pub/tech_tips

2. Security Tools
   Use security tools such as COPS and Tripwire to check for security configuration weaknesses and for modifications made by intruders. We suggest storing these security tools, their configuration files, and databases offline or encrypted. TCP daemon wrapper programs provide additional logging and access control. These tools are available

   ftp://ftp.cert.org/pub/tools

3. CERT Advisories
   Review past CERT advisories (both vendor-specific and generic) and install all appropriate patches or workarounds as described in the advisories. CERT advisories and other security-related information are available from

   http://www.cert.org/

   ftp://ftp.cert.org/pub/

To join the CERT Advisory mailing list, send a request to:
cert-advisory-request@cert.org

Please include contact information, including a telephone number.

Appendix B: ONE-TIME PASSWORDS

Given today's networked environments, CERT recommends that sites concerned about the security and integrity of their systems and networks consider moving away from standard, reusable passwords. CERT has seen many incidents involving Trojan network programs (e.g., telnet and rlogin) and network packet sniffing programs. These programs capture clear-text hostname, account name, password triplets. Intruders can use the captured information for subsequent access to those hosts and accounts. This is possible because 1) the password is used over and over (hence the term "reusable"), and 2) the password passes across the network in clear text.

Several authentication techniques have been developed that address this problem. Among these techniques are challenge-response
technologies that provide passwords that are only used once (commonly called one-time passwords). This document provides a list of sources for products that provide this capability. The decision to use a product is the responsibility of each organization, and each organization should perform its own evaluation and selection.

I. Publicly Available Packages

S/KEY(TM)

The S/KEY package is publicly available (no fee) via anonymous FTP from:

```
thumper.bellcore.com            /pub/nmh directory
```

There are three subdirectories:

```
                skey            UNIX code and documents on S/KEY.
                                Includes the change needed to login,
                                and stand-alone commands (such as "key"),
                                that computes the one-time password for
                                the user, given the secret password and
                                the S/KEY command.
                dos             DOS or DOS/WINDOWS S/KEY programs.  Includes
                                DOS version of "key" and "termkey" which is
                                a TSR program.
                mac             One-time password calculation utility for
                                the Mac.
```

II Commercial Products:

Secure Net Key (SNK)   (Do-it-yourself project)

Digital Pathways, Inc.
201 Ravendale Dr.
Mountainview, Ca. 94043-5216
USA
Phone: 415-964-0707
Fax: (415) 961-7487

Products:
handheld authentication calculators (SNK004) serial line auth interruptors (guardian)

Note: Secure Net Key (SNK) is des-based, and therefore restricted from US export.

```
Secure ID    (complete turnkey systems)
```

Security Dynamics
One Alewife Center
Cambridge, MA 02140-2312

USA
Phone: 617-547-7820
Fax: (617) 354-8836

Products:
SecurID changing number authentication card
ACE server software

SecureID is time-synchronized using a 'proprietary' number generation algorithm

WatchWord and WatchWord II

Racal-Guardata
480 Spring Park Place
Herndon, VA 22070
703-471-0892
1-800-521-6261 ext 217

Products:
Watchword authentication calculator
Encrypting modems

Alpha-numeric keypad, digital signature capability

SafeWord

Enigma Logic, Inc.
2151 Salvio #301
Concord, CA 94520
510-827-5707
Fax: (510)827-2593

Products:
DES Silver card authentication calculator
SafeWord Multisync card authentication calculator

Available for UNIX, VMS, MVS, MS-DOS, Tandum, Stratus, as well as other OS versions. Supports one-time passwords and super smartcards from several vendors.

Appendix C: cpm 1.0 README FILE

cpm - check for network interfaces in promiscuous mode.

Thursday Feb 3 1994
CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890

This program is free software; you can distribute it and/or modify it as long as you retain the Carnegie Mellon copyright statement.

It can be obtained via anonymous FTP from ftp.cert.org:pub/tools/cpm.tar.Z.

This program is distributed WITHOUT ANY WARRANTY; without the IMPLIED WARRANTY of merchantability or fitness for a particular purpose.

This package contains:

README
MANIFEST
cpm.1
cpm.c

To create cpm under SunOS, type:

```
% cc -Bstatic -o cpm cpm.c
```

On machines that support dynamic loading, such as Sun's, CERT recommends that programs be statically linked so that this feature is disabled.

CERT recommends that after you install cpm in your favorite directory, you take measures to ensure the integrity of the program by noting the size and checksums of the source code and resulting binary.

The following is an example of the output of cpm and its exit status.

Running cpm on a machine where both the le0 and le2 interfaces are in promiscuous mode, under *csh(1)*:

```
% cpm
le0
le2
% echo $status
2
%
```

Running cpm on a machine where no interfaces are in promiscuous mode, under *csh(1)*:

```
% cpm
% echo $status
0
%
```

The CERT Coordination Center thanks the members of the FIRST community as well as the many technical experts around the Internet who participated in creating this advisory. Special thanks to Eugene Spafford of Purdue University for his contributions.

UPDATES

- We have seen sniffers for other platforms, i.e., Solaris.
- Sites have reported intruders using sniffers to capture authentication to routers. Using that data, they compromise the routers and modify the configuration file.

Revision History

Sept. 19, 1997 Updated Copyright statement

Apr. 03, 1997 Appendix B - corrected "Public Domain" to read "Publicly Available"

Oct. 09, 1996 Sentence 1 - Clarified the time of the increase in the reports.

Appendix A - Added the URL for our tech tip on root compromises.

Aug. 30, 1996 Information previously in the README was inserted into the advisory. Updated URLs.

July 31, 1996 Appendix B - referred to new tech tips, which replace the single security checklist

Mar. 20, 1996 Sec.III.A.3 - additional information concerning cpm (v. 1.2)

Sept. 21, 1995 Sec. III.A.3 - suggestions regarding cpm

Feb. 02, 1995 Sec. III - additional information on Trojan binaries (III.A), use of the /dev directory (III.A.3), and two more activities (III.A.4 & III.A.5)

Feb. 02, 1995 Updates section - additional information about sniffer activity

2 CA-1994-02: Revised Patch for SunOS /usr/etc/rpc.mountd Vulnerability

Original issue date: February 14, 1994
Last revised: September 19, 1997
Attached copyright statement

A complete revision history is at the end of this file.

THIS IS A REVISED CERT ADVISORY
IT CONTAINS NEW VULNERABILITY AND PATCH INFORMATION
SUPERSEDES CERT ADVISORY CA-91.09 and CA-92.12

The CERT Coordination Center has received information concerning a vulnerability in /usr/etc/rpc.mountd in Sun Microsystems, Inc. SunOS 4.1.1, 4.1.2, 4.1.3, and 4.1.3c. SunOS 4.1.3.u.1, Solaris 2.x, and Solbourne's 4.1B and 4.1C are not vulnerable.

Sun has produced a patch for this vulnerability for sun3 and sun4 architectures. It is available through your local Sun Answer Center as well as through anonymous FTP from the ftp.uu.net system in the /systems/sun/sun-dist directory or from the ftp.eu.net system in the /sun/fixes directory.

This vulnerability is currently being exploited. Please review CERT Advisory CA-94.01 Ongoing Network Monitoring Attacks.

I. Description

If an access list of hosts within /etc/exports is a string over 256 characters or if the cached list of netgroups exceeds the cache capacity then the file system can be mounted by anyone.

II. Impact

Unauthorized remote hosts will be able to mount the file system. This will allow unauthorized users read and write access to files on mounted file systems.

III. Solution

Obtain and install the appropriate patch following the instructions included with the patch.

Patches are available from

ftp://ftp.uu.net/systems/sun/sun-dist/patches/

ftp://ftp.eu.net/sun/fixes/

There is a README file and directory layout to help identify which binaries are appropriate for which architectures.

```
Patch-ID   Filename         BSD          MD5
                            Checksum     Checksum
100296-04  100296-04.tar.Z  15271    40
4e1354ecb7fb9c7e962d7020f31f07bf
```

Revision History

```
Sept. 19,1997  Attached copyright statement
Aug. 30, 1996  Information previously in the README was inserted
               into the advisory. Updated URL format.
June 09, 1995  Solution - recommended source to use for patches
               if the checksums didn't match
Apr. 20, 1994  Solution - noted that Sun ensured that the same
               versions of patches were available at all
               locations and provided files to help determine
               which architectures require the patch.
```

3 CA-1994-03: IBM AIX Performance Tools Vulnerabilities

Original issue date: February 24, 1994
Last revised: September 19, 1997
Updated copyright statement

A complete revision history is at the end of this file.

The CERT Coordination Center has received information concerning vulnerabilities in the "bosext1.extcmds.obj" Licensed Program Product (performance tools). These problems exist on IBM AIX 3.2.4 systems that have Program Temporary Fixes (PTFs) U420020 or U422510 installed and on all AIX 3.2.5 systems.

CERT recommends that affected sites apply the workaround provided in section III below.

I. Description

Vulnerabilities exist in the bosext1.extcmds.obj performance tools in AIX 3.2.5 and in those AIX 3.2.4 systems with Program Temporary Fixes (PTFs) U420020 or U422510 installed. These problems do not exist in earlier versions of AIX.

II. Impact

Local users can gain unauthorized root access to the system.

III. Workaround

A. The recommended workaround is to change the permissions of all the programs in the /usr/lpp/bosperf directory structure

so that the setuid bit is removed and the programs can be executed only by 'root'. This can be accomplished as follows:

```
% su root

# chmod -R u-s,og= /usr/lpp/bosperf/*
```

The programs affected by this workaround include: filemon, fileplace, genkex, genkld, genld, lvedit, netpmon, rmap, rmss, stripnm, svmon, tprof

As a result of this workaround, these programs will no longer be executable by users other than 'root'.

B. Patches for these problems can be ordered as Authorized Program Analysis Report (APAR) IX42332.

To order an APAR from IBM call 1-800-237-5511 and ask for shipment as soon as it is available. APARs may be obtained outside the U.S. by contacting your local IBM representative.

Any further information that we receive on APAR IX42332 will be available by anonymous FTP in the file pub/cert_advisories/CA-94.03.README on ftp.cert.org.

The CERT Coordination Center wishes to thank Jill K. Bowyer of USAF/DISA for reporting this problem and IBM for their prompt response to this problem.

Revision History

```
September 19,1997  Updated Copyright Statement
```

4 CA-1994-04: SunOS rdist Vulnerability

Original issue date: March 17, 1994

**** Superseded by CA-1996-14. ****

5 CA-1994-05: MD5 Checksums

Original issue date: March 18, 1994
Last revised: April 28, 1998
Updated information on obtaining RFCs.

A complete revision history is at the end of this file. This advisory gives the MD5 checksums for a number of SunOS files, along with a tool for checking them. The checksums can be used to assure the integrity of those files.

The CERT Coordination Center is distributing these checksums because of an increasing number of incidents in which intruders who gain root access are modifying system files to install Trojan horses.

Moreover, intruders are modifying files so that they have the same checksum as the original file. This is possible because the standard "sum" program that comes with most UNIX systems was designed to detect accidental modifications to files and is not strong enough to prevent deliberate attempts to yield a specific checksum. The MD5 algorithm by RSA Data Security, Inc. is specifically designed to provide checksums that cannot be deliberately spoofed. We strongly recommend that sites install the MD5 software and use it to validate system software. More information on obtaining MD5 is given below.

