Software Engineering Institute
Carnegie Mellon University

1993 CERT Advisories

CERT Division

http://www.sei.cmu.edu

REV-03.18.2016.0

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.

This report was prepared for the

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

DM17-0052

Table of Contents

1 CA-1993-01: Revised Hewlett-Packard NIS ypbind Vulnerability

Original issue date: January 13, 1993
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 INFORMATION REGARDING AVAILABILITY OF IMAGE KITS SUPERSEDES CERT ADVISORY CA-92.17**

The CERT Coordination Center has received information concerning a vulnerability in the NIS ypbind module for the Hewlett-Packard (HP) HP/UX Operating System for series 300, 700, and 800 computers.

HP has provided revised patches for all of the HP/UX level 8 releases (8.0, 8.02, 8.06, and 8.07). This problem is fixed in HP/UX 9.0. The following patches have been superseded:

Patch ID	Replaced by Patch ID
PHNE_1359	PHNE_1706
PHNE_1360	PHNE_1707
PHNE_1361	PHNE_1708

All HP NIS clients and servers running ypbind should obtain and install the patch appropriate for their machine's architecture as described below.

I. Description

A vulnerability in HP NIS allows unauthorized access to NIS data.

II. Impact

Root on a remote host running any vendor's implementation of NIS can gain root access on any local host running HP's NIS ypbind. Local users of a host running HP's NIS ypbind can also gain root access.

III. Solution

1. All HP NIS clients and servers running ypbind should obtain and install the patch appropriate for their machine's architecture.

   These patches contain a version of ypbind that only accepts ypset requests from a superuser port on the local host. This prevents a non-superuser program from sending rogue ypset requests to ypbind. They also include the mod from the superseded patches which prevented a

superuser on a remote system from issuing a ypset -h command to the local system and binding the system to a rogue ypserver.

These patches may be obtained from HP via FTP (this is NOT anonymous FTP) or the HP SupportLine. To obtain HP security patches, you must first register with the HP SupportLine. The registration instructions are available via anonymous FTP at cert.org (192.88.209.5) in the file "pub/vendors/hp/supportline_and_patch_retrieval".

The new patch files are:

```
Architecture Patch ID   Filename
Checksum

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

Series 300   PHNE_1706  /hp-ux_patches/s300_400/8.X/PHNE_1706
38955 212

Series 700   PHNE_1707  /hp-ux_patches/s700/8.X/PHNE_1707
815 311

Series 800   PHNE_1708  /hp-ux_patches/s800/8.X/PHNE_1708
56971 299
```

2. The instructions for installing the patch are provided in the PHNE_xxxx.text file (this file is created after the patch has been unpacked).

   The checksums listed above are for the patch archive files from HP. Once unpacked, each shell archive contains additional checksum information in the file "patchfilename.text". This checksum is applicable to the binary patch file "patchfilename.updt".

If you have any questions about obtaining or installing the patches, contact the USA HP SupportLine at 415-691-3888, or your local HP SupportLine number. Please note that the telephone numbers in this advisory are appropriate for the USA and Canada.

The CERT Coordination Center wishes to thank Brian Kelley of Ford Motor Company for bringing this vulnerability to our attention. We would also like to thank Hewlett-Packard for their response to this problem.

Revision History

```
September 19,1997  Attached Copyright Statement
```

2 CA-1993-02: New Patch for NeXT NetInfo_writers Vulnerabilities

Original issue date: January 21, 1993
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 INFORMATION**

The CERT Coordination Center has received updated information from NeXT Computer, Inc. concerning vulnerabilities in the distributed printing facility of NeXT computers running all releases of NeXTSTEP software through NeXTSTEP Release 3.0. The online patch described in CERT Advisory CA-93.02 has been replaced with a new patch. The size and checksum information in this Advisory have been updated to reflect the new online patch.

For more information, please contact your authorized support center. If you are an authorized support provider, please contact NeXT through your normal channels.

I. Description

The default NetInfo "_writers" properties are configured to allow users to install printers and FAX modems and to export them to the network without requiring assistance from the system administrator. They also allow a user to configure other parts of the system, such as monitor screens, without requiring help from the system administrator. Vulnerabilities exist in this facility that could allow users to gain unauthorized privileges on the system.

II. Impact

In the case of the "/printers" and the "/fax_modems" directories, the "_writers" property can permit users to obtain unauthorized root access to a system.

In the "/localconfig/screens" directory, the "_writers" property can potentially permit a user to deny normal login access to other users.

III. Solution

To close the vulnerabilities, remove the "_writers" properties from the "/printers", "/fax_modems", and "/localconfig/screens" directories in all NetInfo domains on the network, and from all immediate subdirectories of all "/printers", "/fax_modems", and "/localconfig/screens" directories. The "_writers" properties may be removed using any one of the following three methods:

A. As root, use the "niutil" command-line utility. For example, to remove the "_writers" property from the "/printers" directory:
B. # /usr/bin/niutil -destroyprop . /printers _writers

C. Alternatively, use the NetInfoManager application: open the desired domain, open the appropriate directory, select the "_writers" property, choose the "Delete" command [Cmd-r] from the "Edit" menu, and save the directory.

D. To assist system administrators in editing their NetInfo domains, a shell script, "writersfix", is available via anonymous FTP from next.com (129.18.1.2):

```
Filename                                    Size   Checksum
--------                                    ----   --------
pub/Misc/Utilities/WritersFix.compressed    5600   25625  6
```

After transferring this file using BINARY transfer type, double-click on the file. A "WritersFix" directory will be created in your file system, containing the script ("writersfix") and some documentation ("WritersFix.rtf").

Consider removing "_writers" from other NetInfo directories as well (for example, "/locations"), noting the following trade-off between ease-of-use and security. By removing the "_writers" properties, the network and the computers on the network become more secure, but a system administrator's assistance is required where it previously was not required.

Please refer to the NeXTSTEP Network and System Administration manual for additional information on "_writers". Note that the subdirectories of the "/users" directory have "_writers_passwd" set to the user whose account is described by the directory. This is essential if users are to be able to change their own passwords, and this does not compromise system security.

The CERT Coordination Center wishes to thank Alan Marcum and Eric Larson of NeXT Computer, Inc. for notifying us about the existence of these vulnerabilities and for providing appropriate technical information.

Revision History

```
September 19, 1997  Attached Copyright Statement
```

3 CA-1993-03: SunOS File/Directory Permissions

Original issue date: February 3, 1993
Last revised: September 19, 1997
Attached copyright statement

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

The default permissions on a number of files and directories in SunOS 4.1, 4.1.1, 4.1.2, and 4.1.3 are set incorrectly. These problems are relevant for the sun3, sun3x, sun4, sun4c, and sun4m architectures. They have been fixed in SunOS 5.0. (Note that SunOS 5.0 is the operating system included in the Solaris 2.0 software distribution.)

An updated patch to reset these permissions is available from Sun. CERT has seen an increasing number of attackers exploit these problems on systems and we encourage sites to consider installing this patch.

I. Description

File permissions on numerous files were set incorrectly in the distribution tape of 4.1.x. A typical example is that a file which should have been owned by "root" was set to be owned by "bin".

Not all sites will need or want to install the patch for this problem. The decision of what user id should own most system files and directories depends on the administrative practices of the site. It is quite reasonable to run a system where the majority of files are owned by "bin" as long as the entire system is run in a manner consistent with that practice. As distributed, the SunOS configuration expects most system files to be owned by "root". The fact that some are not creates security problems.

Therefore, sites that are running the SunOS versions listed above as distributed should install the patch described below. Sites that have made an informed choice to configure their system differently may instead want to review the patch script and consider which, if any, of the changes should be made on their system.

II. Impact

Depending on the specific configuration of the local site, the default permissions may allow local users to gain "root" access.

III. Solution

1. Sun has provided a script to reset file and directory permissions to their correct values. The script is available in Sun's Patch #100103 version 11. This patch can be obtained via local Sun Answer Centers worldwide as well as through anonymous FTP from the ftp.uu.net (137.39.1.9) system in the /systems/sun/sun-dist directory.

```
Patch ID     Filename             Checksum
100103-11    100103-11.tar.Z      19847   6
```

Please note that Sun Microsystems sometimes updates patch files. If you find that the checksum is different please contact Sun Microsystems or CERT for verification.

