Software Engineering Institute
Carnegie Mellon University

1997 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-1997-01: Multi-platform Unix FLEXlm Vulnerabilities

Original issue date: January 6, 1997
Last revised: September 26, 1997
Updated copyright statement

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

The text of this advisory was originally released on September 19, 1996, as AUSCERT Advisory AA-96.03 "Multi-platform Unix FLEXlm Vulnerabilities," developed by Australian Computer Emergency Response Team. Because of the seriousness of the problem, we are reprinting the AUSCERT advisory here with their permission. Only the contact information at the end has changed: AUSCERT contact information has been replaced with CERT/CC contact information.

We will update this advisory as we receive additional information. Look for it in an "Updates" section at the end of the advisory.

AUSCERT has received information concerning several problems involving the use of the FLEXlm licence management package on Unix systems. FLEXlm is used by many vendors to licence their products, and is supplied to them by GLOBEtrotter Software (previously, it was supplied by Highland Software). Many vendors have misconfigured the FLEXlm system to run as the root user, and some versions of the FLEXlm licence management daemon lmgrd contain a security vulnerability. These problems may allow local users to create users to create arbitrary files on the system and execute arbitrary programs using the privileges of the user running the FLEXlm daemons.

System administrators are advised that the FLEXlm package may be installed as part of the installation procedures of other vendor and third-party products. Due to the way that the licence management software is often installed, it may be unnecessarily running as root making it possible to gain unauthorised privileged access.

This means that the FLEXlm package may be installed on systems and running as the root user without the knowledge of the system administrator.

Note that the vulnerabilities described here do not affect the security of the FLEXlm licences and licencing restriction. The vulnerabilities allow users to compromise security of the Operating System.

1. Description

The FLEXlm licence management package is used by many vendors to licence their products. Many vendors have misconfigured the FLEXlm system to run as the root user which opens a number of computer security vulnerabilities which can be used to compromise the Unix operating system. This is described in paragraph (a).

In addition, some versions of the FLEXlm licence management daemon lmgrd contain a security vulnerability. This is described in paragraph (b).

(a) Insecure configuration of vendor product installation

Due to some confusion in the documentation supplied to vendors using the FLEXlm package, the FLEXlm licence management software often runs with root privileges. This often occurs due to the FLEXlm daemons being started by the system initialisation scripts. If the daemons are running with root privileges they may be used by local users to gain unauthorised root privileges. This potentially affects all versions of the FLEXlm licence management daemon.

GLOBEtrotter Software advise that the FLEXlm package does not require root privileges to operate correctly. FLEXlm daemons should be started by a non-privileged user with a restrictive umask setting, limiting the associated configuration vulnerabilities.

(b) Security vulnerability in FLEXlm licence management daemon

A vulnerability has been found in the FLEXlm licence management daemon which may allow local users unauthorised access to the account running the FLEXlm licence management daemon.

This vulnerability exists in all versions of the FLEXlm licence management daemon from version 4.0 up to, and including, version 5.0a. A new version of the daemon has been made available by GLOBEtrotter Software that fixes this vulnerability. See Section 3.4.

Versions earlier than version 4.0 do not have this vulnerability. GLOBEtrotter Software advise that all existing versions of the lmgrd daemon may be updated to the most recent version (version 5.0b) without change in functionality. This version of lmgrd will work successfully with all existing FLEXlm-licensed products. See Section 3.4.

1.1 Additional Description Information

This section contains additional information on locating any FLEXlm components, determining the configuration of those components, and identifying information required for the Workarounds/Solutions in Section 3.

(a) Vendor configurations may be customised

Vendors using the FLEXlm licence management package to licence their products have the ability to customise FLEXlm to meet their own needs. This may include names, locations, and content of many files, in addition to how the software is installed and used. Therefore, care is required in locating any vulnerable software or configurations, and implementing workaround solutions.

(b) Determining if FLEXlm is installed

The FLEXlm licence management package is often installed as part of the installation procedures of other vendor and third-party products. The system administrator may not be aware that FLEXlm has been installed.

The following command run as root should determine if the FLEXlm licence management software is installed.

find /etc -type f -exec egrep -il 'lmgrd|flexlm|licdir' {} \;

Any files listed should be investigated further to see if they relate to the FLEXlm licence management product.

In particular, it is important to locate the FLEXlm licence management initialisation files (the files where FLEXlm licence management daemons are started from) as these will become important when discussing the Workarounds/Solutions in Section 3.

(c) Determining the version of the FLEXlm licence management daemon(s)

The version of the FLEXlm licence management daemon can be determined by examining the strings(1) output of the binary daemon and searching for the strings "Copyright" and "FLEXlm".

For example:

strings /usr/local/flexlm/licences/lmgrd | grep -i copyright | grep -i flexlm

Note that more than one version of the FLEXlm licence management daemon may be executing, depending on what products are installed.

The version number is also written to stdout (which may have been redirected to a log file) when the licence management daemon is started.

(d) Identifying the user running the FLEXlm licence management daemons

The licence management daemon is often called "lmgrd" or some derivative containing the string "lmgrd" (for example, lmgrd.abc). On some products, the name of the licence management daemon may have been changed to an arbitrary name (for example, lm_ABC4.ld). It should be possible to locate most running versions of the licence management daemon by examining the files identified in Section 1.1(b) or by using one of the following commands (Note this may locate other processes not related to FLEXlm, and may not locate all FLEXlm related processes):

% ps -auxww | grep -i lm | grep -v grep
#BSD systems

% ps -ef | grep -i lm | grep -v grep
# SYS V systems

If any licence management daemon is running as the root user, then a number of vulnerabilities exist as the daemon was not designed to be run with root privileges.

Note that more than one FLEXlm licence management daemon may be running depending on what products have been installed. It is important to check for all running versions of the daemon.

(e) Locating the licence management files

Each licence management daemon has an associated licence file. The licence file is usually specified by the "-c" option on the command line, the LM_LICENSE_FILE environment variable, or is found in the default location /usr/local/flexlm/licenses/license.dat. The licence file describes which products the daemon is administering and the location of associated daemons. The licence files become important when discussing the Workarounds/Solutions in Section 3.

2. Impact

Any versions of the FLEXlm licence management daemons executing using a system account (for example, bin, daemon, sys) or a privileged account (such as root) may allow local users to create or overwrite arbitrary files on the system. This may be leveraged to gain root access.

FLEXlm licence management daemons containing the security vulnerability (indicated in Section 1(b)) may allow local users unauthorised access to the account running the daemons.

Information on gaining unauthorised access to Unix systems using the FLEXlm Licence Management software has been widely distributed.

3. Workarounds/Solution

Note that all four (4) sections should be reviewed and implemented if appropriate. Each section addresses a different problem.

After the installation of ANY product or upgrade, the system must be checked to verify if a FLEXlm licence management daemon has been added. If a FLEXlm licence management daemon has been added, then Sections 3.1 to 3.4 of this Advisory should be applied to it to ensure a more secure configuration.

3.1 Run as a non-privileged user

GLOBEtrotter Software advise that the FLEXlm licence management software does not require root privileges to operate. The FLEXlm licence management daemon should be run by a non-privileged user.

If the licence management daemon is executing with root or some other system account permissions (such as bin, sys, daemon or any other system account), it must be modified to use a non-privileged user.

If the licence management daemon is already executing as a non-privileged user, then the remainder of Section 3.1 may be skipped.

It is recommended that a new user "flexlm" be created for the specific purpose of running the FLEXlm licence management daemon. In this case, Steps 3.1.1 through 3.1.5 should be followed.

3.1.1 Create a non-privileged account for use by FLEXlm.

For example:

flexlm:*:2000:250:FLEXlm Licence Manager:/nonexistent:/bin/sh

Note the account must have the following properties:

.password set to '*' as interactive access is not required
.a unique userid (the 2000 is only an example)
.a unique groupid (the 250 is only an example)
.a shell of /bin/sh

The following instructions refer to this account as the "flexlm user". If the FLEXlm daemons were already running as a non-privileged user, then this will be the "flexlm user" below.

3.1.2 Locate the licence file(s).

These may be identified in one of three ways:

- specified by the "-c" option to the FLEXlm licence daemons
- specified by the LM_LICENSE_FILE environment variable
- located in the default location: /usr/local/flexlm/licenses/license.dat

Note that there is always a single licence file for each licence daemon, but there may be more than one licence daemon running on a system.

3.1.3 The licence management daemons must use a non-privileged TCP port for communication. The port number chosen may be arbitrary, but all clients must be configured to use the same port.

The port is specified in the licence data file on the SERVER line. It is the fourth (4th) field on this line. For example:

SERVER xyzzy 123456789 1234

the port number is 1234.

3.1.4 Locate where the FLEXlm licence management daemon is started.

This is often in the system startup scripts, but may not exclusively be so. An example startup line is:

$licdir/$lmgrd -c $licdir/$licfile >> /tmp/license_log 2>&1 &

Logging information is written to stdout by the daemons, and is often redirected to a log file when the daemon is started.

3.1.5 Modify the line in the FLEXlm startup files that starts the licence management daemon to look similar to the following:

su flexlm -c "{original command line in startup file}"

where flexlm is the user created in Step 3.1.1. Note that the logging information that is written to stdout from the daemon should not be written to files in /tmp or other world writable directories, but to a specially created directory that the flexlm user can write log information to.

For example:

su flexlm -c "$licdir/$lmgrd -c ... >> /var/log/flexlm/license_log 2>&1 &"

3.2 File Ownership

Regardless of which user is executing the FLEXlm licence management software, additional security vulnerabilities may allow a user to gain unauthorised access to the account running the daemon or engage in denial of service attacks by deleting files.

These vulnerabilities may be limited if you ensure that no files on the system are owned or are writable by the flexlm user. The possible exception to this requirement is log files (see Section 3.1.4) and temporary files. All licence and FLEXlm executable files must be readable or executable by the flexlm user. Additional daemons required by the FLEXlm licence management daemon are specified in the licence data files (located in Section 3.1.2) on the DAEMON line.

These file ownership and mode changes should be done for all versions of FLEXlm.

Note that some vendors may have installed the FLEXlm software owned by the flexlm user. This configuration should be modified as detailed in this section.

3.3 umask Setting

The FLEXlm licence management daemons inherit the umask setting from the environment in which they are started. When FLEXlm is started as part of the system initialisation procedures, the umask is inherited from init(1M) and is usually set to 000. The FLEXlm licence management daemons inherit the umask setting from the environment in which they are started. When FLEXlm is started as part of the system initialisation procedures, the umask is inherited from *init(1M)* and is usually set to 000. This means that FLEXlm will open files which are world and group writable. A more appropriate umask setting is 022.

This should be done for all versions of FLEXlm.

The umask can be set in the FLEXlm startup files which were identified in Section 3.1.4. This should be the first command executed in the startup script for FLEXlm licence management daemons.
For example:

#!/bin/sh
umask 022 # add this line here rest of the FLEXlm startup file

3.4 Vendor Patch for Vulnerability

GLOBEtrotter Software have made a new version of the FLEXlm licence management daemon (version 5.0b) available which rectifies the reported vulnerability in Section 1(b).

All versions of the FLEXlm licence management daemon from version 4.0 up to, and including, version 5.0a should be upgraded immediately.

GLOBEtrotter Software advise that all versions of the FLEXlm lmgrd may be upgraded to the latest version (version 5.0b) without loss of existing functionality. This version of lmgrd will work successfully with all existing FLEXlm-licensed products.

Note that there may be more than one copy of FLEXlm's lmgrd on your system that requires upgrading, depending on what products are installed. The existing licence management daemon(s) should be replaced with the new version, but the location and file name of the version you are replacing should be preserved.

Version 5.0b of the FLEXlm licence management daemon may be found at

http://www.globetrotter.com/lmgrd.htm

MD5 (alpha_u1/lmgrd) = 40ec89f3c9cfcdecfaa442d59db179e1
MD5 (decs_u4/lmgrd) = 0cd60373d0f0bef8f7a2de290306490b
MD5 (hal_u5/lmgrd) = 1e678c62d6346480c6ce097df1a6c708
MD5 (hp300_u8/lmgrd) = ffbdf1c581fd383ca01ba239230f2964
MD5 (hp700_u8/lmgrd) = f972b3a449cd57e8d472a0394613e076
MD5 (i86_d4/lmgrd) = 37256e1abe50116c504b6d2f83a23c55
MD5 (i86_l1/lmgrd) = f1bbfdf13d1145fb3b18afb063b93ac3
MD5 (i86_x5/lmgrd) = e6623c2124205512fc9ed21bc9aee061
MD5 (ncr_u2/lmgrd) = 0919251ca4321dfaa166e008f8d34899
MD5 (nec_u2/lmgrd) = 7e1ae2664219f59e0c26b1a1d97838df
MD5 (ppc_u4/lmgrd) = d4d038cd5bdfa4c44d2523cf11461d63
MD5 (ppc_x5/lmgrd) = f1aae597d4052734b4e01cac76407cf6
MD5 (rm400_u5/lmgrd) = cb2d48efa809cbb3457f835f2db47926
MD5 (rs6000_u3/lmgrd) = fadf0fc424f1fcc11cd04fe8678b79cf
MD5 (sco_u3/lmgrd) = e288917fb8fac8fdc8f1f2a9d985eb50
MD5 (sgi_u4/lmgrd) = 0637f1dae3adb5d7a3597b6d486e18af
MD5 (sgi_u5/lmgrd) = 31f1f1d1b02917f4c9c062c33e4636a4
MD5 (sgir8_u6/lmgrd) = ba0892403ef4bebf38ad22831d3d8183
MD5 (sony_u4/lmgrd) = 032b4521333e7583afd0f783f5555522
MD5 (sun4_u4/lmgrd) = f87130d077d4d1cc8469d9818a085d33
MD5 (sun4_u5/lmgrd) = 36a2930f3dcbe92155866e7a9864b8a5

A copy of these files will be available until 31-Oct-1996 from:
ftp://ftp.auscert.org.au/pub/mirrors/ftp.globetrotter.com/flexlm/unix/.

4. Additional information

4.1 User Manual and Frequently Asked Questions

GLOBEtrotter Software have a user manual that describes the FLEXlm Licence Management system which is available to all users. A FAQ (Frequently Asked Questions) document containing useful information is also available. These can be located at:

http://www.globetrotter.com/manual.htm
http://www.globetrotter.com/faq.htm

4.2 Additional Vendor Information

GLOBEtrotter Software have made available some additional information concerning these security vulnerabilities. It can be accessed at: http://www.globetrotter.com/auscert.htm.

4.3 General misconfiguration description

The misconfiguration of the FLEXlm licence management daemon is a generic problem where software that was not designed to be run with root privileges automatically gains those privileges as a result of being started by the system initialisation scripts. Only those programs that require root privileges should be run as root.

Attention is drawn to the Unix Secure Programming Checklist which addresses this issue, in addition to others. The checklist is available from:
ftp://ftp.auscert.org.au/pub/auscert/papers/secure_programming_checklist.

AUSCERT thanks Peter Marelas from The Fulcrum Consulting Group, GLOBEtrotter Software, DFN-CERT, CERT/CC, and Sun Microsystems for their advice and cooperation in this matter.

UPDATES

Silicon Graphics, Inc.

The solution to this problem is to install version 3.0 of the the License Tools, license_eoe subsystem.
To determine the version of License Tools installed on a particular system, the following command can be used:

% versions license_eoe

I = Installed, R = Removed

Name	Date	Description
I license_eoe	02/13/96	License Tools 1.0
I license_eoe.man	02/13/96	License Tools 1.0 Manual Pages
I license_eoe.man.license_eoe	02/13/96	LIcense Tools 1.0 Manual Pages
I license_eoe.man.relnotes	02/13/96	License Tools 1.0 Release Notes
I license_eoe.sw	02/13/96	License Tools 1.0 Software
I license_eoe.sw.license_eoe	02/13/96	License Tools 1.0 Software

In the above case, version 1.0 of the License Tools is installed and the steps below should be performed. If the output returned indicates "License Tools 3.0," the latest license subsystem is installed and no further action is required.

**** IRIX 4.x ****
The 4.x version of IRIX is not vulnerable as no license manager subsystems were released for this IRIX version. No action is required.

**** IRIX 5.0.x, 5.1.x, 5.2 ****
The 5.0.x, 5.1.x and 5.2 versions of IRIX are not vulnerable as no license manager subsystems were released for these IRIX versions. No action is required.

**** IRIX 5.3 ****
For the IRIX operating system version 5.3 an inst-able new version of software has been generated and made available via anonymous FTP and your service/support provider. The software is version 3.0 of the License Tools, license_eoe subsystem and will install on IRIX 5.3 only.

The SGI anonymous FTP site is sgigate.sgi.com (204.94.209.1) or its mirror, ftp.sgi.com. Software is referred to as License5.3.tar and can be found in the following directories on the FTP server:

~ftp/Security
or
~ftp/Patches/5.3

Checksums
The actual software will be a tar file containing the following files:

Filename: license_eoe
Algorithm #1 (sum -r): 01409 7 license_eoe
Algorithm #2 (sum): 56955 7 license_eoe
MD5 checksum: 38232F3DE67373875577B167B2DA2DA3

Filename: license_eoe.books
Algorithm #1 (sum -r): 33405 809 license_eoe.books
Algorithm #2 (sum): 53177 809 license_eoe.books
MD5 checksum: D1D931936AB681A7B259BD75DCA6D7F9

Filename: license_eoe.idb
Algorithm #1 (sum -r): 59742 54 license_eoe.idb
Algorithm #2 (sum): 32839 54 license_eoe.idb
MD5 checksum: 4F7EE6965539FCFEEDE07E3FFD71CF5A

Filename: license_eoe.man
Algorithm #1 (sum -r): 58166 271 license_eoe.man
Algorithm #2 (sum): 23426 271 license_eoe.man
MD5 checksum: 41946D8E27032A929350B2C27D065DE5

Filename: license_eoe.sw
Algorithm #1 (sum -r): 29827 7692 license_eoe.sw
Algorithm #2 (sum): 52617 7692 license_eoe.sw
MD5 checksum: 720EF1907DD0C3113CB4A98AD602010B

**** IRIX 6.0, 6.0.1 *****
The 6.0.x versions of IRIX are not vulnerable as no license manager subsystems were released for these IRIX versions. No action is required.

**** IRIX 6.1 ****
The license manager software provided with IRIX 6.1 is version 1.0 of the License Tools, license_eoe subsystem for IRIX 6.1. This version is not vulnerable to these security issues.

However, if an upgrade of the License Tools, license_eoe subsystem was done (see above section on determining version installed with versions command), then a security vulnerability might exist. In order to remove this vulnerability, either a downgrade to version 1.0 of the License Tools, license_eoe subsystem is required or upgrade the entire IRIX version to 6.2 and apply the version 3.0 of the License Tools, license_eoe subsystem.

**** IRIX 6.2 ****
For the IRIX operating system version 6.2 an inst-able new version of software has been generated and made available via anonymous FTP and your service/support provider. The software is version 3.0 of the License Tools, license_eoe subsystem and will install on IRIX 6.2 only.

The SGI anonymous FTP site is sgigate.sgi.com (204.94.209.1) or its mirror, ftp.sgi.com. Software is referred to as License6.2.tar and can be found in the following directories on the FTP server:

~ftp/Security
or
~ftp/Patches/6.2

Checksums

The actual software will be a tar file containing the following files:

Filename: license_eoe
Algorithm #1 (sum -r): 53638 7 license_eoe
Algorithm #2 (sum): 7547 7 license_eoe
MD5 checksum: 05A65EE03BEE71A464D4B7AB9962F228

Filename: license_eoe.books
Algorithm #1 (sum -r): 03494 907 license_eoe.books
Algorithm #2 (sum): 25664 907 license_eoe.books
MD5 checksum: AE86ED7D3C36F67C2505C06C41FCD174

Filename: license_eoe.idb
Algorithm #1 (sum -r): 15441 58 license_eoe.idb
Algorithm #2 (sum): 59702 58 license_eoe.idb
MD5 checksum: 811CD48FA5BD57E79B4D36839185EED9

Filename: license_eoe.man
Algorithm #1 (sum -r): 63961 271 license_eoe.man
Algorithm #2 (sum): 25496 271 license_eoe.man
MD5 checksum: 3086F992150A673C5110CCC16E20CA96

Filename: license_eoe.sw
Algorithm #1 (sum -r): 05953 7483 license_eoe.sw
Algorithm #2 (sum): 33599 7483 license_eoe.sw
MD5 checksum: BE52C7C2CCDAB2B491F6FA0412E4A66D

**** IRIX 6.3 ****
The license manager softwares provided with this version of
IRIX are not vulnerable to these security issues.

Sun Microsystems, Inc.

The following patches are now available from Sun.

Patch-ID# 104174-01
Keywords: CERT security license FLEXlm
Synopsis: FLEXlm Licensing (SUNWlicsw, SUNWlit): CERT security advisory patch
Date: Jan/13/97

Solaris Release: 2.4 2.5

SunOS Release: 5.4 5.5

Patch-ID# 104186-01
Keywords: CERT security license FLEXlm
Synopsis: FLEXlm (SUNWlicsw, SUNWlit): CERT security advisory patch
Date: Jan/13/97

Solaris Release: 2.4_x86 2.5_x86 2.5.1_x86

SunOS Release: 5.4_x86 5.5_x86 5.5.1_x86

Patch-ID# 104217-01
Keywords: CERT security license FLEXlm
Synopsis: FLEXlm (SUNWlicsw, SUNWlit) 4.1: CERT security advisory patch

Revision History

```
Sep. 26, 1997 Updated copyright statement

Jan. 22, 1997 Updates - Added SGI and Sun patch information.
```

2 CA-1997-02: HP-UX newgrp Buffer Overrun Vulnerability

Original issue date: January 7, 1997
Last revised: September 26, 1997
Updated copyright statement

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

The text of this advisory was originally released on December 3, 1996, as AA-96.16.HP-UX.newgrp.Buffer.Overrun.Vulnerability, developed by AUSCERT. Because of the seriousness of the problem, we are reprinting the AUSCERT advisory here with their permission. Only the contact information at the end has changed: AUSCERT contact information has been replaced with CERT/CC contact information.

We will update this advisory as we receive additional information. Look for it in an "Updates" section at the end of the advisory.

AUSCERT has received information that a vulnerability exists in the *newgrp(1)* program under HP-UX 9.x and 10.x.

This vulnerability may allow local users to gain root privileges.

Exploit information involving this vulnerability has been made publicly available.

Currently there are no vendor patches available that address this vulnerability. AUSCERT recommends that sites take the steps outlined in section 3 as soon as possible.

This advisory will be updated as more information becomes available.

1. Description

AUSCERT has received information that a vulnerability exists in the HP-UX *newgrp(1)* program. The newgrp command is used to change a users group identification, and is installed by default.

Due to insufficient bounds checking on arguments which are supplied by users, it is possible to overwrite the internal stack space of the newgrp program while it is executing. By supplying a carefully designed argument to the newgrp program, intruders may be able to force newgrp to execute arbitrary commands. As newgrp is setuid root, this may allow intruders to run arbitrary commands with root privileges.

This vulnerability is known to affect both HP-UX 9.x and 10.x.

By default, newgrp is located in /bin under HP-UX 9.x and in /usr/bin under HP-UX 10.x.

Exploit information involving this vulnerability has been made publicly available.

2. Impact

Local users may gain root privileges.

3. Workarounds/Solution

AUSCERT recommends that sites limit the possible exploitation of this vulnerability by immediately removing the setuid permissions as stated in Section 3.1. If the newgrp command is required, AUSCERT recommends the newgrp wrapper program given in Section 3.2 be installed.

AUSCERT recommends that official vendor patches be installed when they are made available. See the Updates section for information about availability of patches.

3.1 Remove setuid and non-root execute permissions

To prevent the exploitation of the vulnerability described in the advisory, AUSCERT recommends that the setuid permissions be removed from the newgrp program immediately. As the newgrp program will no longer work for non-root users, it is recommended that the execute permissions also be removed. Before doing so, the original permissions for newgrp should be noted as they will be needed if sites choose to install the newgrp wrapper program (Section 3.2).

```
For HP-UX 9.x:
# ls -l /bin/newgrp
-r-sr-xr-x 1 root sys 16384 Dec 2 13:45 /bin/newgrp
# chmod 500 /bin/newgrp
# ls -l /bin/newgrp
-r-x------ 1 root sys 16384 Dec 2 13:45 /bin/newgrp
For HP-UX 10.x:
# ls -l /usr/bin/newgrp
-r-sr-xr-x 1 root sys 12288 Dec 2 13:27 /usr/bin/newgrp
# chmod 500 /usr/bin/newgrp
# ls -l /usr/bin/newgrp
-r-x------ 1 root sys 12288 Dec 2 13:27 /usr/bin/newgrp
```

Note that this will remove the ability for any non-root user to run the newgrp program.

3.2 Install newgrp wrapper

AUSCERT has developed a wrapper to help prevent programs from being exploited using the vulnerability described in this advisory. This wrapper, including installation instructions, can be found at: ftp://ftp.auscert.org.au/pub/auscert/tools/overflow_wrapper.c.

This replaces the newgrp program with a wrapper which checks the length of the command line arguments passed to it. If an argument exceeds a certain predefined value (MAXARGLEN), the wrapper exits without executing the newgrp command. The wrapper program can also be configured to syslog any failed attempts to execute newgrp with arguments exceeding MAXARGLEN.

For further instructions on using this wrapper, please read the comments at the top of overflow_wrapper.c.

When compiling overflow_wrapper.c for use with HP-UX newgrp, AUSCERT recommends defining MAXARGLEN to be 16.

The MD5 checksum for Version 1.0 of overflow_wrapper.c is:

MD5 (overflow_wrapper.c) = f7f83af7f3f0ec1188ed26cf9280f6db

AUSCERT recommends that until vendor patches can be installed, sites requiring the newgrp functionality apply this workaround.

AUSCERT thanks Hewlett-Packard for their continued assistance and technical expertise essential for the production of this advisory. AUSCERT also thanks Information Technology Services of the University of Southern Queensland for their assistance.

Updates

April 4, 1997

The CERT/CC has received reports that the vulnerability described in this advisory is being exploited.

January 14, 1997

All HP patches are now available, see HEWLETT-PACKARD SECURITY BULLETIN: #00048, issued on 09 January 1997:

PHCO_9603 for all platforms with HP-UX releases 9.X
PHCO_9604 for all platforms with HP-UX releases 10.00/10.01
PHCO_9605 for all platforms with HP-UX releases 10.10/10.20

Fixing the problem

The vulnerability can be eliminated from HP-UX releases 9.X and 10.X by applying the appropriate patch.

Recommended solution

1. Determine which patch are appropriate for your operating system.
2. Hewlett-Packard's HP-UX patches are available via email and the World Wide Web

To obtain a copy of the Hewlett-Packard SupportLine email service user's guide, send the following in the TEXT PORTION OF THE MESSAGE to support@us.external.hp.com (no Subject is required):

send guide

The users guide explains the HP-UX patch downloading process via email and other services available.

World Wide Web service for downloading of patches is available via our URL: http://us.external.hp.com.

3. Apply the patch to your HP-UX system.

4. Examine /tmp/update.log (9.X), or /var/adm/sw/swinstall.log

(10.X), for any relevant WARNING's or ERROR's.

Revision History

```
Sep. 26, 1997 Updates - added copyright statement

Apr. 04, 1997 Updates - added note that the vulnerability is being
exploited.

Jan. 14, 1997 Updates - added patch information.
```

3 CA-1997-03: Vulnerability in IRIX csetup

Original issue date: January 8, 1997
Last revised: December 15, 1997
Added vendor information for Data General to UPDATES.

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

The CERT Coordination Center has received information about a vulnerability in the csetup program under IRIX versions 5.x, 6.0, 6.0.1, 6.1, and 6.2. csetup is not available under IRIX 6.3 and 6.4.

By exploiting this vulnerability, local users can create or overwrite arbitrary files on the system. With this leverage, they can ultimately gain root privileges.

Exploitation information involving this vulnerability has been made publicly available.

We recommend applying a vendor patch when possible. In the meantime, we urge sites to apply the workaround described in Section III.

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

Note: Development of this advisory was a joint effort of the CERT Coordination Center and AUSCERT.

I. Description

There is a vulnerability in the csetup program under IRIX versions 5.x, 6.0, 6.0.1, 6.1, and 6.2. csetup is not available under IRIX 6.3 and 6.4.

csetup is part of the Desktop System Administration subsystem. The program provides a graphical interface allowing privileged users, as flagged in the objectserver (cpeople (1M)), or root to modify system and network configuration parameters. The csetup program is setuid root to allow those who are flagged as privileged users to modify system critical files.

It is possible to configure csetup to run in DEBUG mode, creating a logfile in a publicly writable directory. This file is created in an insecure manner; and because csetup is running with root privileges at the time the logfile is created, it is possible for local users to create or overwrite arbitrary files on the system.

Exploit information involving this vulnerability has been made publicly available.

II. Impact

Anyone with access to an account on the system can create or overwrite arbitrary files on the system. With this leverage, they can ultimately gain root privileges.

III. Solution

Patch information for this vulnerability is available in SGI"s Security Advisory 19970101-02-PX, available at http://www.sgi.com/Support/Secur/security.html/.

This advisory is a collaborative effort between AUSCERT and the CERT Coordination Center. The CERT Coordination Center acknowledges Yuri Volobuev for reporting the original problem, and Silicon Graphics, Inc. for their strong support in the development of the advisory.

UPDATES

Vendor Information

Below is information we have received from vendors. If you do not see your vendor's name below, contact the vendor directly for information.

Data General

DG/UX does not support csetup and therefore is not vulnerable.

Revision History

```
Dec. 15, 1997 Added vendor information for Data General to UPDATES.

Sep. 26, 1997 Updated copyright statement

May 8, 1997   Updated the Solution section to include URL for
              SGI patch information.
```

4 CA-1997-04: talkd Vulnerability

Original issue date: January 27, 1997
Last revised: September 26, 1997
Updated copyright statement

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

The CERT Coordination Center has received reports of a vulnerability in *talkd(8)* program used by *talk(1)*. By constructing DNS data with particular characteristics, an intruder can remotely execute arbitrary commands with root privileges.

An exploitation script for this problem has been made publicly available, and we have received reports of successful root compromises involving the use of this script.

You may be aware of advisories that have been published by other response teams about this problem. Note that this advisory contains additional material and covers additional aspects of the vulnerability related to a broader set of problems of which this particular problem is only a specific instance.

The CERT/CC team recommends taking steps to solve the general problem (Sec. III.A) and installing a vendor patch to address this particular instance of the problem (Sec. III.B). Until you can install a patch, we urge you to disable the talkd program(s) at your site.

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

I. Description

The CERT Coordination Center has received information of a vulnerability in the *talkd(8)* program used by *talk(1)*. talk is a communication program that copies text from one user's terminal to that of another, possibly remote, user. talkd is the daemon that notifies a user that someone else wishes to initiate a talk conversation.