The list of checksums in Appendix B of this advisory is provided for your convenience. In addition, we are providing a program that can assist you in checking your MD5 output against the values in the database. This checksum list is not complete. We have begun with a number of the more common locations for Trojan horses that we have seen in connection with the continuing "sniffer" attacks reported in CA-94.01 "Ongoing Network Monitoring Attacks." We intend to work with all vendors to expand this list and make more MD5 checksums widely available for anonymous FTP.

Note: After we publish checksums in advisories, files are sometimes updated at individual locations because of system upgrades or patch installation. For current MD5 checksum values, we recommend that you check with your vendor.

We encourage sites to consider installing a more complete package for monitoring system integrity, such as Tripwire from the COAST project (ftp://ftp.cs.purdue.edu/) or the TIGER system from TAMU (ftp://net.tamu.edu/pub/security/TAMU/).

I. Description

Intruders are installing Trojan horses by modifying system files often in such a way that a standard checksum on the file generates the same checksum as the unaltered version.

II. Impact

The Trojan horses give the intruder continued access to a system and/or hide the intruder's activities.

III. Solution

1. Obtain and install MD5.

The MD5 algorithm is in the public domain, and there are several programs available that implement it. The algorithm is documented in RFC 1321, which is available from many archives including ftp://ftp.isi.edu/in-notes/rfc1321.txt.

RFC 1321 itself includes source code for implementing the algorithm. For convenience, that source has been extracted and made available for anonymous FTP on ftp.cert.org: ftp://ftp.cert.org/pub/tools/md5/.

2. Run the "md5check" program listed in Appendix A of this advisory.

This program will check a number of system files and note for each one whether the checksum did or did not match the checksum of a legitimate version.

If the checksum does match, you can be confident that particular file has not been modified by an intruder. Note this does not mean the file is the most recent version for your system - only that it was in fact distributed by Sun.

If the checksum DOES NOT match, consider these possible reasons:

1. The file may be legitimate but not included in this database. (Remember, the database is not complete.) To check this possibility, compare the file against the original distribution media. You may want to add the correct checksum to your copy of the database.
2. You may have made local modifications to the file at your site. To check this possibility, compare the file to a known good version. You may want to add the correct checksum to your copy of the database.
3. The file may be a Trojan horse installed by an intruder. We encourage you to replace this file with a known good version, and check for additional signs of compromise.

Appendix A: "md5check"

The following program is a "nawk" script that can be run against the list of checksums "md5_sun.v1" in Appendix B:

```
% nawk -f md5check md5_sun.v1
```

This program along with a man page and the database below, are available by anonymous FTP from info.cert.org in the "pub/tools/md5check" directory.

```
         Filename          MD5 Checksum

         --------          -----------------------------
         md5check          99108ab5a6007164a910626bbcc5888f
         md5_sun.v1        780a0f1f3717819c59135716e5f6a1ce
------- Cut Here -------
# "md5check" version 1 (3/17/94)
BEGIN { FS = "[ \t]*:[ \t]*"; }
# Print notices from the configuration file
/^##/ { print substr ($0, 3); next; }
# Only handle MD5 checksums currently
/^md5/ {
        source = sprintf("%-7s %-8s %-6s %s", $2, $3, $5, $4);
        file = $6;
        sum = hex_lower($7);
        if (md5[file] == "") {
                print "Checking", file;
                testcmd = "test -r " file;
                if ( system(testcmd) != 0 ) {
                        print " Could not open", file;
                        md5[file] = "x";
                        next;
                } else {
                        md5cmd = "md5 " file
                        md5cmd | getline md5[file];
                        close (md5cmd);
                        # Strip off any leading text and set to low-
ercase
                        sub(".*[ \t]", "", md5[file]);
                        md5[file] = hex_lower(md5[file]);
                }
        }
        if (md5[file] == "x" || file in matched) {
                # Could not open or already matched
                next;
        }
        if (md5[file] == sum) {
                # We have a match - remember which one
                matched[file] = source;
                num_match++;
                if (file in not_matched) {
                        num_no_match--;
                        delete not_matched[file];
                }
        } else {
                if (! (file in not_matched)) {
                        num_no_match++;
                        not_matched[file] = 1;
                }
        }
}
END {
        printf "\n%d files DID NOT MATCH a known checksum\n",
num_no_match;
        printf "%d files did match a known checksum\n", num_match;
        print "\nThe following files DID NOT MATCH a known checksum";
        for (filename in not_matched) {
                printf "\t%s\n", filename;
        }
        print "\nThe following files did match a known checksum";
        for (filename in matched) {
                printf "\t%s\n\t\t%s\n", filename, matched[filename];
        }
}
function hex_lower(s) {
     gsub("A","a",s); gsub("B","b",s); gsub("C","c",s);
     gsub("D","d",s); gsub("E","e",s); gsub("F","f",s);
     return s
}
------- Cut Here -------
```

Appendix B: Checksums from Vendors

Note: After we publish checksums in advisories, files are sometimes updated at individual locations because of system upgrades or patch installation. For current MD5 checksum values, we recommend that you check with your vendor.

Hewlett-Packard Company

To obtain a copy of the HP SupportLine mail service user's guide, send the following (in the TEXT PORTION OF THE MESSAGE to) to the HP SupportLine mail service.

To: support@support.mayfield.hp.com
Message Text:
send guide.txt

To obtain a patch identified within this Security Bulletin, send the following (in the TEXT PORTION OF THE MESSAGE) to the HP SupportLine mail service.

To: support@support.mayfield.hp.com
Message Text:
send xxxxxxxxxxxx
(where xxxxxxxxxxxx represents the specified patch name).

If you have concerns about security issues, please forward them to: security-alert@hp.com.

The security-alert node is monitored during working hours Pacific Daylight Time by multiple HP Security Response Team personnel. We reply to your message only if necessary to obtain additional information.

Solbourne (Grumman Systems Support)

A list of MD5 checksums for Solbourne (Grumman Systems Support) executables under 4.1C is available via anonymous ftp from ftp.nts.gssc.com in directory /pub/docs/, files usr.etc.md5 and bin.md5. These include the files referred to in the advisory.

The MD5 checksums for these executables are included below:

MD5 (bin.md5) = cf3b3d8447ae19fa7e1741939fe82ea9
MD5 (bin.md5.41b) = 7e0c1ae26eda72f1791e235ab244ae44
MD5 (usr.etc.md5) = 1727d1705cc7750b7848df60a4b5788e
MD5 (usr.etc.md5.41b) = 7e02c01cc47ec469c3210a8fabb012ff