2. Uncompress the file, extract the contents of the tar archive, and review the README file.

   % uncompress 100103-11.tar.Z

   % tar xfv 100103-11.tar

   % cat README

3. This patch will reset the group ownership of certain files to either "staff" or "bin". Make sure you have entries in the "/etc/group" file for these accounts.

   % grep '^staff:' /etc/group

   % grep '^bin:' /etc/group

   If you do not have both of these you will need to either add the missing account(s) or modify the patch script (4.1secure.sh) to reflect group ownerships appropriate for your site. (Note that the security problems are fixed by the ownerships and mode bits specified in the patch - not by the group ownerships. Therefore, changing the group ownerships does not invalidate the patch.)

4. As "root", run the patch script.

   # sh 4.1secure.sh

   This patch fixes Sun BugId's 1046817, 1047044, 1048142, 1054480, 1037153, 1039292, and 1042662.

5. The patch script will set "/usr/kvm/crash" to mode 02700 owned by "root". While this is not insecure, since only "root" can run the program, CERT recommends that the setgid bit be removed to prevent abuse if world execute permission were to be added some time later.
   As "root", make "/usr/kvm/crash" not a set-group-id program.

   # chmod 755 /usr/kvm/crash

Revision History

```
September 19,1997  Attached Copyright Statement
```

4 CA-1993-04: Commodore Amiga UNIX finger Vulnerability

Original issue date: February 18, 1993
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 UPDATED INFORMATION**

The CERT Coordination Center has received information concerning a vulnerability in the "finger" program of Commodore Business Machine's Amiga UNIX product. The vulnerability affects Commodore Amiga UNIX versions 1.1, 2.03, 2.1, 2.1p1, 2.1p2, and 2.1p2a. Commodore is aware of the vulnerability, and both a workaround and a patch are available. Affected sites should apply either the workaround or the patch, and directions are provided below.

The Commodore contact e-mail address given in CERT Advisory CA-93.04 was incorrect. This revised advisory provides the correct e-mail address. If you have any further questions, contact David Miller of Commodore via e-mail at davidm@commodore.com .

I. Description

The "finger" command in Amiga UNIX contains a security vulnerability.

II. Impact

Non-privileged users can gain unauthorized access to files.

III. Solution

Commodore has suggested a workaround and a patch, as follows:

Workaround As root, modify the permission of the existing /usr/bin/finger to prevent misuse.

```
# /bin/chmod 0755 /usr/bin/finger
```

Patch

As root, install the "pubsrc" package from the distribution tape.

In the file, "/usr/src/pub/cmd/finger/src/finger.c", add the line:

```
setuid(getuid());
```

immediately before the line reading:

```
display_finger(finger_list);
```

(Optionally) save a copy of the existing /usr/bin/finger and modify its permission to prevent misuse.

```
# /bin/mv /usr/bin/finger /usr/bin/finger.orig
# /bin/chmod 0755 /usr/bin/finger.orig
```

In the directory, "/usr/src/pub/cmd/finger", issue the command:

```
# cd /usr/src/pub/cmd/finger
# make install
```

Revision History

```
September 19,1997 Attached Copyright Statement
```

5 CA-1993-05: OpenVMS and OpenVMS AXP Vulnerability

Original issue date: February 24, 1993
Last revised: September 19, 1997
Attached copyright statement

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

The CERT Coordination Center has received information concerning a potential vulnerability with Digital Equipment Corporation's OpenVMS and OpenVMS AXP. This vulnerability is present in OpenVMS V5.0 through V5.5-2 and OpenVMS AXP V1.0 but has been corrected in OpenVMS V6.0 and OpenVMS AXP V1.5. The Software Security Response Team at Digital Equipment Corporation has provided the following information concerning this vulnerability.

For additional information, please contact your local Digital Equipment Corporation customer service representative.

Beginning of Text Provided by Digital Equipment Corporation

```
23.FEB.1993

SOURCE:  Digital Equipment Corporation

AUTHOR:  Software Security Response Team, Colorado Springs USA

PRODUCT: OpenVMS V5.0 through V5.5-2 & OpenVMS AXP V1.0

PROBLEM: Potential Security Vulnerability - OpenVMS

SOLUTION: A remedial kit is now available for OpenVMS AXP V1.0 and
OpenVMS V5.0 through V5.5-2 (including all SEVMS versions V5.1
through V5.5-2 as applicable) by contacting your normal Digital Ser-
vices Support organization.

SEVERITY LEVEL: High

This potential vulnerability has been corrected in the next release
of OpenVMS V6.0 and OpenVMS AXP V1.5.  For VMS Versions prior to
OpenVMS V5.0, Digital strongly recommends that you upgrade to a
minmum of OpenVMS V5.0 and further, to the latest release of OpenVMS
V5.5-2.

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

           The remedial kits may be identified as:

                VAXSYS01_U2050   VMS V5.0, V5.0-1, V5.0-2

                VAXSYS01_U1051   VMS V5.1
```

VAXSYS01_U1052	VMS V5.2
VAXSYS01_U2053	VMS V5.3 thru V5.3-2
VAXSYS01_U3054	VMS V5.4 thru V5.4-3
VAXSYS02_U2055	OpenVMS V5.5 thru V5.5-2
AXPSYS01_010	OpenVMS AXP V1.0

ADVISORY INFORMATION:

This update kit corrects a potential security vulnerability in the OpenVMS VAX and OpenVMS AXP operating systems. This potential vulnerability may be further exploited in the form of a malicious program that may allow authorized but unprivileged users to obtain all system privileges, potentially giving the unprivileged user control of your OpenVMS system and data.

NOTE:

The update kit must be applied if an update or installation is performed for all versions prior to OpenVMS V6.0 or OpenVMS AXP V1.5. For VMS Versions prior to OpenVMS V5.0, Digital strongly recommends that you upgrade to a minimum of OpenVMS V5.0 and further to the latest release of OpenVMS V5.5-2.

INFORMATION:

Digital strongly recommends that you install the available kit on your system(s), to avoid any potential vulnerability as a result of this problem. Customers with a Digital Services contract may obtain a kit for the affected versions of OpenVMS by contacting your normal support organizations.

- In the U.S. Customers may contact the Customer Support Center at 1(800)354-9000 and request the appropriate kit for your version of OpenVMS, or through DSNlink Text Search database using the keyword text "Potential Security Vulnerability", or DSNlink VTX using the patch number 1084.

- Customers in other geographies should contact their normal Digital Services support organizations.

As always, Digital recommends you to regularly review your system management and security procedures. Digital will continue to review and enhance security features, and work with our customers to further improve the integrity of their systems.

End of Text Provided by Digital Equipment Corporation

The CERT Coordination Center wishes to thank Digital Equipment Corporation's Software Security Response Team for their response to this problem.

Revision History

September 19,1997 Attached Copyright Statement

6 CA-1993-06: wuarchive ftpd Vulnerability

Original issue date: April 9, 1993
Last revised: September 19, 1997
Attached copyright statement

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

The CERT Coordination Center has received information concerning a vulnerability in versions of wuarchive ftpd available before April 8, 1993. Vulnerable wuarchive ftpd versions were available from wuarchive.wustl.edu:/packages/ftpd.wuarchive.shar and many other anonymous FTP sites.

We strongly recommend that any site using versions of wuarchive ftpd dating prior to April 8, 1993, immediately take corrective action or remove this service.

I. Description

A vulnerability exists in the access control mechanism in this version of ftpd.

II. Impact

Anyone (remote or local) can potentially gain access to any account including root on a host running this version of ftpd.

III. Solution

Affected sites may choose to disable anonymous FTP service until they have corrected this problem.

Affected sites can correct this problem through one of the following two procedures:

A. A new version of ftpd has been released that provides new features and also fixes this security problem. Sites can obtain this new version via anonymous FTP from wuarchive.wustl.edu (128.252.135.4). The files are located in:

```
                                                 Size      Checksum
/packages/wuarchive-ftpd/wu-ftpd-2.0.shar      421953       08786
/packages/wuarchive-ftpd/wu-ftpd-2.0.tar       491520       27466
```

Make modifications to your existing wuarchive ftpd sources using the diff output provided below, recompile and install according to the instructions provided.

```
*** ftpd.c.orig
- --- ftpd.c
***************
*** 413,418 ****
- --- 413,420 ----
                end_login();
        }
```

```
+       anonymous = 0;
+
        if (!strcasecmp(name, "ftp") || !strcasecmp(name, "anony-
mous")) {
                if (checkuser("ftp") || checkuser("anonymous")) {
                        reply(530, "User %s access denied.", name);
```

The CERT Coordination Center wishes to thank Scott Paisley, Computer Systems Support Manager, Factory Automated Systems Division, N.I.S.T., for informing us of this vulnerability. We would also like to thank Chris Myers, Washington University, for his quick response to this problem.