As part of the talk connection, talkd does a DNS lookup for the name of the host that the connection is being initiated from. Because there is insufficient bounds checking on the buffer where the hostname is stored, it is possible to overwrite the internal stack space of talkd.

It is possible to force talkd to execute arbitrary commands by carefully manipulating the hostname information. As talkd runs with root privileges, this may allow intruders to remotely execute arbitrary commands with these privileges.

This attack requires an intruder to be able to make a network connection to a vulnerable talkd program and provide corrupt DNS information to that host.

This type of attack is a particular instance of the problem described in CERT advisory CA-96.04, "Corrupt Information from Network Servers," available from http://www.cert.org/advisories/CA-96.04.corrupt_info_from_servers.

Sites that use BIND 4.9.4 Patch Level 1 or later are NOT vulnerable to the general class of host-name/ip-address-based buffer overflow attacks (including this specific problem).

Be aware that there are different versions of the talkd program. Depending on your system, the program may have any of the following names: talkd, otalkd, ntalkd.

To determine whether your site allows talk sessions, check /etc/inetd.conf:

grep -i "^[a-z]*talk" /etc/inetd.conf

Note: An exploitation script for this problem has been made publicly available. The CERT/CC has received reports of successful root compromises involving the use of this script.

II. Impact

Intruders may be able to remotely execute arbitrary commands with root privileges. They do not need access to an account on the system to exploit this vulnerability.

III. Solution

There are several options available to avoid this problem. We recommend that all sites defend against the general class of problem (Sec. A) and also install a patch from your vendor (Sec. B). Until you can install a patch, we urge you to disable the talkd program(s) at your site (Sec C).

Note that disabling the talkd program will defend against the particular attack described in this advisory, but will not defend against the general class of network-based attacks that manipulate hostname/ip-address information to exploit a vulnerability.

A. Defend against the general class of problem

In the general case, the problem described in this advisory is one in which the attacker uses particular hostname/ip-address data to exploit a vulnerability. The exploitation script mentioned above uses the specific case of DNS attacks, but attackers can use other hostname/ip-address resolution methods, such as NIS, /etc/hosts, and so on.

If the following measures are in place for all hostname/address transformation techniques on your system, then your system would be immune not only to this particular talkd exploit, but also to the general class of hostname/ip-address-based buffer overflow attacks.

1. DNS-Based Attacks

To defend against a DNS-based attack, we encourage you to upgrade to BIND 4.9.4 Patch level 1 or later (or your vendor's equivalent). The reason is that BIND 4.9.4 Patch Level 1 conforms to

the RFC (RFC 952) defining valid hostname syntax (described in CERT advisory CA-96.04, "Corrupt Information from Network Servers").

Keep in mind that an upgrade to 4.9.5 may require a sendmail upgrade because of the POSIX extensions in the latest version of BIND (described in CA-96.04). For the latest available version of sendmail, please consult the file ftp://ftp.cert.org/pub/latest_sw_versions/sendmail,

2. Other Network Information Services

For systems that rely on additional name/address transformation techniques (such as NIS, netinfo, and flat files like /etc/hosts), using the recommended version of BIND may be insufficient since DNS lookups--and therefore hostname/ip-address validation--may be bypassed in favor of the alternative technique (NIS, netinfo, etc). Thus, we also encourage sites and vendors to include in the suite of resolution techniques the same code that BIND uses to validate hostnames and IP addresses. This code is described in the next section.

3. In-house Software

Use the hostname and IP address validation subroutines available at the locations listed below. Include them in all programs that use the result of the hostname lookups in any way.

ftp://ftp.cert.org/pub/tools/ValidateHostname/IsValid.c

ftp://ftp.cert.dfn.de/pub/tools/net/ValidateHostname/IsValid.c

The IsValid.c file contains code for the IsValidHostname and IsValidIPAddress subroutines. This code can be used to check host names and IP addresses for validity according to RFCs 952 and 1123, as well as names containing characters drawn from common practice, namely "_" and "/".

The following files are in the directory (from the README):

IsValid.1	The Lex/Flex file containing the code for IsValidHostname and IsValidIPAddress MD5 (IsValid.1 = 2d35040aacae4fb12906eblb48957776
IsValid-raw.c	The C File created by running flex on is IsValid.l MD5 (IsValid-raw.c) = 367c77d3ef84bc63a5c23d90eeb69330
IsValid.c	The edited file created by internalizing variable and function definititions in IsValid-raw.c MD5 (IsValid.c) = ffe45f1256210aeb71691f4f7cdad27f

IsValid.diffs	The set of diffs between IsValid-raw.c and IsValid.c MD5 (IsValid.diffs) = 3619022cf31d735151f8e8c83cce3744
htest.c	A main routing for testing IsValidHostname and IsValidIPAddress MD5 (htest.c) = 2d50b2bffb537cc4e637dd1f07a187f4

B. Install a patch from your vendor

Below is a list of the vendors who have provided information. Details are in Appendix A of this advisory; we will update the appendix as we receive additional information.

If your vendor's name is not on this list, we have not received any information. Please contact the vendor directly.

Berkeley Software Design, Inc. (BSDI)
Cisco Systems
Data General Corporation
FreeBSD, Inc.
Hewlett-Packard Company
IBM Corporation
Linux
NEC Corporation
The Santa Cruz Operation, Inc. (SCO)
Silicon Graphics Inc. (SGI)
Solbourne (Grumman System Support)
Sun Microsystems, Inc.

C. Disable the talkd program(s)

Until you can install a vendor patch, disable any talkd programs found in /etc/inetd.conf by commenting out those lines and restarting inetd.

Example commands executed as root:

grep -i talk /etc/inetd.conf

```
talk    dgram    udp    wait    root    /usr/etc/in.talkd        in.talkd
```

Comment out *all* references to talkd, otalkd or ntalkd.
(Comments in # /etc/inetd.conf begin with "#".)

After editing /etc/inetd.conf, restart inetd. On many Unix systems, this is done by sending the inetd process a HUP signal.

For SYSV:

ps -ef | grep inetd | grep -v grep
kill -HUP {inetd PID}

For BSD:

ps -aux | grep inetd | grep -v grep
kill -HUP {inetd PID}

Note that disabling talkd will solve the specific problem discussed in this advisory. However it will not solve the general problem of network-based attacks that manipulate hostname/ip-address information to exploit a vulnerability.

Appendix A Vendor Information

Below is a list of the vendors who have provided information for this advisory. We will update this appendix as we receive additional information. If you do not see your vendor's name, please contact the vendor directly.

Berkeley Software Design, Inc. (BSDI)

We have released an official patch (U210-035). It's available from our patches@BSDI.COM mail-back server or via anonymous ftp at:

ftp://ftp.bsdi.com/bsdi/patches/patches-2.1/U210-035

Cisco Systems

Cisco MultiNet for OpenVMS - not vulnerable.

Data General Corporation

Data General is not vulnerable.

FreeBSD, Inc.

We have released an advisory dated 1997-01-18, FreeBSD-SA-96:21.
The advisory can be found at
ftp://freebsd.org/pub/CERT/advisories/FreeBSD-SA-96:21.talkd.asc.

Patches are available at ftp://freebsd.org/pub/CERT/patches/SA-96:21.

Hewlett-Packard Company

HPSBUX9704-061
HEWLETT-PACKARD SECURITY BULLETIN: #00061
Description: Security Vulnerability in talkd
Security Bulletins are available from the HP Electronic
Support Center via electronic mail.

User your browser to get to the HP Electronic Support
Center page at:

http://us-support.external.hp.com (for US, Canada, Asia-Pacific, & Latin-America)
http://europe-support.external.hp.com (for Europe)

IBM Corporation

The version of talkd shipped with AIX is vulnerable to the conditions described in this advisory. The APARs listed below will be available shortly. It is recommended that the talkd daemon be turned off until the APARs are applied.

AIX 3.2: APAR IX65474 AIX 4.1: APAR IX65472 AIX 4.2: APAR IX65473	To Order APARs may be ordered using Electronic Fix Distribution (via FixDist) or from the IBM Support Center. For more information on FixDist, reference URL: http://service.software.ibm.com/aixsupport/ or send e-mail to aixserv@austin.ibm.com with a subject of "FixDist". IBM and AIX are registered trademarks of International Business Machines Corporation.

Linux

This bug was fixed in Linux NetKit 0.08 which is shipped with all reasonably up to date Linux distributions. Linux users using NetKit 0.07 or earlier should upgrade to NetKit 0.09. NetKit 0.09 has fixed other bugs and it is strongly recommended Linux users upgrade from NetKit 0.08 to NetKit 0.09. This is available from ftp://ftp.uk.linux.org/pub/linux/Networking/base/NetKit-0.09.tar.gz.

Some vendors have opted to issue NetKit 0.08 with additional fixes rather than 0.09. Consult your vendor for detailed information.

The Linux community would like to thank David A Holland for his continuing work on Linux network security.

NEC Corporation

UX/4800	Vulnerable for all versions.
EWS-UX/V(Rel4.2MP)	Vulnerable for all versions.
EWS-UX/V(Rel4.2)	Vulnerable for all versions.
UP-UX/V(Rel4.2MP)	Vulnerable for all versions.

Patches for these vulnerabilities are in progress.
Contacts for further information by e-mail: UX48-security-support@nec.co.jp.

The Santa Cruz Operation, Inc. (SCO)

SCO is investigating the problem with talkd and will provide updated information for this advisory as it becomes available. At this time SCO recommends disabling talkd on your SCO system as described herein.

Silicon Graphics Inc. (SGI)

For additional information refer to the Silicon Graphics Inc. Security Advisory Number 19970701-01-PX.

The SGI anonymous FTP site is sgigate.sgi.com (204.94.209.1) or its mirror, ftp.sgi.com. Security information and patches can be found in the ~ftp/security and ~ftp/patches directories, respectfully.

Solbourne (Grumman System Support)

We have examined the Solbourne implementation and found that it is vulnerable. Solbourne distributed the Sun application under license. We will distribute a Solbourne patch based on the Sun patch when it becomes available. For the latest information on our patches go to http://ftp.nts.gssc.com/solbourne.html

The workaround of disabling in.talkd can be used.

as root:

```
/etc/inetd.conf - comment out the talkd program

# ps -aux | grep inetd | grep -v grep

# kill -HUP {inetd PID listed in output of last command}
```

Sun Microsystems, Inc.

For additional information refer to the Sun Microsystems, Inc. Security Bulletin Number #00147. Patches are available to all Sun customers via World Wide Web at: ftp://sunsolve1.sun.com/pub/patches/patches.html.

Customers with Sun support contracts can also obtain patches from local Sun answer centers and SunSITEs worldwide.

Sun security bulletins are available via World Wide Web at: http://sunsolve1.sun.com/sunsolve/secbulletins.

Revision History

```
September 26, 1997 Updated copyright statement
```

July 28, 1997 Appendix A - updated patch information for Silicon Graphics, Inc. and Sun Microsystems, Inc.

May 8, 1997 Appendix A - updated patch information for Hewlett-Packard.

Feb. 7, 1997 Appendix A - added an entry for Cisco Systems.

5 CA-1997-05: MIME Conversion Buffer Overflow in Sendmail Versions 8.8.3 and 8.8.4

Original issue date: January 28, 1997
Last revised: April, 8 2003
Updated copyright statement

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

The CERT Coordination Center has received reports of a vulnerability in sendmail versions 8.8.3 and 8.8.4. By sending a carefully crafted email message to a system running a vulnerable version of sendmail, intruders may be able to force sendmail to execute arbitrary commands with root privileges.

The CERT/CC team recommends that you install a vendor patch (Section III.A) or upgrade to sendmail 8.8.5 (Section III.B). We have provided a workaround that you can use on vulnerable versions of 8.8.3 and 8.8.4 until you are able to implement one of these solutions (Section III.C).

Regardless of the solution you apply, we urge you to take the additional precautions described in-Section III.D. Note that this advisory contains additional material to that previously published by other response teams.

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

I. Description

Sendmail version 8 contains support for MIME (Multipurpose Internet Mail Extensions) as defined initially by RFC 1341 and modified by RFC 1521. The central idea behind MIME is the following, taken from the introduction to RFC 1341:

"... designed to provide facilities to include multiple objects in a single message, to represent body text in character sets other than US-ASCII, to represent formatted multi-font text messages, to represent non-textual material such as images and audio fragments, and generally to facilitate later extensions defining new types of Internet mail for use by cooperating mail agents."

The support in sendmail version 8 includes data translations in which a message's body is either stripped to 7-bit ASCII, achieved by forcing the 8th bit to be off, or 8-bit MIME, achieved by leaving the 8th bit as is.

Sendmail can be configured for either of these translations on a mailer-by-mailer basis depending on the flags defined for that mailer. The flags in question here are `7', `8', and `9' (the default). Refer to the "Sendmail Installation and Operations Guide," Section 5.4, for a more complete discussion. A PostScript version of this guide is included in the sendmail distribution in the /doc/op directory.

With the release of sendmail version 8.8.3, a serious security vulnerability was introduced that allows remote users to execute arbitrary commands on the local system with root privileges. By sending a carefully crafted email message to a system running a vulnerable version of sendmail, intruders may be able to force sendmail to execute arbitrary commands with root privileges. Those commands are run on the same system where the vulnerable sendmail is running.

In most cases, the MIME conversion of email is done on final delivery; that is, to the local mailbox or a program. Therefore, this vulnerability may be exploited on systems despite firewalls and other network boundary protective measures.

Versions before 8.8.3 do not contain this vulnerability, but they do contain other vulnerabilities. We strongly recommended that you follow the steps given in Section III below to eliminate those vulnerabilities from your systems.

Determining if you are vulnerable

Systems are vulnerable to this attack if both of the following conditions are true:

1. **The version of sendmail is 8.8.3 or 8.8.4.**
2. To determine the version of sendmail, use the following command:

   ```
   % /usr/lib/sendmail -d0 -bt < /dev/null | grep -i Version
   ```

   If the string returned is "Version 8.8.3" or "Version 8.8.4", then this version of sendmail contains the vulnerability. Typically, sendmail is located in the /usr/lib directory, but it may be elsewhere on your system.

3. **When you examine the sendmail configuration file (usually, /etc/sendmail.cf), the `9' flag is set in the "F=" (Flags) section for any Mailer specifications (Sections starting with `M' in the first column, such as "Mprog" or "Mlocal").**
4. Use of the `9' flag can usually be determined using the following command (depending on your sendmail configuration):

   ```
   % grep '^M.*F=[^,]*9' /etc/sendmail.cf
   ```

   If any lines are output from this command, then the sendmail configuration may be vulnerable.

   The `9' flag is set by default for the local and program mailers when the sendmail.cf file is generated using the m4 files distributed with sendmail version 8.8.x. Versions of sendmail before 8.8.0 did not set this flag by default when generating sendmail.cf. The `9' flag is also set by default in the precompiled example configuration files found in the cf/cf/obj/ subdirectory of the sendmail version 8.8.x distribution.

II. Impact

Remote users can gain root privileges on a machine running sendmail versions 8.8.3 or 8.8.4 that does 7-to-8 bit conversion. They do not need access to an account on the system to exploit the vulnerability.

III. Solution

Install a patch from your vendor if one is available (Section A) or upgrade to the current version of sendmail (Section B). Until you can take one of those actions, we recommend applying the workaround described in Section C. In all cases, you should take the precautions described in Section D.

A. Install a vendor patch.

Below is a list of vendors who have provided information about sendmail. Details are in Appendix A of this advisory; we will update the appendix as we receive more information. If your vendor's name is not on this list, the CERT/CC did not hear from that vendor. Please contact the vendor directly.

Berkeley Software Design, Inc. (BSDI)
Caldera OpenLinux
Cray Research - A Silicon Graphics Company
Data General Corporation
Digital Equipment Corporation
Hewlett-Packard Corporation
IBM Corporation
NEC Corporation
NeXT Software, Inc.
Silicon Graphics, Inc.
Sun Microsystems, Inc.

B. Upgrade to sendmail version 8.8.5.

Eric Allman has released a new version of sendmail which fixes this vulnerability. This can be obtained from the following locations:

ftp://ftp.sendmail.org/pub/sendmail/
ftp://ftp.cs.berkeley.edu/ucb/src/sendmail/
ftp://ftp.auscert.org.au/pub/mirrors/ftp.cs.berkeley.edu/ucb/sendmail/
ftp://ftp.cert.dfn.de/pub/tools/net/sendmail/
ftp://ftp.cert.org/pub/tools/sendmail/

The MD5 checksum for this distribution is:

MD5 (sendmail.8.8.5.patch) = 775c47d16d40ebd2b917dfcc65d92e90

MD5(sendmail.8.8.5.tar.gz) = 7c32c42a91325dd00b8518e90c26cffa

MD5 (sendmail.8.8.5.tar.sig) = b62ba16c7e863853b3efeb955eec4214

MD5 (sendmail.8.8.5.tar.Z) = 7b847383899c0eb65987213a5caf89c8

Also in that directory are .Z and .sig files. The .Z file contains the same bits as the .gz file, but it is compressed using UNIX compress instead of gzip. The .sig is Eric Allman's PGP signature for the uncompressed tar file. The key fingerprint is

```
Type bits/keyID    Date       User ID

pub  1024/BF7BA421 1995/02/23 Eric P. Allman eric@CS.Berkeley.EDU

        Key fingerprint =  C0 28 E6 7B 13 5B 29 02  6F 7E 43 3A 48
4F 45 29

                                  Eric P. Allman  eric@Reference.COM

                                  Eric P. Allman  eric@Usenix.ORG

                                  Eric P. Allman  eric@Sendmail.ORG

                                  Eric P. Allman  eric@CS.Berkeley.EDU
```

When you change to a new version of sendmail, we strongly recommend also changing to the configuration files that are provided with that version. (In fact, it is highly likely that older configuration files will not work correctly with sendmail version 8.) It is now possible to build a sendmail configuration file (sendmail.cf) using the configuration files provided with the sendmail release. Consult the cf/README file for a more complete explanation. Creating your configuration files using this method makes it easier to incorporate future changes to sendmail into your configuration files.

C. Workaround for existing sendmail version 8.8.3 and 8.8.4 installations

Eric Allman, the author of sendmail, has provided the following workaround, which you can use until you can take the steps recommended in Sec. A or B.

The /etc/sendmail.cf file should be modified to remove the use of the `9' flag for all Mailer specifications (lines starting with `M').

As an example, the sendmail.cf file should look similar to the following which is for a Solaris 2.5.1 system running sendmail version 8.8.4:

Mlocal,	P=/usr/lib/ml.local, F=lsDFMAw5:/|@qSnE, S=10/30, R=20/40, T=DNS/RFC822/X-Unix, A=mail -d $u
Mprog,	P=/usr/local/bin/smrsh, F=lsDFMoqeu, S=10/30, R=20/40, D=$z:/, T= X-UNix,
!	A=smrsh -c $u

This can be achieved for the "Mlocal" and "Mprog" Mailers by modifying the ".mc" file to include the following lines:

```
        OSTYPE(solaris2)
        FEATURE(smrsh, /usr/local/bin/smrsh)
+        define(`LOCAL_SHELL_ARGS', `smrsh -c $u')
        define(`LOCAL_MAILER_PATH', /usr/lib/mail.local)
        define(`LOCAL_MAILER_FLAGS',
            ifdef(`LOCAL_MAILER_FLAGS',
                `translit(LOCAL_MAILER_FLAGS, `9')',
                `rmn'))
        define(`LOCAL_SHELL_FLAGS',
            ifdef(`LOCAL_SHELL_FLAGS',
                `translit(LOCAL_SHELL_FLAGS, `9')',
                `eu'))
```

Next, rebuild the sendmail.cf file using m4(1). See also Section III.D for additional precautions that you should take. These precautions have been taken in the example above.

The defines of LOCAL_MAILER_FLAGS and LOCAL_SHELL_FLAGS should be placed in your m4(1) input file *after* the operating system is identified using the OSTYPE directive, and after any other defines of either the LOCAL_MAILER_FLAGS or LOCAL_SHELL_FLAGS.

It is possible to directly edit the sendmail.cf file to resolve this vulnerability. However, take caution to ensure that the sendmail.cf file is not replaced in the future with a new version rebuilt from configuration files that include the `9' flag.

Once the configuration file has been modified, all running versions of sendmail should be killed and the sendmail daemon restarted with the following (done as root):

```
# kill -1 `head -1 /var/run/sendmail.pid`
```

The pathname may be different on your system. Verify that a new daemon was started using "(echo quit; sleep 1) | telnet localhost 25". Alternatively, reboot your system.

D. Take additional precautions

Regardless of which solution you apply, you should take these extra precautions to protect your systems. These precautions do not address the vulnerabilities described herein, but are recommended as good practices to follow for the safer operation of sendmail.

- Use the sendmail restricted shell program (smrsh)
- With *all* versions of sendmail, use the sendmail restricted shell program (smrsh). You should do this whether you use vendor-supplied sendmail or install sendmail yourself. Using

smrsh gives you improved administrative control over the programs sendmail executes on behalf of users.

Many sites have reported some confusion about the need to continue using the sendmail restricted shell program (smrsh) when they install a vendor patch or upgrade to a new version of sendmail. You should always use the smrsh program.

smrsh is included in the sendmail Version 8 distribution in the subdirectory smrsh. See the RELEASE_NOTES file for a description of how to integrate smrsh into your sendmail configuration file.

smrsh is also distributed with some operating systems.

If you are using the m4(1)-based configuration scheme provided with sendmail 8.X, add the following to your configuration file, where /usr/local/bin is replaced by the name of the directory where you have installed smrsh on your system:

FEATURE(smrsh, /usr/local/bin/smrsh)

- Use mail.local
- If you run /bin/mail based on BSD 4.3 UNIX, replace /bin/mail with mail.local, which is included in the sendmail distribution. As of Solaris 2.5 and beyond, mail.local is included with the standard distribution. It is also included with some other operating systems distributions, such as FreeBSD.
  Although the current version of mail.local is not a perfect solution, it is important to use it because it addresses vulnerabilities that are being exploited. For more details, see CERT advisory CA-95.02:

  http://www.cert.org/advisories/CA-95.02.binmail.vulnerabilities.

  To use mail.local, replace all references to /bin/mail with /usr/lib/mail.local. If you are using the M4(1)-based configuration scheme provided with sendmail 8.X, add the following to your configuration file:

  define(`LOCAL_MAILER_PATH', /usr/lib/mail.local)

- WARNING: Check for setuid executable copies of old versions of mail programs
- If you leave setuid executable copies of older versions of sendmail installed in /usr/lib (on some systems it may be installed elsewhere), the vulnerabilities in those versions could be exploited if an intruder gains access to your system. This applies to sendmail.mx as well as other sendmail programs. Either delete these versions or change the protections on them to be non-executable.

  Similarly, if you replace /bin/mail with mail.local, remember to remove old copies of /bin/mail or make them non-executable.

Appendix A Vendor Information

Below is a list of the vendors who have provided information for this advisory. We will update this appendix as we receive additional information. If you do not see your vendor's name, please contact the vendor directly.

Berkeley Software Design, Inc. (BSDI)

Fully patched BSD/OS 2.1 systems are vulnerable to this problem. An official patch is available from the patches server at patches@BSDI.COM or via anonymous ftp from: ftp://ftp.bsdi.com/bsdi/patches/patches-2.1/U210-036.

Caldera OpenLinux

An upgrade for Caldera OpenLinux Base 1.0 can be found at: ftp://ftp.caldera.com/pub/col-1.0/updates/Helsinki/003/RPMS/sendmail-8.8.5-1.i386.rpm.

See also the README at: ftp://ftp.caldera.com/pub/col-1.0/updates/Helsinki/003/README.

Cray Research - A Silicon Graphics Company

Cray Research has not yet released a sendmail based on a version 8.8.3 or later, so this is not a problem for any released Unicos system.

Data General Corporation

The sendmail that ships with DG/UX is not subject to this vulnerability.

Digital Equipment Corporation

This reported problem is not present for Digital's ULTRIX or Digital UNIX Operating Systems Software.
SOURCE:
Digital Equipment Corporation
Software Security Response Team

Hewlett-Packard Corporation

After an investigation based on the information contained in the CERT bulletin, we have come to the conclusion that none of the current versions of HP sendmail (HPUX 9.x, HPUX pre-10.2, HPUX 10.2) are vulnerable to the security hole mentioned in the bulletin.

IBM Corporation

The version of sendmail shipped with AIX is not vulnerable to the 7 to 8 bit MIME conversion vulnerability detailed in this advisory.

IBM and AIX are registered trademarks of International Business Machines Corporation.

NEC Corporation

Systems below are not shipped with a sendmail based on a version 8.8.3 or later, so this problem is not present for them.

UX/4800	Not vulnerable for all versions.
EWS-UX/V(Rel4.2MP)	Not vulnerable for all versions.
EWS-UX/V(Rel4.2)	Not vulnerable for all versions.
UP-UX/V(Rel4.2MP)	Not vulnerable for all versions.
EWS-UX/V(Rel4.0)	Not vulnerable for all versions.
UP-UX/V	Not vulnerable for all versions.

NeXT Software, Inc.

NeXT is not vulnerable to the MIME-buffer overflow attack.

Silicon Graphics, Inc.

The versions of sendmail provided in the distributed Silicon Graphics IRIX operating system versions 5.2, 5.3, 6.0, 6.0.1, 6.1, 6.2 and 6.3 (and in SGI patch 1502, which is the latest released patch for sendmail) are 8.6.x versions of the sendmail program. The latest official released version of sendmail from Silicon Graphics is 8.6.12. As such, Silicon Graphics finds no current version of Silicon Graphics sendmail to be vulnerable to this 8.8.x based attack.

Sun Microsystems, Inc.

Sun is confident that no Sun sendmail is vulnerable to the MIME-buffer overflow attack.

The CERT Coordination Center thanks Eric Allman for his help in developing the patches for sendmail and in the writing of this advisory. Thanks also to DFN-CERT and AUSCERT for their assistance in producing this document.

Revision History

```
Sep. 26, 1997 Updated copyright statement

Mar. 05, 1997 Appendix A, updated NEC entry

Feb. 11, 1997 Sec. III. C, example sendmail.cf file - one line
changed and one added (changes marked at the left margin)

Apr. 08, 2003 Minor formatting changes, no change to contents
```

6 CA-1997-06: Vulnerability in rlogin/term

Original issue date: February 6, 1997
Last revised: February 12, 1998
Added vendor information for NCR Corporation.
November 14, 1997 Added vendor information for Data General Corporation.

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

The CERT Coordination Center has received reports of a vulnerability in many implementations of the rlogin program, including eklogin and klogin. By exploiting this vulnerability, users with access to an account on the system can cause a buffer overflow and execute arbitrary programs as root.

The CERT/CC staff recommends installing a vendor patch for this problem (Sec. III.A). Until you can do so, we urge you to turn off rlogin or replace it with a wrapper (see Sec. III.B.2).

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

I. Description

The rlogin program provided by many UNIX systems, as well as some non-UNIX systems, is described in RFC 1282. Here is an excerpt from that RFC that describes its elemental functionality:

"The rlogin facility provides a remote-echoed, locally flow- controlled virtual terminal with proper flushing of output. It is widely used between Unix hosts because it provides transport of more of the Unix terminal environment semantics than does the Telnet protocol, and because on many Unix hosts it can be configured not to require user entry of passwords when connections originate from trusted hosts."

The key point from this description is that the rlogin program passes the terminal type description from the local host to the remote host. This functionality allows terminal-aware programs such as full-screen text editors to operate properly across a computer-to-computer connection created with rlogin.

To do this, the rlogin program uses the current terminal definition as identified by the TERM environment variable. The protocol described in RFC 1282 explains how this terminal information is transferred from the local machine where the rlogin client program is running to the remote machine where service is sought.

Unfortunately, many implementations of the rlogin program contain a defect whereby the value of the TERM environment variable is copied to an internal buffer without due care. The buffer holding the copied value of TERM can be overflowed. In some implementations, the buffer is a local

variable, meaning that the subroutine call stack can be overwritten and arbitrary code executed. The executed code is under the control of the user running the rlogin program.

In addition, the rlogin program is set-user-id root. rlogin requires these increased privileges so it can allocate a port in the required range, as described in the in.rlogind (or rlogind) manual page: "The server checks the client's source port. If the port is not in the range 0-1023, the server aborts the connection."

In summary, rlogin is a set-user-id root program that in many implementations contains a programming defect whereby an internal buffer can be overflowed and arbitrary code can be executed as root.

II. Impact

Users can become root if they have access to an account on the system.

III. Solution

Install a patch from your vendor if one is available (Section A). Until you can take one of those actions, we recommend applying the workaround described in Section B.

A. Obtain and install a patch for this problem.

Below is a list of vendors who have provided information about rlogin. Details are in Appendix A of this advisory; we will update the appendix as we receive more information. If your vendor's name is not on this list, the CERT/CC did not hear from that vendor. Please contact your vendor directly.

Berkeley Software Design, Inc. (BSDI)
Cray Research - A Silicon Graphics Company
Cygnus Solutions (formerly Cygnus Support)
Data General Corporation
Digital Equipment Corporation
FreeBSD, Inc.
Hewlett-Packard Corporation
IBM Corporation
Linux Systems
NCR Corporation
NEC Corporation
NetBSD
NeXT Software, Inc.
The Open Group
The Santa Cruz Operation (SCO)
Sun Microsystems, Inc.

B. Until you are able to install the appropriate patch, we recommend one of the following workarounds:

1. Turn off rlogin.

If your user community does not use rlogin, turn it off. As root, do the following:

% chmod 0 /usr/bin/rlogin

You may find the rlogin program in some other directory on your system. Example directories are: /bin, /usr/bin, /usr/ucb.

Note: On some systems, rlogin is provided in different forms that do additional work. Examples are eklogin (kerberos authentication plus encryption of the data stream) and klogin (kerberos authentication only). These, too, need to be turned off.

2. Replace the rlogin program with a wrapper.

We have written a prototype wrapper that is available at
ftp://ftp.cert.org/pub/tools/rlogin_wrapper/rlogin_wrapper.c.

The PGP signature for this file is available at
ftp://ftp.cert.org/pub/tools/rlogin_wrapper/rlogin_wrapper.c.asc.

To verify that this file is correct, fetch both the rlogin_wrapper.c and rlogin_wrapper.c.asc files and check the signature with pgp as in

% pgp rlogin_wrapper.c.asc rlogin_wrapper.c

Notes:

- You may have to change this program to get it to compile and work correctly on your system.
- If you have different forms of rlogin, as noted in the previous section, then you will need to replace those forms with the wrapper as well.

Appendix A Vendor Information

Below is a list of the vendors who have provided information for this advisory. We will update this appendix as we receive additional information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact the vendor directly.