Sun Microsystems, Inc.

```
## Checksum Table for Selected SunOS Binary Files (v1: 3/17/94)
##
## PLEASE NOTE:  The entries included in this table do not represent 
complete
##               coverage of all released versions of these files.
##               In particular, checksum data for outdated patch re-
leases is
##               limited.
##
##               Failure to match a checksum for a given file does 
not
##               necessarily indicate the presence of a Trojan bi-
nary.
##               Failure indicates that the file's checksum did not 
match any
##               contained in this table.  The file's authenticity 
should be
##               verified against distribution media or local modi-
fications.
##
##               Success at matching a file's checksum indicates 
that the
##               corresponding file is free from tampering.
##
# (MD5 is the RSA Data Security, Inc. Message Digest Algorithm)
#
# format of data
#
# XSUMTYPE:OSNAME:OSVERSION:SOURCE:ARCH:FILE:XSUM
#/bin/login
md5:SunOS:4.1:100201-
06:sun3:/bin/login:00d95a04ecce2193b9c6e16516d37855
md5:SunOS:4.1:100201-
06:sun4:/bin/login:e746fed42be0433a53cce082acfee23c
md5:SunOS:4.1:100630-
01:sun3:/bin/login:11d5ed4445face25642100ec0ab1ed3c
md5:SunOS:4.1:100630-
01:sun4:/bin/login:b6d013403c54949c0e476afd966ef261
md5:SunOS:4.1.1:Original 
Dist:sun3:/bin/login:073d378264f25245c154be8a12f208e9
md5:SunOS:4.1.1:Original 
Dist:sun4:/bin/login:92611eb1ef1f221c1e9c76db8da44a99
```

```
md5:SunOS:4.1.1:100201-
06:sun3:/bin/login:00d95a04ecce2193b9c6e16516d37855
md5:SunOS:4.1.1:100201-
06:sun4:/bin/login:e746fed42be0433a53cce082acfee23c
md5:SunOS:4.1.1:100630-
01:sun3:/bin/login:11d5ed4445face25642100ec0ab1ed3c
md5:SunOS:4.1.1:100630-
01:sun4:/bin/login:b6d013403c54949c0e476afd966ef261
md5:SunOS:4.1.1:100632-
06:sun4:/bin/login:12c4b39cb94b8dcdad0a10e1c59345c6
md5:SunOS:4.1.1:100633-
01:sun4:/bin/login:9634cda7a353d0043a22ad2b0eebaab2
md5:SunOS:4.1.2:Original
Dist:sun4:/bin/login:637503c0e2b46791820609d87629db91
md5:SunOS:4.1.2:100630-
01:sun4:/bin/login:b6d013403c54949c0e476afd966ef261
md5:SunOS:4.1.2:100631-
01:sun3:/bin/login:65d1e270fbb13984f5e0036b9e4a1011
md5:SunOS:4.1.2:100631-
01:sun4:/bin/login:976a0431dbd23ec1535c1679e215095b
md5:SunOS:4.1.2:100632-
06:sun4:/bin/login:12c4b39cb94b8dcdad0a10e1c59345c6
md5:SunOS:4.1.2:100633-
01:sun4:/bin/login:9634cda7a353d0043a22ad2b0eebaab2
md5:SunOS:4.1.3:100630-
02:sun3:/bin/login:11d5ed4445face25642100ec0ab1ed3c
md5:SunOS:4.1.3:100630-
02:sun4:/bin/login:b6d013403c54949c0e476afd966ef261
md5:SunOS:4.1.3:100632-
06:sun4:/bin/login:12c4b39cb94b8dcdad0a10e1c59345c6
md5:SunOS:4.1.3:Original
Dist:sun4:/bin/login:e88e84d228d05e8f54a0d57d62d0710d
md5:SunOS:4.1.3c:Original
Dist:sun4:/bin/login:e88e84d228d05e8f54a0d57d62d0710d
md5:SunOS:4.1.3_u1:Original
Dist:sun4:/bin/login:4e437a85e05f886ff5082ac58108d882
#/usr/kvm/ps
md5:SunOS:4.1.1:Original
Dist:sun3x:/usr/kvm/ps:ac96820499c2da78d65700e230f66df2
md5:SunOS:4.1.1:Original
Dist:sun3:/usr/kvm/ps:b4633eed82815a233d2ca8d8df8d655e
md5:SunOS:4.1.1:Original
Dist:sun4:/usr/kvm/ps:390ef406ba27b1d591ba6f281986369b
md5:SunOS:4.1.1:Original
Dist:sun4c:/usr/kvm/ps:cb58a8259ff580389b115b7861793b48
md5:SunOS:4.1.2:Original
Dist:sun4:/usr/kvm/ps:efca4ca10a088e557c6c69695dadcfa6
md5:SunOS:4.1.2:Original
Dist:sun4c:/usr/kvm/ps:9d489c87d709a540aced718a04e38e11
md5:SunOS:4.1.2:Original
Dist:sun4m:/usr/kvm/ps:e9e364f3936a5b16d7e2fb812d11e475
md5:SunOS:4.1.2:100981-
02:sun4:/usr/kvm/ps:86b8b5eb7212c94c9c570cd20c9af2ae
md5:SunOS:4.1.2:100981-
02:sun4c:/usr/kvm/ps:4871287498c0ab7b17d97848ebe34d15
```

```
md5:SunOS:4.1.2:100981-
02:sun4m:/usr/kvm/ps:97cc063bafa6aaf032cb1b67b444c5a8
md5:SunOS:4.1.3:Original
Dist:sun4:/usr/kvm/ps:226ab466429f5d4de4f6a108bae1c518
md5:SunOS:4.1.3:Original
Dist:sun4c:/usr/kvm/ps:83b369e5d8c34db4d5d6725140d0b216
md5:SunOS:4.1.3:100981-
02:sun4:/usr/kvm/ps:a4809a70e66b415bae8a165dc4ffb185
md5:SunOS:4.1.3:100981-
02:sun4c:/usr/kvm/ps:cf10e206de67755e801e4c9d96c239a9
md5:SunOS:4.1.3:100981-
02:sun4m:/usr/kvm/ps:d6237550748855bee17ce96465cd1331
md5:SunOS:4.1.3_u1:Original
Dist:sun4m:/usr/kvm/ps:92c3b1495ab80446ddb6979c890cee58
md5:SunOS:4.1.3_u1:Original
Dist:sun4:/usr/kvm/ps:b14b75017dfe75ea1b89d147c6b49cb7
md5:SunOS:4.1.3_u1:Original
Dist:sun4c:/usr/kvm/ps:e24eab973f1b1cfd6bf5b54310a2207f
md5:SunOS:4.1.3_u1:101442-
01:sun4:/usr/kvm/ps:174731efb18020dacde9f205ad04a4bf
#/usr/etc/in.telnetd
md5:SunOS:4.0.3:100125-
05:sun3:/usr/etc/in.telnetd:dce91901f9fd15f7f6f6c94fb7824428
md5:SunOS:4.0.3:100125-
05:sun4:/usr/etc/in.telnetd:2e67031ad7984c22cfacc8a0b4c3d6ee
md5:SunOS:4.0.3c:100125-
05:sun4c:/usr/etc/in.telnetd:943574a9befb9fac3fce2fc111f68d51
md5:SunOS:4.1:100125-
05:sun3:/usr/etc/in.telnetd:2544753907d24a699c9cdfddcab0d2e3
md5:SunOS:4.1:100125-
05:sun3x:/usr/etc/in.telnetd:3af506b9b02b6a299f5e081c3abfce1f
md5:SunOS:4.1:100125-
05:sun4:/usr/etc/in.telnetd:5448303462518cca8390a84b5f312abe
md5:SunOS:4.1.1:Original
Dist:sun3:/usr/etc/in.telnetd:333ffc49f21e675f3099772661549b7d
md5:SunOS:4.1.1:Original
Dist:sun4:/usr/etc/in.telnetd:7706ba7270a28f3470ccbe965f8fc7a1
md5:SunOS:4.1.1:100125-05:sun3:/usr/etc/in.telnetd:c4dca8a653f60fe-
aed63a25786aee2ed
md5:SunOS:4.1.1:100125-
05:sun3x:/usr/etc/in.telnetd:6c409bd315711aae29b8285ffc4bb90c
md5:SunOS:4.1.1:100125-
05:sun4:/usr/etc/in.telnetd:29f24e09ffebc36fb14f9fee4bf2d6fc
md5:SunOS:4.1.1:Original
Dist:sun3x:/usr/etc/in.telnetd:503be2c540d03281fdada476d5b0b247
md5:SunOS:4.1.1:Original
Dist:sun3:/usr/etc/in.telnetd:333ffc49f21e675f3099772661549b7d
md5:SunOS:4.1.1:Original
Dist:sun4c:/usr/etc/in.telnetd:503be2c540d03281fdada476d5b0b247
md5:SunOS:4.1.2:Original
Dist:sun4:/usr/etc/in.telnetd:913095f91bbf06e98635f964951e0e2d
md5:SunOS:4.1.2:Original
Dist:sun4c:/usr/etc/in.telnetd:503be2c540d03281fdada476d5b0b247
md5:SunOS:4.1.2:Original
Dist:sun4m:/usr/etc/in.telnetd:503be2c540d03281fdada476d5b0b247
```

```
md5:SunOS:4.1.3:Original
Dist:sun4:/usr/etc/in.telnetd:b94ac90e4fe63f1c7a0199a27a7c4d80
md5:SunOS:4.1.3:Original
Dist:sun4c:/usr/etc/in.telnetd:503be2c540d03281fdada476d5b0b247
md5:SunOS:4.1.3c:Original
Dist:sun4:/usr/etc/in.telnetd:b94ac90e4fe63f1c7a0199a27a7c4d80
md5:SunOS:4.1.3c:Original
Dist:sun4m:/usr/etc/in.telnetd:503be2c540d03281fdada476d5b0b247
md5:SunOS:4.1.3_u1:Original
Dist:sun4:/usr/etc/in.telnetd:831c59628b1197c612f19289a786eaeb
#/usr/etc/ifconfig
md5:SunOS:4.1.1:Original Dist:sun3x:/usr/etc/ifcon-
fig:c9fe06259a49a58edfc6f1fe68665990
md5:SunOS:4.1.1:Original Dist:sun3:/usr/etc/ifcon-
fig:0da82be29c7173759316f51417fb420a
md5:SunOS:4.1.1:Original Dist:sun4:/usr/etc/ifcon-
fig:c9fe06259a49a58edfc6f1fe68665990
md5:SunOS:4.1.2:Original Dist:sun4:/usr/etc/ifcon-
fig:47d6e495207cc2b7037bd94a12cf565b
md5:SunOS:4.1.2:Original Dist:sun4c:/usr/etc/ifcon-
fig:c9fe06259a49a58edfc6f1fe68665990
md5:SunOS:4.1.2:Original Dist:sun4m:/usr/etc/ifcon-
fig:c9fe06259a49a58edfc6f1fe68665990
md5:SunOS:4.1.3:Original Dist:sun4:/usr/etc/ifcon-
fig:de44e217c94fa4f4c6fdfbcae419cb8b
md5:SunOS:4.1.3:Original Dist:sun4c:/usr/etc/ifcon-
fig:c9fe06259a49a58edfc6f1fe68665990
md5:SunOS:4.1.3c:Original Dist:sun4:/usr/etc/ifcon-
fig:de44e217c94fa4f4c6fdfbcae419cb8b
md5:SunOS:4.1.3c:Original Dist:sun4m:/usr/etc/ifcon-
fig:c9fe06259a49a58edfc6f1fe68665990
md5:SunOS:4.1.3_u1:Original Dist:sun4:/usr/etc/ifcon-
fig:22d9340368aec82ebdd63518613bc6ab
#/usr/lib/libc.a
md5:SunOS:4.1.1:100267-
09:sun3:/usr/5lib/libc.a:af8a721ca332754cdff2a1f1b74b8e8f
md5:SunOS:4.1.1:100267-
09:sun3:/usr/5lib/libc_p.a:1b930986afb11494b4e1e0fd4f9540b0
md5:SunOS:4.1.1:100267-
09:sun3:/usr/lib/libc.a:6b0ff2e11f3042d453ee502787ac29d7
md5:SunOS:4.1.1:100267-
09:sun3:/usr/lib/libc_p.a:ad9bd3c42db06fb0c45674eaafc5c4f8
md5:SunOS:4.1.1:100267-
09:sun4:/usr/5lib/libc.a:8c396b0695abb59fea66bc6615d9f101
md5:SunOS:4.1.1:100267-
09:sun4:/usr/5lib/libc_p.a:d98a993e3f6c308f3679690dd4f5e8d7
md5:SunOS:4.1.1:100267-
09:sun4:/usr/lib/libc.a:da7c2504a1cb5073d7e9bb7de580db32
md5:SunOS:4.1.1:100267-
09:sun4:/usr/lib/libc_p.a:9879d72df71d9956f62f058ddf70d0f8
md5:SunOS:4.1.3_u1:Original
Dist:sun4:/usr/5lib/libc.a:4daced1b11335f613bf7a5792bfeff77
md5:SunOS:4.1.3_u1:Original
Dist:sun4:/usr/5lib/libc_p.a:bd2037193776678e48324f523064b95b
```

```
md5:SunOS:4.1.3_u1:Original
Dist:sun4:/usr/lib/libc.a:ae4bcb481e7267c1def082ed6acf4bd9
md5:SunOS:4.1.3_u1:Original
Dist:sun4:/usr/lib/libc_p.a:696c03eb30c696b712f38907d3c2ee45
md5:SunOS:4.1.1:Original
Dist:sun4:/usr/5lib/libc.a:68686e4ed99b5dcf98ac4e3350ff6645
md5:SunOS:4.1.1:Original
Dist:sun4:/usr/lib/libc.a:cbba2b6e294f0087a0b9116290946d46
md5:SunOS:4.1.1:Original
Dist:sun3:/usr/5lib/libc.a:89b9040707c28810554dfaca6993e7d0
md5:SunOS:4.1.1:Original
Dist:sun3:/usr/lib/libc.a:15d385b850be70a30077e66b67dc5f09
md5:SunOS:4.1.2:Original
Dist:sun4:/usr/5lib/libc.a:e7ab3d2658611114833f25a4279db158
md5:SunOS:4.1.2:Original
Dist:sun4:/usr/lib/libc.a:f95fabcdbaaf34ac3da6174e635724e3
md5:SunOS:4.1.3:Original
Dist:sun4:/usr/5lib/libc.a:c6669804e4def2e1e49ad5628c52ee75
md5:SunOS:4.1.3:Original
Dist:sun4:/usr/lib/libc.a:ab06bfd723df7802d25291576736ce23
md5:SunOS:4.1.3c:Original
Dist:sun4:/usr/5lib/libc.a:5ef2ccf958dc6734c3e412127884c559
md5:SunOS:4.1.3c:Original
Dist:sun4:/usr/lib/libc.a:6f5d5c343b262c03a3f976d2830f4d06
md5:SunOS:4.1.1:Original
Dist:sun4:/usr/5lib/libc_p.a:21766ed7fdb431bb0435e48ea0764d42
md5:SunOS:4.1.1:Original
Dist:sun4:/usr/lib/libc_p.a:709d9a093b637e64234a03f1c48583e7
