Software Engineering Institute
Carnegie Mellon University

1990 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-1990-01: Sun Sendmail Vulnerability

Original issue date: January 29, 1990

Vulnerability in SunOS 3.* and 4.0.* sendmail.

**** Superseded by CA-1996-20, CA-1996-24, and CA-1996-25.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

2 CA-1990-02: Internet Intruder Warning

Original issue date: March 19, 1990
Last revised: September 17, 1997
Attached copyright statement

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

There have been a number of media reports stemming from a March 19 New York Times article entitled "Computer System Intruder Plucks Passwords and Avoids Detection." The article referred to a program that attempts to get into computers around the Internet.

At this point, the Computer Emergency Response Team Coordination Center (CERT/CC) does not have hard evidence that there is such a program. What we have seen are several persistent attempts on systems using known security vulnerabilities. All of these vulnerabilities have been previously reported. Some national news agencies have referred to a "virus" on the Internet; the information we have now indicates that this is NOT true. What we have seen and can confirm is an intruder making persistent attempts to get into Internet systems.

It is possible that a program may be discovered. However, all the techniques used in these attempts have also been used, in the past, by intruders probing systems manually.

As of the morning of March 19, we know of several systems that have been broken into and several dozen more attempts made on Thursday and Friday, March 15 and 16.

Systems administrators should be aware that many systems around the Internet may have these vulnerabilities, and intruders know how to exploit them. To avoid security breaches in the future, we recommend that all system administrators check for the kinds of problems noted in this message.

The rest of this advisory describes problems with system
configurations that we have seen intruders using. In particular, the intruders attempted to exploit problems in Berkeley BSD derived UNIX systems and have attacked DEC VMS systems. In the advisory below, points 1 through 12 deal with Unix, points 13 and 14 deal with the VMS attacks.

If you have questions about a particular problem, please get in touch with your vendor.

The CERT makes copies of past advisories available via anonymous FTP (see the end of this message). Administrators may wish to review these as well.

We've had reports of intruders attempting to exploit the following areas:

1. Use TFTP (Trivial File Transfer Protocol) to steal password files.

   To test your system for this vulnerability, connect to your system using TFTP and try "get /etc/motd". If you can do this, anyone else can get your password file as well. To avoid this problem, disable tftpd.

In conjunction with this, encourage your users to choose passwords that are difficult to guess (e.g. words that are not contained in any dictionary of words of any language; no proper nouns, including names of "famous" real or imaginary characters; no acronyms that are common to computer professionals; no simple variations of first or last names, etc.) Furthermore, inform your users not to leave any clear text username/password information in files on any system.

If an intruder can get a password file, he/she will usually take it to another machine and run password guessing programs on it. These programs involve large dictionary searches and run quickly even on slow machines. The experience of many sites is that most systems that do not put any controls on the types of passwords used probably have at least one password that can be guessed.

2. Exploit accounts without passwords or known passwords (accounts with vendor supplied default passwords are favorites).

   Also uses finger to get account names and then tries simple passwords.

   Scan your password file for extra UID 0 accounts, accounts with no password, or new entries in the password file. Always change vendor supplied default passwords when you install new system software.

3. Exploit holes in sendmail.

   Make sure you are running the latest sendmail from your vendor. BSD 5.61 fixes all known holes that the intruder is using.

4. Exploit bugs in old versions of FTP; exploit mis-configured anonymous FTP

   Make sure you are running the most recent version of FTP which is the Berkeley version 4.163 of Nov. 8 1988. Check with your vendor for information on configuration upgrades. Also check your anonymous FTP configuration. It is important to follow the instructions provided with the operating system to properly configure the files available through anonymous ftp (e.g., file permissions, ownership, group, etc.). Note especially that you should not use your system's standard password file as the password file for FTP.

5. Exploit the fingerd hole used by the Morris Internet worm.

   Make sure you're running a recent version of finger. Numerous Berkeley BSD derived versions of UNIX were vulnerable.

   Some other things to check for:

6. Check user's .rhosts files and the /etc/hosts.equiv files for systems outside your domain.

   Make sure all hosts in these files are authorized and that the files are not world-writable.

7. Examine all the files that are run by cron and at.

We've seen intruders leave back doors in files run from cron or submitted to at. These techniques can let the intruder back on the system even after you've kicked him/her off. Also, verify that all files/programs referenced (directly or indirectly) by the cron and at jobs, and the job files themselves, are not world-writable.

8. If your machine supports uucp, check the L.cmds file to see if they've added extra commands and that it is owned by root (not by uucp!) and world-readable.