Berkeley Software Design, Inc. (BSDI)

Unpatched BSD/OS 2.1 systems are vulnerable to this problem. A patch was issued that resolved this problem in August 1996. The patch is available from the patches@BSDI.COM mail server or via anonymous ftp at: ftp://ftp.bsdi.com/bsdi/patches/patches-2.1/U210-021.

Cray Research - A Silicon Graphics Company

This problem has been corrected in all currently supported versions of Unicos.

Cygnus Solutions (formerly Cygnus Support)

CNS (our product based on Kerberos V4) all releases are not vulnerable.

KerbNet Security System (our product based on Kerberos V5) all releases are not vulnerable. Since our version of rlogin is not installed set-user-id root, it is not vulnerable. To secure a machine which is running our rlogin, all that is necessary is to secure the vendor rlogin.

Data General Corporation

The rlogin program included in DG/UX revisions prior to R4.12/R4.11MU03 do contain this vulnerability. This problem has been fixed in the rlogin program released with DG/UX revisions R4.12/R4.11MU03 and later.

Digital Equipment Corporation

At the time of writing this document, patches(binary kits) are available from your normal Digital Support Channel.

rlogin patches are available for:

DIGITAL UNIX V3.2c, V3.2de1/de2, V3.2g, V3.2g, V4.0, V4.0a, V4.0b. DIGITAL ULTRIX V4.4 VAX & MIPS, V4.5 VAX and MIPS

DIGITAL EQUIPMENT CORPORATION

FreeBSD, Inc.

This vulnerability is present in FreeBSD 2.1.5 and previous versions. It was fixed in all FreeBSD source and binary distributions dated after 1996/07/25.

The following source code patch may be applied to FreeBSD 2.1.5 based distributions, and should work in previous distributions. Users unable to apply this patch and recompile the rlogin binary are encouraged to use the wrapper provided by CERT.

Index: rlogin.c

```
RCS file: /home/ncvs/src/usr.bin/rlogin/rlogin.c,v
retrieving revision 1.5.4.1
retrieving revision 1.5.4.2
diff -c -r1.5.4.1 -r1.5.4.2
```

```
*** rlogin.c    1996/06/23 13:08:27     1.5.4.1
- --- rlogin.c    1996/07/25 18:29:35     1.5.4.2
***************
*** 102,107 ****
- --- 102,108 ----
  char *speeds[] = {
        "0", "50", "75", "110", "134", "150", "200", "300", "600",
"1200",
        "1800", "2400", "4800", "9600", "19200", "38400", "57600",
"115200"
+ #define       MAX_SPEED_LENGTH        (sizeof("115200") - 1)
  };
  #ifdef OLDSUN
***************
*** 259,265 ****
                exit(1);
        }
!       (void)strcpy(term, (p = getenv("TERM")) ? p : "network");
        if (ioctl(0, TIOCGETP, &ttyb) == 0) {
                (void)strcat(term, "/");
                (void)strcat(term, speeds[(int)ttyb.sg_ospeed]);
- --- 260,270 ----
                exit(1);
        }
! #define       MAX_TERM_LENGTH (sizeof(term) - 1 - MAX_SPEED_LENGTH
- 1)
!
!       (void)strncpy(term, (p = getenv("TERM")) ? p : "network",
!                     MAX_TERM_LENGTH);
!       term[MAX_TERM_LENGTH] = '\0';
        if (ioctl(0, TIOCGETP, &ttyb) == 0) {
                (void)strcat(term, "/");
                (void)strcat(term, speeds[(int)ttyb.sg_ospeed]);
```

Hewlett-Packard Corporation

For updated information, please refer to the Hewlett-Packard Security Bulletin "Security Vulnerability with rlogin," Document ID: HPSBUX9707-066.

Use your browser to get to the HP Electronic Support Center page at:

http://us-support.external.hp.com (for US, Canada, Asia-Pacific, & Latin-America)

http://europe-support.external.hp.com (for Europe)

Click on the Technical Knowledge Database, register as a user (remember to save the User ID assigned to you, and your password), and it will connect to a HP Search Technical Knowledge DB page. Near the bottom is a hyperlink to our Security Bulletin archive. Once in the archive there is another link to our current security patch matrix. Updated daily, this matrix is categorized by platform/OS release, and by bulletin topic.

IBM Corporation

See the appropriate release below to determine your action.

AIX 3.2

Apply the following fix to your system:

APAR - IX57724 (PTF - U442613)

To determine if you have this PTF on your system, run the following command:

lslpp -lB U442613

AIX 4.1

Apply the following fix to your system:

APAR - IX57972

To determine if you have this APAR on your system, run the following command:

instfix -ik IX57972

Or run the following command:

lslpp -h bos.net.tcp.client

Your version of bos.net.tcp.client should be 4.1.4.13 or later.

AIX 4.2

No APAR required. Fix already contained in the release.

To Order

APARs may be ordered using Electronic Fix Distribution (via FixDist) or from the IBM Support Center. For more information on FixDist: http://service.software.ibm.com/aixsupport/ or send e-mail to aixserv@austin.ibm.com with a subject of "FixDist".

IBM and AIX are registered trademarks of International Business Machines Corporation.

Linux Systems

Only very out of date Linux systems are vulnerable.

Linux Netkit 0.08 has rlogin fixed. All Linux systems using older NetKits should upgrade to NetKit 0.09. Some vendors have shipped patched Netkit-0.08 releases. Check with your vendor for confirmation.

NetKit 0.09 is available from:
ftp://ftp.uk.linux.org/pub/linux/Networking/base/NetKit-0.09.tar.gz.

NCR Corporation

NCR is delivering a set of operating system dependent patches which contain an update for this problem. Accompanying each patch is a README file which discusses the general purpose of the patch and describes how to apply it to your system.

Recommended solution: Apply one of the following patches depending on the revision of the inet package installed on your system. To check its version execute:

```
pkginfo -x inet

For inet 5.01: - PINET501 (Version 5.01.01.25)


For inet 6.01: - PINET610 (Version 6.01.00.17)

For inet 6.02: - Fix included.
```

NEC Corporation

UX/4800	Not vulnerable for all versions.
EWS-UX/V(Rel4.2MP)	Not vulnerable for all versions.
EWS-UX/V(Rel4.2)	Not vulnerable for all versions.
UP-UX/V(Rel4.2MP)	Not vulnerable for all versions.
EWS-UX/V(Rel4.0)	Not vulnerable for all versions.
UP-UX/V	Not vulnerable for all versions.

NetBSD

This was fixed in NetBSD some time ago, and is part of the 1.2 release. NetBSD 1.1 and prior are vulnerable to this, and the best solution is to upgrade, or at least obtain new src/usr.bin/rlogin source and recompile.

NeXT Software, Inc.

This problem is fixed in OpenStep/Mach release 4.1 and later.

The Open Group

This problem was fixed in OSF's OSF/1 R1.3.3 maintenance release.

The Santa Cruz Operation (SCO)

SCO is investigating this problem and should a patch be necessary, SCO will provide updated information for this advisory. Patches for SCO products are listed at ftp://ftp.sco.COM/SLS/README.

Sun Microsystems, Inc.

The vulnerability in rlogin is fixed by the following patches:

OS version		Patch ID
SunOS 5.5.1	-	104650-02
SunOS 5.5.1_x86	-	104651-02
SunOS 5.5	-	104669-02
SunOS 5.5_x86	-	104670-02
SunOS 5.4	-	105254-10
SunOS 5.4_x86	-	105255-01
SunOS 5.3	-	105253-01
SunOS 4.1.4	-	105260-01
SunOS 4.1.3_U1	-	105259-01

The CERT Coordination Center staff thanks AUSCERT and DFN-CERT for their contributions to the development of this advisory.

Revision History

Feb. 12, 1998 Added vendor information for NCR Corporation.

Nov. 14, 1997 Added vendor information for Data General Corporation.

Oct. 30, 1997 Updated vendor information for Sun.

Sep. 26, 1997 Updated copyright statement

July 28, 1997 Appendix A - updated Hewlett-Packard information.

Feb. 11, 1997 Appendix A - added entries for Cygnus Solutions, NetBSD, and Sun Microsystems.

7 CA-1997-07: Vulnerability in the httpd nph-test-cgi script

Original issue date: February 18, 1997
Last revised: September 26, 1997
Updated copyright statement

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

Because of ongoing activity relating to a vulnerability in the nph-test-cgi script included with some http daemons, the CERT Coordination Center staff is issuing this recommendation to check your cgi-bin directory. By exploiting this vulnerability, users of Web clients can read a listing of files they are not authorized to see.

The CERT/CC team recommends removing the script from your system and checking Appendix A of this advisory for information provided by vendors.

We also urge you to read CERT advisory CA-96.06.cgi_example_code for another CGI-related vulnerability that continues to be exploited.

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

I. Description

A vulnerability in the nph-test-cgi script included with some http daemons makes it possible for the users of Web clients to read a listing of files they are not authorized to read. This script is designed to display information about the Web server environment, but it parses data requests too liberally and thus allows a person to view a listing of arbitrary files on the Web server host.

II. Impact

By exploiting this vulnerability, remote users can read a listing of files they are not authorized to read. Access to an account on the system is not necessary.

III. Solution

We recommend removing or disabling the nph-test-cgi script (see Sec. A). If you must keep the script, follow the suggestion in Sec. B. All readers should also check Appendix A for information supplied by vendors.

A. Remove or disable the script

Some World Wide Web servers include this script by default, but it is possible that some sites have installed this script manually. Therefore, we encourage all sites to check whether they have

this script by searching for the file nph-test-cgi in the cgi-bin directory associated with their web server.

If you find the script, we urge you to either remove the program itself or remove the execute permissions from the program. The nph-test-cgi program is not required to run httpd successfully.

Also note that a web server may have multiple cgi-bin directories. It is not sufficient to look in the regular location only. For example, in the NCSA HTTPd server, you can specify alternate locations for the scripts by setting the ScriptAlias directive in the srm.conf file. See your vendor's documentation to learn if your sever provides this feature. If you are using this feature, you need to remove the nph-test-cgi script or apply the workaround below in every cgi-bin directory.

B. Modify existing scripts

If you must continue to use this test-cgi script, then we encourage you to search for lines of code that echo variables and ensure that the variable string to be echoed is quoted. For instance, lines of the form:

echo QUERY_STRING = $QUERY_STRING

should read

echo QUERY_STRING = "$QUERY_STRING"

C. Vendor Information

Please check Appendix A for information supplied by vendors; we will update the appendix as we receive additional information. If you do not see your vendor's name, then we did not hear from that vendor. Please contact the vendor directly.

Note: Even if your vendor did not ship the nph-test-cgi script, you should check your cgi-bin directory in case someone at your site added such a script later.

IV. Additional Reading

Several resources relating to Web security in general are available. The following resources provide a useful starting point. They include links describing general WWW security, secure httpd setup, and secure CGI programming.

The World Wide Web Security FAQ:
http://www-genome.wi.mit.edu/WWW/faqs/www-security-faq.html.

NSCA's "Security Concerns on the Web" Page: http://hoohoo.ncsa.uiuc.edu/security/.

The following book contains useful information, including sections on secure programming techniques.

Practical Unix & Internet Security, Simson Garfinkel and Gene Spafford, 2nd edition, O'Reilly and Associates, 1996.

(Note that we provide these pointers for your convenience. As this is not CERT/CC material, we cannot be responsible for content or availability. Please contact the administrators of the sites if you have difficulties with access.)

Appendix A Vendor Information

Below is a list of the vendors who have provided information for this advisory. We will update this appendix as we receive additional information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact the vendor directly.

Apache

The latest version of Apache, 1.1.3, does not contain the nph-test-cgi cgi-script. The test-cgi script included with Apache 1.1.3 does contain the filename globbing bug, but does not ship enabled by default.

Apache-SSL

The current version of Apache-SSL is against 1.1.1, and so does not suffer from this problem. Also, Apache-SSL is distributed as patches to Apache, and so does not, in itself, contain any CGI scripts.

Stronghold

Stronghold 1.3.4 ships with no pre-installed CGI scripts.

Microsoft

With regard to NT/IIS we don't ship the script referenced. Also see recommendations at http://www.microsoft.com/intdev and http://www.microsoft.com/pdc

National Center for Supercomputing Applications

The NCSA™ HTTPd comes with a variety of test cgi scripts, including nph-test-cgi. Also included are test-cgi, test-cgi.tcl, and test-env. These test scripts are readily identified by the word "test" in their names. They have been provided at the request of our web server community to test the server installation and facilitate the development of cgi scripts. When working perfectly they provide private information about the server and cgi environment.

Test cgi programs are not intended to be left on an operational server. If using the NCSA HTTPd server for operational use, many configuration issues must be addressed. Among those issues is the use of cgi scripts. No script should be run on a server that has not been carefully reviewed. This is especially true for the test scripts, which were never intended to be left on an operational server.

Users of NCSA HTTPd should be running the most current version (1.5.2a) to ensure that security patches are implemented. Test cgi scripts should be removed from cgi-bin directories before putting a server in operational use.

Please see http://hoohoo.ncsa.uiuc.edu/security for further details on securely installing the NCSA HTTPd server.

To report security vulnerabilities in NCSA products, email the NCSA Incident Response and Security Team (irst@ncsa.uiuc.edu).

NCSA is a trademark of the University of Illinois Board of Trustees.

The CERT Coordination Center thanks David Kennedy of the National Computer Security Association, Ken Rowe of the NCSA(tm) IRST, and Josh Richards for providing information about this problem.

Revision History

```
September 26, 1997  Updated copyright statement

February 21, 1997 Acknowledgements - corrected organization names.
```

8 CA-1997-08: Vulnerabilities in INND

Original issue date: February 20, 1997
Last revised: September 26, 1997
Updated copyright statement

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

A second vulnerability was found in INN (InterNetNews server) after the initial publication of this advisory. We are including it in this advisory as "Topic 2" so that all INN information is in one advisory. Versions 1.5.1 and earlier are vulnerable to this second problem.

Information about the first vulnerability has been widely distributed, and we have received numerous reports of exploitation. INN 1.5 and earlier are vulnerable to this problem.

Both vulnerabilities allow unauthorized users to execute arbitrary commands on the machine running INN by sending a maliciously formed news control message. Because the problem is with the content of news control messages, attacks can be launched remotely and may reach news servers located behind Internet firewalls.

The CERT/CC staff recommends that sites upgrade to INN 1.5.1 and add the patch described in Section III.A. Until you can upgrade, you should apply two patches, as described in Section III.B. You may also want to check with your vendor. Vendors who have provided input for this advisory are listed in Sec. III.C and Appendix A.

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

I. Description

TOPIC 2 - ucbmail

A second vulnerability involving INN has been found. It is similar to *but not the same as* the one described in Topic 1 below.

INN itself attempts to carefully remove certain shell "metacharacters" from data in control messages before passing that data to a shell. The patch for Topic 1 fixes some of the checks that were found to be inadequate. However ucbmail, a program typically configured as the mailer INN should use, lacks similar checks. INN passes some data unchecked to this mailer, which in turn passes the data to a shell for processing.

James Brister, the current maintainer of INN, has made a patch available that checks more data before it is passed to the mailer program. Although only the ucbmail program is known to have this problem, sites are encouraged to apply the patch regardless of what mail program their INN is configured to use.

TOPIC 1 - Information provided with the initial advisory

The INN daemon (innd) processes "newgroup" and "rmgroup" control messages in a shell script (parsecontrol) that uses the shell's "eval" command. However, some of the information passed to eval comes from the message without adequate checks for characters that are special to the shell.

This permits anyone who can send messages to an INN server - almost anyone with Usenet access - to execute arbitrary commands on that server. These commands run with the uid and privileges of the "innd" process on that server. Because such messages are usually passed through Internet firewalls to a site's news server, servers behind such firewalls are vulnerable to attack. Also, the program executes these commands before checking whether the sender is authorized to create or remove newsgroups, so checks at that level (such as running pgpverify) do not prevent this problem.

As of the advisory update of March 18, 1997, we have received numerous reports that the vulnerability is being exploited.

Determining if you are vulnerable

You can determine which version of INN your site is running by connecting to the NNTP port (119) of your news server. For example:

```
% telnet news.your.site 119

Connected to news.your.site

Escape character is '^]'.

200 news.your.site InterNetNews server INN 1.4unoff4 05-Mar-96 ready
```

Type "quit" to exit the connection. Note that this does not indicate whether or not the patch recommended below has been installed.

II. Impact

(Applies to both TOPICS 1 & 2)

Remote, unauthorized users can execute arbitrary commands on the system with the same privileges as the innd (INN daemon) process. Attacks may reach news servers located behind Internet firewalls.

III. Solution

Warning: If you applied any of the solutions offered in the version of this advisory released on Feb. 20, 1997, you must add an additional patch.

(The following apply to both TOPIC 1 and TOPIC 2)

We recommend upgrading to version 1.5.1 and applying the patch developed by James Brister, the current maintainer of INN (Section III. A). If you upgraded previously, you must apply this new patch to protect against the second vulnerability. Until you can upgrade, you need to apply two patches (Section III. B). You may also want to consult your vendor. Vendors who have provided input for this advisory are listed in Sec. III.C and Appendix A.

After installing any of the patches or updates, ensure that you restart your INN server.

A. Upgrade to INN 1.5.1 and apply a patch.

The current version of INN is 1.5.1. It is not vulnerable to the first vulnerability; but it is vulnerable to the second, so a patch is necessary.

When you upgrade to INN 1.5.1, please be sure to read the README file carefully.

INN 1.5.1 and information about it are available from http://www.isc.org/inn.html.

The md5 checksum for the gzip'ed tar file is

MD5 (inn-1.5.1.tar.gz) = 555d50c42ba08ece16c6cdfa392e0ca4

The patch is available from ftp://ftp.isc.org:/isc/inn/patches/security-patch.05.

Note that the advisory originally pointed to patch 04; there was a problem with this patch. You need to install patch 05.

Checksums for patches are in the directory, along with a README.

B. If you do not upgrade to 1.5.1,

apply a patch for the version you are running and then apply the newly released patch that addresses the second vulnerability discussed in this advisory. If you are running INN 1.4sec2, you should upgrade to 1.5.1 as no patches are available.

FIRST apply:

version - patch
1.5 - ftp://ftp.isc.org/isc/inn/patches/security-patch.01
1.4sec - ftp://ftp.isc.org/isc/inn/patches/security-patch.02
1.4unoff3, 1.4unoff4 - ftp://ftp.isc.org/isc/inn/patches/security-patch.03

THEN apply (1.5.1, 1.5, 1.4sec, 1.4unoff3, 1.4unoff4)

ftp://ftp.isc.org:/isc/inn/patches/security-patch.05

Note that the advisory originally pointed to patch 04; there was a problem with this patch. You need to install patch 05.

There are md5 checksums for each file in the directory, and a README file describes what is what.

C. Consult your vendor

Below is a list of vendors who have provided information about INN. Details are in Appendix A of this advisory; we will update the appendix as we receive more information. If your vendor's name is not on this list, the CERT/CC did not hear from that vendor. Please contact your vendor directly.

Berkeley Software Design, Inc. (BSDI)
Caldera
Cray Research - A Silicon Graphics Company
Debian Linux
NEC Corporation
Netscape
Red Hat Linux

Appendix A Vendor Information

Below is a list of the vendors who have provided information for this advisory, along with an indication about whether the information relates to the first vulnerability or both. We will update this appendix as we receive additional information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact the vendor directly.

Berkeley Software Design, Inc. (BSDI)

For TOPIC 1

We ship INN as part of our distribution. BSD/OS 2.1 includes INN 1.4sec and 2.1 users should apply the patch referenced in the advisory. BSD/OS 3.0 includes INN 1.4unoff4 and the patch for that version is already included so BSD/OS 3.0 is not vulnerable as distributed.

Caldera

For TOPIC 1

An upgrade package for Caldera OpenLinux Base 1.0 will appear at Caldera's site: ftp://ftp.caldera.com/pub/col-1.0/updates/Helsinki/004/inn-1.5.1-2.i386.rpm.

MD5 sum is:

3bcd3120b93f41577d3246f3e9276098 inn-1.5.1-2.i386.rpm

Cray Research - A Silicon Graphics Company

For TOPIC 1 and TOPIC 2

Cray Research has never shipped any news server with Unicos.

Debian Linux

For TOPIC 1

The current version of INN shipped with Debian is 1.4unoff4. However the "unstable" (or development) tree contains inn-1.5.1. It can be gotten from any debian mirror in the subdirectory

debian/unstable/binary/news

d3603d9617fbf894a3743a330544b62e 591154 news optional inn_1.5.1-1_i386.deb
205850779d2820f03f2438d063e1dc51 45230 news optional inn-dev_1.5.1-1_i386.deb
badbe8431479427a4a4de8ebd6e1e150 31682 news optional inewsinn_1.5.1-1_i386.deb

NEC Corporation

For TOPIC 1 and TOPIC 2

Products below are shipped with INN mentioned in this advisory, so they are vulnerable and patches are in progress.

Goah/NetworkSV R1.2	vulnerable
Goah/NetworkSV R2.2	vulnerable
Goah/NetworkSV R3.1	vulnerable
Goah/IntraSV R1.1	vulnerable

Netscape

For Topic 2

The Netscape News Server 2.01 and current beta (and future shipping) versions of Netscape Collabra Server are NOT vulnerable to this problem because the Netscape News Server uses its own mailer instead of 'ucbmail'. The Netscape News Server mailer is a simple SMTP front-end that DOES NOT pass anything to the shell. Hence it is immune to the vulnerability outlined in topic 2 of the advisory.

Netscape News Server 1.1 users should apply the patch recommended by the Cert Advisory to solve this problem.

For Topic 1
The Netscape News Server 2.01 is immune to the attack outlined in the advisory.

The News Server 1.1 is, however, subject to the same vulnerability as INN and we have advised customers to install the patch described in the advisory.

Red Hat Linux

For Topics 1 and 2

There is a critical security hole in INN which affects all versions of Red Hat Linux. A new version, inn-1.5.1-6, is now available for Red Hat Linux 4.0 and 4.1 for all platforms. If you are running an earlier version of Red Hat, we strongly encourage you to upgrade to 4.1 as soon as possible, as many critical security fixes have been made. The new version of inn is PGP signed with the Red Hat PGP key, which is available on all Red Hat CDROMs, ftp.redhat.com, and public keyservers.

You may upgrade to the new version as follows:

Red Hat 4.1

i386:

rpm -Uvh ftp://ftp.redhat.com/updates/4.1/i386/inn-1.5.1-6.i386.rpm

alpha:

rpm -Uvh ftp://ftp.redhat.com/updates/4.1/alpha/inn-1.5.1-6.alpha.rpm

rpm -Uvh ftp://ftp.redhat.com/updates/4.1/sparc/inn-1.5.1-6.sparc.rpm

Red Hat 4.0

i386:

rpm -Uvh ftp://ftp.redhat.com/updates/4.0/i386/inn-1.5.1-6.i386.rpm

alpha:

rpm -Uvh ftp://ftp.redhat.com/updates/4.0/alpha/inn-1.5.1-6.alpha.rpm

SPARC

rpm -Uvh ftp://ftp.redhat.com/updates/4.0/sparc/inn-1..5.1-6.sparc.rpm

The CERT Coordination Center thanks James Brister of the Internet Software Consortium for making fixes available and Matt Power of MIT for analyzing and reporting the first problem. We also thank AUSCERT for their contributions to this advisory. James Crawford Ralston of the University of Pittsburgh and Frank Miller of Tektronix Corporation assisted with the March 18, 1997 update.

The second vulnerability addressed in this advisory was discovered by security experts in the Global Security Analysis Laboratory (GSAL) at IBM's T.J. Watson Research Center. We thank

the IBM Emergency Response Service for providing information on this topic. (They published information in ERS-SVA-E01-1997:002.1. Their alert is copyrighted 1997 by International Business Machines Corporation.)

UPDATES

August 15, 1997

The current version is inn-1.5.1sec2, and is available from:
ftp://ftp.isc.org/isc/inn/inn-1.5.1sec2.tar.gz.

March 18, 1997

If you are upgrading to INN 1.5.1, please be sure to read the README file carefully. Note that if you are upgrading to 1.5.1 from a previous release, running a "make update" alone is not sufficient to ensure that all of the vulnerable scripts are replaced (e.g., parsecontrol). Please especially note the following from the INN 1.5.1 distribution README file:

When updating from a previous release, you will usually want to do "make update" from the top-level directory; this will only install the programs. To update your scripts and config files, cd into the "site" directory and do "make clean" -- this will remove any files that are unchanged from the official release. Then do "make diff >diff"; this will show you what changes you will have to merge in. Now merge in your changes (from where the files are, ie. /usr/lib/news...) into the files in $INN/site. (You may find that due to the bug fixes and new features in this release, you may not need to change any of the scripts, just the configuration files). Finally, doing "make install" will install everything.

After installing any of the patches or updates, ensure that you restart your INN server.

Revision History

```
Sep. 26, 1997 Updated copyright statement

Aug. 15, 1997 UPDATES - added information about the latest release.

Apr 04, 1997  Appendix A - added information from Netscape about
Topic 2 Solution sections III.A and B - replaced pointer to patch 04
with patch 05 and noted that you must use patch 05 Contact infor-
mation corrected the URL for FIRST

Apr 03, 1997  Added information on a second vulnerability (labeled
Topic 2), including a new patch that must be applied to many ver-
sions of INN.  Labeled vendor information as input on Topic 1 or 2.
```

Mar 25, 1997 Section III.B - added a note that no patches are available for version 1.4sec2.

Mar 24, 1997 Appendix A - added information from Netscape.

Mar 21, 1997 Appendix A - added information from NEC Corporation.

Mar 18, 1997 Updates section - added a caution for sites upgrading to 1.5.1 Acknowledgments - added J. C. Ralston and F. Miller

Mar 17, 1997 Section III.B - corrected patch information (patch.03 must be used for 1.4unoff3, 1.4unoff4 rather than patch.01); added a URL for INN information. Section III.A and introduction - noted that the vulnerability is being actively exploited.

9 CA-1997-09: Vulnerability in IMAP and POP

Original issue date: April 7, 1997
Last revised: April 28, 1998
Added vendor information for Silicon Graphics Inc. Corrected URL for obtaining RFCs.

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

The CERT Coordination Center has received reports of a vulnerability in some versions of the University of Washington's implementation of the Internet Message Access Protocol (IMAP) and Post Office Protocol (POP). Information about this vulnerability has been publicly distributed.

By exploiting this vulnerability, remote users can obtain unauthorized root access.

As of the August 4, 1997 update, intrusions based on the exploitation of this vulnerability continue to be reported to the CERT/CC.

The CERT/CC team recommends installing a patch if one is available or upgrading to IMAP4rev1. Until you can do so, we recommend disabling the IMAP and POP services at your site.

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

I. Description

The current version of Internet Message Access Protocol (IMAP) supports both online and offline operation, permitting manipulation of remote message folders. It provides access to multiple mailboxes (possibly on multiple servers), and supports nested mailboxes as well as resynchronization with the server. The current version also provides a user with the ability to create, delete, and rename mailboxes. Additional details concerning the functionality of IMAP can be found in RFC 2060 (the IMAP4rev1 specification) available from ftp://ftp.isi.edu/in-notes/rfc2060.txt.

The Post Office Protocol (POP) was designed to support offline mail processing. That is, the client connects to the server to download mail that the server is holding for the client. The mail is deleted from the server and is handled offline (locally) on the client machine.

In the implementation of both protocols on a UNIX system, the server must run with root privileges so it can access mail folders and undertake some file manipulation on behalf of the user logging in. After login, these privileges are discarded. However, in at least the University of Washington's implementation a vulnerability exists in the way the login transaction is handled. (See Appendix A for vendor information.) This vulnerability can be exploited to gain privileged access on the server. By preparing carefully crafted text to a system running a vulnerable version of these servers, remote users may be able to cause a buffer overflow and execute arbitrary instructions with root privileges.

Information about this vulnerability has been widely distributed.

II. Impact

Remote users can obtain root access on systems running a vulnerable IMAP or POP server. They do not need access to an account on the system to do this.

III. Solution

Install a patch from your vendor (see Section A) or upgrade to the latest version of IMAP (Section B). If your POP server is based on the University of Washington IMAP server code, you should also upgrade to the latest version of IMAP. Until you can take one of these actions, you should disable services (Section C). In all cases, we urge you to take the additional precaution described in Section D.

A. Obtain and install a patch from your vendor

Below is a list of vendors who have provided information about this vulnerability. Details are in Appendix A of this advisory; we will update the appendix as we receive more information. If your vendor's name is not on this list, please contact your vendor directly.

Berkeley Software Design, Inc. (BSDI)
Carnegie Mellon University
Cray Research
Digital Equipment Corporation
IBM Corporation
Linux - Caldera, Inc.
Debian
Red Hat
Microsoft Corporation
NetManage, Inc.
Netscape
QUALCOMM, Incorporated
Silicon Graphics Inc.
Sun Microsystems, Inc.
University of Washington

B. Upgrade to the latest version of IMAP

An alternative to installing vendor patches is upgrading to IMAP4rev1, which is available from ftp://ftp.cac.washington.edu/mail/imap.tar.Z.

Please note that checksums change when files are updated. The imap.tar.Z file can undergo frequent changes, therefore the checksums have not been included here.

C. Disable services

Until you can take one of the above actions, temporarily disable the POP and IMAP services. On many systems, you will need to edit the /etc/inetd.conf file. However, you should check your vendor's documentation because systems vary in file location and the exact changes required (for example, sending the inetd process a HUP signal or killing and restarting the daemon).

If you are not able to temporarily disable the POP and IMAP services, then you should at least limit access to the vulnerable services to machines in your local network. This can be done by installing the tcp_wrappers described in Section D, not only for logging but also for access control. Note that even with access control via tcp_wrappers, you are still vulnerable to attacks from hosts that are allowed to connect to the vulnerable POP or IMAP service.

D. Additional precaution

Because IMAP or POP is launched out of inetd.conf, tcp_wrappers can be installed to log connections which can then be examined for suspicious activity. You may want to consider filtering connections at the firewall to discard unwanted/unauthorized connections.

The tcp_wrappers tool is available in
ftp://ftp.cert.org/pub/tools/tcp_wrappers/tcp_wrappers_7.5.tar.gz.

MD5 (tcp_wrappers_7.5.tar.gz) = 8c7a17a12d9be746e0488f7f6bfa4abb

Note that this precaution does not address the vulnerability described in this advisory, but it is a good security practice in general.

Appendix A Vendor Information

Below is a list of the vendors who have provided information for this advisory. We will update this appendix as we receive additional information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact the vendor directly.

Berkeley Software Design, Inc. (BSDI)

We're working on patches for both BSD/OS 2.1 and BSD/OS 3.0 for imap (which we include as part of pine).

Carnegie Mellon University

Cyrus Server 1.5.2, with full IMAP4rev1 and pop3 capabilities, is NOT affected by this report and is NOT vulnerable.

