Software Engineering Institute
Carnegie Mellon University

1991 CERT Advisories

CERT Division

http://www.sei.cmu.edu

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

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

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

This report was prepared for the

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

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

DM17-0052

Table of Contents

1 CA-1991-01: SunOS Mail Vulnerability

Original issue date: February 22, 1991

**** Superseded by CA-1995-02. ****

2 CA-1991-02: SunOS in.telnetd Vulnerability

Original issue date: March 27, 1991
Last revised: September 18, 1997
Attached copyright statement

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

*** THIS IS A REVISED CERT ADVISORY ***

*** CONTAINS NEW INFORMATION AND A CORRECTION ***

I. Description

The Computer Emergency Response Team/Coordination Center (CERT/CC) has obtained information from Sun Microsystems, Inc. regarding a vulnerability affecting SunOS 4.1 and 4.1.1 versions of in.telnetd on all Sun 3 and Sun 4 architectures. This vulnerability also affects SunOS 4.0.3 versions of both in.telnetd and in.rlogind on all Sun3 and Sun 4 architectures. To our knowledge, a vulnerability does not exist in the SunOS 4.1 and 4.1.1 versions of in.rlogind. The vulnerability has been fixed by Sun Microsystems, Inc.

This advisory has been revised to include information on the new patches available for SunOS 4.0.3. The CERT would also like to mention that the name of the compressed tarfile included in the previous CERT Advisory, CA-91:02, was incorrect. It was listed as 1001125-02.tar.Z and it should have been 100125-02.tar.Z. We regret any inconvenience this may have caused.

Please be aware that the new compressed tarfile provided by Sun Microsystems, Inc. includes all of the patched files for SunOS 4.0.3, SunOS 4.1, and SunOS 4.1.1. That is, the tarfile contains the new patches for SunOS 4.0.3 as well as those files previously distributed in the 100125-02.tar.Z tarfile. The installation of the patch differs between SunOS 4.0.3 and SunOS 4.1.x.

II. Impact

The vulnerability allows a user on the system to gain unauthorized access to other accounts, including root.

III. Solution for SunOS 4.0.3 and 4.0.3c

Sun Microsystems, Inc. has patched versions of in.telnetd and in.rlogind available for SunOS 4.0.3 on all Sun 3 and Sun 4 architectures. The Sun Patch ID is 100125-03 which is needed when ordering the patch from a Sun Answer Center. In the US, telephone (800) USA-4SUN. The checksum of the compressed tarfile (filename 100125-03.tar.Z) is 17128 102. The compressed tarfile is available by anonymous FTP on uunet.uu.net (192.48.96.2) in sun-dist/100125-03.tar.Z.

Please note: This compressed tarfile also includes patched versions of in.telnetd for SunOS 4.1 and 4.1.1. Please disregard these files.

SunOS 4.0.3 patch installation instructions are as follows:

```
# mv /usr/etc/in.telnetd /usr/etc/in.telnetd.FCS
# mv /usr/etc/in.rlogind /usr/etc/in.rlogind.FCS
# chmod 600 /usr/etc/in.telnetd.FCS
# chmod 600 /usr/etc/in.rlogind.FCS
```

(These four steps store the old versions as a precaution and change the file modes so that the old versions cannot be executed. After verifying the new versions, the old versions should be removed.)

```
# cp sun{3,3x,4,4c}/{4.0.3,4.0.3c}/in.telnetd /usr/etc/in.telnetd
# cp sun{3,3x,4,4c}/{4.0.3,4.0.3c}/in.rlogind /usr/etc/in.rlogind
```

(Be sure to copy the appropriate versions for your architecture.)

```
# chmod 711 /usr/etc/in.telnetd
# chmod 711 /usr/etc/in.rlogind
# chown root /usr/etc/in.telnetd
# chown root /usr/etc/in.rlogind
# chgrp staff /usr/etc/in.telnetd
# chgrp staff /usr/etc/in.rlogind
# kill {any executing in.telnetd and in.rlogind process(es) (SEE
NOTE)}
```

NOTE: Be careful in killing existing in.telnetd and in.rlogind processes, as they may be legitimate users attempting to login to the system.

IV. Solution for SunOS 4.1 and 4.1.1

Sun Microsystems, Inc. has patched versions of in.telnetd available for SunOS 4.1 and 4.1.1 on all Sun 3 and Sun 4 architectures. The Sun Patch ID is 100125-03 which is needed when ordering the patch from a Sun Answer Center. In the US, telephone (800) USA-4SUN. The checksum of the compressed tarfile (filename 100125-03.tar.Z) is 17128 102. The compressed tarfile is available by anonymous FTP on uunet.uu.net (192.48.96.2) in sun-dist/100125-03.tar.Z. Please note: This tarfile includes patched versions of in.telnetd and in.rlogind for SunOS 4.0.3. Please disregard these files.

Patch installation instructions are as follows:

```
# mv /usr/etc/in.telnetd /usr/etc/in.telnetd.FCS
# chmod 600 /usr/etc/in.telnetd.FCS
```

(These two steps store the old version as a precaution and change the file mode to that the old version cannot be executed; after verifying the new version, the old version should be removed.)

```
# cp sun{3,3x,4,4c}/4.1/in.telnetd /usr/etc/in.telnetd
```

(Be sure to copy the appropriate version for your architecture.)

```
# chmod 711 /usr/etc/in.telnetd
# chown root /usr/etc/in.telnetd
# chgrp staff /usr/etc/in.telnetd
# kill {any executing in.telnetd process(es) (SEE NOTE)}
```

NOTE: Be careful in killing existing in.telnetd processes, as they may be legitimate users attempting to login to the system.