   Also, the L.sys file should not be world-readable or world-writable.

9. Examine the /usr/lib/aliases (mail alias) file for unauthorized entries.

   Some alias files include an alias named "uudecode"; if this alias exists on your system, and you are not explicitly using it, then it should be removed.

10. Look for hidden files (files that start with a period and are normally not shown by ls) with odd names and/or setuid capabilities.

    These can be used to "hide" information or privileged (setuid root) programs, including /bin/sh. Names such as '.. ' (dot dot space space), '...', and .xx have been used, as have ordinary looking names such as '.mail'. Places to look include especially /tmp, /usr/tmp, and hidden directories (frequently within users' home directories).

11. Check the integrity of critical system programs such as su, login, and telnet.

    Use a known, good copy of the program, such as the original distribution media and compare it with the program you are running.

12. Older versions of systems often have security vulnerabilities that are well known to intruders.

    One of the best defenses against problems is to upgrade to the latest version of your vendor's system.

    VMS SYSTEM ATTACKS:

13. The intruder exploits system default passwords that have not been changed since installation.

    Make sure to change all default passwords when the software is installed. The intruder also guesses simple user passwords. See point 1 above for suggestions on choosing good passwords.

14. If the intruder gets into a system, often the programs loginout.exe and show.exe are modified.

    Check these programs against the files found in your distribution media.

This document is available from: http://www.cert.org/advisories/CA-1990-02.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/.

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

Revision History

September 17, 1997 Attached Copyright Statement

3 CA-1990-03: Unisys U5000 /etc/passwd problem

Original issue date: May 7, 1990
Last revised: September 17, 1997
Attached Copyright Statement

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

The CERT/CC has recently verified several reports of unauthorized access to Internet connected Unisys systems. The intruder(s) gained access to these systems by logging into vendor supplied default accounts; accounts that had not been given passwords by the systems' owners.

Gary Garb, Corporate Computer Security Officer for Unisys Corporation, states:

"The Unisys U5000 series UNIX systems are delivered with a number of system logins. The logins are NOT password protected when the customer receives the system. Unless the customer secures these logins, the system is vulnerable to unauthorized access."

"A complete list of these logins can be found in the /etc/passwd file. Each login is described by one record in /etc/passwd which contains a number of fields separated by colons. The second field normally would contain the encrypted password. The system logins will initially have a null second field (indicated by two adjacent colons) in their descriptive records in /etc/passwd."

"The U5000/80/85/90/95 System V Administration Guide, Volume 1 (UP13679) begins with a chapter on "System Identification and Security". On page 1-2 it states, "All logins should have passwords ... Logins that are not needed should be either removed (by deleting from /etc/passwd) or blocked (by locking the login as described in the section "Locking Unused Logins" on page 1-8). The Guide contains complete instructions on controlling logins and passwords."

"It is the user's (system administrator's) responsibility to thoroughly read the Guide and to ensure the security of the system. *Securing the login entries should be of the highest priority and should be accomplished before anyone else has access to the system.*"

The CERT/CC urges administrators of Unisys systems, as well as administrators of systems provided by other vendors, to check their systems and insure all accounts are protected by passwords; passwords that are different from the default passwords provided by the vendor.

Questions regarding the security aspects of Unisys systems should be directed to:

Gary Garb, Corporate Security Officer, Unisys Corporation, (215) 986-4038

This document is available from: http://www.cert.org/advisories/CA-1990-03.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/.

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

Revision History

```
September 17,1997  Attached Copyright Statement
```

4 CA-1990-04: Apollo Domain/OS suid_exec Problem

Original issue date: July 27, 1990
Last revised: September 17, 1997
Attached Copyright Statement

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

The CERT/CC has received the following report of a vulnerability in the Hewlett Packard/Apollo Domain/OS system. This information was provided to the CERT/CC by the Apollo Systems Division of Hewlett Packard:

This message is to alert administrators of Domain/OS systems of a serious security problem in all versions of Domain/OS Release sr10.2 and in Beta versions of sr10.3 earlier than bl67. This problem is NOT present in sr10.1 or earlier versions of Domain/OS. This problem can be referred to as APR number DE278, other APRs have been filed against this problem.

There is a known flaw in the file /etc/suid_exec. This file should be deleted IMMEDIATELY from the /etc directories on all HP/Apollo nodes AND from all authorized areas on HP/Apollo networks from which software can be installed.