Cray Research

Not vulnerable.

Digital Equipment Corporation

This reported problem is not present for Digital's UNIX or Digital ULTRIX Operating Systems Software.

IBM Corporation

AIX 4.2.1 is the only version of AIX currently shipping with IMAP. Previous versions of AIX are not vulnerable.

AIX 4.2.1

The following APAR will be available soon: APAR IX70263

To Order

APARs may be ordered using Electronic Fix Distribution (via FixDist) or from the IBM Support Center. For more information on FixDist, reference URL: http://service.software.ibm.com/aixsupport/ or send e-mail to aixserv@austin.ibm.com with a subject of "FixDist".

IBM and AIX are registered trademarks of International Business Machines Corporation.

Linux Systems

Caldera, Inc.

On systems such as Caldera OpenLinux 1.0, an unprivileged user can obtain root access.

As a temporary workaround, you can disable the POP and IMAP services in /etc/inetd.conf, and then kill and restart inetd.

A better solution is to install the new RPM package that contains the fixed versions of the IMAP and POP daemons. They are located on Caldera's FTP server (ftp.caldera.com):

/pub/openlinux/updates/1.0/006/RPMS/imap-4.1.BETA-1.i386.rpm

The MD5 checksum (from the "md5sum" command) for this package is:

45a758dfd30f6d0291325894f9ec4c18

This and other Caldera security resources are located at: http://www.caldera.com/tech-ref/security/.

Debian

Debian linux is not vulnerable. For more information see http://cgi.debian.org/www-master/debian.org/security.html.

Red Hat

The IMAP servers included with all versions of Red Hat Linux have a buffer overrun which allow *remote* users to gain root access on systems which run them. A fix for Red Hat 4.1 is now available (details on it at the end of this note).

Users of Red Hat 4.0 should apply the Red Hat 4.1 fix. Users of previous releases of Red Hat Linux are strongly encouraged to upgrade or simply not run imap. You can remove imap from any machine running with Red Hat Linux 2.0 or later by running the command "rpm -e imap", rendering them immune to this problem.

All of the new packages are PGP signed with Red Hat's PGP key, and may be obtained from ftp.redhat.com:/updates/4.1.

If you have direct Internet access, you may upgrade these packages on your system with the following commands:

Intel:
rpm -Uvh ftp://ftp.redhat.com/updates/4.1/i386/imap-4.1.BETA-3.i386.rpm
MD5 (imap-4.1.BETA-3.i386.rpm) = 8ac64fff475ee43d409fc9776a6637a6

Alpha:
rpm -Uvh ftp://ftp.redhat.com/updates/4.1/alpha/imap-4.1.BETA-3.alpha.rpm
MD5 (imap-4.1.BETA-3.alpha.rpm) = fd42ac24d7c4367ee51fd00e631cae5b

SPARC:
rpm -Uvh ftp://ftp.redhat.com/updates/4.1/sparc/imap-4.1.BETA-3.sparc.rpm
MD5 (imap-4.1.BETA-3.sparc.rpm) = 751598aae3d179284b8ea4d7a9b78868

Microsoft

Microsoft's Exchange POP and IMAP servers and Microsoft's Commericial Internet System are not vulnerable

NetManage, Inc.

NetManage's ZPOP pop server is not vulnerable.

Netscape

Netscape's POP3/IMAP4 implementation is not vulnerable.

QUALCOMM Incorporated

Our engineers have examined the QPopper source code, which is based on source from UC Berkeley. They determined that QPopper is *NOT* vulnerable to a buffer overflow attack as described in CA-97.09. It strictly checks the size of messages before copying them into its buffer.

Silicon Graphics Inc.

Silicon Graphics Inc. Security Advisory, 19980302-01-I, provides the following information:

The Internet Mail Access Protocol (IMAP) & Post Office Protocol (POP) provide users with an alternative means to process and retrieve their email.

A vulnerability has been discovered in IMAP4 & POP3 that allows remote users to obtain root access.

Silicon Graphics sells and supports the Netscape Mail/Messaging Servers for IRIX which use IMAP4 & POP3 however, their implementations are not vulnerable to this issue and no further action is required.

More information about Netscape product security can be found at the following URL: http://home.netscape.com/assist/security/.

Sun Microsystems, Inc.

The following patches have been released for CERT CA-97.09.

105346-02 SIMS 2.0
105347-02 SIMS 2.0_x86

University of Washington

This vulnerability has been detected in the University of Washington c-client library used in the UW IMAP and POP servers. This vulnerability affects all versions of imapd prior to v10.165, all versions of ipop2d prior to 2.3(32), and all versions of ipop3d prior to 3.3(27).

It is recommended that all sites using these servers upgrade to the latest versions, available in the UW IMAP toolkit: ftp://ftp.cac.washington.edu/mail/imap.tar.Z.

Please note that checksums change when files are updated. The imap.tar.Z file can undergo frequent changes, therefore the checksums have not been included here.

This is a source distribution which includes imapd, ipop2d, ipop3d. and the c-client library. The IMAP server in this distribution conforms with RFC2060 (the IMAP4rev1 specification).

Sites which are not yet prepared to upgrade from IMAP2bis to IMAP4 service may obtain a corrected IMAP2bis server as part of the latest (3.96) UW Pine distribution, available at: ftp://ftp.cac.washington.edu/pine/pine.tar.Z.

MD5 (pine.tar.Z) = 37138f0d1ec3175cf1ffe6c062c9abbf

The CERT Coordination Center thanks the University of Washington's Computing and Communications staff for information relating to this advisory. We also thank Wolfgang Ley of DFN-CERT for his input. We thank Matthew Wall of Carnegie Mellon University for additional insightful feedback.

UPDATES

April 8, 1997

We have received requests for clarification. The vulnerability described in this advisory relates to certain server implementations and is not in the protocol itself. See Appendix A for vendor and server information.

Revision History

Apr. 28. 1998 Added vendor information for Silicon Graphics Inc. Corrected URL for obtaining RFCs.

Jan. 15, 1998 Updated vendor information for Sun Microsystems, Inc.

Sep. 26, 1997 Updated copyright statment

Aug. 27, 1997 Section III.A and Appendix A - added vendor information for IBM Corporation.

Aug 4, 1997 Clarifications in wording have been made to the introduction and paragraph 3 of the description section.

June 3, 1997 Section III.A and Appendix - Added vendor information for NetManage, Inc.

May 1, 1997 Section III.A and Appendix A - Added vendor information for Microsoft Corporation.

Apr 18, 1997 Section III.A and Appendix A - Added vendor information for Debian and Netscape.

Apr 11, 1997 Section III.B. - Removed checksum information for the imap.tar.Z distribution and added an explanation.

Apr 9, 1997 Appendix A - added vendor information for Digital Equipment Corporation and QUALCOMM Incorporated. Updated vendor information for Sun Microsystems, Inc. Added another name to acknowledgment.

Apr 08, 1997 Updates - Added clarification that the vulnerability is an implementation error and not an error in the protocol Appendix - added vendor information for Caldera and the Carnegie Mellon University Cyrus Server

Acknowledgments - Added a name that was inadvertently left out.

10 CA-1997-10: Vulnerability in Natural Language Service

Original issue date: April 24, 1997
Last revised: September 26, 1997
Updated copyright statement

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

The CERT Coordination Center has received reports of a buffer overflow condition that affects some libraries using the Natural Language Service (NLS) on UNIX systems. By exploiting this vulnerability, any local user can execute arbitrary programs as a privileged user. There is a possibility (with some old libraries) that the vulnerability can be exploited by a remote user.

Exploitation information is publicly available.

The CERT/CC team recommends installing patches when they become available.

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

I. Description

A buffer overflow condition affects libraries using the Natural Language Service (NLS). The NLS is the component of UNIX systems that provides facilities for customizing the natural language formatting for the system. Examples of the types of characteristics that can be set are language, monetary symbols and delimiters, numeric delimiters, and time formats.

Some libraries that use a particular environment variable associated with the NLS contain a vulnerability in which a buffer overflow condition can be triggered. The particular environment variable involved is NLSPATH on some systems and PATH_LOCALE on others.

It is possible to exploit this vulnerability to attain unauthorized access by supplying carefully crafted arguments to programs that are owned by a privileged user-id and that have setuid or setgid bits set.

Exploit information involving this vulnerability has been made publicly available.

II. Impact

Local users (users with access to an account on the system) are able to execute arbitrary programs as a privileged user without authorization. There is a possibility (with some old libraries) that the vulnerability can be exploited by a remote user.

III. Solution

Install a patch for this problem when one becomes available. Currently, there is no workaround to use in the meantime.

Below is a list of vendors who have provided information about this problem. Details are in Appendix A of this advisory; we will update the appendix as we receive more information. If your vendor's name is not on this list, the CERT/CC did not hear from that vendor. Please contact your vendor directly.

Berkeley Software Design, Inc. (BSDI)
Cray Research - A Silicon Graphics Company
Data General Corporation
Digital Equipment Corporation
Hewlett-Packard Company
IBM Corporation
Linux Systems
NEC Corporation
NeXT/Apple
The Santa Cruz Operation (SCO)
Solbourne
Sun Microsystems, Inc.

Appendix A Vendor Information

Below is a list of the vendors who have provided information for this advisory. We will update this appendix as we receive additional information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact the vendor directly.

Berkeley Software Design, Inc. (BSDI)

No versions of BSD/OS are vulnerable to this problem.

Cray Research - A Silicon Graphics Company

This problem has been resolved with code that is available in released software packages as described in the FIX AVAILABILITY section below.

FIX AVAILABILITY

For each affected product level, the following table identifies the release that contains the fix:

Affected Product	Release Levels Containing Fix
UNICOS	UNICOS 9.0.2.5
	UNICOS 9.2.0.4

UNICOS/mk	UNICOS/mk 1.5.1
UNICOS MAX	UNICOS MAX 1.3.0.5

RELATED INFORMATION

SPR 704175 POSSIBLE SECURITY PROBLEM IN SETLOCALE

Data General Corporation

We're investigating.

Digital Equipment Corporation

SOURCE:

Digital Equipment Corporation
Software Security Response Team

This reported problem is not present for Digital's ULTRIX or Digital UNIX Operating Systems Software.

Hewlett-Packard Company

HP has completed their testing, HP-UX is not vulnerable.

IBM Corporation

All AIX releases are vulnerable to a variation of this advisory.

AIX 3.2.5

Apply the following fix to your system:

PTFs - U447656 U447671 U447676 U447682 U447705 U447723 (APAR IX67405)

To determine if you have these PTFs on your system, run the following command:

lslpp -lB U447656 U447671 U447676 U447682 U447705 U447723

AIX 4.1

Apply the following fix to your system:

APAR - IX67407

To determine if you have this APAR on your system, run the following command:

instfix -ik IX67407

Or run the following command:

lslpp -h bos.rte.libc

Your version of bos.rte.libc should be 4.1.5.7 or later.

AIX 4.2

Apply the following fixes to your system:

APAR - IX67377 IX65693

To determine if you have these APARs on your system, run the following command:

instfix -ik IX67377 IX65693

Or run the following command:

lslpp -h bos.rte.libc

Your version of bos.rte.libc should be 4.2.0.11 or later.

(APAR IX65693 fixes a problem with the mkgroup command after IX67377 is applied.)

To Order

APARs may be ordered using Electronic Fix Distribution (via FixDist) or from the IBM Support Center. For more information on FixDist, reference URL: http://service.software.ibm.com/aixsupport/ or send e-mail to aixserv@austin.ibm.com with a subject of "FixDist".

IBM and AIX are registered trademarks of International Business Machines Corporation.

Linux Systems

Linux systems running older C libraries are vulnerable. To check which C library is being used type

linux% ldd /bin/ls

libc.so.5 => /lib/libc.so.5.3.12

This indicates the machine is using libc 5.3.12.

C libraries older than 5.3.12 (that is libc5.2.18, libc5.0.9 etc) are vulnerable to this bug and you should upgrade the C library. The release versions of libc 5.4.x are immune to this attack.

If you have libc5.3.12 it is insecure unless it is the modified libc5.3.12 shipped with Red Hat 4.1, or as an upgrade on Red Hat 4.0. You can check this with the package manager:

linux# rpm -q libc

libc-5.3.12-17

Indicates you have version 17 of the package. This is the safe one.

Red Hat 4.0 users who have not already upgraded their libc can obtain this package at ftp://ftp.redhat.com/pub/redhat/old-releases/redhat-4.0/updates/.

NEC Corporation

NEC platforms are not affected by this vulnerability.

NeXT/Apple

No versions of NeXTstep of OpenStep/Mach are vulnerable to this problem.

The Santa Cruz Operation (SCO)

We are investigating this problem and will provide updated information for this advisory when it becomes available.

Solbourne

Solbourne is not vulnerable.

Sun Microsystems, Inc.

Not vulnerable.

The CERT Coordination Center staff thanks Wolfgang Ley of DFN-CERT for his input to this advisory and Bruce Ide for drawing our attention to the problem.

UPDATES

There appear to be several slightly different descriptions for the NLS acronym. They are included here for convenience:

National Language Service
National Language Support
Native Language System
Natural Language Service
Natural Language Support

Revision History

```
Sep. 26, 1997 Updated copyright statement
```

June 3, 1997 Updates section - added other phrases for the the NLS acronym Appendix A - updated Cray Research entry.

May 1, 1997 Section III and Appendix. Updated vendor information for Hewlett-Packard Company. Acknowledgments - added a name upon receiving permission to do so.

11 CA-1997-11: Vulnerability in libXt

Original issue date: May 1, 1997
Last revised: January 5, 1998
Added vendor information for SGI.

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

There have been discussions on public mailing lists about buffer overflows in the Xt library of the X Windowing System made freely available by The Open Group (and previously by the now-defunct X Consortium). The specific problem outlined in those discussions was a buffer overflow condition in the Xt library, and the file xc/lib/Xt/Error.c. Exploitation scripts were made available.

Since then (the latter half of 1996), The Open Group has extensively reviewed the source code for the entire distribution to address the potential for further buffer overflow conditions. These conditions can make it possible for a local user to execute arbitrary instructions as a privileged user without authorization.

The programs that pose a potential threat to sites are those programs that have been built from source code prior to X11 Release 6.3 and have setuid or setgid bits set. Some third-party vendors distribute derivatives of the X Window System, and if you use a distribution that includes X tools that have setuid or setgid bits set, you may be vulnerable as well.

The CERT/CC team recommends upgrading to X11 Release 6.3 or installing a patch from your vendor. If you cannot do one of these, then as a last resort we recommend that you remove the setuid or setgid bits from any executable files contained in your distribution of X; this may have an adverse effect on some system operations.

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

I. Description

There have been discussions on public mailing lists about buffer overflows in the Xt library of the X Windowing System made freely available by The Open Group (and previously by the now-defunct X Consortium). During these discussions, exploitation scripts were made available for some platforms.**

The specific problem outlined in those discussions was a buffer overflow condition in the Xt library and the file xc/lib/Xt/Error.c. It was possible for a user to execute arbitrary instructions as a privileged user using a program built by this distribution with setuid or setgid bits set.

Note that in this case a root compromise was only possible when programs built from this distribution (e.g., xterm) were setuid root.

Since then The Open Group has extensively reviewed the source code for the entire distribution to address the potential for further buffer overflow condition.

If you use a distribution of the X Windowing System earlier than X11 Release 6.3 that you downloaded and compiled yourself, we encourage you to take the steps outlined in either Section IV A or C.

If you use third-party vendor-supplied distributions of the X Windowing System containing setuid root programs, we encourage you to take the steps outlined in Sections IV B or C.

** Note: Discussions of this specific instance of the vulnerability appeared on mailing lists during the second half of 1996. Exploitation scripts were made public at that time.

II. Impact

Platforms that have X applications built with the setuid or setgid bits set may be vulnerable to buffer overflow conditions. These conditions can make it possible for a local user to execute arbitrary instructions as a privileged user without authorization. Access to an account on the system is necessary for exploitation.

III. Finding Potentially Vulnerable Distributions

A. For Sites That Download and Build Their Own Distributions

As discussed earlier, the programs that pose a potential threat to sites are those programs that have been built from source code, prior to X11 Release 6.3 and have setuid or setgid bits set.

Sites that have downloaded the X source code from the X Consortium should be able to identify such programs by looking in the directory hierarchy defined by the "ProjectRoot" constant described in the xc/config/cf/site.def file in the source code distribution. The default is /usr/X11R6.3. The X11R6.3 Installation Guide states:

"ProjectRoot

The destination where X will be installed. This variable needs to be set before you build, as some programs that read files at run-time have the installation directory compiled in to them. Assuming you have set the variable to some value /path, files will be installed into /path/bin, /path/include/X11, /path/lib, and /path/man."

B. For Vendor-Supplied Distributions

Some third-party vendors distribute derivatives of the X Window System. If you use a distribution that includes X tools that have setuid or setgid bits set, then you may need to apply Solution B or C in Section IV.

If you use a distribution that does not have setuid or setgid bits enabled on any X tools, then you do not need to take any of the steps listed below.

Below is a list of vendors who have provided information about this problem. If your vendor's name is not on this list and you need clarification, you should check directly with your vendor.

IV. Solution

If any X tools that you are using are potentially vulnerable (see Section III), we encourage you to take one of the following steps. If the setuid or setgid bits are not enabled on any of the tools in your distribution, you do not need to take any of the steps listed below.

For distributions that were built directly from the source code supplied by The Open Group (and previously by the X Consortium), we encourage you to apply either Solutions A or C. For vendor-supplied distributions, we encourage you to apply either Solutions B or C.

A. Upgrade to X11 Release 6.3

If you download and build your own distributions directly from the source code, we encourage you to install the latest version, X11 Release 6.3. The source code can be obtained from

ftp://ftp.x.org/pub/R6.3/tars/xc-1.tar.gz
ftp://ftp.x.org/pub/R6.3/tars/xc-2.tar.gz
ftp://ftp.x.org/pub/R6.3/tars/xc-3.tar.gz

Note that these distributions are very large. The compressed files consume about 40M of disk space. The uncompressed tar files consume about 150M of disk space.

B. Install a patch from your vendor

Below is a list of vendors who have provided information about this problem. Details are in Appendix A of this advisory; we will update the appendix as we receive more information. If your vendor's name is not on this list, the CERT/CC did not hear from that vendor. Please contact your vendor directly.

Berkeley Software Design, Inc. (BSDI)
Data General Corporation
Digital Equipment Corporation (DEC)
FreeBSD, Inc.
Hewlett-Packard Company
IBM Corporation
NEC Corporation
NeXT Software, Inc.
The Open Group (formerly OSF/X Consortium)
The Santa Cruz Operation, Inc. (SCO)
Silicon Graphics, Inc.
Sun Microsystems, Inc.

C. Remove the setuid bit from affected programs

If you are unable to apply Solutions A or B, then as a last resort we recommend removing the setuid or setgid bits from the executable files in your distribution of X.

Note that this may have an adverse effect on some system operations. For instance, on some systems the xlock program needs to have the setuid bit enabled so that the shadow password file can be read to unlock the screen. By removing the setuid bit from this program, you remove the ability of the xlock program to read the shadow password file. This means that particular version of the xlock program should not be used at all, or it should be killed from another terminal when necessary.

Appendix A Vendor Information

Below is a list of the vendors who have provided information for this advisory. We will update this appendix as we receive additional information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact the vendor directly.

Berkeley Software Design, Inc. (BSDI)

We released a patch for this for the 2.1 BSD/OS release, and it's already fixed in our current release.

Data General Corporation

All versions of DG/UX are vulnerable.

Patches for this vulnerability are in progress.

Digital Equipment Corporation (DEC)

At the time of writing this document, patches(binary kits) are in progress and final testing is expected to begin soon. Digital will provide notice of the completion/availability of the patches through AES services (DIA, DSNlink FLASH) and be available from your normal Digital Support channel.

FreeBSD, Inc.

We're aware of the problem and are trying to correct it with a new release of the Xt library.

Hewlett-Packard Company

HPSBUX9704-058
Description: Security Vulnerability in libXt for HP-UX 9.X & 10.X
HEWLETT-PACKARD SECURITY BULLETIN: #00058 libXt

Security Bulletins are available from the HP Electronic
Support Center via electronic mail.

Use your browser to get to the HP Electronic Support Center page at:

http://us-support.external.hp.com (for US, Canada, Asia-Pacific, & Latin-America)

http://europe-support.external.hp.com (for Europe)

IBM Corporation

See the appropriate release below to determine your action.

AIX 3.2

Apply the following fix to your system:
APAR - IX61784,IX67047,IX66713 (PTF - U445908,U447740)

To determine if you have this PTF on your system, run the following command:
lslpp -lB U445908 U447740

AIX 4.1

Apply the following fix to your system: APAR - IX61031 IX66736 IX66449

To determine if you have this APAR on your system, run the following command:

instfix -ik IX61031 IX66736 IX66449

Or run the following command:

lslpp -h X11.base.lib

Your version of X11.base.lib should be 4.1.5.2 or later.

AIX 4.2

Apply the following fix to your system:

APAR - IX66824 IX66352

To determine if you have this APAR on your system, run the following command:

instfix -ik IX66824 IX66352

Or run the following command:

lslpp -h X11.base.lib

Your version of X11.base.lib should be 4.2.1.0 or later.

To Order

APARs may be ordered using Electronic Fix Distribution (via FixDist) or from the IBM Support Center. For more information on FixDist, reference URL:
http://service.software.ibm.com/aixsupport/.

or send e-mail to aixserv@austin.ibm.com with a subject of "FixDist".

IBM and AIX are registered trademarks of International Business Machines Corporation.

NEC Corporation

EWS-UX/V(Rel4.2) R7.x - R10.x	vulnerable
EWS-UX/V(Rel4.2MP) R10.x	vulnerable
UP-UX/V(Rel4.2MP) R5.x - R7.x	vulnerable
UX/4800 R11.x - current	vulnerable

Patches for this vulnerability are in progress. For further information, please contact by e-mail: UX48-security-support@nec.co.jp.

NeXT Software, Inc.

X-Windows is not part of any NextStep or OpenStep release. We are not vulnerable to this problem.

The Open Group (formerly OSF/X Consortium)

Not vulnerable.

The Santa Cruz Operation, Inc. (SCO)

We are investigating this problem and will provide updated information for this advisory when it becomes available.

Silicon Graphics, Inc.

Silicon Graphics Inc. has investigated the issue and recommends the following steps for neutralizing the exposure. It is HIGHLY RECOMMENDED that these measures be implemented on ALL SGI systems. This issue will be corrected in future releases of IRIX.

For further information, please refer to Silicon Graphics Inc. Security Advisory Number: 19971101-01-PX, "libXt Security Issues."

The SGI anonymous FTP site is sgigate.sgi.com (204.94.209.1) or its mirror, ftp.sgi.com. Security information and patches can be found in the ~ftp/security and ~ftp/patches directories, respectfully.

Sun Microsystems, Inc.

Bulletin Number: #00153
Date: August 25, 1997
Title: Vulnerabilities in libXt

Vulnerable: SunOS versions 5.5.1, 5.5.1_x86, 5.5, 5.5_x86, 5.4, 5.4_x86, 5.3, 4.1.4, and 4.1.3_U1
The vulnerabilities are fixed in Solaris 2.6.

Patches are available to all Sun customers via World Wide Web at:
ftp://sunsolve1.sun.com/pub/patches/patches.html.

Customers with Sun support contracts can also obtain patches from local Sun answer centers and SunSITEs worldwide.

Sun security bulletins are available via World Wide Web at:
http://sunsolve1.sun.com/sunsolve/secbulletins.

Revision History

```
Jan. 5, 1998  Added vendor information for Silicon Graphics, Inc.

Dec. 11, 1997 Appendix A - updated vendor information for Data Gen-
eral Corporation.

Sep. 26, 1997 Updated copyright statement

Aug. 27, 1997 Appendix A - updated vendor information for Sun Mi-
crosystems,Inc.

May 8, 1997   Appendix A - updated vendor information for Hewlett-
Packard.
```

12 CA-1997-12: Vulnerability in webdist.cgi

Original issue date: May 6, 1997
Last revised: September 26, 1997
Updated copyright statement

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

The CERT Coordination Center has received reports of a security vulnerability in the webdist.cgi cgi-bin program, part of the IRIX Mindshare Out Box package, available with IRIX 5.x and 6.x. By exploiting this vulnerability, both local and remote users may be able to execute arbitrary commands with the privileges of the httpd daemon. This may be used to compromise the http server and under certain configurations gain privileged access.

Vendor patches are now available from Silicon Graphics Inc. We encourage you to apply patches as soon as possible. For more information, refer to the Silicon Graphics Inc. Security Advisory Number 19970501-02-PX.

The SGI anonymous FTP site is sgigate.sgi.com (204.94.209.1) or its mirror, ftp.sgi.com. Security information and patches can be found in the ~ftp/security and ~ftp/patches directories, respectively.

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

Note: Development of this advisory was a joint effort of the CERT Coordination Center and AUSCERT. This material was also released as AUSCERT advisory AA-97.14.

I. Description

A security vulnerability has been reported in the webdist.cgi cgi-bin program available with IRIX 5.x and 6.x. webdist.cgi is part of the IRIX Mindshare Out Box software package, which allows users to install software over a network via a World Wide Web interface.

webdist.cgi allows *webdist(1)* to be used via an HTML form interface defined in the file webdist.html, which is installed in the default document root directories for both the Netsite and Out Box servers.

Due to insufficient checking of the arguments passed to webdist.cgi, it may be possible to execute arbitrary commands with the privileges of the httpd daemon. This is done via the webdist program.

When installed, webdist.cgi is accessible by anyone who can connect to the httpd daemon. Because of this, the vulnerability may be exploited by remote users as well as local users. Even if a site's webserver is behind a firewall, it may still be vulnerable.

Determining if your site is vulnerable

All sites are encouraged to check their systems for the IRIX Mindshare Out Box software package, and in particular the Webdist Software package which is a subsystem of the Mindshare Out Box software package. To determine if this package is installed, use the command:

versions outbox.sw.webdist

I = Installed, R = Removed

Name	Date	Description
I outbox	11/06/96	Outbox Environment, 1.2
I outbox.sw	11/06/96	Outbox End-User Software, 1.2
I outbox.sw.webdist	11/06/96	Web Software Distribution Tools, 1.2

II. Impact

Local and remote users may be able to execute arbitrary commands on the HTTP server with the privileges of the httpd daemon. This may be used to compromise the http server and under certain configurations gain privileged access.

III. Solution

Vendor patches are available from Silicon Graphics Inc. We encourage you to apply patches as soon as possible. For more information, refer to the Silicon Graphics Inc. Security Advisory Number 19970501-02-PX, which is available from the SGI anonymous FTP site ftp://sgigate.sgi.com, or its mirror, ftp://ftp.sgi.com.

Security information and patches can be found in the ~ftp/security and ~ftp/patches directories, respectively.

You can also prevent the exploitation of this vulnerability by applying the workaround given in Section III.A or removing the package from your systems (Section III.B).

A. Remove execute permissions

Sites should immediately remove the execute permissions on the webdist.cgi program to prevent its exploitation. By default, webdist.cgi is found in /var/www/cgi-bin/, but sites should check all cgi-bin directories for this program.

```
# ls -l /var/www/cgi-bin/webdist.cgi

-rwxr-xr-x 1 root sys 4438 Nov 6 12:44 /var/www/cgi-bin/webdist.cgi

# chmod 400 /var/www/cgi-bin/webdist.cgi

# ls -l /var/www/cgi-bin/webdist.cgi

-r-------- 1 root sys 4438 Nov 6 12:44 /var/www/cgi-bin/webdist.cgi
```

Note that this will prevent all users from using the webdist program from the HTML form interface.

B. Remove outbox.sw.webdist subsystem

If the Webdist software is not required, we recommend that sites remove it completely from their systems. This can be done with the command:

versions remove outbox.sw.webdist

Sites can check that the package has been removed with the command:

versions outbox.sw.webdist

IV. Additional Measures

Sites should consider taking this opportunity to examine their entire httpd configuration. In particular, all CGI programs that are not required should be removed, and all those remaining should be examined for possible security vulnerabilities.

It is also important to ensure that all child processes of httpd are running as a non-privileged user. This is often a configurable option. See the documentation for your httpd distribution for more details.

Numerous resources relating to WWW security are available. The following pages may provide a useful starting point. They include links describing general WWW security, secure httpd setup, and secure CGI programming.

The World Wide Web Security FAQ:
http://www-genome.wi.mit.edu/WWW/faqs/www-security-faq.html

NSCA's "Security Concerns on the Web" Page: http://hoohoo.ncsa.uiuc.edu/security/

The following book contains useful information including sections on secure programming techniques.

Practical Unix & Internet Security, Simson Garfinkel and Gene Spafford, 2nd edition, O'Reilly and Associates, 1996.

Please note that the CERT/CC and AUSCERT do not endorse the URLs that appear above. If you have any problems with these sites, please contact the site administrator.

This advisory is a collaborative effort between AUSCERT and the CERT Coordination Center. This material was also released as AUSCERT advisory AA-97.14.

We thank Yuri Volobuev for reporting this problem. We also thank Martin Nicholls (The University of Queensland) and Ian Farquhar for their assistance in further understanding this problem and its solution.

Revision History

```
Sep. 26, 1997   Updated copyright statement

May 07, 1997    Introduction - Corrected the AUSCERT advisory num-
ber.

Acknowledgments - Corrected the AUSCERT advisory number and removed
a company name.

August 27, 1997 Introduction and Solution - Added patch information.
```

13 CA-1997-13: Vulnerability in xlock

Original issue date: May 7, 1997
Last revised: January 6, 1998
Updated URLs for Sun Microsystems, Inc.

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

The CERT Coordination Center has received reports that a buffer overflow condition exists in some implementations of xlock. This vulnerability makes it possible for local users (users with access to an account on the system) to execute arbitrary programs as a privileged user.

Exploitation information involving this vulnerability has been made publicly available.

If your system is vulnerable, the CERT/CC team recommends installing a patch from your vendor. If you are not certain whether your system is vulnerable or if you know that your system is vulnerable and you cannot add a patch immediately, we urge you to apply the workaround described in Section III.B.

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

I. Description

xlock is a program that allows a user to "lock" an X terminal. A buffer overflow condition exists in some implementations of xlock. It is possible attain unauthorized access to a system by engineering a particular environment and calling a vulnerable version of xlock that has setuid or setgid bits set. Information about vulnerable versions must be obtained from vendors. Some vendor information can be found in Appendix A of this advisory.

Exploitation information involving this vulnerability has been made publicly available.

Note that this problem is different from that discussed in CERT Advisory CA-97.11.libXt.

II. Impact

Local users are able to execute arbitrary programs as a privileged user without authorization.