This document is available from: http://www.cert.org/advisories/CA-1991-02.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.

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

Conditions for use, disclaimers, and sponsorship information

Revision History

```
September 18,1997  Attached Copyright Statement
```

3 CA-1991-03: Unauthorized Password Change Requests Via Mail Messages

Original issue date: April 4, 1991
Last revised: September 18, 1997
Attached copyright statement

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

I. Description

The Computer Emergency Response Team/Coordination Center (CERT/CC) has received a number of incident reports concerning the receipt of mail instructing the user to immediately change his/her password. The user is further instructed to change the password to one that is specified in the mail message.

These mail messages can be made to look as if they have been sent from a site administrator or root. In reality, they may have been sent by an individual at a remote site, who is trying to gain access to the local machine via the user's account.

Several variations of these mail messages are circulating via the Internet community. We are including one such example at the end of this advisory.

II. Impact

An intruder can gain access to a system through the unauthorized use of the (possibly privileged) accounts whose passwords have been changed.

II. Solution

The CERT/CC recommends the following actions:

1. Any user receiving such a message should verify its authenticity with his/her system administrator before acting on the instructions within the mail message. If a user has changed his/her password per the instructions, he/she should immediately change it again to a secure password and alert his/her system administrator.
2. System administrators should check with their user communities to ensure that no user has changed his/her password in response to one of these mail messages. If this has occurred, immediately have the password changed again. Further, the system should be carefully examined for damage, or changes that may have been caused by the intruder. We also ask that you please contact the CERT/CC.
3. The CERT/CC recommends that system administrators NEVER mail such a request to a user. That is, NEVER send a request for a password change to a user and also specify the new password that should be used.

SAMPLE MAIL MESSAGE as received by the CERT (including spelling errors, etc.)

```
:
{mail header which may or may not be local}
:
This is the system administration:
Because of security faults, we request that you change your password
to "systest001". This change is MANDATORY and should be done
IMMEDIATLY. You can make this change by typing "passwd" at the shell
prompt. Then, follow the directions from there on.
Again, this change should be done IMMEDIATLY. We will inform you
when to change your password back to normal, which should not be
longer than ten minutes.
Thank you for your cooperation,
The system administration (root)
```

END OF SAMPLE MAIL MESSAGE

This document is available from: http://www.cert.org/advisories/CA-1991-03.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.

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

Conditions for use, disclaimers, and sponsorship information

Revision History

```
September 18,1997  Attached Copyright Statement
```

4 CA-1991-04: Social Engineering

Original issue date: April 18, 1991
Last revised: September 18, 1997
Attached copyright statement

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

I. Description

The Computer Emergency Response Team/Coordination Center (CERT/CC) has received several incident reports concerning users receiving requests to take an action that results in the capturing of their password. The request could come in the form of an e-mail message, a broadcast, or a telephone call. The latest ploy instructs the user to run a "test" program, previously installed by the intruder, which will prompt the user for his or her password. When the user executes the program, the user's name and password are e-mailed to a remote site. We are including an example message at the end of this advisory.

These messages can appear to be from a site administrator or root. In reality, they may have been sent by an individual at a remote site, who is trying to gain access or additional access to the local machine via the user's account.

While this advisory may seem very trivial to some experienced users, the fact remains that MANY users have fallen for these tricks (refer to CERT Advisory CA-91.03).

II. Impact

An intruder can gain access to a system through the unauthorized use of the (possibly privileged) accounts whose passwords have been compromised. This problem could affect all systems, not just UNIX systems or systems on the Internet.

III. Solution

The CERT/CC recommends the following actions:

1. Any users receiving such a request should verify its authenticity with their system administrator before acting on the instructions within the message. If a user has received this type of request and actually entered a password, he/she should immediately change his/her password to a new one and alert the system administrator.
2. System administrators should check with their user communities to ensure that no user has followed the instructions in such a message. Further, the system should be carefully examined for damage or changes that the intruder may have caused. We also ask that you contact the CERT/CC.

3. The CERT/CC urges system administrators to educate their users so that they will not fall prey to such tricks.

SAMPLE MESSAGE as received by the CERT (including spelling errors, etc.)

```
OmniCore is experimenting in online - high resolution graphics dis-
play on the UNIX BSD 4.3 system and it's derivitaves. But, we need
you're help in testing our new product - TurboTetris. So, if you are
not to busy, please try out the ttetris game in your machine's /tmp
directory. just type:

/tmp/ttetris

Because of the graphics handling and screen-reinitialazation, you
will be prompted to log on again. Please do so, and use your real
password. Thanks you for your support. You'll be hearing from us
soon!
OmniCore
```

END OF SAMPLE MESSAGE

This document is available from: http://www.cert.org/advisories/CA-1991-04.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.

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

Conditions for use, disclaimers, and sponsorship information

Revision History

```
September 18,1997  Attached Copyright Statement
```

5 CA-1991-05: DEC Ultrix Vulnerability

Original issue date: May 1, 1991
Last revised: September 18, 1997
Attached copyright statement

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

The Computer Emergency Response Team/Coordination Center (CERT/CC) has received information concerning a vulnerability in Digital Equipment Corporation's (DEC) Ultrix operating system versions 4.0 and 4.1 for all DEC architectures. The vulnerability has been fixed in version 4.2 which will be shipped beginning in late May. DEC has also provided a suggested fix for versions 4.0 and 4.1.

I. Description

By default, /usr/bin/chroot is improperly installed in Ultrix versions 4.0 and 4.1.