The files that must be deleted are:

On each node:

```
//<node>/etc/suid_exec
```

In each Authorized Area:

```
<AA>/install/ri.apollo.os.v.10.2/sys5.3/etc/suid_exec

<AA>/install/ri.apollo.os.v.10.2/bsd4.3/etc/suid_exec

<AA>/install/ri.apollo.os.v.10.2.p/sys5.3/etc/suid_exec

<AA>/install/ri.apollo.os.v.10.2.p/bsd4.3/etc/suid_exec
```

You must be 'root' or 'locksmith' in order to delete these files.

The removal of these files will resolve the security vulnerability immediately.

This procedure will require that the install tool should be run with the -x option (continue on error - see Installing Software with Apollo's Release and Installation Tools, Apollo order number 008860-A00, chapter 4) for all subsequent installations until the replacement files have been obtained. The absence of these files in the authorized areas will generate an error message during the installation process, and, if the -x option is not specified when invoking the installation tool, will terminate the install.

This file is normally required by the Korn Shell to run set-id Korn Shell scripts, but is a no-op on HP/Apollo systems since Domain/OS does NOT support the execution of set-id shell scripts. Its purpose is to serve as the 'agent' described in the manual page for the Korn Shell under 'Execution'. An error during compilation introduced the reported vulnerability. The removal of this file will have no affect on the functionality provided by HP/Apollo systems, but will affect the installation procedure as mentioned in the previous paragraph.

HP/Apollo is creating an incremental software release that will replace these files with the correctly compiled version of the suid_exec program. This incremental release will be made available to software maintenance customers shortly. Those users not on a HP/Apollo maintenance contract should be able to order the replacement files as HP/Apollo part number 018669-A00, SR10.2 Incremental Software Release. Once installed, the replacement files will permit normal installation of software. They will NOT permit set-id shell scripts to be run on Domain/OS installations.

The repaired file will also be available as patch_m0170 on 68000-based systems, and patch_p0136 on DN10000-based systems. These patches are scheduled to be on the August patch tape. The problem has already been addressed in the next release of Domain/OS.

For more information, please contact Hewlett Packard/Apollo Customer Service.

Thanks to John G. Griffith of Hewlett Packard for this information.

This document is available from: http://www.cert.org/advisories/CA-1990-04.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/.

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

Revision History

```
September 17,1997  Attached Copyright Statement
```

5 CA-1990-05: SunView selection_svc vulnerability

Original issue date: August 14, 1990
Last revised: September 17, 1997
Attached copyright statement

A complete revision history is at the end of this file. Sun has recently released a patch for a security hole in SunView. This problem affects SunView running on all versions of SunOS (3.5 and before, 4.0, 4.0.1, 4.0.3, and 4.1) and all platforms (Sun3, Sun4, 386i). This vulnerability allows any remote system to read selected files from the workstation running SunView. As noted below in the IMPACT section, the files that can be read are limited.

This vulnerability is in the SunView (aka SunTools) selection_svc facility and can be exploited while SunView is in use; however, as noted below in the IMPACT section, this bug may be exploitable after the user quits using Sunview. This problem cannot be exploited while X11 is in use (unless the user runs X11 after running Sunview; see the IMPACT section). This problem is specific to Sun's SunView software; to our knowledge, this problem does NOT affect other vendor platforms or software.

Obtaining the Patch

To obtain the patch, please call your local Sun Answer Center (in the USA, it's 1-800-USA-4SUN), and ask for patch number 100085-01. You can also reference Sun Bug ID 1039576.

The patch is available for SunOS 4.0.1, 4.0.3 and SunOS 4.1, on Sun3, Sun4, and 386i architectures. Contact Sun for further details.

Impact

On Sun3 and Sun4 systems, a remote system can read any file that is readable to the user running SunView. On the 386i, a remote system can read any file on the workstation running SunView regardless of protections. Note that if root runs Sunview, all files are
potentially accessible by a remote system.

If the password file with the encrypted passwords is world readable, an intruder can take the password file and attempt to guess passwords. In the CERT/CC's experience, most systems have at least one password that can be guessed.

Sunview does not kill the selection_svc process when the user quits from Sunview. Thus, unless the process is killed, remote systems can still read files that were readable to the last user that ran Sunview. Under these circumstances, once a user has run Sunview, start using another window system (such as X11), or even logoff, but still have files accessible to remote systems. However, even though

selection_svc is not killed when Sunview exits, the patch still solves the security problem and prevents remote access.

CONTACT INFORMATION

For further questions, please contact your Sun answer center or send mail to security-features@sun.com.

Thanks to Peter Shipley for discovering, documenting, and helping resolve this problem.