III. Solution

Install a patch from your vendor as described in Solution A. If you are not certain whether your system is vulnerable or if you know that your system is vulnerable and you cannot install a patch immediately, we recommend Solution B.

A. Obtain and install a patch for this problem.

Below is a list of vendors who have provided information about xlock. Details are in Appendix A of this advisory; we will update the appendix as we receive more information. If your vendor's name is not on this list, the CERT/CC did not hear from that vendor. Please contact your vendor directly.

Berkeley Software Design, Inc. (BSDI)
Cray Research - A Silicon Graphics Company
Data General Corporation
Digital Equipment Corporation
FreeBSD, Inc.
Hewlett-Packard Company
IBM Corporation
LINUX
NEC Corporation
The Open Group [This group distributes the publicly available software that was formerly distributed by X Consortium]
Silicon Graphics Inc. (SGI)
Solbourne
Sun Microsystems, Inc.

B. We recommend the following workaround if you are not certain whether your system is vulnerable or if you know that your system is vulnerable and you cannot install a patch immediately.

1. Find and disable any copies of xlock that exist on your system and that have the setuid or setgid bits set.

2. Install a version of xlock known to be immune to this vulnerability.

One such supported tool is xlockmore. The latest version of this tool is 4.02, and you should ensure that this is the version you are using. This utility can be obtained from the following site:
ftp://ftp.x.org/contrib/applications/xlockmore-4.02.tar.gz
MD5 (xlockmore-4.02.tar.gz) = c158e6b4b99b3cff4b52b39219dbfe0e

You can also obtain this version from mirror sites. A list of these sites will be displayed if you are not able to access the above archive due to load.

Appendix A Vendor Information

Below is a list of the vendors who have provided information for this advisory. We will update this appendix as we receive additional information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact the vendor directly.

Berkeley Software Design, Inc. (BSDI)

BSD/OS 2.1 is vulnerable to the xlock vulnerability. BSDI recommends that 2.1 customers either upgrade to BSD/OS 3.0 or remove the setuid permission from /usr/X11/bin/xlock.

Cray Research - A Silicon Graphics Company

Cray Research does not include xlock in its X Window releases, so we are not at risk on the xlock buffer overflow problem.

Data General Corporation

The xlock sources (xlockmore-3.7) that DG includes in its contributed software package have been modified to remove this vulnerability. These will be available when release 8 comes out. We also recommend that our customers who have the current version should change the sprintf calls in resource.c to snprintf calls, rebuild and reinstall the package.

Digital Equipment Corporation

This reported problem is not present for Digital's ULTRIX or Digital UNIX Operating Systems Software.

FreeBSD, Inc.

The xlockmore version we ship in our ports collection is vulnerable in all shipped releases. The port in FreeBSD-current is fixed. Solution is to install the latest xlockmore version (4.02).

Hewlett-Packard Company

We ship an suid root program vuelock that is based on xlock. It does have the vulnerability.

The only workaround is to remove the executable, the patch is "in process".

IBM Corporation

AIX is vulnerable to the conditions described in this advisory. The following APARs will be released soon:

AIX 3.2 : APAR IX68189
AIX 4.1 : APAR IX68190
AIX 4.2 : APAR IX68191

IBM and AIX are registered trademarks of International Business Machines Corporation.

LINUX

Red Hat:
Not vulnerable

Caldera:
Not vulnerable

Debian:
An updated package is on the Debian site

SuSE:

ftp://ftp.suse.com/pub/SuSE-Linux/suse_update/S.u.S.E.-4.4.1/xap1/xlock

And in general the new Xlockmore release fixes the problems.

NEC Corporation

UX/4800	Not vulnerable for all versions.
EWS-UX/V(Rel4.2MP	Not vulnerable for all versions.
EWS-UX/V(Rel4.2)	Not vulnerable for all versions.
UP-UX/V(Rel4.2MP)	Not vulnerable for all versions.

The Open Group

Publicly available software that was formerly distributed by the X Consortium -
Not vulnerable.

Silicon Graphics Inc. (SGI)

Patch information can be found in SGI advisory 19970502-02-PX, available from ftp://sgi-gate.sgi.com/security/

Solbourne

Solbourne is not vulnerable to this attack.

Sun Microsystems, Inc.

Bulletin Number: #00150
Date: August 12, 1997
Title: Vulnerability in xlock
Vulnerable: SunOS versions 5.5.1, 5.5.1_x86, 5.5, 5.5_x86, 5.4, 5.4_x86, 5.3, 4.1.4, and 4.1.3_U1

The vulnerability is fixed in the upcoming release of Solaris.

Patches are available to all Sun customers via World Wide Web at:
ftp://sunsolve.sun.com/pub/patches.html.

Customers with Sun support contracts can also obtain patches from local Sun answer centers and SunSITEs worldwide.

Sun security bulletins are available via World Wide Web at:
http://sunsolve.Sun.COM/pub-cgi/us/secbul.pl.

The CERT Coordination Center thanks David Hedley for reporting the original problem and Kaleb Keithley at The Open Group for his support in the development of this advisory.

Revision History

```
Jan. 06, 1999   Updated URLs for Sun Microsystems, Inc.

Sep. 30, 1997   Updated copyright statement

Aug. 15, 1997   Appendix A - updated information for Sun Microsys-
tems, Inc.

July 21, 1997   Appendix A - added information for SGI.

June 4, 1997    Appendix A - updated vendor information for BSDI.
```

14 CA-1997-14: Vulnerability in metamail

Original issue date: May 21, 1997
Last revised: October 25, 1999
Added vendor information for Data General.

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

The CERT Coordination Center has received reports of a vulnerability in metamail, a program that implements MIME. By exploiting the vulnerability, a sender of a MIME-encoded electronic mail message can cause the receiver of the message to execute an arbitrary command if the receiver processes the message using the metamail package. If the attacker has an account on the target user's local system or if the target user's system supports AFS or another distributed filesystem, then the attacker can arrange for the arbitrary command to be one the attacker created. This affects versions of metamail through 2.7 (the current version).

The CERT/CC team recommends installing a vendor patch, if one is available, patching metamail yourself, or disabling metamail (see Section III).

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

I. Description

Multipurpose Internet Mail Extensions (MIME) is a standard format for extended Internet electronic mail. The MIME format permits email to include enhanced text, graphics, and audio in a standardized and interoperable manner. MIME is described in RFCs 2045 through 2049.

metamail is a package that implements MIME (note: metamail can be obtained from ftp://ftp.funet.fi/pub/unix/mail/metamail/mm2.7.tar.Z). Using a configurable "mailcap" file, metamail determines how to treat blocks of electronic mail text based on the content as described by email headers. Some popular packages for handling electronic mail have hooks that allow metamail to be called automatically while a message is being processed.

A condition exists in metamail in which there is insufficient variable checking in some support scripts. By carefully crafting appropriate message headers, a sender can cause the receiver of the message to execute an arbitrary command if the receiver processes the message using the metamail package.

II. Impact

A sender of a MIME encoded mail message can cause the receiver to execute an arbitrary command. If the attacker has an account on the target user's local system or if the target user's system supports AFS or another distributed filesystem, then the attacker can arrange for the arbitrary command to be one the attacker created.

III. Solution

If your vendor supplies metamail with its distribution, then install a patch from your vendor (Solution A). If your vendor does not distribute metamail with their products or does not have a patch available, use the workaround in Solution B. An alternative for those with sufficient expertise is to patch the metamail scripts as described in Solution C.

A. Install a patch from your vendor, if appropriate

The vendors we have heard from so far are listed below, with details in Appendix A. We will update the appendix as we receive more information.

Berkeley Software Design, Inc. (BSDI)
Cray Research - A Silicon Graphics Company
Digital Equipment Corporation
FreeBSD, Inc.
Hewlett-Packard Company
IBM Corporation
Linux
NEC Corporation
Silicon Graphics Inc.
Solbourne
Sun Microsystems, Inc.

B. Disable metamail scripts

To disable the metamail scripts, remove the execute permissions from the scripts that are located in the mm2.7/src/bin directory of metamail v2.7 (the latest version of metamail). Remember that, depending on your installation of metamail, the scripts may be located in other directories in your operating system.

C. Patch metamail yourself

Sites that need to use metamail and have the expertise may wish to patch the scripts that are part of the metamail distribution. Note that the guidance below is supplied as is, and you need to be sure that you understand the impact (if any) that your modifications will have on metamail functionality.

The scripts referred to in the following material are all located in the mm2.7/src/bin directory of metamail v2.7 (the latest version of metamail). They may be located in other directories in your operating system.

1. Ensure that parameters supplied to the scripts do not contain anywhite space.

Using showexternal as an example, add the following code before any argument processing:

```
# Check argument integrity. Don't trust mail headers

switch ("$1$2$3$4$5$6$7")
```

```
case "*[\t ]*":

echo "Illegal white space in arguments\!"

echo "Command was:"

echo "'$0' '$1' '$2' '$3' '$4' '$5' '$6' '$7'"

exit 2

endsw
```

Add this code to the showexternal script at the very least, prior to any argument processing within that script. We encourage you to add this code to other scripts in mm2.7/src/bin directory to ensure that arguments in those scripts also exclude white space. You may need to adapt the code for your particular system.

Note that this patch may affect functionality in cases (such as filenames) where parameters may have legitimately included white space.

This step addresses the problem referred to in this advisory. As part of a more generally secure programming practice, please also consider the following modifications.

2. Ensure that script parameter references are quoted. For instance, in show external, change this line:

set name=$3

to

set name="$3"

This should be done for every reference to a command line argument in each of the scripts.

Note that csh has a :q operator which is also intended for this purpose. If you prefer, you can use this operator in each case instead of quoting.

3. Any variables in these scripts that take their value (either directlyor indirectly) from a script parameter should also be quoted where necessary.

For instance, in the showexternal script, change the line:

get $name $NEWNAME

to

get "$name" "$NEWNAME"

Also change the following line:

if ($NEWNAME != $name) then

to

if ("$NEWNAME" != "$name") then

Similarly, there will be other instances where $name specifically, and other variables in general, should be quoted.

The reason is that these variables take their value from the script parameters (for example, $name takes its value from $3, and $NEWNAME may take its value from $name).

As before, the :q operator can be used in each case.

Note that in doing this step, some care will be required.

4. Make sure that users have an appropriate umask set for directory and file creation.

Although the value is subject to local restrictions, you may want to use a default value of 027 (depending upon the local environment).

5. Make sure that users have an appropriate value set for the environment variable METAMAIL_TMPDIR.

This environment variable tells metamail where to create the temporary files it needs while processing. If the variable is not set in the user's environment, the default value is /tmp. Since /tmp is accessible by all users, it is possible that use of this value will allow exploitation of race conditions. We recommend setting the value to a protected directory belonging to the user.

6. To ensure that the METAMAIL_TMPDIR is used properly and in a secure manner, consider modifications along the following lines, using the showexternal scripts as an example.

These modifications should reflect and reinforce the suggestions outlined in the previous two items, namely that the temporary directory metamail uses should be protected and accessible only by the user.

Note that the following code fragments are for example only, and sites should adapt this code according to local requirements.

Change these lines:

```
if (! $?METAMAIL_TMPDIR) then

set METAMAIL_TMPDIR=/tmp

endif
```

to

```
# Set a sensible value for the temporary directory, if its not
# already set. If TMPDIR is set previously, then we will
```

```
# assume it is adequately protected.
if (! $?METAMAIL_TMPDIR) then
if ($?TMPDIR) then
set METAMAIL_TMPDIR="$TMPDIR"
else
set METAMAIL_TMPDIR=~/metamail_tmp
endif
endif
# Set a sensible umask value
umask 077
# Make sure that the temporary directory is available
if (! -d "$METAMAIL_TMPDIR") then
if (! -e "$METAMAIL_TMPDIR") then
mkdir "$METAMAIL_TMPDIR"
else
echo "$METAMAIL_TMPDIR exists, but is not a directory"
exit 2
endif
if ( $status != 0 || ! -d "$METAMAIL_TMPDIR" ) then
echo "Error creating $METAMAIL_TMPDIR"
exit 2
endif
endif
```

Appendix A Vendor Information

Below is a list of the vendors who have provided information for this advisory. We will update this appendix as we receive additional information. If you do not see your vendor's name, please contact the vendor directly or use the workaround in Section III.

Berkeley Software Design, Inc. (BSDI)

BSDI ships metamail and is vulnerable to the attack. Patches are in progress.

Cray Research - A Silicon Graphics Company

Cray Research does not ship metamail as part of either Unicos or Unicos/mk.

Data General

Our metamail scripts are Bourne shell scripts from the SVR4.2MP distribution and do not have the parameter quoting problem.

Digital Equipment Corporation

Digital Equipment Corporation
Software Security Response Team
May 19,1997

This reported problem is not present for Digital's ULTRIX or Digital UNIX Operating Systems Software.

- DIGITAL EQUIPMENT CORPORATION

FreeBSD, Inc.

If you installed the metamail package or port then you are vulnerable. All released versions of FreeBSD including 2.2.2R have this flaw in them. The port was corrected as of May 21, 1997. Either update your system from a more recent port, or apply the patches contained in this advisory to those files affected.

Hewlett-Packard Company

HP-UX is vulnerable; patches are in progress.

IBM Corporation

Not vulnerable, metamail is not shipped as part of AIX.

IBM and AIX are registered trademarks of International Business Machines Corporation.

Linux

Debian:

Debian uses its own bourne shell based metamail scripts not the standard ones.

Red Hat: i386
rpm -Uvh ftp://ftp.redhat.com/updates/4.2/i386/metamail-2.7-7.1.i386.rpm

Alpha
rpm -Uvh ftp://ftp.redhat.com/updates/4.2/alpha/metamail-2.7-7.1.alpha.rpm

NEC Corporation

UX/4800	Not vulnerable for all versions.
EWS-UX/V(Rel4.2MP)	Not vulnerable for all versions.
EWS-UX/V(Rel4.2)	Not vulnerable for all versions.
UP-UX/V(Rel4.2MP)	Not vulnerable for all versions.
EWS-UX/V(Rel4.0)	Not vulnerable for all versions.
UP-UX/V	Not vulnerable for all versions.

Silicon Graphics Inc.

At this time, Silicon Graphics does not have any public information for the metamail issue. Silicon Graphics has communicated with CERT and other external security parties and is actively investigating this issue. When more Silicon Graphics information (including any possible patches) is available for release, that information will be released via the SGI security mailing list, wiretap.

For subscribing to the wiretap mailing list and other SGI security related information, please refer to the Silicon Graphics Security Headquarters website located at:
http://www.sgi.com/Support/Secur/security.html.

Solbourne

We do not ship the utility.
We do not anticipate providing a patch, since we do not ship the utility.

Sun Microsystems, Inc.

Sun does not ship metamail with any of our platforms.
Sun has no plans to produce patches.

The CERT Coordination Center staff thanks Olaf Kirch for contributing code to the solution section and thanks BSDI and FreeBSD for their input on the solution.

Revision History

```
Oct 25, 1999 Added vendor information for Data General.

Oct 29, 1997 Updated vendor information for Red Hat.

Sep 30, 1997 Updated copyright statement

May 23, 1997 Appendix A, BSDI - added information.

May 21, 1997 Appendix A, FreeBSD - changed release date of the patch
```

15 CA-1997-15: Vulnerability in SGI login LOCKOUT

Original issue date: May 28, 1997
Last revised: September 30, 1997
Updated copyright statement

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

The text of this advisory was originally released on April 10, 1997, as AUSCERT Advisory AA-97.12, developed by the Australian Computer Emergency Response Team. To more widely broadcast this information, we are reprinting the AUSCERT advisory here with their permission. Only the contact information at the end has changed: AUSCERT contact information has been replaced with CERT/CC contact information.

We will update this advisory as we receive additional information. Look for it in an "Updates" section at the end of the advisory.

AUSCERT has received information that a vulnerability exists in the login program when the LOCKOUT parameter in /etc/default/login is set to a number greater than zero. This vulnerability is known to be present in IRIX 5.3 and 6.2. Other versions of IRIX may also be vulnerable.

This vulnerability may allow users to create arbitrary or corrupt certain files on the system.

Exploit information involving this vulnerability has been made publicly available.

At this stage, AUSCERT is unaware of any official vendor patches. AUSCERT recommends that sites apply the workaround given in Section 3 until vendor patches are made available.

This advisory will be updated as more information becomes available.

1. Description

Under the IRIX operating system, there is a file /etc/default/login which contains default security logging configuration options. If the parameter LOCKOUT is included in this file, and is set to a value greater than zero, it causes accounts to be locked after a specified number of consecutive unsuccessful login attempts by the same user.

When LOCKOUT is enabled users may be able to create arbitrary or corrupt certain files on the system, due to an inadequate check in the login verification process.

Sites can determine if this functionality is enabled by using the command:

```
% grep '^LOCKOUT' /etc/default/login
LOCKOUT=3
```

If the number on the same line as LOCKOUT is greater than zero the vulnerability may be exploited.

Information involving this vulnerability has been made publicly available.

Silicon Graphics Inc. has informed AUSCERT that they are investigating this vulnerability.

2. Impact

Users may create arbitrary or corrupt certain files on the system.

3. Workarounds/Solution

AUSCERT recommends that sites prevent the exploitation of this vulnerability by immediately applying the workaround given in Section 3.1.

Currently there are no vendor patches available that address this vulnerability. AUSCERT recommends that official vendor patches be installed when they are made available.

3.1 Disable the LOCKOUT parameter

To prevent the exploitation of the vulnerability described in this advisory, AUSCERT recommends that the functionality provided with the LOCKOUT parameter be disabled.

The LOCKOUT parameter can be disabled by editing /etc/default/login and commenting out the line containing the LOCKOUT parameter. The comment character for /etc/default/login is "#".

Note that after applying this workaround, accounts will not be automatically locked using the LOCKOUT parameter functionality.

AUSCERT thanks to Alan J Rosenthal from The University of Toronto and Silicon Graphics Inc. for their assistance in this matter.

UPDATES

May 28, 1997

After the AUSCERT advisory was published, we received this information from Silicon Graphics:

At this time, Silicon Graphics does not have any public information for the login LOCKOUT issue. Silicon Graphics has communicated with CERT/CC and other external security parties and is actively investigating this issue. When more Silicon Graphics information (including any possible patches) is availavble for release, that information will be released via the SGI security mailing list, wiretap.

For subscribing to the wiretap mailing list and other SGI security related information, please refer to the Silicon Graphics Security Headquarters website at:
http://www.sgi.com/Support/Secur/security.html.

Revision History

Sept. 30, 1997 Updated copyright statement

Sept. 19, 1997 Updates Section. Added updated vendor information for Silicon Graphics, Inc.

16 CA-1997-16: ftpd Signal Handling Vulnerability

Original issue date: May 29, 1997
Last revised: December 5, 1997
Added vendor information for NCR Corporation to the Updates section.

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

The text of this advisory was originally released by AUSCERT as AA-97.03 ftpd Signal Handling Vulnerability on January 29, 1997, and updated on April 18, 1997. To give this document wider distribution, we are reprinting the updated AUSCERT advisory here with their permission. Only the contact information at the end has changed: AUSCERT contact information has been replaced with CERT/CC contact information.

Although the text of the AUSCERT advisory has not changed, additional vendor information has been added immediately after the AUSCERT text.

We will update this advisory as we receive additional information. Look for it in an "Updates" section at the end of the advisory.

AUSCERT has received information that there is a vulnerability in some versions of ftpd distributed and installed under various Unix platforms.

This vulnerability may allow regular and anonymous ftp users to read or write to arbitrary files with root privileges.

The vulnerabilities in ftpd affect various third party and vendor versions of ftpd. AUSCERT recommends that sites take the steps outlined in section 3 as soon as possible.

This advisory will be updated as more information becomes available.

1. Description

AUSCERT has received information concerning a vulnerability in some vendor and third party versions of the Internet File Transfer Protocol server, ftpd(8).

This vulnerability is caused by a signal handling routine increasing process privileges to root, while still continuing to catch other signals. This introduces a race condition which may allow regular, as well as anonymous ftp, users to access files with root privileges. Depending on the configuration of the ftpd server, this may allow intruders to read or write to arbitrary files on the server.

This attack requires an intruder to be able to make a network connection to a vulnerable ftpd server.

Sites should be aware that the ftp services are often installed by default. Sites can check whether they are allowing ftp services by checking, for example, /etc/inetd.conf:

```
# grep -i '^ftp' /etc/inetd.conf
```

Note that on some systems the inetd configuration file may have a different name or be in a different location.

Please consult your documentation if the configuration file is not found in

/etc/inetd.conf.

If your site is offering ftp services, you may be able to determine the version of ftpd by checking the notice when first connecting.

The vulnerability status of specific vendor and third party ftpd servers can be found in Section 3. Information involving this vulnerability has been made publicly available.

2. Impact

Regular and anonymous users may be able to access arbitrary files with root privileges. Depending on the configuration, this may allow anonymous, as well as regular, users to read or write to arbitrary files on the server with root privileges.

3. Workarounds/Solution

AUSCERT recommends that sites prevent the possible exploitation of this vulnerability by immediately applying vendor patches if they are available. Specific vendor information regarding this vulnerability is given in Section 3.1.

If the ftpd supplied by your vendor is vulnerable and no patches are available, sites may wish to install a third party ftpd which does not contain the vulnerability described in this advisory (Section 3.2).

3.1 Vendor patches

The following vendors have provided information concerning the vulnerability status of their ftpd distribution.

Detailed information has been appended in Appendix A. If your vendor is not listed below, you should contact your vendor directly.

Berkeley Software Design, Inc.
Digital Equipment Corporation
The FreeBSD Project
Hewlett-Packard Corporation
IBM Corporation
The NetBSD Project
The OpenBSD Project
Red Hat Software
Silicon Graphics Inc.

Washington University ftpd (Academ beta version)
Wietse Venema's logdaemon ftpd

3.2 Third party ftpd distributions

AUSCERT has received information that the following third party ftpd distributions do not contain the signal handling vulnerability described in this advisory:

wu-ftpd 2.4.2-beta-12
logdaemon 5.6 ftpd

Sites should ensure they are using the current version of this software. Information on these distributions is contained in Appendix A.

Sites should note that these third party ftpd distributions may offer some different functionality to vendor versions of ftpd. AUSCERT advises sites to read the documentation provided with the above third party ftpd distributions before installing.

Appendix A

Berkeley Software Design, Inc. (BSDI)

BSD/OS 2.1 is vulnerable to the ftpd problem described in this advisory. Patches have been issued and may be retrieved via the patches@BSDI.COM email server or from:
ftp://ftp.bsdi.com/bsdi/patches/patches-2.1/U210-033.

Digital Equipment Corporation

DIGITAL UNIX Versions:

3.2c, 3.2de1, 3.2de2, 3.2f, 3.2g, 4.0, 4.0a, 4.0b

SOLUTION:

This potential security vulnerability has been resolved and an official patch kit is available for DIGITAL UNIX V3.2g, V4.0, V4.0a, and V4.0b.

This article will be updated accordingly when patch kits for DIGITAL UNIX V3.2c, V3.2de1, V3.2de2, V3.2f become available.

The currently available patches may be obtained from your normal Digital support channel or from the following URL. (Select the appropriate version to locate this patch kit.)
ftp://ftp.service.digital.com/patches/public/dunix

VERSION	KIT ID	SIZE	CHECK	SUM
v3.2g	SSRT0448U_v32g.tar	296960	32064	290
v4.0	SSRT0448U_v40.tar	542720	07434	530
v4.0a	SSRT0448U_v40a.tar	542720	43691	530
v4.0b	SSRT0448U_v40b.tar	471040	45701	460

Please refer to the applicable README notes information prior to the installation of patch kits on your system.

Note: The appropriate patch kit must be reinstalled following any upgrade beginning with V3.2c up to and including V4.0b.

The FreeBSD Project

The FreeBSD Project has informed AUSCERT that the vulnerability described in this advisory has been fixed in FreeBSD-current (from January 27, 1997), and will be fixed in the upcoming FreeBSD 2.2 release. All previous versions of FreeBSD are vulnerable.

Hewlett-Packard Corporation

Hewlett-Packard has informed AUSCERT that the ftpd distributed with HP-UX 9.x and 10.x are vulnerable to this problem. Patches are currently in process.

IBM Corporation

The version of ftpd shipped with AIX is vulnerable to the conditions described in the advisory. The following APARs will be available shortly:

AIX 3.2 : APAR IX65536
AIX 4.1 : APAR IX65537
AIX 4.2 : APAR IX65538

To Order

APARs may be ordered using Electronic Fix Distribution (via FixDist) or from the IBM Support Center. For more information on FixDist, reference URL:
http://service.software.ibm.com/aixsupport/ or send e-mail to aixserv@austin.ibm.com with a subject of "FixDist".

IBM and AIX are registered trademarks of International Business Machines Corporation.

The NetBSD Project

NetBSD (all versions) have the ftpd vulnerability described in this advisory. It has since been fixed in NetBSD-current. NetBSD have also made patches available and they can be retrieved from: ftp://ftp.netbsd.org/pub/NetBSD/misc/security/19970123-ftpd.

The OpenBSD Project

OpenBSD 2.0 did have the vulnerability described in this advisory, but has since been fixed in OpenBSD 2.0-current (from January 5, 1997).

Red Hat Software

The signal handling code in wu-ftpd has some security problems which allows users to read all files on your system. A new version of wu-ftpd is now available for Red Hat 4.0 which Red Hat suggests installing on all of your systems. This new version uses the same fix posted to redhat-list@redhat.com by Savochkin Andrey Vladimirovich. Users of Red Hat Linux versions earlier then 4.0 should upgrade to 4.0 and then apply all available security packages.

Users whose computers have direct internet connections may apply this update by using one of the following commands:

Intel:
rpm -Uvh ftp://ftp.redhat.com/updates/4.0/i386/wu-ftpd-2.4.2b11-9.i386.rpm

Alpha:
rpm -Uvh ftp://ftp.redhat.com/updates/4.0/axp/wu-ftpd-2.4.2b11-9.axp.rpm

SPARC:
rpm -Uvhftp://ftp.redhat.com/updates/4.0/sparc/wu-ftpd-2.4.2b11-9.sparc.rpm

All of these packages have been signed with Red Hat's PGP key.

wu-ftpd Academ beta version

The current version of wu-ftpd (Academ beta version), wu-ftpd 2.4.2-beta-12, does not contain the vulnerability described in this advisory. Sites using earlier versions should upgrade to the current version immediately. At the time of writing, the current version can be retrieved from: ftp://ftp.academ.com/pub/wu-ftpd/private/.

logdaemon Distribution

The current version of Wietse Venema's logdaemon (5.6) package contains an ftpd utility which addresses the vulnerability described in this advisory. Sites using earlier versions of this package should upgrade immediately. The current version of the logdaemon package can be retrieved from:

ftp://ftp.win.tue.nl/pub/security/ ftp://ftp.auscert.org.au/pub/mirrors/ftp.win.tue.nl/logdaemon/ ftp://ftp.cert.dfn.de/pub/tools/net/logdaemon/

The MD5 checksum for Version 5.6 of the logdaemon package is:

MD5 (logdaemon-5.6.tar.gz) = 5068f4214024ae56d180548b96e9f368

AUSCERT thanks David Greenman, Wietse Venema (visiting IBM T.J. Watson Research) and Stan Barber (Academ Consulting Services) for their contributions in finding solutions to this vulnerability. Thanks also to Dr Leigh Hume (Macquarie University), CERT/CC, and DFNCERT for their assistance in this matter. AUSCERT also thanks those vendors that provided feedback and patch information contained in this advisory.

UPDATES

Vendor Information Added by CERT/CC

Digital Equipment Corporation

AUG, 1997 DIGITAL UNIX Versions:

3.2C, 3.2DE1, 3.2DE2, 3.2F, 3.2G, 4.0, 4.0A, 4.0B, 4.0C

SOLUTION:

This potential security vulnerability has been resolved and may be obtained from your normal Digital support channel or from the following URL.

NOTE: Previously released singular ECO patches that were identified for this problem have been superseded in the aggregate versions of the ECO patch kits.
ftp://ftp.service.digital.com/patches/public/dunix.

(Select the appropriate version and it's aggregate patch kit).

Please refer to the applicable README notes information prior to the installation of patch kits on your system.

Hewlett-Packard Corporation

HP has covered this in our security bulletin HPSBUX9702-055, 19 February 1997. The Security Bulletin contains pointers to the patches:

SOLUTION: Apply patch:

PHNE_10008 for all platforms with HP-UX releases 9.X
PHNE_10009 for all platforms with HP-UX releases 10.0X/10.10
PHNE_10010 for all platforms with HP-UX releases 10.20

PHNE_10011 for all platforms with HP-UX releases 10.20 (kftpd)

AVAILABILITY: All patches are available now.

IBM Corporation

See the appropriate release below to determine your action.

AIX 3.2

Apply the following fix to your system:

APAR - IX65536 (PTF - U447700)

To determine if you have this PTF on your system, run the following command:

lslpp -lB U447700

AIX 4.1

Apply the following fix to your system:

APAR - IX65537

To determine if you have this APAR on your system, run the following command:

instfix -ik IX65537

Or run the following command:

lslpp -h bos.net.tcp.client

Your version of bos.net.tcp.client should be 4.1.5.3 or later.

AIX 4.2

Apply the following fix to your system:

APAR - IX65538

To determine if you have this APAR on your system, run the following command:

instfix -ik IX65538

Or run the following command:

lslpp -h bos.net.tcp.client

Your version of bos.net.tcp.client should be 4.2.1.0 or later.

To Order

APARs may be ordered using Electronic Fix Distribution (via FixDist) or from the IBM Support Center. For more information on FixDist, reference URL: http://service.software.ibm.com/aixsupport/ or send e-mail to aixserv@austin.ibm.com with a subject of "FixDist".

IBM and AIX are registered trademarks of International Business Machines Corporation.

NCR Corporation

NCR is delivering a set of operating system dependent patches which contain an update for this problem. Accompanying each patch is a README file which discusses the general purpose of the patch and describes how to apply it to your system.

Recommended solution:

Apply one of the following patches depending on the revision of the inet package installed on your system. To check its version execute:

pkginfo -x inet

```
For inet 5.01.xx.xx: - PINET501 (Version later than 05.01.01.49)

For inet 6.01.xx.xx: - PINET601 (Version later than 06.01.00.06)

For inet 6.02.xx.xx: - Fix included in the product as shipped with
                       MP-RAS UNIX 3.02. (In inet package after
                       revision 6.02.00c).
```

Silicon Graphics Inc.

The ftpd program (/usr/etc/ftpd) is installed on all IRIX systems by default.

Patch information for this vulnerability is available in SGI"s Security Advisory 19970801-01-PX, "IRIX ftpd Signal Handling Vulnerability" available at http://www.sgi.com/Support/Secur/security.html/.

Sun Microsystems, Inc.

Not vulnerable.