md5:SunOS:4.1.1:Original Dist:sun3:/usr/5lib/libc_p.a:3e3fcdfeb1636c708f1a2fec14c13b9f
md5:SunOS:4.1.1:Original
Dist:sun3:/usr/lib/libc_p.a:18f6043209f019ec58e50ab4f4771d40
md5:SunOS:4.1.2:Original
Dist:sun4:/usr/5lib/libc_p.a:c0b13f61038a198e6be3c09e137dee0e
md5:SunOS:4.1.2:Original
Dist:sun4:/usr/lib/libc_p.a:a40b2af6cde4734289f06d8325c8cf2e
md5:SunOS:4.1.3:Original
Dist:sun4:/usr/5lib/libc_p.a:bb06ddd972dd5549a3d6cc38a9537893
md5:SunOS:4.1.3:Original
Dist:sun4:/usr/lib/libc_p.a:72c8bee2000b2562225077784ea61bac
md5:SunOS:4.1.3c:Original
Dist:sun4:/usr/5lib/libc_p.a:8ccee0cc285a298c713b8bace38da815
md5:SunOS:4.1.3c:Original
Dist:sun4:/usr/lib/libc_p.a:157a7dc7a8fc77f1a5a06a85d3bab16c
#/usr/kvm/pstat
md5:SunOS:4.1.1:Original
Dist:sun3x:/usr/kvm/pstat:a131828d02092ab56e98ac8d63b1125d
md5:SunOS:4.1.1:Original
Dist:sun4:/usr/kvm/pstat:6de82bb539b54c2bd0be79dfc7712507
md5:SunOS:4.1.1:Original
Dist:sun4c:/usr/kvm/pstat:5e6058397f8e86df7456e36ad54f9b1e
md5:SunOS:4.1.2:Original
Dist:sun4c:/usr/kvm/pstat:a1cfc4f23be423aede09e23bcbf6268a
md5:SunOS:4.1.2:Original
Dist:sun4m:/usr/kvm/pstat:c2abc2313450cfd72ccd93448fef967b
```

```
md5:SunOS:4.1.3:Original
Dist:sun4:/usr/kvm/pstat:0076043c06cd24ae927128f02da9b935
md5:SunOS:4.1.3:Original
Dist:sun4c:/usr/kvm/pstat:225d4542b70f15af39c96a4d3b48a631
md5:SunOS:4.1.3c:Original
Dist:sun4m:/usr/kvm/pstat:e3a519a93a8b6a02fd6c64a6b3db476d
md5:SunOS:4.1.3_u1:Original
Dist:sun4:/usr/kvm/pstat:2a1cbf06988208179adf132349c3a403
md5:SunOS:4.1.3_u1:Original Dist:sun4m:/usr/kvm/pstat:2f3af3afbfa5942575bbcb02b13ebac1
md5:SunOS:4.1.3_u1:Original
Dist:sun4c:/usr/kvm/pstat:d15776947e0d60fc7d5ae755f65e779b
#/usr/etc/in.ftpd
md5:SunOS:4.1.1:Original
Dist:sun3x:/usr/etc/in.ftpd:c95b40609c510cfcc65504972d1f3ae1
md5:SunOS:4.1.1:Original
Dist:sun3:/usr/etc/in.ftpd:7ff869b0d0eeec61b08a81a085759681
md5:SunOS:4.1.1:Original
Dist:sun4:/usr/etc/in.ftpd:7a17e92251d08c56d001a1f5654fcb35
md5:SunOS:4.1.1:Original
Dist:sun4c:/usr/etc/in.ftpd:c95b40609c510cfcc65504972d1f3ae1
md5:SunOS:4.1.2:Original
Dist:sun4:/usr/etc/in.ftpd:8b1bfb5ba15d2898fffa373b1005e7ff
md5:SunOS:4.1.2:Original
Dist:sun4c:/usr/etc/in.ftpd:c95b40609c510cfcc65504972d1f3ae1
md5:SunOS:4.1.2:Original
Dist:sun4m:/usr/etc/in.ftpd:c95b40609c510cfcc65504972d1f3ae1
md5:SunOS:4.1.3:Original
Dist:sun4:/usr/etc/in.ftpd:79a29ae3f1deb02efb743d9cd39f6f2f
md5:SunOS:4.1.3:Original
Dist:sun4c:/usr/etc/in.ftpd:c95b40609c510cfcc65504972d1f3ae1
md5:SunOS:4.1.3c:Original
Dist:sun4:/usr/etc/in.ftpd:79a29ae3f1deb02efb743d9cd39f6f2f
md5:SunOS:4.1.3c:Original
Dist:sun4m:/usr/etc/in.ftpd:c95b40609c510cfcc65504972d1f3ae1
md5:SunOS:4.1.3_u1:Original
Dist:sun4:/usr/etc/in.ftpd:3e8f757252dd562ad80ae79e78d06fb7
#/usr/etc/in.rexecd
md5:SunOS:4.1.1:Original Dist:sun3x:/usr/etc/in.rexecd:fd51458be842565c712f8d57cf5a6f28
md5:SunOS:4.1.1:Original Dist:sun3:/usr/etc/in.rexecd:4d9811877f622348dd454172fbb40a66
md5:SunOS:4.1.1:Original Dist:sun4:/usr/etc/in.rexecd:fd51458be842565c712f8d57cf5a6f28
md5:SunOS:4.1.2:Original Dist:sun4:/usr/etc/in.rexecd:6d9f39193ac39bc9680a4fb44fdfb50f
md5:SunOS:4.1.2:Original Dist:sun4c:/usr/etc/in.rexecd:fd51458be842565c712f8d57cf5a6f28
md5:SunOS:4.1.2:Original Dist:sun4m:/usr/etc/in.rexecd:fd51458be842565c712f8d57cf5a6f28
md5:SunOS:4.1.3:Original Dist:sun4:/usr/etc/in.rexecd:37316f4d63faa445ea448ec7c670f94f
md5:SunOS:4.1.3:Original Dist:sun4c:/usr/etc/in.rexecd:fd51458be842565c712f8d57cf5a6f28
```

```
md5:SunOS:4.1.3c:Original Dist:sun4:/usr/etc/in.rex-
ecd:37316f4d63faa445ea448ec7c670f94f
md5:SunOS:4.1.3c:Original Dist:sun4m:/usr/etc/in.rex-
ecd:fd51458be842565c712f8d57cf5a6f28
md5:SunOS:4.1.3_u1:Original Dist:sun4:/usr/etc/in.rex-
ecd:be66f45bb60f31aaa23377f23c66caca
#/usr/etc/in.rshd
md5:SunOS:4.1.1:Original
Dist:sun3x:/usr/etc/in.rshd:3d81a586add92ef033088d928c7ae7dc
md5:SunOS:4.1.1:Original
Dist:sun3:/usr/etc/in.rshd:17f91e72bbf70d5cf3e75a3068d5c461
md5:SunOS:4.1.1:Original
Dist:sun4:/usr/etc/in.rshd:a4eb9385df064b9a751ede87fd0804a2
md5:SunOS:4.1.1:Original
Dist:sun4c:/usr/etc/in.rshd:3d81a586add92ef033088d928c7ae7dc
md5:SunOS:4.1.2:Original
Dist:sun4:/usr/etc/in.rshd:e45ab7d2dc4c3e7346292f85259c0432
md5:SunOS:4.1.2:Original
Dist:sun4c:/usr/etc/in.rshd:3d81a586add92ef033088d928c7ae7dc
md5:SunOS:4.1.2:Original
Dist:sun4m:/usr/etc/in.rshd:3d81a586add92ef033088d928c7ae7dc
md5:SunOS:4.1.3:Original
Dist:sun4c:/usr/etc/in.rshd:3d81a586add92ef033088d928c7ae7dc
md5:SunOS:4.1.3:Original
Dist:sun4:/usr/etc/in.rshd:686c2bb25752e6bec5090e2732a46207
md5:SunOS:4.1.3c:Original
Dist:sun4:/usr/etc/in.rshd:686c2bb25752e6bec5090e2732a46207
md5:SunOS:4.1.3c:Original
Dist:sun4m:/usr/etc/in.rshd:3d81a586add92ef033088d928c7ae7dc
md5:SunOS:4.1.3_u1:Original
Dist:sun4:/usr/etc/in.rshd:e5ca89c51427d917690fbcc1395507b4
#/usr/etc/in.tftpd
md5:SunOS:4.1.1:Original
Dist:sun3x:/usr/etc/in.tftpd:73ea84bdcff54ace0e601f5c3d2f90b0
md5:SunOS:4.1.1:Original
Dist:sun3:/usr/etc/in.tftpd:ccec1773e5945a0b8397a74ec07112df
md5:SunOS:4.1.1:Original
Dist:sun4:/usr/etc/in.tftpd:e6b495aec9b8a24f5e58ebc19fd1eec7
md5:SunOS:4.1.1:Original
Dist:sun4c:/usr/etc/in.tftpd:73ea84bdcff54ace0e601f5c3d2f90b0
md5:SunOS:4.1.2:Original
Dist:sun4:/usr/etc/in.tftpd:4b924bda12c61674771c84caa0fa1e80
md5:SunOS:4.1.2:Original
Dist:sun4c:/usr/etc/in.tftpd:73ea84bdcff54ace0e601f5c3d2f90b0
md5:SunOS:4.1.2:Original
Dist:sun4m:/usr/etc/in.tftpd:73ea84bdcff54ace0e601f5c3d2f90b0
md5:SunOS:4.1.3:Original
Dist:sun4:/usr/etc/in.tftpd:bfaf4492223126181ca9333220cbcf02
md5:SunOS:4.1.3:Original
Dist:sun4c:/usr/etc/in.tftpd:73ea84bdcff54ace0e601f5c3d2f90b0
md5:SunOS:4.1.3c:Original
Dist:sun4:/usr/etc/in.tftpd:bfaf4492223126181ca9333220cbcf02
md5:SunOS:4.1.3c:Original
Dist:sun4m:/usr/etc/in.tftpd:73ea84bdcff54ace0e601f5c3d2f90b0
```

```
md5:SunOS:4.1.3_u1:Original
Dist:sun4:/usr/etc/in.tftpd:0ff3883f2b99f06d4f897347c58a79d9
#/usr/etc/inetd
md5:SunOS:4.1.1:Original
Dist:sun3x:/usr/etc/inetd:c3a0f2bb985babcd43a438ce53de54ae
md5:SunOS:4.1.1:Original
Dist:sun3:/usr/etc/inetd:0764c23ac95b4ea5a8683c8761337485
md5:SunOS:4.1.1:Original
Dist:sun4:/usr/etc/inetd:c3a0f2bb985babcd43a438ce53de54ae
md5:SunOS:4.1.2:Original
Dist:sun4:/usr/etc/inetd:e6054cbb343d21791c6457e78822d5f1
md5:SunOS:4.1.2:Original
Dist:sun4c:/usr/etc/inetd:c3a0f2bb985babcd43a438ce53de54ae
md5:SunOS:4.1.2:Original
Dist:sun4m:/usr/etc/inetd:c3a0f2bb985babcd43a438ce53de54ae
md5:SunOS:4.1.3:Original
Dist:sun4:/usr/etc/inetd:c3a923cbf5023b48ffdef3d043190a81
md5:SunOS:4.1.3:Original
Dist:sun4c:/usr/etc/inetd:c3a0f2bb985babcd43a438ce53de54ae
md5:SunOS:4.1.3c:Original
Dist:sun4:/usr/etc/inetd:c3a923cbf5023b48ffdef3d043190a81
md5:SunOS:4.1.3c:Original
Dist:sun4m:/usr/etc/inetd:c3a0f2bb985babcd43a438ce53de54ae
md5:SunOS:4.1.3_u1:Original
Dist:sun4:/usr/etc/inetd:722d3e46a2f8e52ffadd7450fbbd1438
#/usr/bin/newgrp
md5:SunOS:4.1.1:Original Dist:sun3:/usr/bin/new-
grp:e3d6e9d43345372f5aa0d5c96570b155
md5:SunOS:4.1.1:Original Dist:sun4:/usr/bin/new-
grp:d3749b2a6e99f14feede9430d1feee46
md5:SunOS:4.1.2:Original Dist:sun4:/usr/bin/new-
grp:875e7cf58cec91c6fb44ec6e5d89ef0f
md5:SunOS:4.1.3:Original Dist:sun4:/usr/bin/new-
grp:7c0aad251ccb8de9c050d53c823f334f
md5:SunOS:4.1.3c:Original Dist:sun4:/usr/bin/new-
grp:7c0aad251ccb8de9c050d53c823f334f
md5:SunOS:4.1.3_u1:Original Dist:sun4:/usr/bin/new-
grp:04edbbb4d06bf056c4959d3b85560fe6


#/usr/bin/passwd

md5:SunOS:4.1.1:Original
Dist:sun3:/usr/bin/passwd:11499df2dfc4f75c5466e09b64fe1097
md5:SunOS:4.1.1:Original
Dist:sun4:/usr/bin/passwd:d4e3ee198d6e3934bc2356ce495e77c7
md5:SunOS:4.1.2:Original
Dist:sun4:/usr/bin/passwd:2dcec1f0e106354a85058f4c2c66e2bd
md5:SunOS:4.1.3:Original
Dist:sun4:/usr/bin/passwd:6fdb875b621de4dbffab6f6782ec2ba3
md5:SunOS:4.1.3c:Original
Dist:sun4:/usr/bin/passwd:6fdb875b621de4dbffab6f6782ec2ba3
md5:SunOS:4.1.3_u1:Original
Dist:sun4:/usr/bin/passwd:97f3231b48d6e29b829357b72043aadc
#/usr/bin/su
```

```
md5:SunOS:4.1.1:Original
Dist:sun3:/usr/bin/su:829e4e39edc3a8d299f5525c866dc324
md5:SunOS:4.1.1:Original
Dist:sun4:/usr/bin/su:94b0bc99dcb9dcdbc3e8ece7e127a906
md5:SunOS:4.1.2:Original
Dist:sun4:/usr/bin/su:23fe0a40ec522c5add89cd6ab2731170
md5:SunOS:4.1.3:Original Dist:sun4:/usr/bin/su:0d2f5665c9be-
fdf2f7aeafa4d77266bb
md5:SunOS:4.1.3c:Original Dist:sun4:/usr/bin/su:0d2f5665c9be-
fdf2f7aeafa4d77266bb
md5:SunOS:4.1.3_u1:Original
Dist:sun4:/usr/bin/su:c49812d55df4712194f832f099d40aa7
#Shared Libraries
md5:SunOS:4.1.1:Original Dist:sun4:/usr/5lib/libc.so.2.6:1d66ab-
bac68785d6f8fa8ff53200845e
md5:SunOS:4.1.1:Original
Dist:sun4:/usr/lib/libc.so.1.6:d4dc2514248834d95ee6b5c77a7eda86
md5:SunOS:4.1.1:Original
Dist:sun3:/usr/5lib/libc.so.1.15:26c5c2e8b147f3f6d96bdff369853cad
md5:SunOS:4.1.1:Original
Dist:sun3:/usr/lib/libc.so.0.15:2262f263e711bff2bd4d9d6f87ea5edd
md5:SunOS:4.1.2:Original
Dist:sun4:/usr/5lib/libc.so.2.7:b1e624d4293907511e4ee9e8e77e74dd
md5:SunOS:4.1.2:Original
Dist:sun4:/usr/lib/libc.so.1.7:76c095597088ee5bc82a2c1ce0a419ce
md5:SunOS:4.1.3:Original
Dist:sun4:/usr/5lib/libc.so.2.8:d3c8366dca51488864cc8d80c106f190
md5:SunOS:4.1.3:Original
Dist:sun4:/usr/lib/libc.so.1.8:aabfb3300f2d872cdc6d9fb10514e246
md5:SunOS:4.1.3c:Original
Dist:sun4:/usr/5lib/libc.so.2.8:af3584319d80525c2ca8e8ea8920d131
md5:SunOS:4.1.3c:Original
Dist:sun4:/usr/lib/libc.so.1.8:91a8dde1c328e474ec08557c211a4dcb
md5:SunOS:4.1.3_u1:Original
Dist:sun4:/usr/5lib/libc.so.2.9:722852b7e5df15de70e3c1a1f96c04d9
md5:SunOS:4.1.3_u1:Original
Dist:sun4:/usr/lib/libc.so.1.9:2d5bc65422472f7d4119712ccf795bf3
```