This document is available from: http://www.cert.org/advisories/CA-1990-05.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/.

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

Revision History

```
September 17,1997  Attached copyright statement
```

6 CA-1990-06: NeXT's System Software

Original issue date: October 3, 1990
Last revised: September 17, 1997
Attached Copyright statement

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

This message is an update of the October 2, 1990 CERT Advisory (CA-90.06). There is one correction and an update that you need to know about.

For Problem #2 SOLUTION, the following line has been added:

```
# /etc/chmod 440 /usr/lib/NextPrinter/npd.old
```

This will disable the old printer program. An updated copy of the CERT Advisory has been included with this message.

NeXT is also making the new printer program, npd, available electronically via anonymous ftp for Internet sites. The archives sites are:

nova.cc.purdue.edu
umd5.umd.edu
cs.orst.edu

In addition, NeXT has asked the CERT to announce that if anyone cannot get it from the archives, NeXT Technical Support can provide it. Requests should go to: ask_next@NeXT.COM.

Thanks,
Computer Emergency Response Team

NeXT's System Software

This message is to alert administrators of NeXT Computers of four potentially serious security problems.

The information contained in this message has been provided by David Besemer, NeXT Computer, Inc. The following describes the four security problems, NeXT's recommended solutions and the known system impact.

Problem #1 Description

On Release 1.0 and 1.0a a script exists in /usr/etc/restore0.9 that is a setuid shell script. The existence of this script is a potential security problem.

Problem #1 Impact

The script is only needed during the installation process and isn't needed for normal usage. It is possible for any logged in user to gain root access.

Problem #1 Solution

NeXT owners running Release 1.0 or 1.0a should remove /usr/etc/restore0.9 from all disks. This file is installed by the "BuildDisk" application, so it should be removed from all systems built with the standard release disk, as well as from the standard release disk itself (which will prevent the file from being installed on system built with the standard release disk in the future). You must be root to remove this script, and the command that will remove the script is the following:

```
# /bin/rm /usr/etc/restore0.9
```

Problem #2 Description

On NeXT computers running Release 1.0 or 1.0a that also have publicly accessible printers, users can gain extra permissions via a combination of bugs.

Problem #2 Impact

Computer intruders are able to exploit this security problem to gain access to the system. Intruders, local users and remote users are able to gain root access.

Problem #2 Solution

NeXT computer owners running Release 1.0 or 1.0a should do two things to fix a potential security problem. First, the binary /usr/lib/NextPrinter/npd must be replaced with a more secure version. This more secure version of npd is available through your NeXT support center. Upon receiving a copy of the more secure npd, you must become root and install it in place of the old one in /usr/lib/NextPrinter/npd. The new npd binary needs to be installed with the same permission bits (6755) and owner (root) as the old npd binary. The commands to install the new npd binary are the following:

```
# /bin/mv /usr/lib/NextPrinter/npd /usr/lib/NextPrinter/npd.old

# /bin/mv newnpd /usr/lib/NextPrinter/npd
```

(In the above command, "newnpd" is the npd binary that you obtained from your NeXT support center.)

```
# /etc/chown root /usr/lib/NextPrinter/npd

# /etc/chmod 6755 /usr/lib/NextPrinter/npd

# /etc/chmod 440 /usr/lib/NextPrinter/npd.old
```

The second half of the fix to this potential problem is to change the permissions of directories on the system that are currently owned and able to be written by group "wheel". The command that will remove write permission for directories owned and writable by group "wheel" is below. This command is all one line, and should be run as root.

```
# find / -group wheel ! -type l -perm -20 ! -perm -2 -ls -exec chmod

g-w {} \; -o -fstype nfs -prune
```

Problem #3 Description

On NeXT computers running any release of the system software, public access to the window server may be a potential security problem.

The default in Release 1.0 or 1.0a is correctly set so that public access to the window server is not available. It is possible, when upgrading from a prior release, that the old configuration files will be reused. These old configuration files could possibly enable public access to the window server.

Problem #3 Impact

This security problem will enable an intruder to gain access to the system.

Problem #3 Solution

If public access isn't needed, it should be disabled.

1. Launch the Preferences application, which is located in /NextApps
2. Select the UNIX panel by pressing the button with the UNIX certificate on it.
3. If the box next to Public Window Server contains a check, click on the box to remove the check.

Problem #4 Description

On NeXT computers running any release of the system software, the "BuildDisk" application is executable by all users.

Problem #4 Impact

Allows a user to gain root access.