Revision History

```
September 19, 1997  Attached Copyright Statement
```

7 CA-1993-07: Cisco Router Packet Handling Vulnerability

Original issue date: April 22, 1993
Last revised: September 19, 1997
Attached copyright statement

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

The CERT Coordination Center has received information indicating that under some circumstances Cisco routers will pass IP source routed packets which should have been denied. Routers which do not use the "no ip source-route" command are not affected. This vulnerability applies to all models of Cisco routers. This problem occurs with the following releases of software: 8.2, 8.3, 9.0, 9.1 and 9.17.

Cisco Systems and CERT recommend that sites using Cisco routers to provide firewall protection take action to eliminate this vulnerability from their networks.

This security issue is fixed in Cisco software releases 8.3(7.2), 9.0(5), 9.1(4) 9.17(2.1) and in all later releases. Customers who are using software release 8.2 must upgrade to a later release and should contact Cisco's Technical Assistance Center (TAC) at 800-553-2447 (Internet: tac@cisco.com) for more information.

Cisco recommends that customers whose routers may be affected by this vulnerability upgrade their software to the following versions:

```
Release  (Update)
  8.3      (8)
  9.0      (5)
  9.1      (4)
  9.17     (3)
```

These releases are available on Cisco's Customer Information On-Line (CIO) service for those customers having a maintenance contract. Other customers may obtain these releases through Cisco's Technical Assistance Center or by contacting their local Cisco distributor.

I. Description

A vulnerability exists in Cisco routers such that a router which is configured to suppress source routed packets with the following command:

```
no ip source-route
```

may allow traffic which should be suppressed.

II. Impact

This vulnerability can allow unauthorized traffic to pass through the router/gateway.

III. Solution

Cisco recommends that affected customers upgrade to a later version. Customers who cannot upgrade immediately may be able use access lists to prevent unauthorized traffic.

Customers who have questions should contact the Cisco Technical Assistance Center at 800-553-2447 for assistance. Internet: tac@cisco.com

---

The CERT Coordination Center wishes to thank Cisco Systems for responding to this problem.

Revision History

```
September 19,1997  Attached Copyright Statement
```

8 CA-1993-08: SCO /bin/passwd Vulnerability

Original issue date: May 24, 1993
Last revised: September 19, 1997
Attached copyright statement

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

The CERT Coordination Center and the Santa Cruz Operation, Inc., (SCO) have recently identified a potential for compromising system integrity on several releases of SCO's Operating Systems. This potential will not allow unauthorized access to a system, but it may deny legitimate users the ability to log onto the system.

The releases of SCO product that are affected are as follows:

```
      SCO UNIX System V/386 Release 3.2 Operating System Version 2.0

      SCO UNIX System V/386 Release 3.2 Operating System Version 4.0

      SCO UNIX System V/386 Release 3.2 Operating System Version 4.0
with Maintenance Supplement Version 4.1

      SCO Open Desktop Release 1.1.x

      SCO Open Desktop Release 2.0
```

Santa Cruz Operation and CERT recommend that sites using these SCO products take action to eliminate this vulnerability from their systems. This problem will be corrected in upcoming releases of SCO operating systems.

The Santa Cruz Operation has provided a Support Level Supplement (SLS), as described below. They have also provided an interim workaround until sites can obtain and install the Supplement.

If you have any questions about obtaining or installing the security supplement, contact SCO Support during normal business hours or send electronic mail to support@sco.com .

USA/Canada: 6am-5pm Pacific Daylight Time (PDT)

1-800-347-4381 (voice)
1-408-427-5443 (fax)

Pacific Rim, Asia, and Latin American customers: 6am-5pm Pacific Daylight Time (PDT)

1-408-425-4726 (voice)
1-408-427-5443 (fax)

Europe, Middle East, Africa: 9am-5:30pm British Standard Time (BST)

+44 (0)923 816344 (voice)
+44 (0)923 817781 (fax)

I. Description

A problem exists in /bin/passwd in the SCO operating system versions detailed above.

II. Impact

This vulnerability can deny legitimate users the ability to log onto the system.

III. Solution

The Santa Cruz Operation and CERT recommend that all affected sites obtain and install the Support Level Supplement. Instructions are provided below.

The Santa Cruz Operation and CERT also recommend that sites consider applying the following workaround until they are able to obtain and install the Support Level Supplement.

A. Workaround

This workaround will prevent users from changing their passwords until the Support Level Supplement is installed.

As root, modify the permission on the existing /bin/passwd to prevent misuse.

```
# /bin/chmod 2110 /bin/passwd
```

Before installing the update, the permissions should again be reset. As root, modify the permission on the existing /bin/passwd.

```
# /bin/chmod 2111 /bin/passwd
```

B. Supplement

SCO has prepared a Support Level Supplement (SLS) to address this issue. This is free to all customers, regardless of Support status. Sites can obtain this update via anonymous FTP from ftp.sco.COM (132.147.106.6). The files are located in:

Filename	File Contents	Size	Checksum
/SLS/uod368.Z	Update	105857	62288
/SLS/uod368.ltr	ASCII Cover letter and installation instructions	5514	29520

The update may also be obtained from SCO via:

- anonymous UUCP in the /usr/spool/uucppublic/SLS directory on the SOS bulletin board
- CompuServe in the SCO Unix Library Section of the SCO Forum
- hardcopy format (on diskette) from the media department at SCO Support.

To retrieve and install the SCO Support Level Supplement, you must follow the instructions below. The detailed instructions described below will not be included in future advisories.

Beginning of Text provided by SCO

```
FTP download information:

=========================

You must have a connection to the Internet to use this service, and
should be familiar with the FTP command.

The command to use is:

ftp ftp.sco.COM

      or

ftp 132.147.106.6

You will be prompted for a login and password.  Log in as "anony-
mous" and use your E-MAIL address as the password. On ftp.sco.COM
the fix and the cover letter files are in the ./SLS directory. You
will want to "cd" to this directory, set "binary", and "get" the
files uod368.Z and uod368.ltr. Note that these files are also avail-
able from UUNET via anonymous FTP at ftp.uu.net in the /sco-ar-
chive/SLS directory.

UUCP download information:

==========================

for the USA, Canadian, Pacific Rim, Asia, and Latin American custom-
ers:

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

Machine name:   sosco

UUCP user:      uusls           (no password)

Modem Phone numbers:

Telebit Trailblazer Plus      408-429-1786      9600 baud

Telebit 1500 V.32, 2@         408-425-3502      2400, 9600 baud
```

Hayes V Series 9600, 2@ 408-427-4470 9600 baud

for Europe, the Middle East, and Africa:

Machine name: scolon

UUCP user: uusls

Password: bbsuucp

Modem Phone numbers:

Dowty Trailblazer +44 (0)923 210911

The following information explains how to transfer the SLS from the machine sosco using UUCP. A similar procedure can be used for scolon, by changing the Systems file entry appropriately. This information assumes that you are using an SCO Operating System to download the files. Other systems may or may not be similar in their UUCP setup. Before attempting to transfer, you must have a modem configured to dial out from your computer. For more information on configuring a modem, see the chapter on "Adding Terminals and Modems" in the System Administrator's Guide.

Once you have your modem configured for dialing out, you must set up your UUCP configuration to recognize the SCO system which contains the files. If you have a 2400 baud or lower speed modem, add the following line to the end of the "Systems" configuration file in the directory /usr/lib/uucp:

sosco Any ACU Any 14084253502 ogin:-@-ogin:-@-ogin: uusls

or

sosco Any ACU Any 14084274470 ogin:-@-ogin:-@-ogin: uusls

If you have a Telebit brand modem, use the following line:

sosco Any ACU Any 14084291786 ogin:-@-ogin:-@-ogin: uusls

Once your system is configured, you can use the uucp(C) command to request files from the remote system. All files for Support Level Supplements reside in /usr/spool/uucppublic/SLS.

The first file that should be downloaded is "uod368.Z" (the actual fix). The uucp(C) command to transfer this file into the local directory

/usr/spool/uucppublic on your system would be:

uucp sosco!/usr/spool/uucppublic/SLS/uod368.Z /usr/spool/uucppub-
lic/uod368.Z

(If you are using the C shell command interpreter, you must enter a backslash character "\" before the exclamation mark "!" to prevent the C shell history mechanism from intercepting the rest of the command line.)