Revision History

```
Dec. 5,  1997 Addedd vendor information for NCR Corporation to the
Updates section.
```

Oct. 30, 1997 UPDATES, Vendor Information Added by CERT/CC -added information for NCR.

Sep. 30, 1997 Updated copyright statement

Aug. 15, 1997 Section 3.1 and UPDATES - Added by CERT/CC.Vendor patch information for Digital Equipment Corporation and Silicon Graphics, Inc.

June 3, 1997 Minor editorial formatting change.

June 9, 1997 UPDATES, Vendor Information Added by CERT/CC - added information for Sun Microsystems, Inc.

17 CA-1997-17: Vulnerability in suidperl(sperl)

Original issue date: May 29, 1997
Last revised: December 5, 1997
Added vendor information for NCR Corporation.

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

The CERT Coordination Center has received reports of a buffer overflow condition in suidperl built from Perl 4.n and Perl 5.n distributions on UNIX systems. By calling this program with appropriately crafted parameters, unauthorized local users can execute arbitrary commands as root. This vulnerability is being actively exploited.

The CERT/CC team recommends installing a vendor patch if one is available (see Section III.B). Until you can do so, we recommend disabling suidperl (Section III.A). Two other alternatives are to install suidperl or sperl from version 5.003 source code along with the patch provided in Appendix B of this advisory (see also Section III.C), or upgrade to Perl version 5.004 (Section III.D). Note that Perl4 is no longer supported.

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

I. Description

On some systems, setuid and setgid scripts (scripts written in the C shell, Bourne shell, or Perl, for example, with the set user or group ID permissions enabled) are insecure due to a race condition in the kernel. For those systems, Perl versions 4 and 5 attempt to work around this vulnerability with a special program named suidperl, also known as sperl. This program attempts to emulate the set-user-ID and set-group-ID features of the kernel.

There is a buffer overflow condition in suidperl built from Perl 4.n and Perl 5.n distributions earlier than version 5.004. If this program is called with appropriately crafted parameters, an attacker can execute arbitrary commands as root. This vulnerability is being actively exploited.

II. Impact

Users executing Perl scripts with the setuid bit set can execute arbitrary commands with the effective uid of the owner of the Perl script. Attackers can execute commands as root.

III. Solution

Use the command in Section A to help you determine if your system is vulnerable and, if it is, to (optionally) disable the suidperl and sperl programs (see Section A). If you find that your system is vulnerable, replace the suidperl and sperl programs with new versions.

Section B describes how to do that if your site uses versions of suidperl and sperl that are provided as part of a vendor-supplied distribution. Sites that installed suidperl and sperl programs themselves from the Perl source distribution should patch the distribution as described in Section C or upgrade to version 5.004 as described in Section D. Note that Perl4 is no longer supported.

A. Determine if your system is vulnerable and disable vulnerable programs

To determine if a system is vulnerable to this problem and to disable the programs that are believed to be vulnerable, use the following find command or a variant. Consult your local system documentation to determine how to tailor the find program on your system.

After you have run this command on all your systems, they will no longer be vulnerable. Note that after disabling the suidperl and sperl programs, they will no longer be able to emulate the set-user-ID and set-group-ID features of the kernel.

You will need to run the find command on each system you maintain because the command examines files on the local disk only. Substitute the names of your local file systems for FILE_SYSTEM_NAMES in the example. Example local file system names are /, /usr, and /var. You must do this as root.

Note that this is one long command, though we have separated it onto five lines using backslashes.

```
find FILE_SYSTEM_NAMES -xdev -type f -user root \

\ ( -name'sperl4.[0-9][0-9][0-9]' \

-o -name 'sperl5.00[0-3]' \

-o -name 'suidperl' \) \

-perm -04000 -print -ok chmod ug-s '{}' \;
```

This command will find all files on a system that are
- only in the file system you name (FILE_SYSTEM_NAMES -xdev)
- regular files (-type f)
- owned by root (-user root)
- named appropriately (-name 'sperl4.[0-9][0-9][0-9]' -o -name 'sperl5.00[0-3]' -o -name 'suidperl')
- setuid root (-perm -04000)

Once found, those files will

- have their names printed (-print)
- have their modes changed, but only if you type `y' in response to the prompt (-ok chown ug-s '{}' \;)

B. Obtain and install the appropriate patch from your vendor

If your vendor ships suidperl or sperl, you may be vulnerable and need a patch. Appendix A contains information provided by the following vendors. If your vendor is not on this list, please contact the vendor directly.

Berkeley Software Design, Inc. (BSDI)
Cray Research - A Silicon Graphics Company
Data General Corporation
Hewlett-Packard Company
IBM Corporation
Linux
NCR Corporation
The Santa Cruz Operation, Inc. (SCO)
Silicon Graphics, Inc. (SGI)

Until you can install a patch, we recommend disabling suidperl. The find command above will help you do that. If you need suidperl or sperl, see the alternatives in Sections C and D below.

C. Install suidperl or sperl from 5.003 source code and apply a patch.

Follow the instructions below, which were provided by Chip Salzenberg.
If you would like to keep using setuid Perl scripts, fix Perl yourself by following these steps:

1. Go to your Perl 5.003 source directory, or else obtain a fresh Perl 5.003 distribution from http://www.perl.com/CPAN/src/5.0/perl5.003.tar.gz or another CPAN archive accessible to you.

This file is approximately 1.5 megabytes in size.

2. Using the "patch" program, apply the patch that is enclosed below in Appendix B.

3. Build and install the patched Perl 5.003. (If you have never built Perl before, be sure to read the "INSTALL" file first.)

Perl 5.003 binaries that have had this patch applied, and therefore are safe from all known attacks, can be identified by the output of the "perl -v" command: the "locally applied patches" list will include "SUIDBUF - Buffer overflow fixes for suidperl security".

D. Install suidperl or sperl from 5.004 source code (no patch needed).

If you would like to upgrade to Perl version 5.004, follow these steps:

1. Obtain a fresh Perl 5.004 distribution from http://www.perl.com/CPAN/src/5.0/perl5.004.tar.gz or another CPAN archive accessible to you.

This file is approximately 2.5 megabytes in size.

2. Build and install Perl 5.004 according to the instructions given in the "INSTALL" file.

Do NOT apply the patch.

Perl 5.004 binaries, which are safe from all known attacks, can be identified by the output of the "perl -v" command: it should say "This is perl, version 5.004". (Unlike the 5.003 patch mentioned in Section C, the "locally applied patches" list will NOT include "SUIDBUF - Buffer overflow fixes for suidperl security". The fact that it is version 5.004 is sufficient in this case.)

Appendix A Vendor Information

Below is a list of the vendors who have provided information for this advisory. We will update this appendix as we receive additional information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact the vendor directly.

Berkeley Software Design, Inc. (BSDI)

BSD/OS is vulnerable to the suidperl (sperl) buffer overflow problem. We will be releasing a patch for BSDI 3.0 and perl 5.003 and are currently working on patches for BSD/OS 3.0 and Perl 4.036. We will also be developing patches for the perl versions shipped with BSD/OS 2.1.

Cray Research - A Silicon Graphics Company

Cray Research does not ship perl as part of either Unicos or Unicos/mk.

Data General Corporation

The only perl executables that are shipped with DG/UX are:

/bin/perl

and

/bin/perl5 /* in R420 */

These are not set uid programs.

Therefore, no versions of DG/UX are vulnerable to this problem.

Hewlett-Packard Company

HP does not ship this product.

IBM Corporation

AIX versions do not have Perl as part of the standard product. However, the SP2's PSSP software does contain suidperl, but the program is not installed with the setuid bit set.

IBM and AIX are registered trademarks of International Business Machines Corporation.

Linux

Red Hat 4.2 is not vulnerable.

Red Hat 4.1/4.0 you can get the upgraded RPM from ftp.redhat.com

If you wish to check whether you have the fixed perl run perl -v and check for
Locally applied patches:

SUIDBUF - Buffer overflow fixes for suidperl security

NCR Corporation

NCR MP-RAS SVR4 Unix does have safe kernel support for setuid scripts so that suidperl is not necessary. If you have installed a version of perl that includes suidperl, you should remove suidperl and install a version of perl built so as not to require it.

perl as delivered from NCR on later MP-RAS releases does not install sperl/suidperl, and as such are not vulnerable.

Status per MP-RAS UNIX SVR4 release:

```
MP-RAS 2.03.x and lower - perl not directly included in product.
MP-RAS 3.00.x/3.01.x - perl not installed setuid. perl 5.001 based.
MP-RAS 3.02.x and later - perl delivered with the necessary
setuid change included, but binary not
installed setuid as well. perl 5.003 based.
```

For all directly delivered perl binaries, sperl/suidperl are not included and no perl binary are installed setuid.

The Santa Cruz Operation, Inc. (SCO)

suidperl is not included in any SCO products.

SCO CMW+ and SCO OpenServer do not have kernel support for setuid scripts, but you may have installed suidperl in order to emulate that functionality - in that case you should replace your version of perl with version 5.004, or patch your source code as noted in this advisory.

SCO UnixWare does have safe kernel support for setuid scripts so that suidperl is not necessary. If you have installed a version of perl that includes suidperl, you should remove suidperl and install a version of perl built so as not to require it.

Silicon Graphics, Inc. (SGI)

At this time, Silicon Graphics does not have any public information for this suidperl/sperl issue. Silicon Graphics has communicated with CERT and other external security parties and is actively investigating this issue. When more Silicon Graphics information (including any possible patches) is available for release, that information will be released via the SGI security mailing list, wiretap.

For subscribing to the wiretap mailing list and other SGI security related information, please refer to the Silicon Graphics Security Headquarters website located at:
http://www.sgi.com/Support/Secur/security.html.

Sun Microsystems, Inc.

Sun does not ship this product.

Appendix B Source Code Patch Information

The following patch information has been supplied by Chip Salzenberg. If you built suidperl or sperl from 5.003 source code, we encouraged you to apply this patch (see the explanation in Section III.C above).

Patch follows.

```
Index: patchlevel.h
***************
*** 41,42 ****
- --- 41,43 ----
+ ,"SUIDBUF - Buffer overflow fixes for suidperl security"
,NULL
};
Index: perl.c
*************** char *s;
*** 1212,1216 ****
# endif
#endif
! fputs("\n\t+ suidperl security patch", stdout);
fputs("\n\nCopyright 1987-1996, Larry Wall\n",stdout);
#ifdef MSDOS
- --- 1212,1216 ----
# endif
#endif
! fputs("\n\t+ two suidperl security patches", stdout);
fputs("\n\nCopyright 1987-1996, Larry Wall\n",stdout);
#ifdef MSDOS
Index: gv.c
*************** gv_fetchfile(name)
*** 59,67 ****
char *name;
{
! char tmpbuf[1200];
GV *gv;
! sprintf(tmpbuf,"::_<%s", name);
gv = gv_fetchpv(tmpbuf, TRUE, SVt_PVGV);
sv_setpv(GvSV(gv), name);
if (*name == '/' && (instr(name,"/lib/") || instr(name,".pm")))
- --- 59,80 ----
```

```
char *name;
{
! char smallbuf[256];
! char *tmpbuf;
! STRLEN tmplen;
GV *gv;
! tmplen = strlen(name) + 4;
! if (tmplen < sizeof smallbuf)
! tmpbuf = smallbuf;
! else
! New(603, tmpbuf, tmplen + 1, char);
! tmpbuf[0] = ':';
! tmpbuf[1] = ':';
! tmpbuf[2] = '_';
! tmpbuf[3] = '<';
! strcpy(tmpbuf + 4, name);
gv = gv_fetchpv(tmpbuf, TRUE, SVt_PVGV);
+ if (tmpbuf != smallbuf)
+ Safefree(tmpbuf);
sv_setpv(GvSV(gv), name);
if (*name == '/' && (instr(name,"/lib/") || instr(name,".pm")))
Index: toke.c
*************** static char *scan_const _((char *start))
*** 22,26 ****
static char *scan_formline _((char *s));
static char *scan_heredoc _((char *s));
! static char *scan_ident _((char *s, char *send, char *dest, I32
ck_uni));
static char *scan_inputsymbol _((char *start));
static char *scan_pat _((char *start));
- --- 22,27 ----
static char *scan_formline _((char *s));
static char *scan_heredoc _((char *s));
! static char *scan_ident _((char *s, char *send, char *dest, STRLEN
destlen,
! I32 ck_uni));
static char *scan_inputsymbol _((char *start));
static char *scan_pat _((char *start));
*************** static char *scan_str _((char *start));
*** 28,32 ****
static char *scan_subst _((char *start));
static char *scan_trans _((char *start));
! static char *scan_word _((char *s, char *dest, int allow_package,
STRLEN *slp));
```

```
static char *skipspace _((char *s));
static void checkcomma _((char *s, char *name, char *what));
- --- 29,34 ----
static char *scan_subst _((char *start));
static char *scan_trans _((char *start));
! static char *scan_word _((char *s, char *dest, STRLEN destlen,
! int allow_package, STRLEN *slp));
static char *skipspace _((char *s));
static void checkcomma _((char *s, char *name, char *what));
*************** static char * filter_gets _((SV *sv, FIL
*** 47,50 ****
- --- 49,54 ----
static void restore_rsfp _((void *f));
+ static char too_long[] = "Identifier too long";
+
/* The following are arranged oddly so that the guard on the switch
statement
* can get by with a single comparison (if the compiler is smart
enough).
*************** int allow_tick;
*** 475,479 ****
(allow_tick && *s == '\'') )
{
! s = scan_word(s, tokenbuf, allow_pack, &len);
if (check_keyword && keyword(tokenbuf, len))
return start;
- --- 479,483 ----
(allow_tick && *s == '\'') )
{
! s = scan_word(s, tokenbuf, sizeof tokenbuf, allow_pack, &len);
if (check_keyword && keyword(tokenbuf, len))
return start;
*************** register char *s;
*** 847,851 ****
unsigned char un_char = 0, last_un_char;
char *send = strchr(s,']');
! char tmpbuf[512];
if (!send) /* has to be an expression */
- --- 851,855 ----
unsigned char un_char = 0, last_un_char;
char *send = strchr(s,']');
! char tmpbuf[sizeof tokenbuf * 4];
if (!send) /* has to be an expression */
*************** register char *s;
```

```
*** 872,876 ****
weight -= seen[un_char] * 10;
if (isALNUM(s[1])) {
! scan_ident(s,send,tmpbuf,FALSE);
if ((int)strlen(tmpbuf) > 1 && gv_fetchpv(tmpbuf,FALSE, SVt_PV))
weight -= 100;
- --- 876,880 ----
weight -= seen[un_char] * 10;
if (isALNUM(s[1])) {
! scan_ident(s, send, tmpbuf, sizeof tmpbuf, FALSE);
if ((int)strlen(tmpbuf) > 1 && gv_fetchpv(tmpbuf,FALSE, SVt_PV))
weight -= 100;
*************** GV *gv;
*** 942,946 ****
{
char *s = start + (*start == '$');
! char tmpbuf[1024];
STRLEN len;
GV* indirgv;
- --- 946,950 ----
{
char *s = start + (*start == '$');
! char tmpbuf[sizeof tokenbuf];
STRLEN len;
GV* indirgv;
*************** GV *gv;
*** 952,956 ****
gv = 0;
}
! s = scan_word(s, tmpbuf, TRUE, &len);
if (*start == '$') {
if (gv || last_lop_op == OP_PRINT || isUPPER(*tokenbuf))
- --- 956,960 ----
gv = 0;
}
! s = scan_word(s, tmpbuf, sizeof tmpbuf, TRUE, &len);
if (*start == '$') {
if (gv || last_lop_op == OP_PRINT || isUPPER(*tokenbuf))
*************** yylex()
*** 1629,1633 ****
case '*':
if (expect != XOPERATOR) {
! s = scan_ident(s, bufend, tokenbuf, TRUE);
```

```
expect = XOPERATOR;
force_ident(tokenbuf, '*');
- --- 1633,1637 ----
case '*':
if (expect != XOPERATOR) {
! s = scan_ident(s, bufend, tokenbuf, sizeof tokenbuf, TRUE);
expect = XOPERATOR;
force_ident(tokenbuf, '*');
*************** yylex()
*** 1645,1649 ****
case '%':
if (expect != XOPERATOR) {
! s = scan_ident(s, bufend, tokenbuf + 1, TRUE);
if (tokenbuf[1]) {
expect = XOPERATOR;
- --- 1649,1653 ----
case '%':
if (expect != XOPERATOR) {
! s = scan_ident(s, bufend, tokenbuf + 1, sizeof tokenbuf - 1,
TRUE);
if (tokenbuf[1]) {
expect = XOPERATOR;
*************** yylex()
*** 1748,1752 ****
s++;
if (s < bufend && isALPHA(*s)) {
! d = scan_word(s, tokenbuf, FALSE, &len);
while (d < bufend && (*d == ' ' || *d == '\t'))
d++;
- --- 1752,1756 ----
s++;
if (s < bufend && isALPHA(*s)) {
! d = scan_word(s, tokenbuf, sizeof tokenbuf, FALSE, &len);
while (d < bufend && (*d == ' ' || *d == '\t'))
d++;
*************** yylex()
*** 1847,1851 ****
}
! s = scan_ident(s-1, bufend, tokenbuf, TRUE);
if (*tokenbuf) {
expect = XOPERATOR;
- --- 1851,1855 ----
}
```

```
! s = scan_ident(s - 1, bufend, tokenbuf, sizeof tokenbuf, TRUE);
if (*tokenbuf) {
expect = XOPERATOR;
*************** yylex()
*** 1956,1960 ****
case '$':
if (s[1] == '#' && (isALPHA(s[2]) || strchr("_{$:", s[2]))) {
! s = scan_ident(s+1, bufend, tokenbuf+1, FALSE);
if (expect == XOPERATOR) {
if (lex_formbrack && lex_brackets == lex_formbrack) {
- --- 1960,1965 ----
case '$':
if (s[1] == '#' && (isALPHA(s[2]) || strchr("_{$:", s[2]))) {
! s = scan_ident(s + 1, bufend, tokenbuf + 1, sizeof tokenbuf - 1,
! FALSE);
if (expect == XOPERATOR) {
if (lex_formbrack && lex_brackets == lex_formbrack) {
*************** yylex()
*** 1982,1986 ****
TOKEN(DOLSHARP);
}
! s = scan_ident(s, bufend, tokenbuf+1, FALSE);
if (expect == XOPERATOR) {
if (lex_formbrack && lex_brackets == lex_formbrack) {
- --- 1987,1991 ----
TOKEN(DOLSHARP);
}
! s = scan_ident(s, bufend, tokenbuf + 1, sizeof tokenbuf - 1,
FALSE);
if (expect == XOPERATOR) {
if (lex_formbrack && lex_brackets == lex_formbrack) {
*************** yylex()
*** 2016,2024 ****
if (*s == '{' && strEQ(tokenbuf, "$SIG") &&
(t = strchr(s,'}')) && (t = strchr(t,'='))) {
! char tmpbuf[1024];
STRLEN len;
for (t++; isSPACE(*t); t++) ;
if (isIDFIRST(*t)) {
! t = scan_word(t, tmpbuf, TRUE, &len);
if (*t != '(' && perl_get_cv(tmpbuf, FALSE))
warn("You need to quote \"%s\"", tmpbuf);
- --- 2021,2029 ----
```

```
if (*s == '{' && strEQ(tokenbuf, "$SIG") &&
(t = strchr(s,'}')) && (t = strchr(t,'='))) {
! char tmpbuf[sizeof tokenbuf];
STRLEN len;
for (t++; isSPACE(*t); t++) ;
if (isIDFIRST(*t)) {
! t = scan_word(t, tmpbuf, sizeof tmpbuf, TRUE, &len);
if (*t != '(' && perl_get_cv(tmpbuf, FALSE))
warn("You need to quote \"%s\"", tmpbuf);
*************** yylex()
*** 2093,2097 ****
case '@':
! s = scan_ident(s, bufend, tokenbuf+1, FALSE);
if (expect == XOPERATOR)
no_op("Array",s);
- --- 2098,2102 ----
case '@':
! s = scan_ident(s, bufend, tokenbuf + 1, sizeof tokenbuf - 1,
FALSE);
if (expect == XOPERATOR)
no_op("Array",s);
*************** yylex()
*** 2129,2133 ****
: !GvHV(gv) )))
{
! char tmpbuf[1024];
sprintf(tmpbuf, "Literal @%s now requires backslash",tokenbuf+1);
yyerror(tmpbuf);
- --- 2134,2138 ----
: !GvHV(gv) )))
{
! char tmpbuf[sizeof tokenbuf + 40];
sprintf(tmpbuf, "Literal @%s now requires backslash",tokenbuf+1);
yyerror(tmpbuf);
*************** yylex()
*** 2293,2297 ****
keylookup:
bufptr = s;
! s = scan_word(s, tokenbuf, FALSE, &len);
if (*s == ':' && s[1] == ':' && strNE(tokenbuf, "CORE"))
- --- 2298,2302 ----
keylookup:
bufptr = s;
```

```
! s = scan_word(s, tokenbuf, sizeof tokenbuf, FALSE, &len);
if (*s == ':' && s[1] == ':' && strNE(tokenbuf, "CORE"))
*************** yylex()
*** 2338,2342 ****
if (*s == '\'' || *s == ':' && s[1] == ':') {
! s = scan_word(s, tokenbuf + len, TRUE, &len);
if (!len)
croak("Bad name after %s::", tokenbuf);
- --- 2343,2348 ----
if (*s == '\'' || *s == ':' && s[1] == ':') {
! s = scan_word(s, tokenbuf + len, sizeof tokenbuf - len,
! TRUE, &len);
if (!len)
croak("Bad name after %s::", tokenbuf);
*************** yylex()
*** 2557,2561 ****
s += 2;
d = s;
! s = scan_word(s, tokenbuf, FALSE, &len);
tmp = keyword(tokenbuf, len);
if (tmp < 0)
- --- 2563,2567 ----
s += 2;
d = s;
! s = scan_word(s, tokenbuf, sizeof tokenbuf, FALSE, &len);
tmp = keyword(tokenbuf, len);
if (tmp < 0)
*************** yylex()
*** 3244,3250 ****
if (isIDFIRST(*s) || *s == '\'' || *s == ':') {
! char tmpbuf[128];
expect = XBLOCK;
! d = scan_word(s, tmpbuf, TRUE, &len);
if (strchr(tmpbuf, ':'))
sv_setpv(subname, tmpbuf);
- --- 3250,3256 ----
if (isIDFIRST(*s) || *s == '\'' || *s == ':') {
! char tmpbuf[sizeof tokenbuf];
expect = XBLOCK;
! d = scan_word(s, tmpbuf, sizeof tmpbuf, TRUE, &len);
if (strchr(tmpbuf, ':'))
sv_setpv(subname, tmpbuf);
*************** char *what;
```

```
*** 4091,4102 ****
static char *
! scan_word(s, dest, allow_package, slp)
register char *s;
char *dest;
int allow_package;
STRLEN *slp;
{
register char *d = dest;
for (;;) {
if (isALNUM(*s))
*d++ = *s++;
- --- 4097,4112 ----
static char *
! scan_word(s, dest, destlen, allow_package, slp)
register char *s;
char *dest;
+ STRLEN destlen;
int allow_package;
STRLEN *slp;
{
register char *d = dest;
+ register char *e = d + destlen - 3; /* two-character token, ending
NUL */
for (;;) {
+ if (d >= e)
+ croak(too_long);
if (isALNUM(*s))
*d++ = *s++;
*************** STRLEN *slp;
*** 4119,4129 ****
static char *
! scan_ident(s,send,dest,ck_uni)
register char *s;
register char *send;
char *dest;
I32 ck_uni;
{
register char *d;
char *bracket = 0;
char funny = *s++;
- --- 4129,4141 ----
static char *
```

```
! scan_ident(s, send, dest, destlen, ck_uni)
register char *s;
register char *send;
char *dest;
+ STRLEN destlen;
I32 ck_uni;
{
register char *d;
+ register char *e;
char *bracket = 0;
char funny = *s++;
*************** I32 ck_uni;
*** 4134,4143 ****
s = skipspace(s);
d = dest;
if (isDIGIT(*s)) {
! while (isDIGIT(*s))
*d++ = *s++;
}
else {
for (;;) {
if (isALNUM(*s))
*d++ = *s++;
- --- 4146,4161 ----
s = skipspace(s);
d = dest;
+ e = d + destlen - 3; /* two-character token, ending NUL */
if (isDIGIT(*s)) {
! while (isDIGIT(*s)) {
! if (d >= e)
! croak(too_long);
*d++ = *s++;
+ }
}
else {
for (;;) {
+ if (d >= e)
+ croak(too_long);
if (isALNUM(*s))
*d++ = *s++;
```

End of patch.

The CERT Coordination Center staff thanks Chip Salzenberg for supplying a fix, Larry Wall for tweaking the fix, and Warner Losh for his work on patches.

Revision History

```
Dec. 5, 1997  Added vendor information for NCR Corporation.

Sep. 30, 1997 Updated copyright statement

June 9, 1997  Appendix A - added information from Sun Microsys-
tems,Inc.
```

18 CA-1997-18: Vulnerability in the at(1) program

Original issue date: June 12, 1997
Last revised: January 5, 1998
Updated vendor information for Silicon Graphics, Inc.

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

The CERT Coordination Center has received reports of a buffer overflow condition in some versions of the *at(1)* program. By carefully specifying the data that overflows this buffer, any user can execute arbitrary commands as root.

The CERT/CC team recommends installing a vendor patch if one is available (see Section III.A). Until you can do so, we recommend disabling *at(1)* (see Section III.B).

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

I. Description

The *at(1)* program can be used by local users to schedule commands to be executed at a later time. When those commands are run, they are run as the user who originally ran *at(1)*. That user will be referred to as the scheduling user.

As a precaution, the scheduling user's list of commands is stored in a file in a directory that is not writable by other users. The file's ownership is changed to that of the scheduling user, and that information is used to define the identity of the process that runs the commands when the appointed time arrives. These measures are intended to prevent other users from changing the scheduling user's list of commands or creating new lists to be executed as another user. To achieve this additional level of security, the *at(1)* program runs as set-user-id root.

Some versions of *at(1)* contain a programming defect that can result in a buffer local to *at(1)* being overflowed. Through the careful specification of the data that overflows this buffer, arbitrary commands can be executed with the identity of *at(1)* process, root in this case.

II. Impact

Any user with an account on a system that contains a defective version of *at(1)* can execute programs as root.

III. Solution

A. Install a patch from your vendor

Below is a list of vendors who have provided information about at. Details are in Appendix A of this advisory; we will update the appendix as we receive more information. If your vendor's name is not on this list, the CERT/CC did not hear from that vendor. Please contact your vendor directly.

Berkeley Software Design, Inc. (BSDI)
Cray Research - A Silicon Graphics Company
Data General Corporation
Digital Equipment Corporation
Hewlett-Packard Company
IBM Corporation
NCR Corporation
Santa Cruz Operation, Inc. (SCO)
Silicon Graphics, Inc.
Sun Microsystems, Inc.

B. Until you are able to install the appropriate patch, we recommend the following workaround:

Turn off *at(1)* by setting its mode to 0. Do the following as root:

chmod 0 /usr/bin/at

Note that the location of *at(1)* varies from system to system. Consult your system's documentation for the correct location.

After you turn off the *at(1)* command, users will not be able to use it. As an alternative to *at(1)*, consider using the *crontab(1)* command if your system provides it.

Appendix A. Vendor Information

Below is a list of the vendors who have provided information for this advisory. We will update this appendix as we receive additional information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact the vendor directly.

Berkeley Software Design, Inc. (BSDI)

No versions of BSD/OS are susceptible to this problem.

Cray Research - A Silicon Graphics Company

Neither Unicos nor Unicos/mk is believed to be vulnerable.

Data General Corporation

No versions of DG/UX are vulnerable to this problem.

Digital Equipment Corporation

Information about this reported problem, and subsequent attempts to reproduce the problem have been unsuccessful for Digital's ULTRIX or Digital UNIX Operating Systems Software. Should further information or testing indicate this problem can be reproduced on Digital's products, a solution will be provided accordingly. At that time Digital will provide notice of the completion/availability of the patches through AES services (DIA, DSNlink FLASH) and be available from your normal Digital Support channel.

DIGITAL EQUIPMENT CORPORATION 6 / 09 / 97

Hewlett-Packard Company

Hewlett Packard has published information relating to this problem in Security Bulletin #00023. It is available from the HP Electronic Support Center. The center's Web page is at http://us-support.external.hp.com (for US, Canada, Asia-Pacific, and Latin-America) or http://europe-support.external.hp.com (for Europe).

IBM Corporation

See the appropriate release below to determine your action.

AIX 3.2

Apply the following fixes to your system:

PTF - U443452 U443486 U444191 U444206 U444213 U444243
APAR - IX60796

To determine if you have these PTFs on your system, run the following commands:

lslpp -lB U443452 U443486 U444191 U444206 U444213 U444243

AIX 4.1

Apply the following fixes to your system:

APAR - IX60894
APAR - IX60890

To determine if you have this APAR on your system, run the following commands:

instfix -ik IX60894
instfix -ik IX60890

Or run the following commands:

lslpp -h bos.rte.cron
lslpp -h bos.rte.libc

Your version of bos.rte.cron should be 4.1.4.8 or later.
Your version of bos.rte.libc should be 4.1.4.18 or later.

AIX 4.2

Apply the following fixes to your system:

APAR - IX60892
APAR - IX61125

To determine if you have this APAR on your system, run the following commands:

instfix -ik IX60892
instfix -ik IX61125

Or run the following commands:

lslpp -h bos.rte.cron
lslpp -h bos.rte.libc

Your version of bos.rte.cron should be 4.2.0.1 or later.
Your version of bos.rte.libc should be 4.2.0.5 or later.

To Order

APARs may be ordered using Electronic Fix Distribution (via FixDist) or from the IBM Support Center. For more information on FixDist, reference URL:
http://service.software.ibm.com/aixsupport/.

or send e-mail to aixserv@austin.ibm.com with a subject of "FixDist".

IBM and AIX are registered trademarks of International Business Machines Corporation.

NCR Corporation

The at binary that ships with some NCR MP-RAS SVR4 releases contains a vulnerability that could allow a user to execute random commands as root.

NCR is delivering a set of operating system dependent patches which contain a new version of the at command. Accompanying each patch is a README file which discusses the general purpose of the patch and describes how to apply it to your system.

Recommended solution:

Apply one of the following patches based on your operating system revision:

```
MP-RAS 3.00.x                  - PBASEI300 (Version after 8/18-97)

MP-RAS 3.01.x                  - PBASEE300 (Version after 8/26-97)

MP-RAS 3.02.x and later        - Not vulnerable
```

The patches described above provide a new version of the at executable, which fixes the vulnerability.