Problem #4 Solution

Change the permissions on the "BuildDisk" application allowing only root to execute it. This can be accomplished with the command:

```
# chmod 4700 /NextApps/BuildDisk
```

To remove "BuildDisk" from the default icon dock for new users, do the following:

1. Create a new user account using the UserManager application.
2. Log into the machine as that new user.
3. Remove the BuildDisk application from the Application Dock by dragging it out.
4. Log out of the new account and log back in as root.
5. Copy the file in ~newuser/.NeXT/.dock to /usr/template/user/.NeXT/.dock

   (where ~newuser is the home directory of the new user account)

6. Set the protections appropriately using the following command:

   ```
   # chmod 555 /usr/template/user/.NeXT/.dock
   ```

7. If you wish, with UserManager, remove the user account that you created in step 1.

In release 2.0, the BuildDisk application will prompt for the root password if it is run by a normal user. CONTACT INFORMATION

For further questions, please contact your NeXT support center.

NeXT has also reported that these potential problems have been fixed in NeXT's Release 2.0, which will be available in November, 1990.

Thanks to Corey Satten and Scott Dickson for discovering, documenting, and helping resolve these problems.

This document is available from: http://www.cert.org/advisories/CA-1990-06.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/.

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

Revision History

```
September 17,1997 Attached Copyright statement
```

7 CA-1990-07: VMS ANALYZE/PROCESS_DUMP

Original issue date: October 25, 1990
Last revised: September 17, 1997
Attached Copyright Statement

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

The CERT/CC has received a report of a security vulnerability which exists under specific conditions in Digital VMS Software (Versions 4.0 to 5.4). The DESCRIPTION, IMPACT, SOLUTION, and CONTACT INFORMATION sections below have been provided to the CERT/CC by the Digital Equipment Corporation.

I. Description

Non-privileged users can acquire system privileges through the ANALYZE/PROCESS_DUMP routine.

II. Impact

Non-privileged users who gain increased privileges might deliberately or inadvertently affect the integrity of system information and/or affect the integrity of the computing resource.

III. Solution

Digital is currently working on a permanent solution to this problem. While a permanent fix is being completed, Digital recommends that the following actions be taken on every VMS system (this includes all nodes in a VAXcluster system).

After taking the following actions, non-privileged users will not be able to use the ANALYZE/PROCESS_DUMP command.

1. Log into the system account.
2. $ SET PROC/PRIV=ALL
3. a) For VMS versions prior to V5.0,

   Modify SYS$MANAGER:SYSTARTUP.COM to include the following lines:

```
$ SET NOON

    $ MCR INSTALL ANALIMDMP.EXE/DELETE
```

   as the first two commands in this file.

   b) For VMS versions V5.0 and later,

   Modify SYS$MANAGER:SYSTARTUP_V5.COM to include the following lines:

```
$ SET NOON

    $ MCR INSTALL ANALIMDMP.EXE/DELETE
```

as the first two commands in this file.

c) For MicroVMS systems,

The image ANALIMDMP.EXE is not installed by default, but SYSTARTUP.COM contains a suggestion for installing the image if you have multiple users on your system. You must ensure that this image is not installed by SYSTARTUP.COM. You can use the following command to verify that the image is not installed:

```
$ MCR INSTALL ANALIMDMP/LIST

$ MCR INSTALL ANALIMDMP/DELETE
```

This command removes the installed image from the active system.

4. **(Optional) Restart your systems and verify that the image is not installed using the following command:**

```
$ MCR INSTALL ANALIMDMP/LIST
```

You should receive a message similar to the following:

```
%INSTALL-W-FAIL, failed to LIST entry for ANALIMDMP.EXE

    -INSTALL-E-NOKFEFND, Known File Entry not found
```

For further questions, please contact your Digital Customer Support Center.

The CERT/CC thanks Digital for the information above, and thanks Clive Walmsley, Royal Signal and Radar Establishment, Malvern England, for reporting this problem to CERT/CC.

This document is available from: http://www.cert.org/advisories/CA-1990-07.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/.

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

Revision History

```
September 17,1997  Attached Copyright Statement
```

8 CA-1990-08: IRIX 3.3 and 3.31 /usr/sbin/Mail

Original issue date: October 31, 1990
Last revised: September 17, 1997
Attached Copyright statement

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

The CERT/CC has received the following report of a vulnerability in /usr/sbin/Mail, present only in IRIX 3.3 and 3.3.1. This information was provided to the CERT/CC by Robert Stephens, of Silicon Graphics Inc.

I. Description

/usr/sbin/Mail can fail to reset its group id to the group id of the caller.