II. Impact

System users can gain unauthorized privileges.

III. Solution

Change the permission on the file /usr/bin/chroot.

```
# chmod 700 /usr/bin/chroot
```

Our thanks to Eric R. Jorgensen and Brian Ellis of UnixOps / Distributed Computing Services at the University of Colorado, Boulder, for bringing this problem to our attention. The CERT/CC would also like to thank Digital for their response to this vulnerability.

This document is available from: http://www.cert.org/advisories/CA-1991-05.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.

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

Conditions for use, disclaimers, and sponsorship information

Revision History

```
September 18,1997  Attached Copyright Statement
```

6 CA-1991-06: NeXT rexd, /private/etc, Username me Vulnerabilities

Original issue date: May 14, 1991
Last revised: September 18, 1997
Attached copyright statement

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

The Computer Emergency Response Team/Coordination Center (CERT/CC) and NeXT Computer, Inc. have received information concerning three vulnerabilities in NeXT computers running various releases (see below) of NeXTstep software. For more information, please contact your authorized support center. If you are an authorized support provider, please contact NeXT through your normal channels.

PROBLEM 1 Description

By default, *rexd(8C)* is enabled in NeXTstep versions 2.0 and 2.1. (Note that no NeXT software uses rexd.)

PROBLEM 1 Impact

Leaving rexd enabled allows remote users to execute processes on a NeXT computer.

PROBLEM 1 Solution

Comment out or remove the rexd line in /etc/inetd.conf (unless you're using the remote execution facility), and either restart the computer or cause inetd to re-read it's configuration file, using:

```
kill -HUP <inetd pid>
```

PROBLEM 2 Description

The /private/etc directory is shipped with group write permission enabled in all NeXTstep versions through and including 2.1.

PROBLEM 2 Impact

Group write permission in /private/etc enables any user in the "wheel" group to modify files in the /private/etc directory.

PROBLEM 2 Solution

Turn off group write permission for the /private/etc directory, using the command:

```
chmod g-w /private/etc
```

or the equivalent operations from the Workspace Manager's Inspector panel.

PROBLEM 3 Description

Username "me" is a member of the "wheel" group in all NeXTstep versions through and including 2.1.

PROBLEM 3 Impact

Having username "me" in the "wheel" group enables "me" to use the *su(8)* command to become root (the user must still know the root password, however).

PROBLEM 3 Solution

Unless you have specific reason(s) not to, remove the user "me" from the wheel group.

The CERT/CC would like to thank NeXT Computer, Inc. for their response to this vulnerability. CERT/CC would also like to thank Fuat Baran for his technical assistance.

This document is available from: http://www.cert.org/advisories/CA-1991-06.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.

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

Conditions for use, disclaimers, and sponsorship information

Revision History

```
September 18,1997  Attached Copyright Statement
```

7 CA-1991-07: SunOS Source Tape Installation Vulnerability

Original issue date: May 20, 1991
Last revised: September 18, 1997
Attached copyright statement

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

The Computer Emergency Response Team/Coordination Center (CERT/CC) has received the following information from Sun Microsystems, Inc. (Sun). Sun has given the CERT/CC permission to distribute their Security Bulletin. It contains information regarding a fix for a vulnerability in SunOS 4.0.3, SunOS 4.1 and SunOS 4.1.1.

The following Sun Microsystems Security Bulletin only applies to systems that have installed the Sun Source tapes.

For more information, please contact Sun Microsystems at 1-800-USA-4SUN.

SUN MICROSYSTEMS SECURITY BULLETIN: #00107

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.

Sun Bug ID : 1059621
Synopsis : security hole created by installing sunsrc
Sun Patch ID: Not applicable see fix below.

This applies to sites that have installed Sun Source tapes only.

The Sun distribution of sources (sunsrc) has an installation procedure which creates the directory /usr/release/bin and installs two setuid root files in it: makeinstall and winstall. These are both binary files which exec other programs: "make -k install" (makeinstall) or "install" (winstall).

This makes it possible for users on that system to become root.

The solution:

```
    chmod ug-s /usr/release/bin/{makeinstall, winstall}
```

(if the sources have already been installed)

and/or

edit the makefile in sunsrc/release and change the SETUID definition (if the sources have been extracted from tape but not installed yet)

Special thanks to CERT and Tel-Aviv University for reporting this problem.

Brad Powell
Sun Microsystems
Software Security Coordinator.

The CERT/CC would like to thank Sun Microsystems, Inc. for their response to this vulnerability. We would also like to thank Ariel Cohen from Tel-Aviv University, School of Mathematical Sciences for reporting the problem.

This document is available from: http://www.cert.org/advisories/CA-1991-07.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.

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

Conditions for use, disclaimers, and sponsorship information

Revision History

```
September 18,1997  Attached Copyright Statement
```

8 CA-1991-08: AT&T System V Release 4 /bin/login Vulnerability

Original issue date: May 23, 1991
Last revised: September 18, 1997
Attached copyright statement

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

The Computer Emergency Response Team/Coordination Center (CERT/CC) has received information concerning a security vulnerability in AT&T's UNIX(r) System V Release 4 operating system. AT&T is providing a software upgrade for Release 4 operating system vendors and a patch for AT&T Computer Systems customers. AT&T has also provided a suggested fix for all Release 4 based systems.

I. Description

A security vulnerability exists in /bin/login in AT&T's System V Release 4 operating system.

II. Impact

System users can gain unauthorized privileges.