Next you would repeat the above procedure for "uod368.ltr" (the cover letter for the fix).

Obtaining a hard copy of the SLS:

==========

This SLS is available in hard copy form. Customers should order it from their Support provider or by calling SCO Support during normal business hours.

Please be sure to ask for "Support Level Supplement UOD368, the Security Supplement". This is free to all customers, regardless of Support status.

USA/Canada:

1-800-347-4381 (voice)

1-408-427-5443 (fax)

Pacific Rim, Asia, and Latin American customers:

1-408-425-4726 (voice)

1-408-427-5443 (fax)

Europe, Middle East, Africa:

+44 (0)923 816344 (voice)

+44 (0)923 817781 (fax)

Installation Preparation:

```
=========================
```

1. Uncompress the file:

```
      uncompress uod368.Z
```

2. Format a diskette that is large enough to contain the file

   using the format(C) command.

3. Use the dd(C) command to transfer the file to diskette.

```
       dd if=uod368 of=/dev/fd0135ds18  for 3.5" diskettes or

       dd if=uod368 of=/dev/fd096ds15  for 5.25" diskettes
```

Follow the directions in the uod368.ltr file to install the Supplement.

End of Text provided by SCO

Revision History

```
September 19,1997  Attached Copyright Statement
```

9 CA-1993-09: SunOS Expreserve Vulnerability

Original issue date: June 11, 1993

**** Superseded by CA-1996-19. ****

10 CA-1993-10: Anonymous FTP Activity

Original issue date: July 14, 1993
Last revised: October 8, 1997
Attached copyright statement

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

The CERT Coordination Center has been receiving a continuous stream of reports from sites that are experiencing unwanted activities within their anonymous FTP areas. We recognize that this is not a new problem, and we have been striving to handle requests for assistance on a one-to-one basis with the reporting administrator. However, since this activity does not seem to be diminishing, CERT believes that a broad distribution of information concerning this problem and corresponding solution suggestions should help to address the widespread nature of this activity.

We are seeing three types of activity regarding anonymous FTP areas.

- Improper configurations leading to system compromise.
- Excessive transfer of data causing deliberate over-filling of disk space thus leading to denial of service.
- Use of writable areas to transfer copyrighted software and other sensitive information.

This advisory provides an updated version of the anonymous FTP configuration guidelines that is available from CERT. The purpose of these guidelines is to assist system administrators at sites that offer anonymous FTP services. These guidelines are intended to aid a system administrator in configuring anonymous FTP capabilities so as to minimize unintended use of services or resources. Systems administrators should be aware that anonymous FTP capabilities should be configured and managed according to the policies established for their site.

You may obtain future copies of these guidelines through anonymous FTP from cert.org in ftp://ftp.cert.org/pub/tech_tips.

ANONYMOUS FTP CONFIGURATION GUIDELINES

Anonymous FTP can be a valuable service if correctly configured and administered. The first section of this document provides general guidance in initial configuration of an anonymous FTP area. The second section addresses the issues and challenges involved when a site wants to provide writable directories within their anonymous FTP areas. The third section provides information about previous CERT advisories related to FTP services.

The following guidelines are a set of suggested recommendations that have been beneficial to many sites. CERT recognizes that there will be sites that have unique requirements and needs, and that these sites may choose to implement different configurations.

I. Configuring anonymous FTP
A. FTP daemon

Sites should ensure that they are using the most recent version of their FTP daemon.

B. Setting up the anonymous FTP directories

The anonymous FTP root directory (~ftp) and its subdirectories should not be owned by the ftp account or be in the same group as the ftp account. This is a common configuration problem. If any of these directories are owned by ftp or are in the same group as the ftp account and are not write protected, an intruder will be able to add files (such as a .rhosts file) or modify other files. Many sites find it acceptable to use the root account. Making the ftp root directory and its subdirectories owned by root, part of the system group, and protected so that only root has write permission will help to keep your anonymous FTP service secure.

Here is an example of an anonymous FTP directory setup:

```
drwxr-xr-x  7   root    system  512 Mar 1      15:17 ./
drwxr-xr-x 25   root    system  512 Jan 4      11:30 ../
drwxr-xr-x  2   root    system  512 Dec 20     15:43 bin/
drwxr-xr-x  2   root    system  512 Mar 12     16:23 etc/
drwxr-xr-x 10   root    system  512 Jun 5      10:54 pub/
```

Files and libraries, especially those used by the FTP daemon and those in ~ftp/bin and ~ftp/etc, should have the same protections as these directories. They should not be owned by ftp or be in the same group as the ftp account; and they should be write protected.

C. Using proper password and group files

We strongly advise that sites not use the system's /etc/passwd file as the password file or the system's /etc/group as the group file in the ~ftp/etc directory. Placing these system files in the ~ftp/etc directory will permit intruders to get a copy of these files. These files are optional and are not used for access control.

We recommend that you use a dummy version of both the ~ftp/etc/passwd and ~ftp/etc/group files. These files should be owned by root. The dir command uses these dummy versions to show owner and group names of the files and directories instead of displaying arbitrary numbers.

Sites should make sure that the ~/ftp/etc/passwd file contains no account names that are the same as those in the system's /etc/passwd file. These files should include only those entries that are relevant to the FTP hierarchy or needed to show owner and group names. In addition, ensure that the password field has been cleared. The examples below show the use of asterisks (*) to clear the password field.

Below is an example of a passwd file from the anonymous FTP area on cert.org:

```
    ssphwg:*:3144:20:Site Specific Policy Handbook Working
Group::
```

```
cops:*:3271:20:COPS Distribution::

cert:*:9920:20:CERT::

tools:*:9921:20:CERT Tools::

ftp:*:9922:90:Anonymous FTP::

nist:*:9923:90:NIST Files::
```

Here is an example group file from the anonymous FTP area on cert.org:

```
cert:*:20:

ftp:*:90:
```

II. Providing writable directories in your anonymous FTP configuration

There is a risk to operating an anonymous FTP service that permits users to store files. CERT strongly recommends that sites do not automatically create a "drop off" directory unless thought has been given to the possible risks of having such a service. CERT has received many reports where these directories have been used as "drop off" directories to distribute bootlegged versions of copyrighted software or to trade information on compromised accounts and password files. CERT has also received numerous reports of files systems being maliciously filled causing denial of service problems.

This section discusses three ways to address these problems. The first is to use a modified FTP daemon. The second method is to provide restricted write capability through the use of special directories. The third method involves the use of a separate directory.

. Modified FTP daemon

If your site is planning to offer a "drop off" service, CERT suggests using a modified FTP daemon that will control access to the "drop off" directory. This is the best way to prevent unwanted use of writable areas. Some suggested modifications are:

1. Implement a policy where any file dropped off cannot be accessed until the system manager examines the file and moves it to a public directory.
2. Limit the amount of data transferred in one session.
3. Limit the overall amount of data transferred based on available disk space.
4. Increase logging to enable earlier detection of abuses.

For those interested in modifying the FTP daemon, source code is usually available from your vendor. Public domain sources are available from:

```
wuarchive.wustl.edu    ~ftp/packages/wuarchive-ftpd

ftp.uu.net             ~ftp/systems/unix/bsd-
sources/libexec/ftpd

gatekeeper.dec.com     ~ftp/pub/DEC/gwtools/ftpd.tar.Z
```

The CERT Coordination Center has not formally reviewed, evaluated, or endorsed the FTP daemons described. The decision to use the FTP daemons described is the responsibility of

each user or organization, and we encourage each organization to thoroughly evaluate these programs before installation or use.

A. Using protected directories

If your site is planning to offer a "drop off" service and is unable to modify the FTP daemon, it is possible to control access by using a maze of protected directories. This method requires prior coordination and cannot guarantee protection from unwanted use of the writable FTP area, but has been used effectively by many sites.