Santa Cruz Operation, Inc. (SCO)

All SCO operating systems are vulnerable. SCO has made an interim fix available for anonymous ftp:

ftp://ftp.sco.com/SSE/sse007.ltr.Z - cover letter
ftp://ftp.sco.com/SSE/sse007.tar.Z - replacement binaries

The fix includes binaries for the following SCO operating systems:

- SCO CMW+ 3.0
- SCO Open Desktop/Open Server 3.0, SCO UNIX 3.2v4
- SCO OpenServer 5.0
- SCO UnixWare 2.1

Silicon Graphics, Inc.

Silicon Graphics Inc. has investigated the issue and recommends the following steps for neutralizing the exposure. It is HIGHLY RECOMMENDED that these measures be implemented on ALL SGI systems. This issue will be corrected in future releases of IRIX.

For further information, please refer to Silicon Graphics Inc. Security Advisory Number: 19971102-01-PX, "Vulnerability in at(1) program."

The SGI anonymous FTP site is sgigate.sgi.com (204.94.209.1) or its mirror, ftp.sgi.com. Security information and patches can be found in the ~ftp/security and ~ftp/patches directories, respectfully.

Sun Microsystems, Inc.

```
Bulletin Number:        #00160

Date:                   December 3, 1997
```

Sun security bulletins are available via World Wide Web at:
http://sunsolve.sun.com/sunsolve/secbulletins.

The following patches are available in relation to the at problem.

OS version	Patch ID
SunOS 5.5.1	103690-05
SunOS 5.5.1_x86	103691-05
SunOS 5.5	103723-05
SunOS 5.5_x86	103724-05
SunOS 5.4	102693-05
SunOS 5.4_x86	102694-05
SunOS 5.3	101572-08

Technical information for this advisory was drawn in part from a posting by Don Farmer to the bugtraq mailing list.

Thanks to Wolfgang Ley of DFN-CERT for his help in developing this advisory.

Revision History

Jan. 5, 1998 Updated vendor information for Silicon Graphics, Inc.

Dec. 5, 1997 Updated vendor information for NCR Corporation and Sun Microsystems, Inc.

Sep. 30, 1997 Updated copyright statement

Aug. 28, 1997 Section III and Appendix A - added vendor information for NCR Corporation.

Aug. 16, 1997 Appendix A - added Data General information.

July 14, 1997 Appendix A - updated Hewlett-Packard information.

June 25, 1997 Section IIIA and Appendix A - Added vendor information for Berkeley Software Design, Inc. (BSDI).

June 12, 1997 Section IIIA and Appendix A - Added vendor information for Digital Equipment Corporation.

19 CA-1997-19: lpr Buffer Overrun Vulnerability

Original issue date: June 25, 1997
Last revised: April 7, 1998
Added vendor information for Silicon Graphics Inc.

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

The technical content of this advisory was originally published by AUSCERT (AA-96.12), who last updated the information on June 19, 1997. We use it here with their permission.

There is a vulnerability in the BSD-based printing software, lpr, available on a variety of Unix platforms. This vulnerability may allow local users to gain root privileges.

Exploit information involving this vulnerability has been publicly available for some time. Recently, the CERT/CC has received reports that the vulnerability is being actively exploited.

We recommend installing a vendor patch if one is available. Until you can do so, we recommend using the wrapper described in Section III.B.

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

I. Description

A vulnerability exists in the BSD-based lpr printing package found on many Unix systems.

Due to insufficient bounds checking on arguments that are supplied by users, it is possible to overwrite the internal stack space of the lpr program while it is executing. This can allow an intruder to cause lpr to execute arbitrary commands by supplying a carefully designed argument to lpr. These commands will be run with the privileges of the lpr program. When lpr is installed setuid or setgid, it may allow intruders to gain those privileges.

When lpr is setuid root, it may allow intruders to run arbitrary commands with root privileges.

For information from vendors relating to this vulnerability, please check Appendix A of this advisory. In addition to the products mentioned, be aware that platforms using the BSD-based lpr systems, in which lpr is installed setuid or setgid, may also be vulnerable.

Note also that the vulnerability described in this advisory is not present in the LPRng printing package.

II. Impact

Local users may gain root privileges. It is necessary to have access to an account on the system to exploit this vulnerability.

III. Solution

The lpr printing package is available on many different systems. As vendor patches are made available sites are encouraged to install them. Until vendor patches are available, we recommend applying the workaround referred to in III.B.

A. Install vendor patches

Specific vendor information has been placed in Appendix A. If the BSD- based lpr printing software is used and your vendor is not listed in Appendix A, please contact your vendor directly.

B. Install lpr wrapper

Until you can install a vendor patch, we encourage you install a wrapper developed by AUSCERT to help prevent lpr being exploited using this vulnerability.

The source for the wrapper, including installation instructions, can be found at ftp://ftp.auscert.org.au/pub/auscert/tools/overflow_wrapper/overflow_wrapper.c.

This wrapper replaces the lpr program and checks the length of the command line arguments which are passed to it. If an argument exceeds a certain predefined value (MAXARGLEN), the wrapper exits without executing the lpr command. The wrapper program can also be configured to syslog any failed attempts to execute lpr with arguments exceeding MAXARGLEN. For further instructions on using this wrapper, please read the comments at the top of overflow_wrapper.c.

When compiling overflow_wrapper.c for use with lpr, AUSCERT recommends defining MAXARGLEN to be 32.

The MD5 checksum for the current version of overflow_wrapper.c can be retrieved from ftp://ftp.auscert.org.au/pub/auscert/tools/overflow_wrapper/CHECKSUM.

The CHECKSUM file has been digitally signed using the AUSCERT PGP key.

Appendix A Vendor information

Below is a list of the vendors who have provided information. We will update this appendix as we receive additional information. If you do not see your vendor's name, please contact the vendor directly.

Berkeley Software Design, Inc. (BSDI)

BSD/OS 3.0 is not vulnerable to the problem.

BSDI have issued a patch which addresses this vulnerability under BSD/OS 2.1. This patch is available from:
ftp://ftp.bsdi.com/pub/bsdi/patches/patches-2.1/U210-028.

Digital Equipment Corporation

Digital Equipment Corporation
Software Security Response Team

This reported problem is not present for Digital's ULTRIX or Digital UNIX Operating Systems Software.

- DIGITAL EQUIPMENT CORPORATION 06/19/97

FreeBSD

This problem was fixed prior to the release of FreeBSD 2.1.6 and 2.2. Users running older versions of the OS should review the security advisory describing this vulnerability (SA-96.18) at: ftp://freebsd.org/pub/CERT/advisories/FreeBSD-SA-96:18.lpr.asc.

Patches can be found in the directory: ftp://freebsd.org/pub/CERT/patches/SA-96:18.

IBM Corporation

AIX is not vulnerable to the lpr buffer overflow. The version of lpr shipped with AIX is not installed with the setuid bit turned on.

IBM and AIX are registered trademarks of International Business Machines Corporation.

Linux

The Linux Emergency Response Team have released a Linux Security FAQ Update which addresses this vulnerability. This Update contains information regarding various Linux distributions. It is available from:
ftp://bach.cis.temple.edu/pub/Linux/Security/FAQ/updates/Update-11-25-1996.vulnerability-lpr-.0.06-v1.2

NCR Corporation

The lpr command is not installed as a set-uid command on NCR MP-RAS Unix SVR4 systems, which means MP-RAS is not vulnerable.

NEXT

The NEXT group has addressed the vulnerability described in this advisory in release 4.2 of OpenStep/Mach.

The Santa Cruz Operation, Inc. (SCO)

SCO has determined that the following SCO operating systems are not vulnerable:

- SCO CMW+ 3.0
- SCO Open Desktop/Open Server 3.0, SCO UNIX 3.2v4

- SCO OpenServer 5.0
- SCO UnixWare 2.1

Silicon Graphics Inc.

For patch information, see Silicon Graphics Inc. Security Advisory, Number 19980402-01-PX, "lp(1) Security Vulnerabilities," available from: ftp://sgigate.sgi.com/security/19980402-01-PX.

Sun Microsystems, Inc.

All versions of Solaris are not affected. SunOS 4.1.3_U1 and SunOS 4.1.4 are vulnerable. Sun recommends that sites using SunOS 4.1.3_U1 and SunOS 4.1.4 apply the workaround provided in this advisory.

The CERT Coordination Center staff thanks AUSCERT for permission to republish the information in their advisory AA-96.12. AUSCERT originally thanked Alexander O. Yuriev, the FreeBSD security team, IBM, and the CERT/CC for their assistance in the production of their advisory.

Revision History

```
Apr.  7, 1998   Added vendor information for Silicon Graphics Inc.

Dec.  5, 1997   Added vendor information for NCR Corporation.

Sep. 30, 1997  Updated copyright statement
```

20 CA-1997-20: JavaScript Vulnerability

Original issue date: July 8, 1997
Last revised: November 9, 1999
Updated broken links.

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

The CERT Coordination Center has received reports of a vulnerability in JavaScript that enables remote attackers to monitor a user's Web activities. The vulnerability affects several Web browsers that support JavaScript.

The vulnerability can be exploited even if the browser is behind a firewall and even when users browse "secure" HTTPS-based documents.

The CERT/CC team recommends installing a patch from your vendor or upgrading to a version that is not vulnerable to this problem (see Section III. A). Until you can do so, we recommend disabling JavaScript (see Section III.B).

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

I. Description

Several web browsers support the ability to download JavaScript programs with an HTML page and execute them within the browser. These programs are typically used to interact with the browser user and transmit information between the browser and the Web server that provided the page.

JavaScript programs are executed within the security context of the page with which they were downloaded, and they have restricted access to other resources within the browser. Security flaws exist in certain Web browsers that permit JavaScript programs to monitor a user's browser activities beyond the security context of the page with which the program was downloaded. It may not be obvious to the browser user that such a program is running, and it may be difficult or impossible for the browser user to determine if the program is transmitting information back to its web server.

The vulnerability can be exploited even if the Web browser is behind a firewall (if JavaScript is permitted through the firewall) and even when users browse "secure" HTTPS-based documents.

II. Impact

This vulnerabilit permits remote attackers to monitor a user's browser activity, including:

- observing the URLs of visited documents,
- observing data filled into HTML forms (including passwords), and

- observing the values of cookies.

III. Solution

The best solution is to obtain a patch from your vendor or upgrade to a version that is not vulnerable to this problem. If a patch or upgrade is not available, or you cannot install it right away, we recommend disabling JavaScript until the fix is installed.

A. Obtain and install a patch for this problem.

See Appendix A for the current information from vendors. We will update the appendix when we receive further information.

B. Disable JavaScript.

Until you are able to install the appropriate patch, we recommend disabling JavaScript in your browser. Note that JavaScript and Java are two different languages, and this particular problem is only with JavaScript. Enabling or disabling Java rather than JavaScript will have no effect on this problem.

The way to disable JavaScript is specific to each browser. The option, if available at all, is typically found as one of the Options or Preferences settings.

Appendix A Vendor Information

Below is information we have received from vendors. We will update this appendix as we receive additional information.

Hewlett-Packard

For more information please refer to the Hewlett-Packard Security Advisory "Security Advisory in Netscape shipped with HP-UX", Document ID: HPSBUX9707-065.

Use your browser to get to the HP Electronic Support Center page:
http://us-support.external.hp.com (for US, Canada, Asia-Pacific, & Latin-America) or
http://europe-support.external.hp.com (for Europe).

Click on the Technical Knowledge Database, register as a user (remember to save the User ID assigned to you, and your password), and it will connect to a HP Search Technical Knowledge DB page. Near the bottom is a hyperlink to our Security Bulletin archive. Once in the archive there is another link to our current security patch matrix. Updated daily, this matrix is categorized by platform/OS release, and by bulletin topic.

IBM Corporation

Netscape for IBM's OS/2 Operating System is vulnerable. The vulnerable version and the patched version are both 2.02.

To tell if you need to download and reinstall, open the Netscape folder on the OS/2 desktop. Click on the icon marked "Installation Utility." When the "Installation and Maintenance" program starts, make sure "02.02.00 Netscape for OS/2" is highlighted and hit control-S. On the product status panel that opens up, highlight "Netscape Navigator" and then press the "Service Level" button next to it. Ignore the install date -- that's the date Navigator was installed. If "Level" is not "000004" or later, you should download Netscape Navigator for OS/2 from the above mentioned URL and install it.

Microsoft

Microsoft Internet Explorer 3.* and 4.* are vulnerable. Microsoft has announced their patch plans for this problem at: http://www.microsoft.com/ie/security/default.asp.

Netscape

Netscape Navigator/Communicator versions 2.*, 3.* and 4.* are vulnerable. See: http://www.netscape.com/security/index.html for details.

The CERT Coordination Center thanks Vinod Anupam of Bell Labs, Lucent Technologies, for identifying and analyzing this problem, and vendors for their support in responding to this problem.

Revision History

```
Sept. 30, 1997 Updated copyright statement

Sept. 17, 1997 Appendix A - updated Netscape's URLs

               Updated our copyright statement

July 28, 1997  Appendix A - added information for Hewlett-Packard
and IBM.

               Section III.A - slight wording change.

July 14, 1997  Section III.B - fixed a typographical error.

July 11, 1997  Updated Appendix A with vendor information

               for vulnerable browers.

November 9, 1999   Updated broken links.
```

21 CA-1997-21: SGI Buffer Overflow Vulnerabilities

Original issue date: July 16, 1997
Last revised: January 15, 1998
Updated vendor information for SGI.

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

The technical content of this advisory was originally published by AUSCERT (AA-97.19, AA-97.20, AA-97.21, AA-97.22, AA-97.23, AA-97.24). We use it here with their permission.

Some SGI IRIX systems have buffer overflow vulnerabilities in the following programs:

df
pset
eject
login/scheme
ordist
xlock

These vulnerabilities may allow local users to gain root privileges. Exploit information involving these vulnerabilities has been made publicly available.

A more detailed discussion of each problem appears in Section I.

All these buffer overflow problems can be addressed by similar workarounds or by installing a wrapper developed by AUSCERT (see Section III).

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

I. Description

Due to insufficient bounds checking on arguments that are supplied by users, it is possible to overwrite the internal stack space of the programs listed above while they are executing. By supplying a carefully designed argument to one of these programs, intruders may be able to force the program to execute arbitrary commands. As the programs (except pset) are setuid root, this may allow intruders to run arbitrary commands with root privileges. As pset is setgid sys, this may allow intruders to run arbitrary commands with the privileges of group sys. This may then be leveraged to gain root privileges.

A. df

df(1) is a program used to display statistics about the amount of used and free disc space on file systems.

You can determine if this program is installed by typing

% ls -l /sbin/df

df is installed by default in /sbin. We encourage you to check for the presence of this program regardless of the version of IRIX installed.

B. pset

pset(1M) is a program used to display and modify information concerning the use of processor sets in the current system. The pset command is used on multi-processor systems to restrict the execution of different classes of jobs.

You can determine if this program is installed by typing

% ls -l /sbin/pset

pset is installed by default in /sbin. We encourage you to check for the presence of this program regardless of the version of IRIX installed.

C. eject

eject(1) is a program used to eject a removable media device, such as floppy, CDROM, or tape. If the floppy or CDROM is mounted, eject will first try to unmount it.

You can determine if this program is installed by typing

% ls -l /usr/sbin/eject

eject is installed by default in /usr/sbin. We encourage you to check for the presence of this program regardless of the version of IRIX installed.

D. login/scheme

login(1) is a program used at the beginning of each terminal session that allows users to identify themselves to the session. Under current versions of IRIX, this functionality is supplied by the program /usr/lib/iaf/scheme. The login program is a symbolic link to /usr/lib/iaf/scheme.

The login program is installed in /usr/bin/login. Under default configurations, this is a symbolic link to /usr/lib/iaf/scheme.

% ls -l /usr/bin/login

lrwxr-xr-x 1 root sys 17 Nov 22 1994 /usr/bin/login -> ../lib/iaf/scheme

% ls -l /usr/lib/iaf/scheme

-rwsr-xr-x 1 root sys 65832 Nov 22 1994 /usr/lib/iaf/scheme

Although this vulnerability has been verified only under IRIX 6.2, it is believed to affect other versions of IRIX, including IRIX 5.x.

E. ordist

ordist(1c) is a program used to maintain identical copies of files over multiple hosts. It preserves the owner, group, mode and mtime of a file if possible.

You can determine if this program is installed by typing

% ls -l /usr/bsd/ordist

ordist is installed by default in /usr/bsd. We encourage you to check for the presence of this program regardless of the version of IRIX installed.

F. xlock

xlock(1) is a program that locks the local X display until a password is entered.

You can determine if this program is installed by typing

% ls -l /usr/bin/X11/xlock

xlock is installed by default in /usr/bin/X11. We encourage you to check for the presence of this program regardless of the version of IRIX installed.

For more information about vulnerabilities in xlock, see
www.cert.org/advisories/CA-97.13.xlock.

II. Impact

A. df

Local users may gain root privileges.

B. pset

Local users may gain the privileges of group sys. These privileges may then be used to gain root privileges.

C. eject

Local users may gain root privileges.

D. login/scheme

Local users may gain root privileges.

E. ordist

Local users may gain root privileges.

F. xlock

Local users may gain root privileges.

III. Solution

There are several possible solutions for these problems. In Section A, we recommend installing vendor patches. In Section B, we discuss workarounds you can use until you install vendor patches. If the workaround is inappropriate for your site, an alternative is to install a wrapper program developed by AUSCERT. Information about the wrapper is in Section C.

A. Vendor patches

Currently there are no vendor patches available that address these vulnerabilities. The CERT/CC recommends installing official vendor patches when they are available.

B. Workaround

You should prevent the exploitation of this vulnerability by immediately applying the workaround, which is to remove the setuid and non-root execute permissions of the df, eject, login/scheme, ordist, and xlock programs and to remove the setgid and non-root execute permissions of pset.

If the functionality provided by these programs is required by non-root users, apply the wrapper discussed in Section C.

1. df

To prevent the exploitation of the vulnerability described in this advisory, you should remove setuid permissions from the df program immediately. As df will no longer work for non-root users, we recommend removing the execute permissions for them also.

```
# ls -l /sbin/df

-r-sr-xr-x 1 root sys 23136 Nov 22 1994 /sbin/df

# chmod 500 /sbin/df

# ls -l /sbin/df

-r-x------ 1 root sys 23136 Nov 22 1994 /sbin/df
```

2. pset

To prevent the exploitation of this vulnerability, we recommend that you remove the setgid permissions from the pset program immediately. As pset will no longer work for non-root users, we recommend removing the execute permissions for them also.

```
# ls -l /sbin/pset

-rwsr-sr-x 1 root sys 31704 Nov 22 1994 /sbin/pset

# chmod 500 /sbin/pset
```

ls -l /sbin/pset

-r-x------ 1 root sys 31704 Nov 22 1994 /sbin/pset

3. eject

To prevent the exploitation of the vulnerability described in this advisory, you should remove the setuid permissions from the eject program immediately. As eject will no longer have its full functionality for non-root users, we also recommend removing the execute permissions for these users.

ls -l /usr/sbin/eject

-rwsr-xr-x 1 root sys 45892 Nov 28 15:09 /usr/sbin/eject

chmod 500 /usr/sbin/eject

ls -l /usr/sbin/eject

-r-x------ 1 root sys 45892 Nov 28 15:09 /usr/sbin/eject

4. login/scheme

To prevent the exploitation of the vulnerability described in this advisory, remove the setuid permissions from the scheme program immediately.

ls -l /usr/lib/iaf/scheme

-rwsr-xr-x 1 root sys 58324 Nov 28 1996 /usr/lib/iaf/scheme

chmod 500 /usr/lib/iaf/scheme

ls -l /usr/lib/iaf/scheme

-r-x------ 1 root sys 58324 Nov 28 1996 /usr/lib/iaf/scheme

5. ordist

To prevent the exploitation of the vulnerability described in this advisory, you should remove the setuid permissions from the ordist program immediately. As ordist will no longer work for non-root users, we recommend removing the execute permissions for them also.

ls -l /usr/bsd/ordist

-rwsr-xr-x 1 root sys 70564 Nov 28 15:07 /usr/bsd/ordist

chmod 500 /usr/bsd/ordist

ls -l /usr/bsd/ordist

-r-x------ 1 root sys 70564 Nov 28 15:07 /usr/bsd/ordist

6. xlock

To prevent the exploitation of the vulnerability described in this advisory, you should remove the setuid permissions be from the xlock program immediately. As xlock will no longer work for non-root users, we recommend removing the execute permissions for them also.

ls -l /usr/bin/X11/xlock

-rwsr-xr-x 1 root sys 95188 Nov 28 1996 /usr/bin/X11/xlock

chmod 500 /usr/bin/X11/xlock

ls -l /usr/bin/X11/xlock

-r-x------ 1 root sys 95188 Nov 28 1996 /usr/bin/X11/xlock

C. Workaround

AUSCERT has developed a wrapper to help prevent programs from being exploited using the vulnerabilities described in this advisory. Sites that have a C compiler can obtain the source, and compile and install the wrapper as described in Section 1, below. For sites without a C compiler, AUSCERT has made pre-compiled binaries available as described in Section 2.

1. Installing the wrapper from source

The source for the wrapper, including installation instructions, can be found at ftp://ftp.auscert.org.au/pub/auscert/tools/overflow_wrapper/overflow_wrapper.c.

This wrapper replaces the vulnerable programs and checks the length of the command line arguments which are passed to it. If an argument exceeds a certain predefined value (MAXARGLEN), the wrapper exits without executing the command. The wrapper program can also be configured to syslog any failed attempts to execute the command with arguments exceeding MAXARGLEN. For further instructions on using this wrapper, please read the comments at the top of overflow_wrapper.c.

When compiling overflow_wrapper.c, AUSCERT recommends defining MAXARGLEN to be 32.

The MD5 checksum for the current version of overflow_wrapper.c can be retrieved from ftp://ftp.auscert.org.au/pub/auscert/tools/overflow_wrapper/CHECKSUM.

The CHECKSUM file has been digitally signed using the AUSCERT PGP key.

2. Installing the wrapper binaries

Pre-compiled wrapper binary is provided for sites that wish to install the wrapper but do not have a C compiler available. AUSCERT has compiled the wrapper on IRIX 5.3; however later versions of IRIX should be able to use the wrapper binary without recompilation.

The pre-compiled binaries for the wrapper program can be retrieved for each vulnerability. Sites are encouraged to carefully read the installation notes in the README file before installation.

a. df

The following compile time options have been used to create the binaries:

REAL_PROG="'/sbin/df.real"'
MAXARGLEN=32
SYSLOG

More information on these options can be found in the overflow_wrapper.c source code.

You can get the pre-compiled binaries for the wrapper program from
ftp://ftp.auscert.org.au/pub/auscert/tools/AA-97.19-df_wrapper.tar.Z.

MD5 (AA-97.19-df_wrapper.tar.Z) = 9d21e6358129cccbe3768757a5361f56

AA-97.19-df_wrapper.tar.Z contains a README file with installation instructions, as well as a pre-compiled binary.

b. pset

The following compile time options have been used to create the binaries:

REAL_PROG="'/sbin/pset.real"'
MAXARGLEN=32
SYSLOG

More information on these options can be found in the overflow_wrapper.c source code.

You can get pre-compiled binaries for the wrapper program from
ftp://ftp.auscert.org.au/pub/auscert/tools/AA-97.20-pset_wrapper.tar.Z.

MD5 (AA-97.20-pset_wrapper.tar.Z) = 875367aec70936fc5f4531b0ba8ebc03

AA-97.20-pset_wrapper.tar.Z contains a README file with installation instructions, as well as a pre-compiled binary.

c. eject

The following compile time options have been used to create the binaries:

REAL_PROG="'/usr/sbin/eject.real"'
MAXARGLEN=32
SYSLOG

More information on these options can be found in the overflow_wrapper.c source code.

The pre-compiled binaries for the wrapper program can be retrieved from
ftp://ftp.auscert.org.au/pub/auscert/tools/AA-97.21-eject_wrapper.tar.Z.

MD5 (AA-97.21-eject_wrapper.tar.Z) = 276bf0f51c89e54d4c584a9e8dd9265d

AA-97.21-eject_wrapper.tar.Z contains a README file with installation instructions, as well as a pre-compiled binary.

d. login/scheme

The following compile time options have been used to create the binaries:

REAL_PROG="'/usr/lib/iaf/scheme.real"'
MAXARGLEN=32
SYSLOG

More information on these options can be found in the overflow_wrapper.c source code.

The pre-compiled binaries for the wrapper program can be retrieved from ftp://ftp.auscert.org.au/pub/auscert/tools/AA-97.22-scheme_wrapper.tar.Z.

MD5 (AA-97.22-scheme_wrapper.tar.Z) = dc302aa275a4009d1545180bfce8ebf4

AA-97.22-scheme_wrapper.tar.Z contains a README file with installation instructions, as well as a pre-compiled binary.

e. ordist

The following compile time options have been used to create the binaries:

REAL_PROG="'/usr/bsd/ordist.real"'
MAXARGLEN=32
SYSLOG

More information on these options can be found in the overflow_wrapper.c source code.

The pre-compiled binaries for the wrapper program can be retrieved from ftp://ftp.auscert.org.au/pub/auscert/tools/AA-97.23-ordist_wrapper.tar.Z.

MD5 (AA-97.23-ordist_wrapper.tar.Z) = 0eed9d9a52658181a1ce9b4ce2ed7fd2

AA-97.23-ordist_wrapper.tar.Z contains a README file with installation instructions, as well as a pre-compiled binary.

f. xlock

The following compile time options have been used to create the binaries:

REAL_PROG="'/usr/bin/X11/xlock.real"'
MAXARGLEN=32
SYSLOG

More information on these options can be found in the overflow_wrapper.c source code.

The pre-compiled binaries for the wrapper program can be retrieved from ftp://ftp.auscert.org.au/pub/auscert/tools/AA-97.24-xlock_wrapper.tar.Z.

MD5 (AA-97.24-xlock_wrapper.tar.Z) = fe12913cd0f7bb78193488dd58cc2f4f

AA-97.24-xlock_wrapper.tar.Z contains a README file with installation instructions, as well as a pre-compiled binary.

The CERT Coordination Center staff thanks AUSCERT for permission to republish the information in six AUSCERT advisories:

AA-97.19.IRIX.df.buffer.overflow.vul
AA-97.20.IRIX.pset.buffer.overflow.vul
AA-97.21.IRIX.eject.buffer.overflow.vul
AA-97.22.IRIX.login.scheme.buffer.overflow.vul
AA-97.23-IRIX.ordist.buffer.overflow.vul
AA-97.24.IRIX.xlock.buffer.overflow.vul

AUSCERT originally thanked Ian Farquhar and the Prentice Center, University of Queensland for their assistance in the production of AA-97.22.

UPDATES

January 15, 1998

Silicon Graphics Inc. has issued Security Advisory, "IRIX df Buffer Overrun Vulnerability," 19970505-02-PX, November 18, 1997.

This SGI addresses the vulnerabilities discussed in the following documents:

AUSCERT Advisory AA-97.19 and CERT Advisory CA-97.21

September 19, 1997

Silicon Graphics Inc. has issued Security Advisory, "IRIX LOCKOUT and login/scheme Buffer Overrun" 19970508-02-PX, September 15, 1997.

This SGI advisory addresses the vulnerabilities discussed in the following documents:

AUSCERT AA-97.12 and CERT CA-97.
AUSCERT AA-97.22 and CERT CA-97.21

Patches for these vulnerabilities are available via anonymous FTP and your service/support provider.

The SGI anonymous FTP site is sgigate.sgi.com (204.94.209.1) or its mirror, ftp.sgi.com. Security information and patches can be found in the ~ftp/security and ~ftp/patches directories, respectfully.

For subscribing to the wiretap mailing list and other SGI security related information, please refer to the Silicon Graphics Security Headquarters website located at http://www.sgi.com/Support/Secur/security.html .

Revision History

```
Jan. 15, 1998  Updated vendor information for SGI.

Sept. 30, 1997 Updated copyright statemen

Sept. 19, 1997 Updates Section. Added updated vendor information
               for Silicon Graphics, Inc.

Aug. 11, 1997  Updates Section. Added updated vendor
               information for Silicon Graphics, Inc.

July 28, 1997  Section III.C.1 - Clarified information about wrap-
per.
```

22 CA-1997-22: BIND - the Berkeley Internet Name Daemon

Original issue date: August 13, 1997
Last revised: May 26, 1998
Updated vendor information for Sun Microsystems

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

***** This advisory supersedes CA-96.02. *****

Several vulnerabilities in the Berkeley Internet Name Daemon (BIND) have been fixed in the current version of BIND. One of those vulnerabilities is now being exploited, a vulnerability that results in cache poisoning (malicious or misleading data from a remote name server is saved [cached] by another name server).

The vulnerability has been fixed in BIND version 4.9.6; however, we recommend upgrading according to our instructions in Section III.B or installing vendor patches (see Appendix A). We also urge you to take the additional precautions described in Section III.C.

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

I. Description

The Berkeley Internet Name Daemon (BIND) is an implementation of the Domain Name Service (DNS) written primarily for UNIX Systems. BIND consists of three parts:

- The client part. This part contains subroutine libraries used by programs that require DNS services. Example clients of these libraries are telnet, the X Windows System, and ssh (the secure shell). The client part consists of subroutine libraries, header files, and manual pages.

- The server part. This part contains the name server daemon (named) and its support program (named-xfer). These programs provide one source of the data used for mapping between host names and IP addresses. When appropriately configured, these name server daemons can interoperate across a network (the Internet for example) to provide the mapping services for that network. The server part consists of the daemon, its support programs and scripts, and manual pages.

- The tools part. This part contains various tools for interrogating name servers in a network. They use the client part to extract information from those servers. The tools part consists of these interrogation tools and manual pages.

As BIND has matured, several vulnerabilities in the client, server, and tools parts have been fixed. Among these is server cache poisoning. Cache poisoning occurs when malicious or misleading data received from a remote name server is saved (cached) by another name server. This "bad" data is then made available to programs that request the cached data through the client interface.

Analysis of recent incidents reported to the CERT Coordination Center has shown that the cache poisoning technique is being used to adversely affect the mapping between host names and IP addresses. Once this mapping has been changed, any information sent between hosts on a network may be subjected to inspection, capture, or corruption.

Although, the new BIND distributions do address important security problems, not all known problems are fixed. IN particular, several problems can be fixed only with the use of cryptographic authentication techniques. Implementing and deploying this solution is non-trivial; work on this task is currently underway within the Internet community.

II. Impact

The mapping between host names and IP addresses may be changed. As a result, attackers can inspect, capture, or corrupt the information exchanged between hosts on a network.

III. Solution

Install a patch from your vendor or implement the "best practice" workaround we recommend in Section III.B. In either case, take the extra precautions described in Section III.C.

A. Obtain and install a patch for this problem.

Information from vendors can be found in Appendix A of this advisory; we will update the appendix as we receive more information.