III. Solution

A. AT&T Computer Systems customers

Log into the root account. Change the execution permission on the file /bin/login.

```
chmod 500 /bin/login
```

Contact AT&T Computer Systems at 800-922-0354 to obtain a fix. The numbers associated with the fix are 156 (3.5" media) and 157 (5.25" media).

International customers should contact their local AT&T Computer Systems representative.

B. All other System V Release 4 based systems

Log into the root account. Change the execution permission on the file /bin/login.

```
chmod 500 /bin/login
```

Release 4 customers should contact their operating system supplier for details on the availability of the software update.

The CERT/CC would like to thank AT&T for their timely response to our report of this vulnerability.

This document is available from: http://www.cert.org/advisories/CA-1991-08.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.

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

Conditions for use, disclaimers, and sponsorship information

Revision History

```
September 18,1997  Attached copyright statement
```

9 CA-1991-09: SunOS rpc mountd Vulnerability

Original issue date: July 15, 1991

**** Superseded by CA-1994-02. ****

10 CA-1991-10: REVISION NOTICE: New Patch for SunOS /usr/lib/lpd

Original issue date: September 12, 1991
Last revised: September 18, 1997
Attached copyright statement

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

***** THIS IS A REVISED CERT ADVISORY *****
***** CONTAINS NEW INFORMATION *****

There were a number of problems with various early versions of Sun Microsystems, Inc. (Sun) /usr/lib/lpd patch (Patch ID 100305-xx). While security problems were fixed in the patches, a remote print spooling problem was introduced. Sun believes all the problems have been fixed and they are now releasing the enclosed information concerning a new patch version. They have given the CERT/CC permission to distribute this information.

The Computer Emergency Response Team/Coordination Center (CERT/CC) recommends that all affected sites follow the information provided by Sun Microsystems in this bulletin.

START OF SUN-SUPPLIED INFORMATION

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.

This is more an update on the lpd fix than any new information.

First the update.

After a lengthy beta test cycle, there is now available a new version of the lpd security fix. The patch-ID# is 100305-06.

This patch is available via anonymous ftp from the ftp.uu.net system in the sun-dist directory as 100305-06.tar.Z, or through your local Sun Answer Center. The checksum information for the file available from ftp.uu.net is:

```
24474   440   100305-06.tar.Z
```

Some history.

An lpd bug was discovered where lpd could be used to remove system files (/etc/passwd or /.rhosts as examples). This bug was fixed with 100305-01.

A second bug was also shown that could still be used to remove system files. This fix was rolled into 100305-02.

An lpc problem that touched one of the same modules as in the lpd fix was fixed and the subsequent change rolled into the lpd patch 100305-03.

Two additional problems were sent to Sun: one having to do with RPC calls to lpd and the second having to do with postscript calls to lpd, thus 100305-04.

It was in creating the -04 version that we unknowingly introduced a remote spool problem on the SunOS 4.1.1 version of the patch. The problem was that if the remote queue had jobs in it, the local job sent was often truncated to zero length.

The -05 version was an attempt to back out the last few changes to remove the remote print problem. Unfortunately, it did not. It was at this time that we decided to do a lengthy evaluation and test cycle to ensure that the newest version fixed all the reported problems as well as fixed the remote spool bug we had introduced.

The 100305-06 patch is the result of that lengthy test cycle.

Thank you all for your support through all this.

Brad Powell
Software Security Coordinator
Sun Microsystems.

END OF SUN-SUPPLIED INFORMATION

This document is available from: http://www.cert.org/advisories/CA-1991-10.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.

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

Conditions for use, disclaimers, and sponsorship information

Revision History

```
September 18,1997  Attached copyright statement
```

11 CA-1991-11: ULTRIX LAT/Telnet Gateway Vulnerability

Original issue date: August 14, 1991
Last revised: September 18, 1997
Attached copyright statement

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

The Computer Emergency Response Team/Coordination Center (CERT/CC) has received information concerning a vulnerability in LAT/Telnet gateway software in Digital Equipment Corporation's (DEC) ULTRIX versions 4.1 and 4.2 on all architectures. Information regarding the exploitation of this vulnerability has been publicly disclosed so we recommend taking immediate action. Until you are able to apply the patch we recommend that sites disable the LAT/telnet service.

DEC has made a patch available which consists of new /usr/ucb/telnet binaries.

The patch is available through DEC's Customer Support Centers. Sites within the USA should call 1-800-525-7100. Sites in Europe and elsewhere should contact DEC through their normal channels.

I. Description

A vulnerability exists such that ULTRIX 4.1 and 4.2 systems running the LAT/Telnet gateway software can allow unauthorized privileged access. Although you may not be running the LAT/Telnet service at this time, the CERT/CC urges all sites to install the patch. This will ease any future installation of the gateway software.

The LAT/Telnet software requires special installation and is NOT part of the default ULTRIX configuration.

II. Impact

Anyone who can access a terminal or modem connected to the LAT server running the LAT/Telnet service can gain unauthorized root privileges.

III. Solution

Obtain the appropriate version of the patch kit for your system architecture from your DEC Customer Support Center, and install according to the accompanying instructions.

The CERT/CC would like to thank George Michaelson of The Prentice Centre, University of Queensland, Australia and John Annen of Davidson College for bringing this to our attention. We would also like to thank DEC for their response to this vulnerability and CIAC for their assistance.

This document is available from: http://www.cert.org/advisories/CA-1991-11.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/.