The CERT Coordination Center gratefully acknowledges the help of CIAC and, in particular, Steve Weeber of CIAC for providing us with an initial version of the "md5check" script and Tony Bartoletti for an initial checksum database. We also wish to thank SUN Microsystems for supplying checksum information.

Revision History

```
Apr. 28, 1998  Updated information on obtaining RFCs.

Sep. 19,1997   Updated copyright statement
```

Aug. 30, 1996 Information previously in the README was inserted into the advisory. Updated URL format.

Sep. 18, 1995 Intro. and Appendix B - Added note about checking with vendors for current checksum values. (as received) Appendix B, Hewlett-Packard & Solbourne

- added checksums

Sun - corrected one line of Sun entry:

md5:SunOS:4.1.3_u1:Original Dist:sun4:/usr/bin/login"

is now "md5:SunOS:4.1.3_u1:Original

Dist:sun4:bin/login" and has a new checksum

Sept. 18, 1995 - Intro. - Updated the URL for Tripwire.

6 CA-1994-06: Writable /etc/utmp Vulnerability

Original issue date: March 21, 1994
Last revised: September 19, 1997
updated copyright statement

A complete revision history is at the end of this file.

The CERT Coordination Center has received information concerning a vulnerability that exists on systems where the file /etc/utmp is writable by any user on the system.

This vulnerability is being actively exploited; please review CA-94.01 Ongoing Network Monitoring Attacks.

The problem is known to affect Sun Microsystems, Inc. SunOS 4.1.X and Solaris 1.1.1 operating systems. Solbourne Computer, Inc. and other Sparc products using SunOS 4.1.X or Solaris 1.1.1 are also affected. Solaris 2.x and SunOS 4.1.3_U1 (Solaris 1.1.1) are not affected by this problem.

Patches can be obtained from Sun Answer Centers worldwide. They are also available via anonymous FTP from ftp.uu.net in the /systems/sun/sun-dist directory, and in Europe from ftp.eu.net in the /sun/fixes directory.

We queried several vendors in addition to Sun. The following vendors reported that their operating systems, as distributed by the vendor, are not affected by this problem:

Convex Computer Corporation
Digital Equipment Corporation
Data General Corporation
Hewlett-Packard Company IBM
Intergraph
Motorola, Inc.
NeXT, Inc.
Pyramid Technology Corporation
Sequent Computer Systems
Sony Corporation

Currently, we are not aware of /etc/utmp being writable on other systems. If your operating system is not explicitly mentioned above, and if you determine that /etc/utmp is writable by someone other than root, we encourage you to contact your vendor.

If /etc/utmp on your system is writable only by the root account, you need not be concerned about the vulnerability.

We recommend that sites check their /etc/utmp file to be sure it is not writable by users other than root. If it is generally writable, you should obtain patches from the system vendor or protect /etc/utmp as described below.

I. Description

If the file /etc/utmp is writable by users other than root, programs that trust the information stored in that file can be subverted.

II. Impact

This vulnerability allows anyone with access to a user account to gain root access.

III. Solution

The solutions to this vulnerability are to either (a) protect the file, or (b) patch all the programs that trust it.

Note that SunOS 4.1.3_U1 (Solaris 1.1.1) is _not_ vulnerable to this problem.

A. To protect the file, make /etc/utmp writable only by root:

```
                  # chown root /etc/utmp


                  # chmod 644 /etc/utmp
```

B. Patches from Sun Microsystems

Program	Patch ID	Patch File Name
in.comsat	100272-07	100272-07.tar.Z
dump	100593-03	100593-03.tar.Z
syslogd	100909-02	100909-02.tar.Z
in.talkd	101480-01	101480-01.tar.Z
shutdown	101481-01	101481-01.tar.Z
write	101482-01	101482-01.tar.Z

Program	BSD	SVR4	MD5 Digital Signature
	Checksum	Checksum	
in.comsat	26553 39	64651 78	912ff4a0cc8d16a10eecbd7be102d45c
dump	52095 242	41650 484	cdba530226e8735fae2bd9bcbfa47dd0
syslogd	61539 108	38239 216	b5f70772384a3e58678c9c1f52d81190
in.talkd	47917 44	32598 88	5c3dfd6f90f739100cfa4aa4c97f01df
shutdown	46562 80	56079 159	bfc257ec795d05646ffa733d1c03855b
write	61148 41	48636 81	f93276529aa9fc25b35679ebf00b2d6f

C. Clarifications added April 1, 1994

1. If you make /etc/utmp writable only by root, this should only affect programs that allocate pseudo terminal interfaces and want to add an appropriate entry to the /etc/utmp file. Such programs include *script(1)*, *cmdtool(1)*, *gfxtool(1)*, *shelltool(1)*, and *tektool(1)*. These programs will no longer be able to add an entry to /etc/utmp which means that programs such as *who(1)*, *syslogd(1)*, and others that use /etc/utmp will not know that an account is using that pseudo tty.

2. No program should be made setuid root just to workaround this problem. Setuid programs must be written very carefully to avoid creating yet more vulnerabilities.

3. The installation instructions on the syslogd patch do not point out that, until you stop and re-start syslogd (or reboot the system), the old version is still running and the security hole has not been closed.

Revision History

```
Sep. 19,1997   Updated copyright statement

Aug. 30, 1996  Information previously in the README was inserted
into the advisory.

Apr. 01, 1994  Intro. and Sec. III - added note that SunOS 4.1.3_U1
is not vulnerable.

Apr. 01, 1994  Sec. III.C - added this new section, which contains
clarifications.
```

7 CA-1994-07: wuarchive ftpd Trojan Horse

Original issue date: April 6, 1994
Last revised: September 23, 1997
Updated copyright statement

A complete revision history is at the end of this file.

The CERT Coordination Center has received confirmation that some copies of the source code for the wuarchive FTP daemon (ftpd) were modified by an intruder, and contain a Trojan horse.

We strongly recommend that any site running the wuarchive ftpd take steps to immediately install version 2.3, or disable their FTP daemon.

I. Description

Some copies of the source code for versions 2.2 and 2.1f of the wuarchive ftpd were modified by an intruder, and contain a Trojan horse. If your FTP daemon was compiled from the intruder-modified source code, you are vulnerable.

It is possible that previous versions of the source code for the server were modified in a similar manner.

If you are running the wuarchive ftpd, but not providing anonymous FTP access, you are still vulnerable to this Trojan horse.

II. Impact

An intruder can gain root access on a host running an FTP daemon that contains this Trojan horse.

III. Solution

We strongly recommend that any site running the wuarchive ftpd (version 2.2 or earlier) take steps to install the current version.

If you cannot install the new version in a timely manner, you should disable FTP service. It is not sufficient to disable anonymous FTP. You must disable the FTP daemon.

Sites can obtain version 2.4 via anonymous FTP from
ftp://ftp.uu.net/networking/ftp/wuarchive-ftpd.

We recommend that you turn off your FTP server until you have installed the new version.

Be certain to verify the checksum information to confirm that you have retrieved a valid copy.

```
CHECKSUMS
System V sum
```

```
        ============
        51092    16  patch_2.3-2.4.Z
        20337   362  wu-ftpd-2.4.tar.Z
        Berkeley sum
        ============
        09291     8  patch_2.3-2.4.Z
        38213   181  wu-ftpd-2.4.tar.Z
        md5 checksum
        ============
        MD5 (patch_2.3-2.4.Z)   = 5558a04d9da7cdb1113b158aff89be8f
        MD5 (wu-ftpd-2.4.tar.Z) = cdcb237b71082fa23706429134d8c32e
```

The CERT Coordination Center wishes to thank Bryan O'Connor and Chris Myers of Washington University in St. Louis for their invaluable assistance in resolving this problem. CERT also gratefully acknowledges the help of Neil Woods and Karl Strickland.