Protect the top level directory (~ftp/incoming) giving only execute permission to the anonymous user (chmod 751 ~ftp/incoming). This will permit the anonymous user to change directory (cd), but will not allow the user to view the contents of the directory.

```
    drwxr-x--x  4   root    system  512 Jun 11      13:29 in-
coming/
```

Create subdirectories in the ~ftp/incoming using names known only between your local users and the anonymous users that you want to have "drop off" permission. The same care used in selecting passwords should be taken in selecting these subdirectory names because the object is to choose names that cannot be easily guessed. Please do not use our example directory names of jAjwUth2 and MhaLL-iF.

```
drwxr-x-wx 10   root    system  512 Jun 11      13:54 jAjwUth2/

drwxr-x-wx 10   root    system  512 Jun 11      13:54 MhaLL-iF/
```

This will prevent the casual anonymous FTP user from writing files in your anonymous FTP file system. It is important to realize that this method does not protect a site against the result of intentional or accidental disclosure of the directory names. Once a directory name becomes public knowledge, this method provides no protection at all from unwanted use of the area. Should a name become public, a site may choose to either remove or rename the writable directory.

B. Using a single disk drive

If your site is planning to offer a "drop off" service and is unable to modify the FTP daemon, it may be desirable to limit the amount of data transferred to a single file system mounted as ~ftp/incoming.

If possible, dedicate a disk drive and mount it as ~ftp/incoming. If this dedicated disk becomes full, it will not cause a denial of service problem.

The system administrator should monitor this directory (~ftp/incoming) on a continuing basis to ensure that it is not being misused.

III. Related CERT Advisories

The following CERT Advisories directly relate to FTP daemons or impact on providing FTP service:

CA-93.06.wuarchive.ftpd.vulnerability.
CA-92.09.AIX.anonymous.ftp.vulnerability.
CA-88.01.ftpd.hole

Past advisories are available for anonymous FTP from cert.org.

Revision History

```
October 8, 1997  Attached copyright statement
```

11 CA-1993-11: UMN UNIX gopher and gopher+ Vulnerabilities

Original issue date: August 9, 1993
Last revised: September 19, 1997
Attached copyright statement

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

The CERT Coordination Center has received information concerning vulnerabilities in versions of the UMN UNIX gopher and gopher+ server and client available before August 6, 1993. Vulnerable versions were available on boombox.micro.umn.edu:/pub/gopher/Unix/gopher1.12s.tar.Z, boombox.micro.umn.edu:/pub/gopher/Unix/gopher2.03.tar.Z, and many other anonymous FTP sites mirroring these software versions.

We strongly recommend that any site using versions of UMN UNIX gopher and gopher+ dated prior to August 6, 1993 (including version 1.12, 1.12s, 2.0+, 2.03, and all earlier versions) immediately take corrective action.

If you have further questions regarding UMN UNIX gopher or gopher+ software, send e-mail to: gopher@boombox.micro.umn.edu

I. Description

Several vulnerabilities have been identified in UMN UNIX gopher and gopher+ when configured as a server or public access client.

Intruders are known to have exploited these vulnerabilities to obtain password files. Other actions may also have been taken by intruders exploiting these vulnerabilities. CERT has already contacted those sites currently known to have been victims of these activities. However, sites may want to check for weak passwords, or consider changing passwords, after installing the new gopher software.

II. Impact

Anyone (remote or local) can potentially gain unrestricted access to the account running the public access client, thereby permitting them to read any files accessible to this account (possibly including /etc/passwd or other sensitive files).

In certain configurations, anyone (remote or local) can potentially gain access to any account, including root, on a host configured as a server running gopherd.

III. Solution

Affected sites should consider disabling gopherd service and public gopher logins until they have installed the new software.

New versions of the UMN UNIX gopher and gopher+ software have been released that provide bug fixes and correct these security problems. Sites can obtain these new versions via anonymous FTP from boombox.micro.umn.edu (134.84.132.2). The files are located in:

```
Filename                                Size     Checksum
--------                                ------   -----------
Gopher:
/pub/gopher/Unix/gopher1.12S.tar.Z      306872   46311   300
Gopher+:
/pub/gopher/Unix/gopher2.04.tar.Z       294872   29411   288
```

The CERT Coordination Center wishes to thank Matt Schroth, Williams College, and others for informing us of these vulnerabilities. We would also like to thank Paul Lindner, University of Minnesota, for his quick response to these problems.

Revision History

```
September 19,1997  Attached Copyright Statement
```

12 CA-1993-12: Novell LOGIN.EXE Vulnerability

Original issue date: September 16, 1993
Last revised: September 19, 1997
Attached copyright statement

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

The CERT Coordination Center has received information concerning a security vulnerability in Novell's NetWare 4.x login program (LOGIN.EXE). This vulnerability affects NetWare 4.0 and 4.01. It does not affect NetWare 2.x, NetWare 3.x, or Netware for UNIX.

Novell is making available a security enhancement to the login program for NetWare 4.x. CERT strongly recommends that sites using of Novell NetWare 4.X replace their current LOGIN.EXE program on all affected systems with this security-enhanced version as soon as possible.

I. Description:

A security vulnerability exists in LOGIN.EXE in Novell NetWare 4.X. In some environments, a user's name and password may be temporarily written to disk.

II. Impact:

User accounts may be readily compromised.

III. Solution:

NetWare 4.x sites should obtain and install on all affected systems the security-enhanced LOGIN.EXE program. CERT strongly recommends that sites replace their current LOGIN.EXE with the security-enhanced version as soon as possible.

This new file is available via anonymous FTP from first.org. The files are located in:

```
Filename                      Size     Checksum
--------                      ------   --------------------------
/pub/software/seclog.exe      166276   00193 163 (Standard UNIX Sum)
                                       58886 325 (System V Sum)
```

This file is also available at no charge through NetWare resellers, on NetWire in library 14 of the NOVLIB forum, or by calling +1-800-NETWARE. NetWare customers outside the U.S. may call Novell at +1-303-339-7027 or +31-55-384279 or may fax a request for SECLOG.EXE v4.02 to Novell at +1-303-330-7655 or +31-55-434455. Fax requests should include company name, contact name, postal address, and phone number.

The distribution SECLOG.EXE is a self-extracting archive that contains a patched file and a text file of installation instructions. The patch file (LOGIN.EXE) and the text file (SECLOG.TXT) are created by executing the distribution file SECLOG.EXE. After extracting the files, the dir command should produce the following output:

```
SECLOG   EXE  166276    xx-xx-xx   xx:xxx

LOGIN    EXE  354859    08-25-93   11:43a

SECLOG   TXT    5299    09-02-93   11:16a
```

Note that the date and time shown for SECLOG.EXE will reflect when this file was created on your system.

To install the patch, follow the directions contained in the text file SECLOG.TXT.

After installing the patch, sites should instruct all users to change their passwords.

The CERT Coordination Center would like to thank Karyn Pichnarczyk and the contribution of CIAC to this advisory. We would also like to acknowledge Richard Colby of Chem Nuclear Geotech, Inc., for reporting this vulnerability to CIAC, and Novell for their efforts in the resolution of this vulnerability.

Revision History

```
September 19,1997   Attached Copyright Statement
```

13 CA-1993-13: SCO Home Directory Vulnerability

Original issue date: September 17, 1993
Last revised: September 19, 1997
Attached copyright statement

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

The CERT Coordination Center has received information indicating that SCO Operating Systems may be vulnerable to a potential compromise of system security. This vulnerability allows unauthorized access to the "dos" and "asg" accounts, and, as a result of this access, unauthorized access to the "root" account may also occur.

The following releases of SCO products are affected by this vulnerability:

```
SCO UNIX System V/386 Release 3.2 Operating System

SCO UNIX System V/386 Release 3.2 Operating System Version 2.0

SCO UNIX System V/386 Release 3.2 Operating System version 4.x

SCO UNIX System V/386 Release 3.2 Operating System Version 4.0
with Maintenance Supplement Version 4.1 and/or Version 4.2

SCO Network Bundle Release 4.x

SCO Open Desktop Release 1.x

SCO Open Desktop Release 2.0

SCO Open Desktop Lite Release 3.0

SCO Open Desktop Release 3.0

SCO Open Server Network System Release 3.0

SCO Open Server Enterprise System Release 3.0
```

CERT and The Santa Cruz Operation recommend that all sites using these SCO products take action to eliminate the source of vulnerability from their systems. This problem will be corrected in upcoming releases of SCO operating systems.

I. Description

The home directories of the users "dos" and "asg" are /tmp and /usr/tmp respectively. These directories are designed to have global write permission.

II. Impact

This vulnerability may allow unauthorized users to gain access to these accounts. This vulnerability may also corrupt certain binaries in the system and thus prevent regular users from running them, as well as introduce a potential for unauthorized root access.