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

Conditions for use, disclaimers, and sponsorship information

Revision History

```
September 18,1997  Attached Copyright
```

12 CA-1991-12: Trusted Hosts Configuration Vulnerability

Original issue date: August 22, 1991
Last revised: September 18, 1997
Attached copyright statement

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

The Computer Emergency Response Team/Coordination Center (CERT/CC) has received information concerning a vulnerability in the configuration of several system files. This advisory discusses a workaround since there are no permanent patches available at this time.

This vulnerability is present in a very large number of UNIX-based operating systems. Therefore, we recommend that ALL sites take the corrective actions listed below.

I. Description

The presence of a '-' as the first character in /etc/hosts.equiv, /etc/hosts.lpd and .rhosts files may allow unauthorized access to the system.

II. Impact

Remote users can gain unauthorized root access to the system.

III. Solution

Rearrange the order of entries in the hosts.equiv, hosts.lpd, and .rhosts files so that the first line does not contain a leading '-' character.

Remove hosts.equiv, hosts.lpd, and .rhosts files containing only entries beginning with a '-' character.

.rhosts files in ALL accounts, including root, bin, sys, news, etc., should be examined and modified as required. .rhosts files that are not needed should be removed.

Please note that the CERT/CC strongly cautions sites about the use of hosts.equiv and .rhosts files. We suggest that they NOT be used unless absolutely necessary.

The CERT/CC wishes to thank Alan Marcum, NeXT Computer, for bringing this security vulnerability to our attention. We would also like to thank CIAC for their assistance in testing this vulnerability.

This document is available from: http://www.cert.org/advisories/CA-1991-12.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.

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

Conditions for use, disclaimers, and sponsorship information

Revision History

```
September 18,1997  Attached Copyright Statement
```

13 CA-1991-13: Ultrix Mail Vulnerability

Original issue date: August 23, 1991

**** Superseded by CA-1995-02. ****

14 CA-1991-14: SGI IRIX /usr/sbin/fmt Vulnerability

Original issue date: August 26, 1991
Last revised: September 18, 1997
Attached copyright statement

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

The Computer Emergency Response Team/Coordination Center (CERT/CC) has received information concerning a vulnerability of mail messages in Silicon Graphics Computer Systems' IRIX versions prior to 4.0 (this includes all 3.2 and 3.3.* versions). This problem has been fixed in version 4.0.

Information regarding the exploitation of this vulnerability is inherently disclosed by any discussion of the problem (including this Advisory) so we recommend taking immediate action. Until you are able to apply the patch, mail at your site is vulnerable to being read by any ordinary user logged in at that site.

Silicon Graphics has provided the enclosed patch instructions.

I. Description

A vulnerability exists such that IRIX pre-4.0 (e.g., 3.3.3) systems with the basic system software ("eoe1.sw.unix") installed can allow unauthorized read access to users' mail messages, by exploiting a configuration error in a standard system utility. Due to the ease of exploiting this vulnerability and the simplicity of the corrective action, the CERT/CC urges all sites to install the patch given below.

II. Impact

Anyone who can log in on a given IRIX pre-4.0 (3.2, 3.3, 3.3.*) system can read mail messages which have been delivered to any other user on that same system.

III. Solution

As "root", execute the following commands:

```
chmod 755 /usr/sbin/fmt
chown root.sys /usr/sbin/fmt
```

If system software should ever be reloaded from a 3.2 or 3.3.* installation tape or from a backup tape created before the patch was applied, repeat the above procedure immediately after the software has been reloaded, before enabling logins by normal users.

[Fixed in IRIX 4.0.]

The CERT/CC would like to thank Silicon Graphics for bringing this vulnerability and solution to our attention.

This document is available from: http://www.cert.org/advisories/CA-1991-14.html

CERT/CC Contact Information

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

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

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

Using encryption

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

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

Getting security information

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

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

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

Conditions for use, disclaimers, and sponsorship information

Revision History

```
September 18,1997  Attached Copyright Statement
```

15 CA-1991-15: Mac/PC NCSA Telnet Vulnerability

Original issue date: September 10, 1991
Last revised: September 18, 1997
Attached copyright statement

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

The Computer Emergency Response Team/Coordination Center (CERT/CC) has received information concerning a vulnerability in the default configurations of National Center for Supercomputing Applications (NCSA) Telnet for both the Macintosh and the PC. The vulnerability also affects the version of NCSA Telnet with IBM 3270 terminal emulation distributed by Clarkson University. Two workarounds are available that correct this problem.

NCSA has committed to changing the default configurations in future releases. Maintenance updates for both the Macintosh and the PC are planned to be released in about 2 months.

NCSA provides two e-mail addresses for Telnet questions, comments, and bug reports:

PC Telnet pctelnet@ncsa.uiuc.edu

Mac Telnet mactelnet@ncsa.uiuc.edu

I. Description

The default configuration of NCSA Telnet for both the Macintosh and the PC has a serious vulnerability in its implementation of an ftp server.

The default configuration file enables ftp via the "ftp=yes" line. However, sites should be aware that ftp is also enabled in the absence of any ftp statement in the configuration file.

II. Impact

Any Internet user can connect via ftp to a PC or Macintosh running the default configuration of NCSA Telnet and gain unauthorized read and write access to any of its files, including system files.

III. Solution

Either disable ftp server functionality or provide password protection as described below.

To disable the ftp server, add an "ftp=no" line in the configuration file.

If the ftp server option is enabled (via either an "ftp=yes" line in the configuration file or the absence of an ftp statement in the configuration file), then the Telpass program (included with both Mac and PC versions) can be used to provide password protection. Telpass is used to enter usernames and encrypted passwords into a password file. The configuration file specifies the name and location of the password file in the "passfile=" statement. The usage of Telpass is documented in Chapter 5 of version 2.4 of the Macintosh version documentation and Chapter 7 of version 2.3 of the PC version. Note that the documentation (as well as the package itself) is available by anonymous ftp from ftp.ncsa.uiuc.edu (141.142.20.50).