II. Impact

Can allow any user logged onto the system to read any other user's (including root's) mail.

III. Solution

A fixed /usr/sbin/Mail binary has been made available for anonymous ftp from SGI.COM ([192.48.153.1]). The correct binary can be found at:

sgi/Mail/Mail

under the ftp directory.

Note that this binary must be installed with the same group (mail) and permissions (2755) as your existing 3.3 or 3.3.1 /usr/sbin/Mail.

For further questions, please contact your Silicon Graphics support center (Geometry Partners HOTLINE number: (800) 345-0222)

This document is available from: http://www.cert.org/advisories/CA-1990-08.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/.

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

Revision History

```
September 17,1997  Attached Copyright Statement
```

9 CA-1990-09: VAX/VMS Break-ins

Original issue date: November 8, 1990
Last revised: September 17, 1997
Attached copyright statement

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

I. Description

Several VAX/VMS systems are presently being subjected to intrusions by a persistent intruder(s). The intruder utilizes DECnet, TCP/IP, and/or X25 access paths to gain unauthorized entry into accounts (privileged and non-privileged). Once a privileged account is breached, the intruder disables auditing & accounting and installs a trojan horse image on the system. In the most recent attacks, the intruder has installed the image VMSCRTL.EXE in SYS$LIBRARY. (Note that VMSCRTL.EXE is not a vendor-supplied filename.) The command procedure DECW$INSTALL_LAT.COM is placed in SYS$STARTUP and installs the image. Note that these images and command files are sufficiently camouflaged so as to appear to be valid VMS system files, even upon close inspection.

There is no evidence that the intruder is exploiting any system vulnerability to gain access to the affected systems. The intruder uses valid username/password combinations to gain access to accounts. The intruder most likely obtains these username/password combinations by systematically searching through text files on the user disks of penetrated systems for clear-text username/password pairs. These username/password combinations are often valid on remote systems, which allows the intruder to access them as well. Once a privileged account is accessed, the intruder will use the AUTHORIZE utility to detect and exploit dormant accounts (especially dormant privileged accounts). The intruder has also assigned privileges to dormant non-privileged accounts.

II. Impact

Unauthorized users who gain privileged and/or non-privileged system access might deliberately or inadvertently affect the integrity of system information and/or affect the integrity of the computing resource.

III. Solution

The following steps are recommended for detecting whether systems at your site have been compromised:

1. Search for SYS$LIBRARY:VMSCRTL.EXE and SYS$STARTUP:DECW$INSTALL.COM.

   (This can be done with the following DCL command: $ DIR device:[*...]/SINCE=date /MODIFIED). Note that to call the command procedure which installs the image, the intruder

will utilize SYSMAN to modify SYS$STARTUP:VMS$LAYERED.DAT. Thus, there will be an unexplained modification to SYS$STARTUP:VMS$LAYERED.DAT. This may be the surest indication of an intrusion, since the intruder could easily change the names and locations of the trojan horse image and its accompanying command procedure.

2. If you discover that auditing or accounting has been disabled for a period of time

   Go into AUTHORIZE and ensure that no password or other changes were made during that time. Password changes while auditing and accounting have been disabled may indicate unauthorized access into your system.

The following pre-emptive actions are suggested:

1. DISUSER all dormant accounts, especially dormant privileged accounts.
2. Advise all users of the security problems inherent in placing username/password combinations in text files. Consider searching your user disks for such occurrences.
3. Change all vendor-supplied default passwords (e.g., MAILER, DECNET, SYSTEM) and make sure all passwords are difficult to guess.
4. Make sure that all privileged users have only the minimum privileges that are REQUIRED to perform their current tasks.
5. Closely monitor all relevant audit trails.

This document is available from: http://www.cert.org/advisories/CA-1990-09.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/.

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

Revision History

```
September 17,1997 Attached copyright statement
```

10 CA-1990-10: Rumor of Alleged Attack

Original issue date: November 16, 1990
Last revised: September 17, 1997
Attached copyright statement

A complete revision history is at the end of this file. There have been several recent reports in the media and other places about an alleged attack on some telephone systems, apparently in response to the sentencing today in Atlanta of three members of a computer intruder group called "Legion of Doom". As of this time (Nov. 16 at 4:30 PM EST), CERT/CC has not received any evidence to substantiate this rumor.

Caution (not panic) is advisable.

This document is available from: http://www.cert.org/advisories/CA-1990-10.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/.