UPDATES

Added April 7, 1994

The Trojan horse described in CA-94.07 provides a back-door password for any username other than "anonymous." It would be trivial for an intruder to modify the back-door password or other details of the Trojan horse code. The "diff" described in #1 below will help you detect only the Trojan horse referenced in the advisory. It will not detect any other Trojan horses.

Clarifications:

1) If you have modified any version of the wuarchive ftpd and cannot install the new version, 2.3, you may detect the existence of the discovered Trojan horse with the following diff on ftpd.c:

```
1013,1015c1013,1014
<         if ((pw == NULL || *pw->pw_passwd == '\0' ||
<             strcmp(xpasswd, pw->pw_passwd)) &&
<             (strcmp(passwd, "NULL"))) {
- ---
<         if (pw == NULL || *pw->pw_passwd == '\0' ||
<             strcmp(xpasswd, pw->pw_passwd)) {
```

2) Since the versions containing the Trojan horse were found in a number of locations, it is possible that your version of the wuarchive ftpd software contains the Trojan horse regardless of the distribution site from which you obtained the source code.

3) If you have any questions concerning the wuarchive ftpd software, send mail to:

Bryan D. O'Connor
Office of the Network Coordinator
bryan@fegmania.wustl.edu Washington University in Saint Louis
http://fegmania.wustl.edu/~bryan

Revision History

```
Sep. 23, 1997  Updated copyright statement
Aug. 30, 1996  Information previously in the README was inserted
               into the advisory.
Feb. 02, 1995  Sec. III - Inserted a pointer and checksums for
               wu-ftpd-2.4.
Apr. 07, 1994  Updates - Added clarifications and additional
               assistance.
```

8 CA-1994-08: ftpd Vulnerabilities

Original issue date: April 14, 1994
Last revised: September 23, 1997
Updated Copyright Statement

A complete revision history is at the end of this file.

The CERT Coordination Center has received information concerning two vulnerabilities in some ftpd implementations. The first is a vulnerability with the SITE EXEC command feature of the FTP daemon (ftpd) found in versions of ftpd that support the SITE EXEC feature. This vulnerability allows local or remote users to gain root access. The second vulnerability involves a race condition found in the ftpd implementations listed in Section I. below. This vulnerability allows local users to gain root access.

Sites using these implementations are vulnerable even if they do not support anonymous FTP.

As these vulnerabilities are widely known, we strongly recommend that any site running a version of ftpd listed below take steps to immediately upgrade or disable their FTP daemon. Also potentially at risk are sites whose ftpd is derived from the DECWRL or wuarchive ftpd code containing the SITE EXEC feature.

For additional information or assistance, contact the developer or vendor of your ftpd implementation.

We will update this advisory as we receive additional information. Please check advisory files regularly for updates that relate to your site.

I. Description

There is a vulnerability in the SITE EXEC command feature of ftpd that allows any remote or local user to obtain root access. There is also a vulnerability due to a race condition in these implementations.

Versions known to be vulnerable to these problems are:
wuarchive ftpd versions 2.0-2.3 (version 2.2 patched the SITE EXEC problem, but not the race condition) DECWRL ftpd versions prior 5.93
BSDI ftpd version 1.1 prior to patch 5

The SITE EXEC vulnerability affects your ftpd only if the SITE EXEC command feature has been explicitly activated at your site. This functionality is not activated by default. Sites that have not enabled the SITE EXEC feature are not at risk from this vulnerability. However, since the race condition does not have an easily applied workaround, CERT recommends that you upgrade to one of the versions listed below.

II. Impact

Anyone (remote or local) can gain root access on a host running a vulnerable FTP daemon. Support for anonymous FTP is not required to exploit this vulnerability.

III. Solution

Affected sites can solve both of these problems by upgrading to the latest version of ftpd. These versions are listed below. Be certain to verify the checksum information to confirm that you have retrieved a valid copy.

If you cannot install the new version in a timely manner, you should disable FTP service until you have corrected this problem. It is not sufficient to disable anonymous FTP. You must disable the FTP daemon.

For wuarchive ftpd, you can obtain version 2.4 via anonymous FTP from wuarchive.wustl.edu, in the "/packages/wuarchive-ftpd" directory. If you are currently running version 2.3, a patch file is available.

BSD	SVR4		
File	Checksum	Checksum	MD5 Digital Signature
wu-ftpd-2.4.tar.Z	38213 181	20337 362	cdcb237b71082fa23706429134d8c32e
patch_2.3-2.4.Z	09291 8	51092 16	5558a04d9da7cdb1113b158aff89be8f

For DECWRL ftpd, sites can obtain version 5.93 via anonymous FTP from gatekeeper.dec.com in the "/pub/misc/vixie" directory.

BSD	SVR4		
File	Checksum	Checksum	MD5 Digital Signature
ftpd.tar.gz	38443 60	1710 119	ae624eb607b4ee90e318b857e6573500

For BSDI systems, patch 005 should be applied to version 1.1 of the BSD/386 software. You can obtain the patch file via anonymous FTP from ftp.bsdi.com in the "/bsdi/patches-1.1" directory.

BSD	SVR4		
File	Checksum	Checksum	MD5 Digital Signature
BU110-005	35337 272	54935 543	1f454d4d9d3e1397d1eff0432bd383cf

The CERT Coordination Center wishes to thank Neil Woods and Karl Strickland for finding and reporting the wustl FTP daemon bug. We also wish to thank Bryan O'Connor and Chris Myers of Washington University in St. Louis, Paul Vixie of Vixie Enterprises, and Tony Sanders of BSDI for their invaluable assistance in resolving this problem.

Revision History

Sep. 23, 1997	Updated copyright statement
Aug. 30, 1996	Removed references to README files because advisories themselves are now updated.

9 CA-1994-09: /bin/login Vulnerability

Original issue date: May 23, 1994
Last revised: March 10, 1998
Updated vendor information for DEC.

A complete revision history is at the end of this file.

The CERT Coordination Center has learned of a vulnerability in /bin/login. This vulnerability potentially affects all IBM AIX 3 systems and Linux systems. At this time, we believe that only IBM AIX 3 and Linux systems are at risk.

Included with this advisory is an appendix that lists the vendors who have responded to our inquiries, and the status of their investigation into this vulnerability report. We will update this advisory as we receive additional information.

I. Description of IBM AIX vulnerability

A vulnerability exists in /bin/login on all IBM AIX 3 systems.

II. Impact of IBM AIX vulnerability

Remote users can obtain unauthorized root access on the affected hosts.

III. Solution for IBM AIX vulnerability

IBM is working on an official fix, which is still under development. The reference number for this fix is APAR IX44254. Until you obtain the official fix from IBM, we encourage you to apply the workaround or install the emergency fix below.

A. Workaround

The recommended workaround is to disable the rlogin daemon:

1. As root, edit /etc/inetd.conf

    Comment out the line 'login ... rlogin'

2. Run 'inetimp'

3. Run 'refresh -s inetd'

B. Emergency fix

The emergency fix for the different levels of AIX 3 affected by this vulnerability is available via anonymous FTP from software.watson.ibm.com:/pub/rlogin/rlogin.tar.Z. Installation instructions are included in the README file (which is included in rlogin.tar.Z).

```
Checksum information for rlogin.tar.Z:
BSD:      25285   317
SystemV:  13021 633 rlogin.tar.Z
MD5:      MD5 (rlogin.tar.Z) = 803ee38c2e3b8c8c575e2ff5e921034c
```

C. Official fix

The official fix for this problem can be ordered as APAR IX44254.

To order an APAR from IBM in the U.S., call 1-800-237-5511 and ask IBM to ship it as soon as it is available. According to IBM, this fix will be available in approximately two weeks. APARs may be obtained outside the U.S. by contacting your local IBM representative.

IV. Description of Linux vulnerability

A vulnerability exists in /bin/login for Linux systems.

V. Impact of Linux vulnerability

Any user, remote or local, can obtain unauthorized root access on the affected hosts.

VI. Solution for Linux vulnerability

A set of tools has been released by Florian La Roche <flla@stud.uni-sb.de> under the name "NetKit." It is available via the FTP sites listed below. An excerpt from the README provides the following general information:

This directory contains a collection of net source programs for LINUX.

```
NetKit-A  A is the first character in the alphabet -> basic things
          contains a collection of LINUX-specific programs and
          several small utility programs found somewhere in the
           Internet or on News
           (contains also net-032 from Alan Cox)
NetKit-B  B like BSD, even if we only think about LINUX
          contains source code derived from NetBSD
NetKit-M  M like mail
          contains context diffs and some source code to make a
          good mail system
NetKit-N  N like news
```

```
         contains context diffs for a good News system
         (news readers and also INN for your own newsfeed)
NetKit-X  X like eXtra
          will maybe be necessary, if NetKit-A grows too large
     sunacm.swan.ac.uk:/pub/misc/Linux/Networking/PROGRAMS/Packages
     ------------------------------------------------------------------------
     MD5 (NetKit-A-0.05.bin.tar.gz) = afe45e04f359b0ff99e66cc58b4e758c
     MD5 (NetKit-A-0.05.tar.gz) = a17fae1b58e1cf8a79aef30296f65672
     MD5 (NetKit-A-0.06.bin.tar.gz) = e0f813427341b070ab9f8374ad721134
     MD5 (NetKit-A-0.06.tar.gz) = adb00607cb2887c44f5aa8981fb8120b
     MD5 (NetKit-B-0.04.bin.tar.gz) = ffe7099a0271a85eb22c78f7c3373bc6
     MD5 (NetKit-B-0.04.tar.gz) = 156be1d3571b1681485b47255f7e202c
     MD5 (NetKit-B-0.05.bin.tar.gz) = 3b270017ce28328c5596291e6d2687f0
     MD5 (NetKit-B-0.05.tar.gz) = ba2327f741a265edc252e86b442a0a0d
     MD5 (NetKit-M-0.01.tar.gz) = 392cbe6454965ad0d9e12f98af4cdd4a
     MD5 (NetKit-N-0.01.tar.gz) = 55957726205a52621a15938c3bea593b
     sunsite.unc.edu:/pub/Linux/system/Network/sunacm
     ------------------------------------------------------------------------
     MD5 (NetKit-A-0.05.bin.tar.gz) = afe45e04f359b0ff99e66cc58b4e758c
     MD5 (NetKit-A-0.05.tar.gz) = a17fae1b58e1cf8a79aef30296f65672
     MD5 (NetKit-A-0.06.bin.tar.gz) = e0f813427341b070ab9f8374ad721134
     MD5 (NetKit-A-0.06.tar.gz) = adb00607cb2887c44f5aa8981fb8120b
     MD5 (NetKit-B-0.04.bin.tar.gz) = ffe7099a0271a85eb22c78f7c3373bc6
     MD5 (NetKit-B-0.04.tar.gz) = 156be1d3571b1681485b47255f7e202c
     MD5 (NetKit-B-0.05.bin.tar.gz) = 3b270017ce28328c5596291e6d2687f0
     MD5 (NetKit-B-0.05.tar.gz) = ba2327f741a265edc252e86b442a0a0d
     MD5 (NetKit-M-0.01.tar.gz) = 392cbe6454965ad0d9e12f98af4cdd4a
     MD5 (NetKit-N-0.01.tar.gz) = 55957726205a52621a15938c3bea593b
```

To address the local access problem, we encourage you to install a version of /bin/login that does not allow the -f option in the form "-f<user>", but only allows this option in the form "-f <user>", as two arguments. At this time, we do not know which versions of login.c are vulnerable.