The instructions for enabling password protection differ between the Macintosh and PC versions, but in both cases they involve enabling the "passfile" option in the configuration file, and creating usernames and encrypted passwords with the Telpass program.

CERT/CC strongly urges all sites running NCSA Telnet to implement one of these two workarounds.

The CERT/CC would like to thank NCSA and Clarkson University for their assistance.

This document is available from: http://www.cert.org/advisories/CA-1991-15.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.

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

Conditions for use, disclaimers, and sponsorship information

Revision History

```
September 18,1997  Attached Copyright Statement
```

16 CA-1991-16: SunOS SPARC Integer_Division Vulnerability

Original issue date: September 18, 1991

**** The patch cited in this advisory has been made obsolete by patches described in CA-1992-15. ****

17 CA-1991-17: DECnet-Internet Gateway Vulnerability

Original issue date: September 26, 1991
Last revised: September 18, 1997
Attached copyright statement

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

The Computer Emergency Response Team/Coordination Center (CERT/CC) has received information concerning a vulnerability in the configuration of the DECnet-Internet gateway software for Digital Equipment Corporation's (DEC) ULTRIX versions 4.0, 4.1, and 4.2 on all Digital architectures.

Digital Equipment Corporation is aware of this problem and a resolution for this vulnerability will be included in a future release. Digital and the CERT/CC strongly recommend that sites exposed to this vulnerability immediately institute the workaround detailed in this advisory.

I. Description

When installing the DECnet-Internet gateway software it is necessary to create a guest account on the ULTRIX gateway host. By default, this account has /bin/csh as its shell. By virtue of the guest account having a valid shell, the DECnet-Internet gateway software can be exploited to allow unauthorized root access.

II. Impact

Anyone using the DECnet-Internet gateway can gain unauthorized root privileges on the ULTRIX gateway host.

III. Solution

This section describes a workaround for this vulnerability. Disable the guest account by editing the /etc/passwd file and setting the shell field for the guest account to /bin/false. Also, ensure the guest account has the string "NoLogin" in the password field as detailed in the DECnet-Internet installation manual. Even if you have not installed or are not running the DECnet- Internet gateway software, Digital recommends that you implement the workaround solution stated above.

The CERT/CC wishes to thank R. Scott Butler of the Du Pont Company for bringing this vulnerability to our attention and for his further assistance with the temporary workaround.

This document is available from: http://www.cert.org/advisories/CA-1991-17.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.

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

Conditions for use, disclaimers, and sponsorship information

Revision History

```
September 18,1997  Attached Copyright Statement
```

18 CA-1991-18: Active Internet tftp Attacks

Original issue date: September 27, 1991
Last revised: September 18, 1997
Attached copyright statement

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

The Computer Emergency Response Team/Coordination Center (CERT/CC) would like to alert you to automated tftp probes that have been occurring over the last few days. These probes have attacked Internet sites throughout the world and in most cases the file retrieved was /etc/passwd. However, other files such as /etc/rc may have been retrieved.

The CERT/CC is working with the site(s) that were used by intruders to launch the attacks. We are actively contacting those sites where we believe the retrievals were successful. We are urging all sites to carefully check their system configurations concerning tftp usage.

I. Description

Unrestricted tftp access allows remote sites to retrieve a copy of any world-readable file.

II. Impact

Anyone on the Internet can use tftp to retrieve copies of a site's sensitive files. For example, the recent incident involved retrieving /etc/passwd. The intruder can later crack the password file and use the information to login to the accounts. This method may provide access to the root account.

III. Solution

A. Sites that do not need tftp should disable it immediately by editing the system configuration file to comment out, or remove, the line for tftpd.

This file may be /etc/inetd.conf, /etc/servers, or another file depending on your operating system. To cause the change to be effective, it will be necessary to restart inetd or force inetd to read the updated configuration file.

B. Sites that must use tftp (for example, for booting diskless

clients) should configure it such that the home directory is changed. Example lines from /etc/inetd.conf might look like:

```
ULTRIX 4.0
tftp   dgram  udp  nowait  /etc/tftpd  tftpd -r /tftpboot
SunOS 4.1
```

```
tftp   dgram  udp  wait  root  /usr/etc/in.tftpd in.tftpd -s
/tftpboot
```

As in item A. above, inetd must be restarted or forced to read the updated configuration file to make the change effective.

C. If your system has had tftp configured as unrestricted, the CERT/CC urges you to consider taking one of the steps outlined above and change all the passwords on your system.

This document is available from: http://www.cert.org/advisories/CA-1991-18.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.

NO WARRANTY

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

Conditions for use, disclaimers, and sponsorship information

Revision History

```
September 18,1997 Attached Copyright Statement
```

19 CA-1991-19: AIX TFTP Daemon Vulnerability

Original issue date: October 17, 1991
Last revised: September 18, 1997
Attached copyright statement

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

The Computer Emergency Response Team/Coordination Center (CERT/CC) has received information concerning a vulnerability in the TFTP daemon in all versions of AIX for IBM RS/6000 machines.

IBM is aware of this problem and a fix is available as apar number "ix22628". This patch is available for all AIX releases from "GOLD" to the current release.