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

Revision History

```
September 17,1997  Attached copyright statement
```

11 CA-1990-11: Security Probes from Italy

Original issue date: December 10, 1990
Last revised: September 17, 1997
Attached copyright statement

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

Many sites on the Internet received messages from "miners@ghost.unimi.it " (131.175.10.64) on Sunday, December 9. The messages stated that "miners" is a group of researchers and students in the computer science department at the state university of Milano in Italy; a group testing for a "common bug" in network hosts. In addition to the messages, a number of sites detected probes from the unimi.it domain. Later today, a number of individuals received a follow up message from "postmaster@ghost.unimi.it " explaining the activities.

We have received reports that this activity has now stopped, and an unofficial explanation has been provided by several administrators at the University of Milano. The rest of this message describes the sequence of events and the security holes that were probed.

Following the original messages from miners@ghost and postmaster@ghost, another message was sent on the afternoon of December 10th from several administrators at the University of Milano. They stated that the authorities at the University had been informed and that the attempts had stopped. They also noted that they had not been informed of the tests in advance.

The administrators at the University of Milano have sent us a copy of the scripts that were used to probe the Internet sites. These scripts checked for the existence of the sendmail WIZ and DEBUG commands, and attempted to get /etc/motd and/or /etc/passwd via TFTP and by exploiting an old vulnerability in anonymous FTP. The scripts also attempted to rsh to a site and try to cat /etc/passwd. Finally, the scripts mailed to root at each site they tested with the message from "miners@ghost.unimi.it ".

The administrators at the University of Milano state that the group that did this was doing this to discover which (if any) sites might have had these security flaws, and then to let the sites know about these vulnerabilities. They have stated that they still intend to inform sites that have these vulnerabilities.

To our knowledge, no site was actually broken into (as of December 10, 1990). Nonetheless, CERT* does not condone this type of activity.

Most of the information in this advisory is based on information given to us via e-mail from individuals at the University of Milano. We have not yet been able to check this information with any officials at the University; if we learn of any other significant information, we will update this advisory.

This document is available from: http://www.cert.org/advisories/CA-1990-11.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/.

Conditions for use, disclaimers, and sponsorship information

Revision History

```
September 17,1997  Attached Copyright statement
```

12 CA-1990-12: SunOS TIOCCONS Vulnerability

Original issue date: December 20, 1990
Last revised: September 17, 1997
Attached copyright statement

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

The following information was sent to us from Sun Microsystems. It contains availability information regarding a fix for a vulnerability in SunOS 4.1 and SunOS 4.1.1. (A version for SunOS 4.0.3 is currently in testing and should be available shortly.) For more information, please contact Sun Microsystems at 1-800-USA-4SUN.

Sun Microsystems Security Bulletin

This information is only to be used for the purpose of alerting customers to problems. Any other use or re-broadcast of this information without the express written consent of Sun Microsystems shall be prohibited.

Sun expressly disclaims all liability for any misuse of this information by any third party.

These patches are available through your local Sun answer centers worldwide. As well as through anonymous ftp to ftp.uu.net in the ~ftp/sun-dist directory.

Please refer to the BugID and PatchID when requesting patches from Sun answer centers.

NO README information will be posted in the patch on UUNET. Please refer the the information below for patch installation instructions.

```
Sun Bug ID   : 1008324

Synopsis     : TIOCCONS redirection of console input/output is a security

               violation.

Sun Patch ID : for SunOS 4.1, SunOS 4.1_PSR_A 100187-01

Sun Patch ID : for SunOS 4.1.1 100188-01

Available for: Sun3, Sun3x, Sun4 Sun4c

               SunOS 4.1, SunOS 4.1_PSR_A, SunOS 4.1.1
```

Checksum of compressed tarfile on ftp.uu.net:~ftp/sun-dist

```
sum of SunOS 4.1 tarfile 100187-01.tar.Z  : 14138   142

sum of SunOS 4.1.1 tarfile 100188-01.tar.Z: 24122   111
```

README information follows:

Patch-ID# 100188-01
Keywords: TIOCCONS
Synopsis: SunOS 4.1.1: TIOCCONS redirection of console is a security violation.
Date: 17/Dec/90

SunOS release: 4.1.1

Unbundled Product:

Unbundled Release:

Topic:

BugId's fixed with this patch: 1008324

Architectures for which this patch is available: sun3 sun3x sun4 sun4c

Patches which may conflict with this patch:

Obsoleted by: Next major release of SunOS

Problem Description: TIOCCONS can be used to re-direct console output/input away from "console"

Patch contains kernel object modules for:

`/sys/sun?/OBJ/cons.o`

`/sys/sun?/OBJ/zs_async.o`

`/sys/sun?/OBJ/mcp_async.o`

`/sys/sun?/OBJ/mti.o`

Where sun? is one of sun4, sun4c, sun3, sun3x, sun4/490-4.1_PSR_A

NOTE: The sun4c does not use mti.o nor mcp_async.o since this architecture does not have VME slots and therefore cannot use the ALM-2 Asynchronous Line Multiplexor or Systech MTI-800/1600. So those modules are not needed.