III. Solution

All affected sites should follow these instructions:

1. Log onto the system as "root"
2. Choose the following sequence of menu selections from the System Administration Shell, which is invoked by typing "sysadmsh"

```
3. a. Accounts-->User-->Examine-->
      [select the "dos" account] -->Identity
      -->Home directory-->Create-->Path-->
      [change it to /usr/dos instead of /tmp]--> confirm
4. b. Accounts-->User-->Examine-->
      [select the "asg" account] -->Identity
      -->Home directory-->Create-->Path-->
      [change it to /usr/asg instead of /usr/tmp]--> confirm
```

5. If DOS binaries have been modified, or sites are unable to determine if modification has occurred, we strongly recommend removing and reinstalling the DOS package of the Operating System Extended Utilities. This can be done using custom(ADM).

   Sites may also want to check their systems for signs of further compromise. This can be facilitated through the use of programs such as COPS. Other security advice and suggestions can be found in CERT's security checklist. This checklist may be obtained through anonymous FTP from cert.org in pub/tech_tips/security_info.

   Note: COPS may be obtained from many sites, including via anonymous FTP from cert.org in the pub/tools directory.

If you have further questions about this issue, please contact SCO Support and ask for more information concerning this CERT advisory, CA-93.13, "SCO Home Directory Vulnerability."

Electronic mail: support@sco.COM

USA/Canada: 6am-5pm Pacific Daylight Time (PDT)

1-800-347-4381 (voice)
1-408-427-5443 (fax)

Pacific Rim, Asia, and Latin American customers: 6am-5pm Pacific (PDT)

1-408-425-4726 (voice)
1-408-427-5443 (fax)

Europe, Middle East, Africa: 9am-5:30pm British Standard Time (BST)

+44 (0)923 816344 (voice)
+44 (0)923 817781 (fax)

The CERT Coordination Center wishes to thank Christopher Durham of the Santa Cruz Operation for reporting this problem and his assistance in responding to this problem.

Revision History

```
September 19,1997   Attached Copyright Statement
```

14 CA-1993-14: Internet Security Scanner (ISS)

Original issue date: September 30, 1993
Last revised: September 19, 1997
Attached Copyright Statement
August 30, 1996 - Information previously in the README was inserted into the advisory.

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

The CERT Coordination Center has received information concerning software that allows automated scanning of TCP/IP networked computers for security vulnerabilities. This software was posted to the comp.sources.misc Usenet newsgroup. The software package, known as ISS or Internet Security Scanner, will interrogate all computers within a specified IP address range, determining the security posture of each with respect to several common system vulnerabilities. The software was designed as a security tool for system and network administrators. ISS does not attempt to gain access to a system being tested. However, given its wide distribution and ability to scan remote networks, the CERT/CC believes that it is likely ISS will also be used to locate vulnerable hosts for malicious reasons.

While none of the vulnerabilities ISS checks for are new, their aggregation into a widely available automated tool represents a higher level of threat to networked machines. The CERT/CC staff has analyzed the operation of the program and strongly recommends that administrators take this opportunity to re-examine systems for the vulnerabilities described below. Detailed below are available security tools that may assist in the detection and prevention of malicious use of ISS. Finally, common symptoms of an ISS attack are outlined to allow detection of malicious use.

Vulnerabilities probed by ISS

The following vulnerabilities are currently tested for by the ISS tool. Administrators should verify the state of their systems and perform corrective actions as indicated.

Default Accounts

The accounts "guest" and "bbs", if they exist, should have non-trivial passwords. If login access to these accounts is not needed, they should be removed, or disabled by placing a "*" in the password field and the string "/bin/false" in the shell field in /etc/passwd. See the system manual entry for "*passwd(1)*" for more information on changing passwords and disabling accounts.

For example, the /etc/passwd entry for a disabled guest account should resemble the following:

```
guest:*:2311:50:Guest
User:/home/guest:/bin/false
```

lp Account

The account "lp", if it exists, should not allow logins. It should be disabled by placing a "*" in the password field and the string "/bin/false" in the shell field in /etc/passwd.

Decode Alias

Mail aliases for decode and uudecode should be disabled on UNIX systems. If the file /etc/aliases contains entries for these programs, they should be removed, or disabled by placing a "#" at the beginning of the line and then executing the command "newaliases". Consult the manual page for "*aliases(1)*" for more information on UNIX mail aliases.

A disabled decode alias should appear as follows:

```
# decode: "|/usr/bin/uudecode"
```

Sendmail

The sendmail commands "wiz" and "debug" should be disabled. This may be verified by executing the following commands:

```
% telnet <hostname> 25

220 host Sendmail 5.65 ready at Wed, 29 Sep 93
20:28:46 EDT

wiz

You wascal wabbit!  Wandering wizards won't win!

(or 500 Command unrecognized)

quit

% telnet <hostname> 25

220 host Sendmail 5.65 ready at Wed, 29 Sep 93
20:28:46 EDT

debug

500 Command unrecognized

quit
```

If the "wiz" command returns "Please pass, oh mighty wizard", your system is vulnerable to attack. The command should be disabled by adding the following line to the sendmail.cf configuration file containing the string:

```
OW*
```

For this change to take effect, kill the sendmail process, refreeze the sendmail.cf file, and restart the sendmail process.

If the "debug" command responds with the string "200 Debug set", you should immediately obtain a newer version of sendmail software from your vendor.

Anonymous FTP

Anonymous FTP allows users without accounts to have restricted access to certain directories on the system. The availability of anonymous FTP on a given system may be determined by executing the following commands:

```
% ftp hostname

Connected to hostname.

220 host FTP server ready.

Name (localhost:jdoe): anonymous

530 User anonymous unknown.

Login failed.
```

The above results indicate that anonymous FTP is not enabled. If the system instead replies with the string "331 Guest login ok" and then prompts for a password, anonymous FTP access is enabled.

The configuration of systems allowing anonymous FTP should be checked carefully, as improperly configured FTP servers are frequently attacked. Refer to CERT Advisory CA-93.10 for more information.

NIS

ISS attempts to guess the NIS domainname. The program will try to grab the password file from ypserv.

See CERT Advisory CA-92.13 for more information regarding SunOS 4.x machines using NIS.

See CERT Advisory CA-93.01 for more information regarding HP machines using NIS.

NFS

File systems exported under NFS should be mountable only by a restricted set of hosts. The UNIX "showmount" command will display the file systems currently exported by a given host:

```
% /usr/etc/showmount -e hostname
```

```
export list for hostname:

/usr          hosta:hostb:hostc

/usr/local    (everyone)
```

The above output indicates that this NFS server is exporting two partitions: /usr, which can be mounted by hosta, hostb, and hostc; and /usr/local which can be mounted by anyone. In this case, access to the /usr/local partition should be restricted. Consult the system manual entry for "*exports(5)*" or "NFS(4P)" for more information.

rusers

The UNIX rusers command displays information about accounts currently active on a remote system. This may provide an attacker with account names or other information useful in mounting an attack. To check for the availability of rusers information on a particular machine, execute the following command:

```
% rusers -l hostname

hostname: RPC: Program not registered
```

If the above example had instead generated a list of user names and login information, a rusers server is running on the host. The server may be disabled by placing a "#" at the beginning of the appropriate line in the file /etc/inetd.conf and then sending the SIGHUP signal to the inetd process. For example, a disabled rusers entry might appear as follows:

```
#rusersd/2 dgram rpc/udp wait root /usr/etc/rus-
ersd rusersd
```

rexd

The UNIX remote execution server rexd provides only minimal authentication and is easily subverted. It should be disabled by placing a "#" at the beginning of the rexd line in the file /etc/inetd.conf and then sending the SIGHUP signal to the inetd process. The disabled entry should resemble the following:

```
#rexd/1 stream rpc/tcp wait root /usr/etc/rexd
rexd
```

See CERT Advisory CA-92.05 for more information regarding IBM AIX machines using rexd.

Available Tools

There are several available security tools that may be used to prevent or detect malicious use of ISS. They include the following:

COPS

The COPS security tool will also detect the vulnerabilities described above. It is available from ftp://info.cert.org/pub/tools/cops/1.04

ISS

Running ISS on your systems will provide you with the same information an attacker would obtain, allowing you to correct vulnerabilities before they can be exploited. Note that the current version of the software is known to function poorly on some operating systems.