NOTE: THIS IS AN UPDATED PATCH FROM ONE RECENTLY MADE AVAILABLE and fixes a security hole in the original patch. The SCCS id of the correct patch is tftpd.c 1.13.1.3 (*not* 1.13.1.2 or earlier versions). This can be checked using the following "what" command.

```
 % what /etc/tftpd
/etc/tftpd:
56      1.13.1.3  tftpd.c, tcpip, tcpip312 10/10/91 09:01:48
tftpsubs.c      1.2  com/sockcmd/tftpd,3.1.2,9048312 10/8/89 17:40:55
```

IBM customers may call IBM Support (800-237-5511) and ask that the fix be shipped to them. The fix will appear in the upcoming 2009 update and the next release of AIX.

I. Description

Previous versions of tftpd did not provide a method for restricting TFTP access.

II. Impact

If TFTP is enabled at your site, anyone on the Internet can retrieve copies of your site's world-readable files, such as /etc/passwd.

III. Solution

A. Sites that do not need to allow tftp access should disable it.

This can be done by editing /etc/inetd.conf and deleting or commenting out the tftpd line:

```
#tftp     dgram     udp    wait    nobody  /etc/tftpd     tftpd -n
```

and then, as root, restarting inetd with the "refresh" command.

```
# refresh -s inetd
```

For more details on starting/stopping tftp, refer to documentation for the System Resource Controller (SRC) or the System Management Interface Tool (SMIT).

B. Sites that must run tftpd (for example, to support X terminals) should obtain and install the above patch AND create a /etc/tftpaccess.ctl file to restrict the files that are accessible.

The /etc/tftpaccess.ctl file should be writable only by root. Although the new /etc/tftpaccess.ctl mechanism provides a very general capability, the CERT/CC strongly recommends that sites keep this control file simple. For example, the following tftpaccess.ctl file is all that is necessary to support IBM X terminals:

```
# /etc/tftpaccess.ctl
# By default, all files are restricted if /etc/tftpaccess.ctl ex-
ists.
# Allow access to X terminal files.
        allow:/usr/lpp/x_st_mgr/bin
```

NOTE: Be CERTAIN to create the /etc/tftpaccess.ctl file.
If it does not exist then all world-readable files are accessible as in the current version of tftpd.

Installation Instructions:

1. Create an appropriate /etc/tftpaccess.ctl file.

2. From the directory containing the new tftpd module, issue the following commands as root.

```
    # chmod 644 /etc/tftpaccess.ctl
    # chown root.system /etc/tftpaccess.ctl
    # mv /etc/tftpd /etc/tftpd.old
    # cp tftpd /etc
    # chmod 755 /etc/tftpd
    # chown root.system /etc/tftpd
    # refresh -s inetd
```

The CERT/CC wishes to thank Karl Swartz of the Stanford Linear Accelerator Center for bringing this vulnerability to our attention.

This document is available from: http://www.cert.org/advisories/CA-1991-19.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.

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

Conditions for use, disclaimers, and sponsorship information

Revision History

```
September 18,1997  Attached Copyright Statement
```

20 CA-1991-20: rdist Vulnerability

Original issue date: October 22, 1991

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

21 CA-1991-21: NFS Jumbo Patch, SunOS 4.1

Original issue date: December 6, 1991
Last revised: September 18, 1997
Attached copyright statement

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

The Computer Emergency Response Team/Coordination Center (CERT/CC) has received information concerning several vulnerabilities in Sun Microsystems, Inc. (Sun) Network File System (NFS) and the fsirand program. These vulnerabilities affect SunOS versions 4.1.1, 4.1, and 4.0.3 on all architectures.

Sun has provided separate patches for these vulnerabilities for SunOS 4.1.1, and has provided an initial patch for SunOS 4.1. Sun will be providing complete patches for 4.1 and 4.0.3 at a later date. On SunOS 4.1.1 systems, Sun states that patch 100173-07 must be installed before patch 100424-1. The patches are available through your local Sun Answer Centers worldwide as well as through anonymous ftp from the ftp.uu.net (192.48.96.2) system in the /sun-dist directory.

Fix	PatchID	Filename	Checksum
NFS Jumbo 4.1.1	100173-07	100173-07.tar.Z	07044 209
NFS Jumbo 4.1	100121-08	100121-08.tar.Z	61464 287
fsirand 4.1.1	100424-01	100424-01.tar.Z	63070 50

Please note that Sun will occasionally update patch files. If you find that the checksum is different please contact Sun or the CERT/CC for verification.

Sun recommends that sites upgrade to SunOS 4.1.1 to benefit from the security improvements. In addition, they recommend the installation of all security-related patches applicable to the version of SunOS that you are running.

A general NFS security note: due to security flaws in the protocol, the CERT/CC recommends filtering SunRPC and NFS IP packets (sockets 111 and 2049) between the local network and the Internet. This will prevent intruders outside your local network from accessing your files.

NFS Jumbo Patch, SunOS 4.1.1

I. Description

This patch fixes several SunOS NFS bugs (not all security-related). The patch file, 100173-07.tar.Z, contains fixes for SunOS version 4.1.1. The BugIDs fixed in this patch are:

```
1039977 1032959 1029628 1037476 1038302 1034328 1045536 1030884 1045993
1047557 1052330 1053679 1041409 1065361 1066287 1064433 1070654
```

See the README file provided with the patch for more information.

II. Impact

These vulnerabilities (and bugs) have multiple impacts, including crashing the system, allowing unauthorized system access, and causing a problem with file group ownership.