The fix consists of adding permission checking to setcons, the routine that does the work of console redirection, and changing its callers to supply additional information required for the check and to see whether or not the check succeeded. Setcons now uses uid and gid information supplied to it as new arguments to perform a VOP_ACCESS call for VREAD permission on the console. If the caller doesn't have permission to read from the console, setcons rejects the redirection attempt.

Install

As Root:

save aside the object modules from the FCS tapes as a precaution:

```
# mv /sys/sun?/OBJ/cons.o /sys/sun?/OBJ/cons.o.orig

# mv /sys/sun?/OBJ/tty_pty.o /sys/sun?/OBJ/tty_pty.o.orig

# mv /sys/sun?/OBJ/zs_async.o /sys/sun?/OBJ/zs_async.o.orig

# mv /sys/sun?/OBJ/mcp_async.o /sys/sun?/OBJ/mcp_async.o.orig

# mv /sys/sun?/OBJ/mti.o /sys/sun?/OBJ/mti.o.orig
```

copy the new ".o" files to the OBJ directory:

```
# cp sun?/*.o /sys/sun?/OBJ/
```

build and install a new kernel:

```
rerun /etc/config <kernel-name> and do a "make" for the new kernel
```

Please refer to the System and Network Administration Manual for details on how to configure and install a custom kernel.

Patch-ID# 100187-01
Keywords: TIOCCONS
Synopsis: SunOS 4.1 4.1_PSR_A: TIOCCONS redirection of console is a security violation.
Date: 17/Dec/90

SunOS release: 4.1 4.1_PSR_A

Unbundled Product:

Unbundled Release:

Topic:

BugId's fixed with this patch: 1008324

Architectures for which this patch is available: sun3 sun3x sun4 sun4c sun4-490_4.1_PSR_A

Patches which may conflict with this patch:

Obsoleted by: Next major release of SunOS

Problem Description

TIOCCONS can be used to re-direct console output/input away from "console"

Patch contains kernel object modules for:

```
/sys/sun?/OBJ/cons.o

/sys/sun?/OBJ/zs_async.o

/sys/sun?/OBJ/mcp_async.o

/sys/sun?/OBJ/mti.o
```

Where sun? is one of sun4, sun4c, sun3, sun3x, sun4/490-4.1_PSR_ABR

NOTE: The sun4c does not use mti.o nor mcp_async.o since this architecture does not have VME slots and therefore cannot use the ALM-2 Asynchronous Line Multiplexed or Systech MTI-800/1600. So those modules are not needed.

The fix consists of adding permission checking to setcons, the routine that does the work of console redirection, and changing its callers to supply additional information required for the check and to see whether or not the check succeeded. Setcons now uses uid and gid information supplied to it as new arguments to perform a VOP_ACCESS call for VREAD permission on the console. If the caller doesn't have permission to read from the console, setcons rejects the redirection attempt.

Install

As Root:

Save aside the object modules from the FCS tapes as a precaution:

```
# mv /sys/sun?/OBJ/cons.o /sys/sun?/OBJ/cons.o.orig

# mv /sys/sun?/OBJ/tty_pty.o /sys/sun?/OBJ/tty_pty.o.orig

# mv /sys/sun?/OBJ/zs_async.o /sys/sun?/OBJ/zs_async.o.orig

# mv /sys/sun?/OBJ/mcp_async.o /sys/sun?/OBJ/mcp_async.o.orig

# mv /sys/sun?/OBJ/mti.o /sys/sun?/OBJ/mti.o.orig
```

copy the new ".o" files to the OBJ directory:

```
# cp sun?/*.o /sys/sun?/OBJ/
```

Build and install a new kernel: rerun /etc/config <kernel-name> and do a "make" for the new kernel

Please refer to the System and Network Administration Manual for details on how to configure and install a custom kernel.

This document is available from: http://www.cert.org/advisories/CA-1990-12.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/.

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

Conditions for use, disclaimers, and sponsorship information

Revision History

```
September 17, 1997  Attacced copyright statement
```