Appendix

We have received feedback from the following, who indicated that their products are not vulnerable:

Amdahl
Apple
BSD
BSDI
Digital Equipment Corporation
FreeBSD
Harris
HP
Linux
Motorola
NeXT
Pyramid
SCO
Sequent
SGI

Solbourne
Sony
Sun

CERT has received feedback from the following vendors, who have made patches available to address the /bin/login vulnerability. Please note that vendors sometimes update patch files. If you find that the checksum is different, please contact the vendor.

IBM - Please see Sec. III, "Solution for IBM AIX vulnerability" for details.

Briefly--

Official patch: APAR IX44254.
Emergency fix: Available via anonymous FTP from:

software.watson.ibm.com:/pub/rlogin

This directory contains the latest available emergency fix for APAR IX44254. As updates become available, any new versions will be placed in this directory with the name rlogin<#>.tar.Z with <#> being incremented for each update. See the README.FIRST file in that directory for details.

LINUX - Please see Sec. VI, "Solution for Linux vulnerability" for details.

Briefly--
"Netkit" is available from

sunacm.swan.ac.uk:/pub/misc/Linux/Networking/PROGRAMS/Packages sun-
site.unc.edu:/pub/Linux/system/Network/sunacm

The CERT Coordination Center wishes to thank Axel Clauberg of University of Cologne for reporting the IBM AIX problem, and IBM for their assistance in responding to this problem.

UPDATES

We are aware that there have been several /bin/login wrapper programs posted as proposed workarounds for this vulnerability. None of the wrappers that CERT has reviewed have fully addressed all aspects of this vulnerability. CERT will not undertake any further review of such wrappers. Instead, we encourage sites to apply the appropriate workaround or patches available, as described in CA-94.09.bin.login.vulnerability.

Frequently Asked Question about this CERT advisory:

Question: Why is rshd not mentioned in this advisory?

Answer: From the man page for RSH(1C):

```
          rsh hostname [ -l username ] [ -n ] [ command ]
```

rsh connects to the specified hostname and executes the specified command.
If you omit [command], instead of executing a single command, rsh logs you in on the remote host using *rlogin(1C)*.

```
          rsh hostname [ -l username ] [ -n ]
```

Exploitation of the vulnerability via rsh requires the use of rlogind, which then invokes /bin/login. Exploitation of this vulnerability by this method is addressed by this advisory.

CERT/CC are not aware of any exploitation method for this vulnerability via the following usage:

```
          rsh hostname [ -l username ] [ -n ] command
```

Revision History

```
Mar. 10, 1998  Updated vendor information for DEC.

Sep. 23, 1997  Updated copyright statement

Aug. 30, 1996  Information previously in the README was inserted
into the advisory. The result is a major update to patch information
in Sections III and VI.

Mar. 29, 1996  Updates section - Removed duplicate information from
the "Frequently Asked Question" section

Feb. 02, 1995  Section III - Updated Linux patch information

May  27, 1994  Updates section - Included caveat concerning other
/bin/login wrapper programs and comments about rshd
```

10 CA-1994-10: IBM AIX bsh Vulnerability

Original issue date: June 3, 1994
Last revised: September 23, 1997
Updated copyright statement

A complete revision history is at the end of this file. The CERT Coordination Center has learned of a vulnerability in the batch queue (bsh) of IBM AIX systems running versions prior to and including AIX 3.2.

CERT recommends disabling the batch queue by following the workaround instructions in Section III below. Section III also includes information on how to obtain fixes from IBM if the bsh queue functionality is required by remote systems.

We will update this advisory as we receive additional information. Please check advisory files regularly for updates that relate to your site.

I. Description

The queueing system on IBM AIX includes a batch queue, "bsh", which is turned on by default in /etc/qconfig on all versions of AIX 3 and earlier.

II. Impact

If network printing is enabled, remote and local users can gain access to a privileged account.

III. Solution

In the next release of AIX, the bsh queue will be turned off by default. CERT/CC recommends that the bsh queue be turned off using the workaround described in Section A below unless there is an explicit need to support this functionality for remote hosts. If this functionality must be supported, IBM provides fixes as outlined in Sections B and C below. For questions concerning these workarounds or fixes, please contact IBM at the number provided below.

A. Workaround

Disable the bsh queue by following one of the two procedures outlined below:

1. As root, from the command line, enter:

```
# chque -qbsh -a"up = FALSE"
```

2. From SMIT, enter:

- Spooler
- Manage Local Printer Subsystem

- Change/Show Characteristics of a Queue
  - select bsh
- Activate the Queue
  - select no

B. Emergency fix

Obtain and install the emergency fix for the version(s) of AIX used at your site. Fixes for the various levels of AIX are available by anonymous FTP from software.watson.ibm.com. The files are located in /pub/aix/bshfix.tar.Z in compressed tar format. Installation instructions are included in the README file included as part of the tar file.

The directory /pub/aix contains the latest available emergency fix for APAR IX44381. As updates become available, any new versions will be placed in this directory with the name bshfix<#>.tar.Z with <#> being incremented for each update. See the README.FIRST file in that directory for details.

IBM may remove this emergency fix file without prior notice if flaws are reported. Due to the changing nature of these files, no checksum information is available.

C. Official fix

The official fix for this problem can be ordered as APAR IX44381.

To order APARs from IBM in the U.S., call 1-800-237-5511 and ask that it be shipped to you as soon as it is available. To obtain APARs outside of the U.S., contact your local IBM representative.

The CERT Coordination Center wishes to thank Gordon C. Galligher of Information Resources, Inc. for reporting this problem and IBM Corporation for their support in responding to this problem.

Revision History

```
Sep. 23. 1997   Updated copyright statement

Aug. 30, 1996   Removed references to README files because adviso-
ries themselves are now updated.
```

11 CA-1994-11: Majordomo Vulnerabilities

Original issue date: June 9, 1994
Last revised: September 23, 1997
Updated copyright statement

A complete revision history is at the end of this file.

The CERT Coordination Center has received reports of vulnerabilities in all versions of Majordomo up to and including version 1.91. These vulnerabilities enable intruders to gain access to the account that runs the Majordomo software, even if the site has firewalls and TCP wrappers.

We recommend that all sites running Majordomo replace their current version with version 1.92 (see Section III for instructions). It is possible to apply a quick fix to versions prior to 1.92, but we strongly recommend obtaining 1.92 instead.

We will update this advisory as we receive additional information. Please check advisory files regularly for updates that relate to your site.

I. Description

Two vulnerabilities have recently been found in Majordomo. These vulnerabilities enable intruders to gain access to the account that runs the Majordomo software, thus gaining the ability to execute arbitrary commands. The vulnerabilities can be exploited without a valid user name and password on the local machine, and firewalls and TCP wrapper protection can be bypassed. The CERT/CC has received reports that the vulnerabilities are currently being exploited.

II. Impact

Intruders can install and execute programs as the user running the Majordomo software.

III. Solution

A. Recommended solution for all versions through 1.92

Obtain and install Majordomo version 1.93.

This version is available from

ftp://ftp.pgh.net/pub/majordomo/

ftp://ftp.greatcircle.com/pub/majordomo/

MD5 (majordomo-1.93.README) = 068bb343f23d3119cd196ed4222ab266
MD5 (majordomo-1.93.tar.Z) = c589a3c3d420d68e096eafdfdac0c8aa

B. Quick fix for versions 1.91 and earlier

Until you are able to install the new version of Majordomo, you should install the following quick fix, which has two steps. If you are running Majordomo 1.90 and earlier, you must take both steps. If you are running version 1.91, you need only take the first step.

Step 1 - Disable new-list by either renaming the new-list program or removing it from the aliases file.

If you have version 1.90 and earlier, go on to Step 2.

Step 2 - In every place in the Majordomo code where there is a string of any of these forms,

```
"|/usr/lib/sendmail -f<whatever> $to"      #majordomo.pl

"|/usr/lib/sendmail -f<whatever> $reply_to" #request-answer

"|/usr/lib/sendmail -f<whatever> $reply_to $list-approval" # new-
list

"|/usr/lib/sendmail -f<whatever> \$to"      #majordomo.cf
```

Change that string to

```
"|/usr/lib/sendmail -f<whatever> -t
```

Generally, you will find the strings in the request-answer file, the majordomo.pl file, and your local majordomo.cf file.

Note: If you are running a mailer other than sendmail, this step may not fix the vulnerability. You should obtain and install version 1.92 as described in Section A above.

The CERT Coordination Center thanks Brent Chapman of Great Circle Associates and John Rouillard of the University of Massachusetts at Boston for their support in responding to the problem.

Revision History

```
Sep. 23, 1997  Updated copyright statement

Aug. 30, 1996  Information previously in the README was inserted

               into the advisory. Changed URL format.

June 09, 1995  Sec. III.A - pointer to majordomo 1.93

June 1994      Sec. III.A - Added alternative FTP sites
```

```
          Sec. III.B - Revised step 2 of the workaround
```

12 CA-1994-12: Sendmail Vulnerabilities

Original issue date: July 14, 1994

**** Superseded by CA-1996-20, CA-1996-24, and CA-1996-25. ****

13 CA-1994-13: SGI IRIX Help Vulnerability

Original issue date: August 11, 1994
Last revised: September 23, 1997
Updated copyright statement

A complete revision history is at the end of this file.

The CERT Coordination Center has received information about a vulnerability in the Silicon Graphics, Inc. IRIX operating system, versions 5.1.x and 5.2. This vulnerability enables users to gain unauthorized root access. To exploit the vulnerability, a person must log into an account on the system or have physical access to the system console.

SGI has developed a patch for the vulnerability. Because the vulnerability has been widely discussed in public forums on the Internet, we recommend that you install the patch as soon as possible. Section III below contains instructions for obtaining the patch, along with a workaround you can use until you install it.

We will update this advisory as we receive additional information. Please check advisory files regularly for updates that relate to your site.

I. Description

A vulnerability exists in the SGI help system and print manager, enabling users to get unauthorized root access if they can log into an account on the system or get physical access to the system console. The vulnerability is present in the SGI IRIX operating system, versions 5.1.x and 5.2. SGI reports that the problem will be permanently corrected in a future release of IRIX.

In public discussions, the vulnerability has been referred to by various names, including clogin, printer manager, and SGI Help.

II. Impact

Individuals with accounts on the system or physical access to the system console can obtain root access.

III. Solutions

A. For IRIX 5.2

If you are running IRIX 5.2, obtain and install patch65 according to the instructions provided. These instructions can be found in the "relnotes.patchSG0000065" file in the patch65.tar file (see below).

To install this patch successfully, you need to have the latest SGI "inst" program installed (this is available as patch00 or patch34).

SGI has provided instructions for determining if the new install program is on your system. We have placed these in an appendix at the end of this advisory.

These patches are available by anonymous FTP from ftp.sgi.com and from sgigate.sgi.com in the "/security" directory.

Filename	patch65.tar
Standard Unix Sum	63059 1220
System V Sum	15843
MD5	af8c120f86daab9df74998b31927e397
Filename	patch34.tar.Z
Standard Unix Sum	11066 15627
System V Sum	1674 31253
MD5	2859d0debff715c5beaccd02b6bebded

Patches are available on CD. Contact your nearest SGI service provider for distribution.

B. For IRIX 5.1.x

If you are running versions 5.1.x, SGI recommends that you upgrade to version 5.2, if possible, and then follow the instructions in Section III.A. above. If you cannot upgrade to 5.2, see the workaround instructions in III.C.