ISS version 3.1 is available from
ftp://iss.net/pub/iss/iss13.tar.gz
ftp://info.cert.org/pub/tools/iss/

MD5 checksum for the files:

MD5 (iss13.tar.gz) = 1caa02756876d41a659a828dae561a92
MD5 (iss13.tar) = 793d7a12577de33ba2dac52c2126c938

TCP Wrappers

Access to most UNIX network services can be more closely controlled using software known as a TCP wrapper. The wrapper provides additional access control and flexible logging features that may assist in both the prevention and detection of network attacks. This software is available via anonymous FTP from cert.org in the directory pub/tools/tcp_wrappers.

Detecting an ISS Attack

Given the wide distribution of the ISS tool, CERT feels that remote attacks are likely to occur. Such attacks can cause system warnings to be generated that may prove useful in tracking down the source of the attack. The most probable indicator of an ISS attack is a mail message sent to "postmaster" on a scanned system similar to the following:

```
From: Mailer-Daemon@hostname (Mail Delivery Subsystem)

Subject: Returned mail: Unable to deliver mail

Message-Id: <9309291633.AB04591@>

To: Postmaster@hostname

   ----- Transcript of session follows -----

<<< VRFY guest

550 guest... User unknown

<<< VRFY decode

550 decode... User unknown
```

```
    <<< VRFY bbs
    550 bbs... User unknown
    <<< VRFY lp
    550 lp... User unknown
    <<< VRFY uudecode
    550 uudecode... User unknown
    <<< wiz
    500 Command unrecognized
    <<< debug
    500 Command unrecognized
    421 Lost input channel to remote.machine
       ----- No message was collected -----
```

According to Eric Allman, the author of sendmail, log information may be displayed differently depending on the particular configuration and version of sendmail being used.

Typically the most probable indicator of such an attack is a mail message sent to "postmaster" for the scanned system. Please note, however, that other possible indications of an ISS attack for other sendmail configurations may appear as shown below.

For sendmail 8.x, you might see output similar to the following:

```
Apr  8 03:19:17 HOSTNAME sendmail[27374]: wwww.xxx.yyy.zzz
[123.456.789.0]: VRFY decode

Apr  8 03:19:18 HOSTNAME sendmail[27375]: wwww.xxx.yyy.zzz
[123.456.789.0]: VRFY bbs

Apr  8 03:19:18 HOSTNAME sendmail[27376]: wwww.xxx.yyy.zzz
[123.456.789.0]: VRFY lp

Apr  8 03:19:18 HOSTNAME sendmail[27377]: wwww.xxx.yyy.zzz
[123.456.789.0]: VRFY uudecode

Apr  8 03:19:18 HOSTNAME sendmail[27372]: "wiz" command from
wwww.xxx.yyy.zzz [123.456.789.0]

Apr  8 03:19:18 HOSTNAME sendmail[27372]: "debug" command from
wwww.xxx.yyy.zzz [123.456.789.0]
```

Other versions may display different messages, for example:

```
Apr  8 03:19:19 HOSTNAME ftpd[27378]: FTP LOGIN REFUSED (ftp not in
/etc/passwd) FROM wwww.xxx.yyy.zzz [123.456.789.0], anonymous

Apr  8 03:19:19 HOSTNAME ftpd[27378]: USER anonymous

Apr  8 03:19:19 HOSTNAME ftpd[27378]: PASS password

Apr  8 03:19:19 HOSTNAME ftpd[27378]: reply: 503-Login with USER
first.

Apr  8 03:19:19 HOSTNAME ftpd[27378]: cmd failure - not logged in

Apr  8 03:19:19 HOSTNAME ftpd[27378]: reply: 530-Please login with
USER and PASS.

Apr  8 03:19:19 HOSTNAME ftpd[27378]: PWD

Apr  8 03:19:19 HOSTNAME ftpd[27378]: cmd failure - not logged in

Apr  8 03:19:19 HOSTNAME ftpd[27378]: reply: 530-Please login with
USER and PASS.

Apr  8 03:19:19 HOSTNAME ftpd[27378]: MKD test

Apr  8 03:19:19 HOSTNAME ftpd[27378]: cmd failure - not logged in

Apr  8 03:19:19 HOSTNAME ftpd[27378]: reply: 530-Please login with
USER and PASS.

Apr  8 03:19:19 HOSTNAME ftpd[27378]: RMD test

Apr  8 03:19:19 HOSTNAME ftpd[27378]: QUIT

Apr  8 03:19:19 HOSTNAME ftpd[27378]: reply: 221-Goodbye.
```

The CERT Coordination Center would like to thank Steve Weeber from the Department of Energy's CIAC Team for his contribution to this advisory.

Revision History

```
Sep. 19, 1997  Updated Copyright Statement

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

June 09, 1995  "Available Tools" section - gave pointers to ISS ver-
sion 3.1
```

Feb. 02, 1995 "Detecting an ISS Attack" section - added details from the sendmail author about logs

15 CA-1993-15: /usr/lib/sendmail, /bin/tar, and /dev/audio Vulnerabilities

Original issue date: October 21, 1993
Last revised: September 19, 1997
Attached copyright statement

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

The CERT Coordination Center has learned of several vulnerabilities affecting Sun Microsystems, Inc. (Sun) operating systems. Three separate vulnerabilities are described in this advisory. The first and third vulnerabilities affect all versions of SunOS 4.1.x and all versions of Solaris 2.x. The second affects all systems running any version of Solaris 2.x (but does not affect SunOS 4.1.x systems).

Patches can be obtained from local Sun Answer Centers worldwide as well as through anonymous FTP from the ftp.uu.net (192.48.96.9) system in the /systems/sun/sun-dist directory. In Europe, these patches are available from ftp.eu.net in the /sun/fixes directory.

Information concerning specific patches is outlined below. Please note that Sun sometimes updates patch files. If you find that the checksum is different, please contact Sun.

I. /usr/lib/sendmail Vulnerability

This vulnerability affects all versions of SunOS 4.1.x including 4.1.1, 4.1.2, 4.1.3, 4.1.3c, and all versions of Solaris 2.x including Solaris 2.1 (SunOS 5.1) and Solaris 2.2 (SunOS 5.2). Sun is preparing a version of this patch for Solaris 2.3 but no patch ID is available at this time.

This vulnerability is being actively exploited and we strongly recommend that sites take immediate and corrective action.

A. Description

A vulnerability exists in /usr/lib/sendmail such that remote users may gain access to affected systems.

B. Impact

Unauthorized access to affected systems may occur.

C. Solution

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

System	Patch ID	Filename	BSD Checksum	Solaris Checksum
SunOS 4.1.x	100377-07	100377-07.tar.Z	36122 586	11735 1171

```
Solaris 2.1  100840-03  100840-03.tar.Z  01153  194  39753  388
Solaris 2.2  101077-03  101077-03.tar.Z  49343  177  63311  353
```

The checksums shown above are from the BSD-based checksum (on 4.1.x, /bin/sum; on Solaris, /usr/ucb/sum) and from the SVR4 version that Sun has released with Solaris (/usr/bin/sum).

II. Solaris 2.x /bin/tar Vulnerability

This vulnerability exists in all versions of Solaris 2.x including Solaris 2.1 and Solaris 2.2. Information about patches for current versions of Solaris is described below. Sun is preparing a patch for the upcoming Solaris 2.3 release. The patch ID will be 101327-01, and it will be available as soon as Solaris 2.3 is shipped.

This vulnerability does not exist in SunOS 4.1.x systems.

A. Description

A security vulnerability exists in /bin/tar such that tarfiles created using this utility may incorporate portions of the /etc/passwd file.

B. Impact

Usernames and other information from /etc/passwd and /etc/group may be disclosed. However, since Solaris 2.x uses shadow passwords, encrypted passwords should not appear in /etc/passwd and therefore should not be disclosed by this vulnerability.

C. Solution

We recommend that all affected sites take the following steps to secure their systems.

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

```
System       Patch ID   Filename         BSD         Solaris
                                         Checksum    Checksum
------       --------   ---------------  ---------   -----------
Solaris 2.1  100975-02  100975-02.tar.Z  37034 374   13460  747
Solaris 2.2  101301-01  101301-01.tar.Z  22089 390    4703  779
```

   The checksums shown above are from the BSD-based checksum (on 4.1.x, /bin/sum; on Solaris, /usr/ucb/sum) and from the SVR4 version that Sun has released with Solaris 2.x (/usr/bin/sum).

2. If your site is not using shadow passwords, we recommend that all passwords be changed, especially those for sensitive accounts such as root.