III. Solution

Obtain the patch from Sun or from ftp.uu.net and install, following the provided instructions, with the following exception:

line 112 of the README file currently reads:

```
  mv /sys/`arch -k`/OBJ/nfs_subr.o /sys/arch -k`/OBJ/nfs_subr.o.FCS
                                        ^^^^^^^^
```

it should read:

```
  mv /sys/`arch -k`/OBJ/nfs_subr.o /sys/`arch -k`/OBJ/nfs_subr.o.FCS
                                        ^^^^^^^^^
```

(Note the one-character difference.)

NFS Jumbo Patch, SunOS 4.1

I. Description

This patch fixes several SunOS NFS bugs (not all security-related). The patch file, 100121-08.tar.Z, contains fixes for SunOS version 4.1. The BugIDs fixed in this patch are:

```
1026933 1034007 1039977 1029628 1037476 1038327 1038302
1034328 1045536 1045993 1047557 1030884 1052330 1053679
```

See the README file provided with the patch for more information.

II. Impact

These vulnerabilities (and bugs) have multiple impacts, including crashing the system, allowing unauthorized system access, and causing a problem with file group ownership.

III. Solution

Obtain the patch from Sun or from ftp.uu.net and install, following the provided instructions.

fsirand, SunOS 4.1.1

I. Description

A security vulnerability exists in SunOS NFS relating to the way in which it allocates file handles. The patch file, 100424-01.tar.Z, contains a fix for SunOS version 4.1.1. The BugID fixed in this patch is 1063470.

II. Impact

The fsirand program could allow a remote system user to guess NFS file handles, thereby potentially allowing them to mount and access your NFS file systems.

III. Solution

Obtain the patch from Sun or from ftp.uu.net and install, following the provided instructions. You must install PatchID 100173-07 before installing this patch.

The CERT/CC wishes to thank Bob Drzyzgula of the Federal Reserve Board, Leendert van Doorn of Vrije University, and Wietse Venema of Eindhoven University for their assistance.

This document is available from: http://www.cert.org/advisories/CA-1991-21.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.

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

Conditions for use, disclaimers, and sponsorship information

Revision History

```
September 18, 1997  Attached Copyright Statement
```

22 CA-1991-22: SunOS OpenWindows Vulnerability

Original issue date: December 16, 1991

**** Superseded by CA-1993-18. ****

23 CA-1991-23: Hewlett-Packard/Apollo Domain/OS crp Vulnerability

Original issue date: December 18,1991
Last revised: September 18, 1997
Attached copyright statement

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

The Computer Emergency Response Team/Coordination Center (CERT/CC) has received information concerning a vulnerability in the crp facility in Hewlett Packard/Apollo Domain/OS. This vulnerability is present on all HP/Apollo Domain/OS SR10 systems up through SR10.3. Patches that address this problem will be available in the SR10.3 patch tape (~Feb 92) and in the SR10.4 software release. Contact your local sales office for more information.

I. Description

There is a security problem with the /usr/apollo/bin/crp facility. A user who is not running crp is not vulnerable to this problem.

II. Impact

A person at a remote or local site can obtain the privileges of the user who is running crp.

III. Workaround

The suggested workaround is to disable two system calls that are made by /usr/apollo/bin/crp. The following steps should be executed by root or another appropriate userid that has the privilege to write in the directories involved.

1. Create a file "crplib.c" containing the four-line C program:

```
     extern void pad_$dm_cmd(void);
void pad_$dm_cmd() { }
extern void pad_$def_pfk(void);
      void pad_$def_pfk() { }
```

2. Compile this program using '-pic':

```
(AEGIS)  /com/cc crplib.c -pic
 (UNIX)   /bin/cc -c crplib.c -W0,-pic
```

3. Copy the result to somewhere accessible to all users (/lib/crplib is recommended).

```
(AEGIS)  /com/cpf crplib.bin /lib/crplib
```

```
      (AEGIS)  /com/edacl -p root prwx -g wheel rx -w rx
/lib/crplib
(UNIX)   /bin/cp crplib.o /lib/crplib

      (UNIX)   /bin/chmod 755 /lib/crplib
```

4. a) Ensure that all users do an 'inlib' of that file before running crp.

One way to ensure this would be to replace the /usr/apollo/bin/crp command by a shell script that does the inlib. Doing this step will force crp to use the null functions defined in step 1 above.

```
     (AEGIS)  /com/chn /usr/apollo/bin/crp crp.orig
      (UNIX)   /bin/mv /usr/apollo/bin/crp
/usr/apollo/bin/crp.orig
```

b) Create the file /usr/apollo/bin/crp containing the shell script:

```
     (AEGIS) #!/com/sh
        /com/sh -c inlib /lib/crplib ';' /usr/apollo/bin/crp.orig
^*
(UNIX)      #!/bin/sh
inlib /lib/crplib
              exec /usr/apollo/bin/crp.orig "$@"
```

c) Make this script executable.

```
      (AEGIS)       /com/edacl -p root prwx -g wheel rx -w rx
/usr/apollo/bin/crp
      (UNIX) /bin/chmod 755 /usr/apollo/bin/crp
```

NOTE: This workaround will prevent crp from making use of the two system calls; and therefore, it may affect the functionality of various software programs since they will be unable to define programmable function keys, create new windows on the client node, or execute background processes using the Display Manager interface.

The CERT/CC wishes to thank Paul Szabo of the University of Sydney for bringing this problem to our attention and providing a workaround. We would also like to thank Jim Richardson of the University of Sydney for his assistance and Hewlett Packard/Apollo for their timely response to the report of this vulnerability.

This document is available from: http://www.cert.org/advisories/CA-1991-23.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.

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

Conditions for use, disclaimers, and sponsorship information

Revision History

```
September 18,1997  Attached Copyright Statement
```