C. Workaround

If you cannot install the patches or are delayed in obtaining them, SGI recommends removing the help subsystem using the following command (as root):

```
# versions remove sgihelp.sw.eoe
```

PLEASE NOTE: Removal of this subsystem will affect other installed software that use the SGI Help system. After the removal, certain help functions from within applications will return non-fatal error messages about the missing subsystem.

At a later date, when the patch can be installed on the system, you will need to re-install the previously removed SGI Help software prior to installing patch65. This can be found on your original software distribution (CD labeled as IRIX 5.2). As root, use the command:

```
        # inst -f /CDROM/dist/sgihelp
```

```
                Inst> install sgihelp.sw.eoe

                Inst> go
```

The installation documentation provides further information.

Appendix

There are three patches related to this issue - patch00, patch34, and patch65.

Patch34 is an update to patch00 which modifies the "inst" program to be able to handle patch updates. At least one of patch00 or patch34 is required to be installed before installing patch65. To determine if the new inst program is already installed on your system, the following command can be issued:

```
# versions patch\*

I = Installed, R = Removed

Name                           Date      Description

I  patchSG0000034              08/10/94   Patch SG0000034

I  patchSG0000034.eoe1_sw      08/10/94   IRIX Execution Environment
Software

I  patchSG0000034.eoe1_sw.unix 08/10/94   IRIX Execution Environment
```

If patchSG0000000 or patchSG0000034 (as seen above) is loaded, then it is only necessary to download patch65 as described in the advisory. This is important since patch34 is rather large (16MB).

Otherwise, download both patch34 and patch65. Install patch34 first, then patch65. To install patch34, uncompress and untar "patch34.tar.Z" and follow the instructions in the "README.FIRST" file.

These patches are available by anonymous FTP from ftp.sgi.com in the "security" directory:

```
        # versions patch\*

        I = Installed, R = Removed

           Name                 Date      Description

        I  patchSG0000034       08/10/94  Patch SG0000034

        I  patchSG0000034.eoe1_sw 08/10/94 IRIX Execution Environ-
ment Software

        I  patchSG0000034.eoe1_sw.unix 08/10/94 IRIX Execution Envi-
ronment
```

The CERT Coordination Center wishes to thank Silicon Graphics, Inc., for their cooperation in responding to this problem and members of the AUSCERT and CIAC response teams for their contributions to this advisory.

Revision History

```
Sep. 23, 1997  Updated copyright statement

Aug. 30, 1996  Information previously in the README was inserted

               into the advisory.
```

14 CA-1994-14 Trojan Horse in IRC Client for UNIX

Original issue date: October 19, 1994
Last revised: September 23, 1997
Updated copyright statement

A complete revision history is at the end of this file.

The CERT Coordination Center has learned of a Trojan horse in some copies of ircII version 2.2.9, the source code for the Internet Relay Chat (IRC) client for UNIX systems. Reports we have received thus far indicate that the corrupt code was available as early as May 1994. The Trojan horse provides a back door through which intruders can gain unauthorized access to accounts of IRC users. Intruders are actively exploiting this back door. If you obtained ircII 2.2.9 from any site in May or later, you may be vulnerable.

Because it is unknown how far the corrupt version of the IRC client has propagated and because intruders may have corrupted other versions, the CERT staff recommends obtaining and installing ircII version 2.6.

Because no special privileges are needed to install and run the IRC source code, any user on your system may have installed the corrupt code. Thus, we also recommend that you inform your users of this potential problem and its solution.

We will update this advisory as we receive additional information. Please check advisory files regularly for updates that relate to your site.

I. Description

A Trojan horse was found in some copies of the source code for the Internet Relay Chat client for UNIX systems, ircII version 2.2.9. Intruders are actively exploiting this Trojan horse.

The Trojan horse creates a back door and enables intruders to gain unauthorized access to accounts of IRC users. If IRC is run from a system account, such as root or bin, the Trojan horse enables intruders to gain unauthorized access to the system account. In addition, because it is possible to compile, install, and run IRC source code without special privileges, any user on your system may have installed corrupt code.

The source code containing the Trojan horse was available from many FTP sites as early as May 1994 (at this time, we do not have a specific date).

II. Impact

Remote users can gain unauthorized access to any account running the IRC client, including a system account if it is running IRC.

III. Solution

If you want to try to determine whether your copy of ircII contains the Trojan horse, perform a search on the IRC client to find the strings JUPE or GROK. For example,

```
% strings /usr/local/bin/irc | grep 'JUPE|GROK'
```

```
% strings /usr/local/bin/irc | egrep 'JUPE|GROK'
```

If the strings JUPE or GROK are present in the IRC client, your source code may contain the Trojan horse. Keep in mind, however, that back doors can easily be changed to respond to other words, so you may be vulnerable even if you do not find JUPE or GROK.

Thus, even if you believe that your IRC source code is clean, we urge you to install ircII version 2.6, the most recent version of IRC. Also, the maintainer of the code reports that version 2.6 contains many bug fixes and extra portability.

IRC source code is available by anonymous FTP from many locations, including the following:

sungear.mame.mu.oz.au:/pub/irc
alpha.gnu.ai.mit.edu:/ircII
ftp.funet.fi:/pub/unix/irc/ircII
coombs.anu.edu.au:/pub/irc/ircii

```
File                  Size     MD5 Checksum

--------              ------   -----------------------------

ircii-2.6.tar.gz      366361   3FC5FBD18CB3E6C071F51FD8C6C59017

ircii-2.6help.tar.gz  111733   D9D535B7A06BED2A2EA6676B20BDA481

ircii-2.5to2.6-diff   19644    0C05C96B10CB87186BD921536AE3FDF2
```

As of Feb. 2, 1995, an ircii2.6-sco-patch is available:

```
File                  Size     MD5 Checksum

--------              ------   -----------------------------

ircii-2.6.tar.gz      366361   3FC5FBD18CB3E6C071F51FD8C6C59017

ircii-2.6help.tar.gz  111733   D9D535B7A06BED2A2EA6676B20BDA481

ircii-2.5to2.6-diff   19644    0C05C96B10CB87186BD921536AE3FDF2

ircii-2.6-sco-patch   65143    45161113B0E435FB993CE00436A819A1
```

IV. Informing Users

Because users may have installed IRC source code on their own, we recommend informing all your users about the Trojan horse and the new version of IRC.

In addition, you may want to find any user-installed copies of IRC that may be vulnerable. If so, you could use the find command to locate these binaries. As an example, the following command will enable you to find all files named "irc" in a subdirectory of /usr/users:

```
% find /usr/users -name irc -type f -print
```

The CERT Coordination Center wishes to thank Matthew Green for his assistance with this advisory.

This document is available from: http://www.cert.org/advisories/CA-1994-14.html

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from http://www.cert.org/CERT_PGP.key.

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site: http://www.cert.org/.

NO WARRANTY

Any material furnished by Carnegie Mellon University and the Software Engineering Institute is furnished on an "as is" basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied as to any matter including, but not limited to, warranty of fitness for a particular purpose or merchantability, exclusivity or results obtained from use of the material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

Conditions for use, disclaimers, and sponsorship information

Revision History

```
Sep. 23, 1997  Updated copyright statement

Aug. 30, 1996  Information previously in the README was inserted

               into the advisory.

Feb. 02, 1995  Sec. III - Added filenames and checksums for ircii2.6-sco-patch.

Oct. 20, 1994  Sec. III - Added example command using egrep.

               Included alhpa.gnu.ai.mit.edu as a source of ircII.
```

15 CA-1994-15: NFS Vulnerabilities

Original issue date: December 19, 1994
Last revised: Septmeber 23, 1997
Updated copyright statement

A complete revision history is at the end of this file.

The CERT Coordination Center is experiencing an increase in reports of root compromises caused by intruders using tools to exploit a number of NFS (Network File System) vulnerabilities.

CERT recommends limiting your exposure to these attacks by implementing the security measures described in Section III below.

We will update this advisory as we receive additional information. Please check advisory files regularly for updates that relate to your site.

I. Description

There are tools being used by intruders to exploit a number of NFS vulnerabilities. These tools are widely available and widely distributed.

II. Impact

The impact varies depending on which vulnerabilities are present. In the worst case, intruders gain unauthorized root access from a remote host.

III. Security Measures

A. Filter packets at your firewall/router.

Filter TCP port 111, UDP port 111 (portmapper), TCP port 2049, and UDP port 2049 (nfsd).

Note: Some sites may run NFS on a port other than 2049. To determine which port is running NFS, enter the following command on the machine in question:

```
        rpcinfo -p
```

If NFS is on a different port, then that is the port number to block at the firewall.

Consult your vendor or your firewall documentation for detailed instructions on how to configure the ports.

This measure will prevent access to NFS at your site from outside your firewall, but it will not protect you from attacks launched from your local network, behind your firewall.

B. Use a portmapper that disallows proxy access.

Be sure that you do this for every host that runs a portmapper. For Solaris, 2.x, use a version of rpcbind that disallows proxy access.

A portmapper that disallows proxy access protects all hosts with the modified portmapper from attacks that originate either inside or outside your firewall. Because this security measure addresses only the portmapper vulnerability, we recommend combining it with measure A above. Wietse Venema has developed a portmapper that disallows proxy access. It is available by anonymous FTP from

```
ftp.win.tue.nl: /pub/security/portmap_3.shar.Z

ftp.cert.org:   /pub/tools/nfs_tools/portmap_3.shar.Z

MD5 checksum:   f6a3ad98772e7a402ddcdac277adc4a6
```

For Solaris systems, Venema has developed a version of rpcbind that does not allow proxy access. Solaris users should install this program, not the portmapper. Rpcbind is available by anonymous FTP from the same sites as the portmapper:

```
ftp.win.tue.nl:/pub/security/rpcbind_1.1.tar.Z

ftp.cert.org:  /pub/tools/nfs_tools/rpcbind_1.1.tar.Z

MD5 checksum:  58437adcbea0a55e37d3a3211f72c08b
```

C. Check the configuration of the /etc/exports files on your hosts.

In particular:

1. Do *not* self-reference an NFS server in its own exports file.
2. Do not allow the exports file to contain a "localhost" entry.
3. Export file systems only to hosts that require them.
4. Export only to fully qualified hostnames.
5. Ensure that export lists do not exceed 256 characters.
   If you have aliases, the list should not exceed 256 characters *after* the aliases have been expanded. (See CA-94.02.REVISED.SunOS.rpc.mountd.vulnerability)
6. Use the *showmount(8)* utility to check that exports are correct.
7. Wherever possible, mount file systems to be exported read only and export file systems read only.

D. Ensure that your systems are current with patches and workarounds available from your vendor and identified in CERT advisories.

The following advisories address problems related to NFS:

CA-91.21.SunOS.NFS.Jumbo.and.fsirand
CA-92.12.REVISED.SunOS.rpc.mountd.vulnerability
CA-93.15.SunOS.and.Solaris.vulnerabilities
CA-94.02.REVISED.SunOS.rpc.mountd.vulnerability

Vendors may have additional patches not covered by a CERT advisory, so be sure to contact your vendor for further information.

The CERT Coordination Center thanks Steve Bellovin, Casper Dik, Leendert van Doorn, and Wietse Venema for their support in responding to this problem.

Revision History

```
Sep. 23, 1997  Updated copyright statement

Aug. 30, 1996  Information previously in the README was inserted

               into the advisory.

Feb. 02, 1995  Sec. III - Added a note about checking port numbers.
```