3. Depending upon the sensitivity of the information contained in the /etc/passwd file, sites may wish to replace existing tar files where this is possible. Restoring an existing archive file, and then producing a new tarfile with the patched tar, will result in a clean archive file.

III. /dev/audio Vulnerability

This vulnerability affects all Sun systems with microphones. This includes all versions of SunOS 4.1.x including 4.1.1, 4.1.2, 4.1.3, 4.1.3c, and all versions of Solaris 2.x including Solaris 2.1 (SunOS 5.1) and Solaris 2.2 (SunOS 5.2). Sun is addressing this problem in Solaris 2.3.

A. Description

/dev/audio is set to a default mode of 666. There is also no indication to the user of the system that the microphone is on.

B. Impact

Any user with access to the system can eavesdrop on conversations held in the vicinity of the microphone.

C. Solution

To prevent unauthorized listening with the microphone, the permissions of the audio data device (/dev/audio) should allow only the user logged in on the console of the machine to read /dev/audio. To prevent unauthorized changes in playback and record settings, the permissions on /dev/audioctl should be similarly changed.

Any site seriously concerned about the security risks associated with the microphone should either switch off the microphone, or unplug the microphone to prevent unauthorized listening.

1. Restricting access on 4.x systems

   Use *fbtab(5)* to restrict the access to these devices. See the man page for more information about this procedure.

2. Restricting access on Solaris 2.x systems

   To restrict access to these devices to a specific users, the permissions on the device files must be manually changed.

   As root:

   ```
   # chmod 600 /dev/audio
   # chown <console user's username>.<desired group> /dev/audio
   # chmod 600 /dev/audioctl
   # chown <console user's username>.<desired group> /dev/audio
   ```

The CERT Coordination Center wishes to thank Paul De Bra, Department of Computing Science, Eindhoven University of Technology; David Slade of Bellcore; and Mabry Tyson of SRI for reporting these vulnerabilities, and Sun Microsystems, Inc. for their response to these problems.

Revision History

```
September 19,1997  Attached Copyright Statement
```

16 CA-1993-16: Sendmail Vulnerability

Original issue date: November 4, 1993

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

17 CA-1993-17: xterm Logging Vulnerability

Original issue date: November 11, 1993
Last revised: September 19, 1997
Attached copyright statement

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

The CERT Coordination Center is working on eliminating a vulnerability in xterm. This vulnerability potentially affects all systems running xterm with the setuid or setgid bit set. This vulnerability has been found in X Version 11, Release 5 (X11R5) and earlier versions of X11.

CERT is working with the vendor community to address this vulnerability.

I. Description

A vulnerability in the logging function of xterm exists in many versions of xterm that operate as a setuid or setgid process. The vulnerability allows local users to create files or modify any existing files.

If the setuid or setgid privilege bit is not set on the xterm program, the vulnerability cannot be exploited.

It is possible that the xterm on your system does not allow logging. In this case, the vulnerability cannot be exploited. To determine if logging is enabled, run xterm with the "-l" option. If an "XtermLog.axxxx" file is created in the current directory, xterm supports logging. You can also check the output of "xterm -help" to see whether the "-l" option is described as "not supported".

Another way to determine if logging is available is to look for the "Log to File" item in the Main Options menu (press Control mouse button 1). If the X Consortium's public patch has been installed as distributed, the option "Log to File" should not appear in the menu.

II. Impact

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

III. Solutions

All of the following solutions require that a new version of xterm be installed. When installing the new xterm, it is important either to remove the old version of xterm or to clear the setuid and setgid bits from the old xterm.

CERT suggests one of the following solutions.

A. Install vendor supplied patch if available. CERT is hopeful that patches will be forthcoming. We will be maintaining a status file, xterm-patch-status, and we will add patch availability information to this file as it becomes known. The file is available from:

http://www.cert.org/advisories/CA-1993-17/patch-status.txt

For more up-to-date information, contact the vendor.

B. If your site is using the X Consortium's X11R5, install the public patch #26. This patch is available via anonymous FTP from ftp.x.org as the file /pub/R5/fixes/fix-26. Install all patch files up to and including fix-26.

By default, the patch disables logging. If you choose to enable logging, a variation of the vulnerability still exists.

Checksum information:

```
BSD Unix Sum:  19609 47

System V Sum:  51212 94

MD5 Checksum:  e270560b6e497a0a71881d4ff4db8c05
```

C. If your site is using an earlier version of the X Consortium's X11, upgrade to X11R5. Install all patches up to and including fix-26.

D. If you are unable to upgrade to the X Consortium's X11R5, modify the xterm source code to remove the logging feature. Familiarity with X11 and its installation and configuration is recommended before implementing these modifications.

The CERT Coordination Center wishes to thank Stephen Gildea of the X Consortium for his assistance in responding to this problem.

Revision History

```
September 19,1997  Attached Copyright Statement
```

18 CA-1993-18: SunOS/Solbourne loadmodule and modload Vulnerability

Original issue date: December 15, 1993
Last revised: September 19, 1997
Attached copyright statement

A complete revision history is at the end of this file. **This advisory supersedes CA-91.22.**

The CERT Coordination Center has received information concerning a vulnerability in /usr/etc/modload and $OPENWINHOME/bin/loadmodule in Sun Microsystems, Inc. SunOS 4.1.1, 4.1.2, 4.1.3, and 4.1.3c and OpenWindows 3.0 on all sun4 and Solbourne Computer, Inc. architectures. The problem does not exist in Solaris 2.x, Solaris x86, and sun3 architectures (OpenWindows 3.0 was not released for the sun3 architecture).

Sun has produced a patch for these vulnerabilities for 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.

Solbourne has announced a workaround that is included below.

I. Description

loadmodule(8) and *modload(8)* can be exploited to execute a user's program using the effective UID of root.

II. Impact

This vulnerability allows a local user to gain root access.

III. Solution

A. SunOS Solution

Obtain and install the appropriate patches according to the instructions included with the patches.

```
Module          Patch ID        Filename
----------      ---------       ---------------
loadmodule      100448-02       100448-02.tar.Z
                BSD Checksum = 19410 5
                MD5 Checksum = 0215910cf65e055ed3042070bd961a22
modload         101200-02       101200-02.tar.Z
                BSD Checksum = 41677 28
                MD5 Checksum = 626ab2917204eb6e6eb5f165cca3e908
```

B. Solbourne Solution

Solbourne systems do not support the "loadmodule" functionality. This vulnerability can be fixed on Solbourne systems by removing the setuid bit:

```
chmod 0755 /usr/openwin/bin/loadmodule
```

The modload program does not need to replaced or changed.

The CERT Coordination Center wishes to thank Sun Microsystems, Inc. and Solbourne Computers, Inc. for their support in responding to this problem.

Revision History

```
September 19,1997  Attached Copyright Statement
```

19 CA-1993-19: Solaris System Startup Vulnerability

Original issue date: December 16, 1993
Last revised: September 19, 1997
Added Sun patch information.
Attached copyright statement

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

The CERT Coordination Center has received information concerning a vulnerability in the system startup scripts on Solaris 2.x and Solaris x86 systems. The changes described below will be integrated into the upcoming Solaris release.

I. Description

If *fsck(8)* fails during system boot, a privileged shell is run on the system console. This behavior can represent a security vulnerability if users, who would normally not have root access, have physical access to the console at boot time. An attacker can force the failure to occur.

II. Impact

This vulnerability allows anyone with physical access to the system console to gain root access.

III. Solution

A simple change to each of two system scripts can be used to close this potential security hole. The new behavior will cause the system to run the privileged shell only if the user at the console enters the correct root password.

If you wish to make the change on your own systems, edit both /sbin/rcS and /sbin/mountall, changing every occurrence of:

```
/sbin/sh < /dev/console
```

to:

```
/sbin/sulogin < /dev/console
```

As distributed by Sun, /sbin/rcS contains one occurrence of this string, at line 152; and /sbin/mountall contains two, one at line 66 and one at line 250.

Once these changes are made, sulogin will request the root password in the event *fsck(8)* fails, before starting a privileged shell. The success or failure of sulogin will be logged in /var/adm/sulog.

The CERT Coordination Center wishes to thank Sun Microsystems, Inc. for their support in responding to this problem.

UPDATES

September 19, 1997:

BUG 1124898 is fixed in Solaris 2.4

Revision History

```
Sept 19, 1997  Updates - Added Sun patch information.
               Attached copyright statement
```