B. Until you are able to install the appropriate patch, we recommend the following workaround.

The "best practice" for operating the publicly available BIND system can be either:

- a heterogeneous solution that involves first installing BIND release 4.9.6 and then release 8.1.1, or
- a homogeneous solution that involves installing only BIND release 8.1.1.

In the paragraphs below, we describe how to determine which solution you should use.

Note: Although the security posture in BIND version 8.1.1 is identical to that of version 4.9.6, version 8.1.1 is the version that will continue to undergo changes and improvements, hence our selection of its use as the "best practice."

1. Shared Object Client Subroutine Library

If your system and its programs rely on the shared object client subroutine library that comes with some releases of BIND, probably named libresolv.so, then you need the shared object subroutine library and other client software from release 4.9.6. (As of this writing, BIND version 8 does not yet support the client part as a shared object library.) This client software is available at ftp://ftp.isc.org/isc/bind/src/4.9.6/bind-4.9.6-REL.tar.gz.

MD5 (bind-4.9.6-REL.tar.gz) = 76dd66e920ad0638c8a37545a6531594

Follow the instructions in the file named INSTALL in the top-level directory.
After installing this client part, install the server and tool parts from release 8.1.1. This software is available at ftp://ftp.isc.org/isc/bind/src/8.1.1/bind-src.tar.gz.

MD5 (bind-src.tar.gz) = 7487b8d647edba2053edc1cda0c6afd0

Follow the instructions in the src/INSTALL file. Note that this version will install the client libraries and header files in a non-standard place, /usr/local/lib and /usr/local/include. The src/INSTALL file describes what is being installed and where.

When you install release 4.9.6 first, its client, server, and tools parts will be installed in the production locations. When you then install release 8.1.1, the server and tools parts will be overwritten by that release's versions, but the 4.9.6 client part will not.

2. No Shared Object Client Subroutine Library

If you do not need the shared object client subroutine library, then you need only upgrade to release 8.1.1. This software is available at ftp://ftp.isc.org/isc/bind/src/8.1.1/bind-src.tar.gz.

MD5 (bind-src.tar.gz) = 7487b8d647edba2053edc1cda0c6afd0

Follow the instructions in src/INSTALL. Note that the client subroutine library and header files are installed in /usr/local/lib and /usr/local/include respectively. To use these when building other systems, you will need to refer to their installed locations.

Note: ftp://ftp.isc.org/isc/bind/src/ is mirrored in Germany at
ftp://ftp.cert.dfn.de/pub/tools/net/bind/src/.

As new versions of BIND are released in the future, you will be able to find them at these sites, as well as other mirrors. You can also check ftp://info.cert.org/pub/latest_sw_versions/ for version information.

C. Take additional precautions.

As good security practice in general, filter at a router all name-based authentication services so that you do not rely on DNS information for authentication. This includes the services rlogin, rsh (rcp), xhost, NFS, and any other locally installed services that provide trust based on domain name information.

Appendix A Vendor Information

Below is a list of the vendors who have provided information for this advisory. We will update this appendix as we receive additional information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact the vendor directly.

Berkeley Software Design, Inc. (BSDI)

Patches from BSDI

ftp://ftp.bsdi.com/bsdi/patches/patches-2.1/U210-038
md5 checksum: 8ce46cd2d1aff3b294a84ae54e82a824

ftp://ftp.bsdi.com/bsdi/patches/patches-3.0/M300-025
md5 checksum: d7b5c6094089955cd1af207dab05bc0f

Cray Research - A Silicon Graphics Company

Cray Research has determined that the version of BIND shipped with all current releases of Unicos and Unicos/mk are susceptible to the problem described in this advisory. We are currently working on upgrading our version of BIND to the 4.9.6 release.

Digital Equipment Corporation

xref CASE ID: SSRT0494U

At the time of writing this document, patches(binary kits) are in progress and final patch testing is expected to begin soon. Digital will provide notice of the completion/availability of the patches through AES services (DIA, DSNlink FLASH) and be available from your normal Digital Support channel.

DIGITAL EQUIPMENT CORPORATION AUG/97

Hewlett-Packard Company

HP is vulnerable. Patches in process.

IBM Corporation

IBM is currently working on the following APARs which will be available soon:

AIX 4.1: IX70236
AIX 4.2: IX70237

To Order

APARs may be ordered using Electronic Fix Distribution (via FixDist) or from the IBM Support Center. For more information on FixDist, reference URL:
http://service.software.ibm.com/aixsupport/ or send e-mail to aixserv@austin.ibm.com with a subject of "FixDist".

IBM and AIX are registered trademarks of International Business Machines Corporation.

NEC Corporation

NEC is vulnerable. The systems affected by this problem are as follows:

UX/4800
UX/4800(64)
EWS-UX/V(Rel4.2MP)
EWS-UX/V(Rel4.2)
UP-UX/V(Rel4.2MP)

Patches are in progress and will be made available from
ftp://ftp.meshnet.or.jp/pub/48pub/security.

Siemens-Nixdorf Informationssysteme AG

We are investigating this problem and will provide updated information for this advisory when it becomes available.

The Santa Cruz Operation

The following SCO operating systems are vulnerable:

- SCO Open Desktop/Open Server 3.0, SCO UNIX 3.2v4
- SCO OpenServer 5.0
- SCO UnixWare 2.1

SCO CMW+ 3.0 is not vulnerable as bind is not supported on CMW+ platforms.

SCO has made an interim fix available for anonymous ftp:

ftp://ftp.sco.com/SSE/sse008.ltr.Z - cover letter

ftp://ftp.sco.com/SSE/sse008.tar.Z - replacement binaries

The fix includes binaries for the following SCO operating systems:

- SCO Open Desktop/Open Server 3.0, SCO UNIX 3.2v4
- SCO OpenServer 5.0
- SCO UnixWare 2.1

Sun Microsystems

```
The following patches relate to the BIND vulnerability:

        SunOS version   Patch Id

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

        5.6             105755-03

        5.6_x86         105756-03

        5.5.1           103663-11

        5.5.1_x86       103664-11
```

```
        5.5             103667-09

        5.5_x86         103668-09

        5.4             102479-11

        5.4_x86         102480-09

        5.3             101359-08
```

Sun recommended security patches (including checksums) are available from: http://sunsolve.sun.com/sunsolve/pubpatches/patches.html

The CERT Coordination Center staff thanks Paul Vixie and Wolfgang Ley for their contributions to this advisory.

Revision History

May 26, 1998 Updated vendor information for Sun Microsystems

Sept. 30, 1997 Updated copyright statement

Sept. 19, 1997 Appendix A - Added information for BSDI.

Aug. 20, 1997 Introduction - Clarified that 4.9.6 is not vulnerable.

Section III - Added a note why sites should upgrade to 8.1.1.

23 CA-1997-23: Buffer Overflow Problem in rdist

Original issue date: January 15, 1998
Last revised: December 9, 1998
Updated vendor information for Sun Microsystems, Inc.

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

The CERT Coordination Center has received reports of a vulnerability in rdist that enables anyone with access to a local account to gain root privileges. This is not the same vulnerability as the one discussed in CA-96.14.

Section III.A contains instructions on how to determine if your site is vulnerable. If your implementation of rdist is vulnerable, the CERT/CC team encourages you to follow your vendor's instructions (Sec. III.B and Appendix A) or install a freely available version of the rdist program that is not installed as set-user-id root and is, therefore, not susceptible to the exploitation described in this advisory (Sec. III.C).

For information on the earlier problem with rdist, see
http://www.cert.org/advisories/CA-96.14.rdist_vul.html.

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

I. Description

The rdist program is a UNIX Operating System utility used to distribute files from one host to another. On some systems, rdist opens network connections using a privileged port as the source port. This requires root privileges, and to attain these privileges rdist on such systems is installed set-user-id root.

A new vulnerability has been found in some set-user-id root implementations of rdist. The vulnerability lies in the function expstr(), where macros supplied as arguments are expanded using sprintf(). It is possible to overwrite stack frames and call specially pre-crafted native machine code. If the appropriate machine code is supplied, an attacker can execute arbitrary programs (such as the shell) with set-user-id root privileges.

Note that this vulnerability is distinct from that discussed in CERT advisoryCA-96.14.

II. Impact

On systems with a vulnerable copy of rdist, anyone with access to a local account can gain root access.

III. Solution

We urge you to follow the steps in Section A to determine if your system is vulnerable and, if it is, to turn off rdist while you decide how to proceed.

If your system is vulnerable and you need the functionality that rdist provides, you should install a vendor patch (Section B). Until you can do so, you may want to use a freely available version of rdist that does not need to be installed as set-user-id root and is, therefore, not susceptible to the exploitation described in this advisory (Section C).

A. How to check for set-user-id root versions of rdist

To find set-user-id root versions of rdist and to disable the programs that are possibly vulnerable, use the following find command or a variant. Consult your local system documentation to determine how to tailor the find program on your system.

You will need to run the find command on each system you maintain because the command examines files on the local disk only. Substitute the names of your local file systems for FILE_SYSTEM_NAMES in the example. Example local file system names are /, /usr, and /var. You must do this as root.

Note that this is one long command, though we have separated it onto three lines using backslashes.

```
find FILE_SYSTEM_NAMES -xdev -type f -user root \

-name '*rdist*' -perm -04000 -exec ls -l '{}' \; \

-ok chmod 0500 '{}' \;
```

This command will find all files on a system that
- are only in the file system you name (FILE_SYSTEM_NAMES -xdev) - are regular files (-type f)
- are owned by root (-user root)
- have "rdist" as a component of the name (-name '*rdist*') - are setuid (-perm -04000)

Once found, those files will
- have their names and details printed (-exec ls -l '{}')
- have the setuid mode removed (making the file available only to root) but only if you type `y' in response to the prompt (-ok chmod 0500 '{}' \;)

B. Obtain and install the appropriate patch

Below is a list of vendors who have provided information for this advisory. Details are in Appendix A, and we will update the appendix as we receive more information.

Berkeley Software Design, Inc. (BSDI)
Caldera
Digital Equipment Corp.
FreeBSD, Inc.

Hewlett-Packard Company
IBM Corporation
NEC Corporation
NCR Corporation
The Santa Cruz Operation, Inc. (SCO)
Siemens-Nixdorf
Silicon Graphics Inc. (SGI)
Sun Microsystems, Inc.

If your vendor's name is not on this list, please contact the vendor directly.

C. If you need the functionality that rdist provides but a patched version is not yet available from your vendor, consider installing rdist-6.1.3,

which is freely available from ftp://usc.edu/pub/rdist/rdist-6.1.3.tar.gz

MD5 (rdist-6.1.3.tar.gz) = 8a76b880b023c5e648b7cb77b9608b9f

The README file in the distribution explains how to configure and install this version of rdist.

We recommend that you configure this version of rdist to use rsh instead of rcmd. Here is the relevant text from the README:

"By default rdist uses *rsh(1c)* to make connections to remote hosts. This has the advantage that rdist does not need to be setuid to "root". This eliminates most potential security holes. It has the disadvantage that it takes slightly more time for rdist to connect to a remote host due to the added overhead of doing a fork() and then running the *rsh(1c)* command."

Some sites with sufficient expertise use the ssh program in conjunction with rdist, instead of using rcmd or rsh. If you have the expertise, you may want to implement this configuration.

For further details on this option see "Ssh (Secure Shell) FAQ - Frequently asked questions," Section 4.4, "Can I use rdist with ssh?" It is available from
http://www.uni-karlsruhe.de/~ig25/ssh-faq/ssh-faq-4.html.

For details on how to obtain ssh, see FAQ Section 3.4, "Where can I obtain ssh?" This section can be found in http://www.uni-karlsruhe.de/~ig25/ssh-faq/ssh-faq-3.html.

Appendix A Vendor Information

Below is a list of the vendors who have provided information for this advisory. We will update this appendix as we receive additional information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact the vendor directly.

Berkeley Software Design, Inc. (BSDI)

BSDI shipped a patch for this for our 2.1 release (U210-018) when the original Bugtraq advisory was released. The 3.0 version of rdist is not vulnerable and in fact is no longer even setuid.

Caldera

This message is to inform CERT that neither Caldera Network Desktop nor Caldera OpenLinux ship rdist SUID and are thus not vulnerable. See our advisory on this subject at: http://www.caldera.com/tech-ref/security/SA-1997.23.txt.

Digital Equipment Corp.

This reported problem is not present for Digital's ULTRIX or Digital UNIX Operating Systems Software.

DIGITAL EQUIPMENT CORPORATION

FreeBSD, Inc.

2.1.0 is vulnerable.
2.1.5, 2.1.6 and 2.1.7 are and 2.1-stable are not. In any case, upgrading to 2.1.7 or even better, 2.1-stable should be considered.
If there is demand, we'll release a patch for 2.1.0

All 2.2 releases, 2.2-stable and FreeBSD-current are not vulnerable.

Hewlett-Packard Company

HP is -not- vulnerable; the problem didn't exist in 9.X, and has been fixed in 10.X with Security Bulletin #36 (HPSBUX9608-036) last year. Patch numbers change frequently because of cumulative patching, so please check current patch ID information either by bulletin or by platform/release at our HP Electronic Support Center in the "Security Patch Matrix," which is updated every 24 hours.

1) From your Web browser, access the URL: http://us-support.external.hp.com (US,Canada,Asia-Pacific, and Latin-America) or http://europe-support.external.hp.com (Europe).

2) On the HP Electronic Support Center main screen, select the hyperlink "Support Information Digests".

3) On the "Welcome to HP's Support Information Digests" screen, under the heading "Register Now", select the appropriate hyperlink "Americas and Asia-Pacific", or "Europe".

4) On the "New User Registration" screen, fill in the fields for the User Information and Password and then select the button labeled "Submit New User".

5) On the "User ID Assigned" screen, select the hyperlink "Support Information Digests".

**Note what your assigned user ID and password are for future reference.

6) You should now be on the "HP Support Information Digests Main" screen. You might want to verify that your email address is correct as displayed on the screen. From this screen, you may also view/subscribe to the digests, including the security bulletins digest.

To get a patch matrix of current HP-UX and BLS security patches referenced by either Security Bulletin or Platform/OS, click on following screens in order:

Technical Knowledge Database
Browse the HP Security Bulletins Archive
HP-UX Security Patch Matrix

IBM Corporation

All versions of AIX are vulnerable to this buffer overflow. There is no 3.2 fix. It is recommended that 3.2 customers upgrade to a higher level. The following APARs will be available for AIX version 4 soon.

AIX 3.2: upgrade to 4.1.5 or higher
AIX 4.1: IX70876
AIX 4.2: IX70875

To Order

APARs may be ordered using Electronic Fix Distribution (via FixDist) or from the IBM Support Center. For more information on FixDist, reference URL:
http://service.software.ibm.com/aixsupport/.

or send e-mail to aixserv@austin.ibm.com with a subject of "FixDist".

IBM and AIX are registered trademarks of International Business Machines Corporation.

NEC Corporation

The following systems are NOT affected by this vulnerability:

UX/4800
UX/4800(64)
EWS-UX/V(Rel4.2MP)
EWS-UX/V(Rel4.2)

UP-UX/V(Rel4.2MP)
To report a new vulnerability, contact <UX48-security-support@nec.co.jp>.

NCR Corporation

NCR is delivering a set of operating system dependent patches which contain an update for this problem. Accompanying each patch is a README file which discusses the general purpose of the patch and describes how to apply it to your system.

Recommended solution:

Apply one of the following patches depending on the revision of the inet package installed on your system. To check its version execute:

pkginfo -x inet

For inet 5.01.xx.xx: - PINET501 (Version later than 05.01.01.59)
For inet 6.01.xx.xx: - PINET601 (Version later than 06.01.00.19)
For inet 6.01.xx.xx: - PINET601 (Version later than 06.02.00.01)

OpenBSD

OpenBSD does not have this problem. None of the versions of rdist distributed are setuid or set-gid.

The Santa Cruz Operation, Inc. (SCO)

SCO has determined that the following SCO operating systems are not vulnerable:

- SCO CMW+ 3.0
- SCO Open Desktop/Open Server 3.0
- SCO OpenServer 5.0
- SCO UnixWare 2.1

Siemens-Nixdorf Informationssysteme AG

Rdist has not been shipped with ReliantUNIX versions prior to 5.43C. The latest ReliantUNIX-Y/N version 5.43C contains a vulnerable rdist.

For this version we recommend to remove the set-user-id root bit from /usr/ucb/rdist following the instructions given in section III.A.

ReliantUNIX-Y/N 5.44A will be shipped with rdist 6.1.3. Patches for ReliantUNIX-N/Y 5.43C are available on requirement. Please ask SNI's customers service for details."

Silicon Graphics Inc. (SGI)

Silicon Graphics Inc. issued Security Advisory, "IRIX ordist Buffer Overrun Vulnerability," 19970509-02-PX, August 5, 1997.

Patches are available via anonymous FTP and your service/support provider.

The SGI anonymous FTP site is sgigate.sgi.com (204.94.209.1) or its mirror, ftp.sgi.com. Security information and patches can be found in the ~ftp/security and ~ftp/patches directories, respectfully.

For subscribing to the wiretap mailing list and other SGI security related information, please refer to the Silicon Graphics Security Headquarters website located at:
http://www.sgi.com/Support/security/security.html.

Sun Microsystems, Inc.

Please refer to Sun Microsystems, Inc. Security Bulletin, "rdist," Number: #00179, distributed November 18, 1998 for additional information relating to this vulnerability.

Patches and Checksums are available to all Sun customers via World Wide Web at: http://sunsolve.sun.com/sunsolve/pubpatches/patches.html.

Sun security bulletins are available via World Wide Web at: http://sunsolve.sun.com/pub-cgi/secbul.pl.

The CERT Coordination Center thanks Hiroshi Nakano of Ryukoku University, Japan for reporting this problem. We also thank Wolfgang Ley of DFN-CERT for his assistance with the Solutions section of the advisory.

Revision History

```
Dec.  9, 1998   Updated vendor information for Sun Microsystems,
Inc.

May 27, 1998    Updated vendor information for Sun Microsystems.

Jan. 15, 1998   Updated vendor information for NCR.

Nov. 14, 1997   Updated vendor information for Siemens-Nixdorf.

Oct. 3, 1997    Appendix A - added information for Caldera.

Sept. 30, 1997  Updated copyright statement

Sept. 15, 1997  Appendix A - added information for OpenBSD and Sili-
con Graphics, Inc.
```

24 CA-1997-24: Buffer Overrun Vulnerability in Count.cgi cgi-bin Program

Original issue date: November 5, 1997
Last revised: November 14, 1997
UPDATES - Corrected a URL.

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

The text of this advisory was originally released on October 31, 1997, as AA-97.27, developed by the Australian Computer Emergency Response Team. To more widely broadcast this information, we are reprinting the AUSCERT advisory here with their permission. Only the contact information at the end has changed: AUSCERT contact information has been replaced with CERT/CC contact information.

We will update this advisory as we receive additional information. Look for it in an "Updates" section at the end of the advisory.

The Australian Computer Emergency Response Team (AUSCERT) has received information that a buffer overrun vulnerability exists in the Count.cgi cgi-bin program.

A new version of Count.cgi has been released addressing this vulnerability.

AUSCERT recommends that sites that have the Count.cgi cgi-bin program installed take the steps outlined in Section 3 as soon as possible.

I. Description

AUSCERT has received information that a vulnerability exists in the Count.cgi cgi-bin program. The Count.cgi cgi-bin program is used to record and display the number of times a WWW page has been accessed.

Due to insufficient bounds checking on arguments which are supplied by users, it is possible to overwrite the internal stack space of the Count.cgi program while it is executing. By supplying a carefully designed argument to the Count.cgi program, intruders may be able to force Count.cgi to execute arbitrary commands with the privileges of the httpd process.

The Count.cgi program is extremely widely used. Sites are encouraged to check for its existence and its possible exploitation.

To check whether exploitation of this vulnerability has been attempted at your site, search for accesses to the Count.cgi program in your access logs. An example of how to do this is:

```
# grep -i 'Count.cgi' {WWW_HOME}/logs/access_log
```

Where {WWW_HOME} is the base directory for your web server.

If this command returns anything, further investigation is necessary. Specifically, look for accesses to Count.cgi that contain long strings of nonsensical characters.

If sites find any evidence showing that they have been probed using this vulnerability, they are encouraged to report the incident to AUSCERT or their local incident response team. Reports of all attacks help AUSCERT gain a better overview of intruder activity within the constituency.

II. Impact

Remote user may be able to execute arbitrary commands with the privileges of the httpd process which answers HTTP requests. This may be used to compromise the http server and under certain configurations gain privileged access.

III. Workarounds/Solution

AUSCERT recommends that sites upgrade to the current version of Count.cgi (Section III.A). For sites that can not immediately install the current version of Count.cgi, it is recommended that the workaround described in Section 3.2 be applied.

A. Upgrade to the current Count.cgi version

The author of Count.cgi has recently released version 2.4 which addresses the vulnerability described in this advisory. AUSCERT recommends that sites upgrade to the latest version as soon as possible. The current version is available from: http://www.fccc.edu/users/muquit/Count.html.

B. Remove execute permissions

To prevent the exploitation of the vulnerability described in this advisory, AUSCERT recommends that the execute permissions be removed from Count.cgi immediately. Note that this will have the side effect of preventing the page hit counter from being incremented and displayed on web pages using Count.cgi. The remainder of such web pages should still display.

IV. Additional measures

It is important to note that attacks similar to this may succeed against any CGI program which has not been written with due consideration for security. Sites using HTTP servers, and in particular CGI applications, are encouraged to develop an understanding of the security issues involved.

Sites should consider taking this opportunity to examine their httpd configuration and web servers. In particular, all CGI programs that are not required should be removed, and all those remaining should be examined for possible security vulnerabilities.

It is also important to ensure that all child processes of httpd are running as a non-privileged user. This is often a configurable option. See the documentation for your httpd distribution for more details.

Numerous resources relating to WWW security are available. The following pages may provide a useful starting point. They include links describing general WWW security, secure httpd setup and secure CGI programming.

The World Wide Web Security FAQ:
http://www-genome.wi.mit.edu/WWW/faqs/www-security-faq.html.

NSCA's "Security Concerns on the Web" Page:
http://hoohoo.ncsa.uiuc.edu/security/.

The following books contain useful information including sections on secure programming techniques.

Web Security Sourcebook, Aviel Rubin, Daniel Geer and Marcus Ranum, John Wiley & Sons, Inc., 1997.

Practical Unix & Internet Security, Simson Garfinkel and Gene Spafford, 2nd edition, O'Reilly and Associates, 1996.

Please note that the URLs and books referenced in this advisory are not under AUSCERT's control and therefore AUSCERT cannot be responsible for their availability or content.

AUSCERT thanks Muhammad Muquit for his assistance in the preparation of this advisory.

UPDATES

November 14, 1997

CERT/CC received word that the URL for NSCA's "Security Concerns on the Web" in the AUSCERT advisory was not correct and should be changed to the following URL:
http://hoohoo.ncsa.uiuc.edu/security-1.0/.

Our thanks to Zachary Uram at Carnegie Mellon University for bringing this to our attention.

Revision History

```
Nov. 14, 1997  UPDATES - Corrected a URL.
```

25 CA-1997-25: Sanitizing User-Supplied Data in CGI Scripts

Original issue date: November 10, 1997
Last revised: July 15, 2003
Fixed cgi_metacharacters link

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

The CERT Coordination Center has received reports and seen mailing list discussions of a problem with some CGI scripts, which allow an attacker to execute arbitrary commands on a WWW server under the effective user-id of the server process. The problem lies in how the scripts are written, NOT in the scripting languages themselves.

The CERT/CC team urges you to check all CGI scripts that are available via the World Wide Web services at your site and ensure that they sanitize user-supplied data. We have written a tech tip on how to do this (see Section III).

We will update the tech tip (rather than this advisory) if we receive additional information.

I. Description

Some CGI scripts have a problem that allows an attacker to execute arbitrary commands on a WWW server under the effective user-id of the server process. The cause of the problem is not the CGI scripting language (such as Perl and C). Rather, the problem lies in how an individual writes his or her script. In many cases, the author of the script has not sufficiently sanitized user-supplied input.

II. Impact

If user-supplied data is not sufficiently sanitized, local and remote users may be able to execute arbitrary commands on the HTTP server with the privileges of the httpd daemon. They may then be able to compromise the HTTP server and under certain configurations gain privileged access.

III. Solution

We strongly encourage you to review all CGI scripts that are available via WWW services at your site. You should ensure that these scripts sufficiently sanitize user-supplied data.

We recommend carrying out this review on a regular basis and whenever new scripts are made available.

For advice about what to look for and how to address the problem, see our tech tip on meta-characters in CGI scripts, available from http://www.cert.org/tech_tips/cgi_metacharacters.html.

Note that because this problem is of a general nature, the tech tip demonstrates only the concept of the problem and its solution. The programmer and/or system administrator must ensure that any solution implemented is robust and does not break intended functionality.

If you believe that a script does not sufficiently sanitize user-supplied data then we encourage you to disable the script and consult the script author for a patch.

If the script author is unable to supply a patched version, sites with sufficient expertise may wish to patch the script themselves, adapting the material in our tech tip to meet whatever specification is required (such as the appropriate RFC).

(NOTE: We cannot offer any further assistance on source code patching than that given in the tech tip mentioned above.)

The CERT Coordination Center thanks Wietse Venema for some of the material used in the cgi_metacharacters tech tip.

We thank Mark Mills, Andrew McNaughton and Greg Bacon for their communication with us about the content of the tech tip.

Revision History

```
Jul. 15, 2003 Fixed cgi_metacharacters link

Feb. 13, 1998 Updated tech tip, and removed Appendix A

Nov. 13, 1997 Minor editorial change

Nov. 12, 1997 Updated the Appendix to fix coding error
```

26 CA-1997-26: Buffer Overrun Vulnerability in statd(1M) Program

Original issue date: December 5, 1997
Last revised: March 08, 1999
Updated patch information for Sun Microsystems

A complete revision history is at the end of this file. The text of this advisory was originally released on December 5, 1997, as AA-97.29, developed by the Australian Computer Emergency Response Team. To more widely broadcast this information, we are reprinting the AUSCERT advisory here with their permission. Only the contact information at the end has changed: AUSCERT contact information has been replaced with CERT/CC contact information.

We will update this advisory as we receive additional information. Look for it in an "Updates" section at the end of the advisory.

AUSCERT has received information that a vulnerability exists in the statd(1M) program, available on a variety of Unix platforms.

This vulnerability may allow local users, as well as remote users to gain root privileges.

Exploit information involving this vulnerability has been made publicly available.

This vulnerability is different to the statd vulnerability described in CERT/CC advisory CA-96.09.

The vulnerability in statd affects various vendor versions of statd. AUSCERT recommends that sites take the steps outlined in section 3 as soon as possible.

This advisory will be updated as more information becomes available.

I. Description

AUSCERT has received information concerning a vulnerability in some vendor versions of the RPC server, statd(1M).

statd provides network status monitoring. It interacts with lockd to provide crash and recovery functions for the locking services on NFS.

Due to insufficient bounds checking on input arguments which may be supplied by local users, as well as remote users, it is possible to overwrite the internal stack space of the statd program while it is executing a specific rpc routine. By supplying a carefully designed input argument to the statd program, intruders may be able to force statd to execute arbitrary commands as the user running statd. In most instances, this will be root.

This vulnerability may be exploited by local users. It can also be exploited remotely without the intruder requiring a valid local account if statd is accessible via the network.

Sites can check whether they are running statd by:

On system V like systems:

```
        # ps -fe |grep statd

        root   973     1  0 14:41:46 ?        0:00
/usr/lib/nfs/statd
```

On BSD like systems:

```
        # ps -auxw |grep statd

        root       156  0.0  0.0   52    0 ?  IW   May  3  0:00
rpc.statd
```

Specific vendor information regarding this vulnerability can be found in Section III.

II. Impact

This vulnerability permits attackers to gain root privileges. It can be exploited by local users. It can also be exploited remotely without the intruder requiring a valid local account if statd is accessible via the network.

III. Workarounds/Solution

The statd program is available on many different systems. As vendor patches are made available sites are encouraged to install them immediately (Section 3.1).

If you are not using NFS in your environment then there is no need for the statd program to be running and it can be disabled (Section 3.2).

3.1 Vendor information

The following vendors have provided information concerning the vulnerability in statd.

BSDI
Data General Corporation
Digital Equipment Corporation
Hewlett-Packard
IBM Corporation
The NetBSD Project
Red Hat Software
Sun Microsystems

Specific vendor information has been placed in Appendix A.

If the statd program is required at your site and your vendor is not listed, you should contact your vendor directly.

If you do not require the statd program then it should be disabled (Section 3.2).

3.2 Disabling statd

The statd daemon is required as part of an NFS environment. If you are not using NFS there is no need for this program and it can be disabled. The statd (or rpc.statd) program is often started in the system initialisation scripts (such as /etc/rc* or /etc/rc*.d/*). If you do not require statd it should be commented out from the initialisation scripts. In addition, any currently running statd should be identified using ps(1) and then terminated using kill(1).

Appendix A Vendor information

The following information regarding this vulnerability for specific vendor versions of statd has been made available to AUSCERT. For additional information, sites should contact their vendors directly.

BSDI

No versions of BSD/OS are vulnerable to this problem.

Data General Corporation

This problem is under investigation.

Digital Equipment Corporation

A DIGITAL EQUIPMENT CORPORATION ADVISORY, SSRT0456U, concerning

"DIGITAL UNIX rpc.statd V3.2g, V4.0, V4.0a, V4.0b, V4.0c, V4.0d" was issued April 30, 1998. For more information, please see the World Wide Web at the following FTP address: http://www.service.digital.com/html/patch_service.html

Use the FTP access option, select DIGITAL_UNIX directory then choose the appropriate version directory and download the patch accordingly.

Hewlett-Packard

HP is not vulnerable.

IBM Corporation

AIX 3.2 and 4.1 are vulnerable to the statd buffer overflow. However, the buffer overflow described in this advisory was fixed when the APARs for CERT CA-96.09 was released. See the appropriate release below to determine your action.

AIX 3.2

Apply the following fix to your system:

APAR - IX56056 (PTF - U441411)

To determine if you have this PTF on your system, run the following command:

lslpp -lB U441411

AIX 4.1

Apply the following fix to your system:

APAR - IX55931

To determine if you have this PTF on your system, run the following

command:

instfix -ik IX55931

Or run the following command:

lslpp -h bos.net.nfs.client

Your version of bos.net.nfs.client should be 4.1.4.7 or later.

AIX 4.2

No APAR required. Fix already contained in the release.

APARs may be ordered using Electronic Fix Distribution (via

FixDist) or from the IBM Support Center. For more information on

FixDist, reference URL:

http://service.software.ibm.com/aixsupport/

or send e-mail to aixserv@austin.ibm.com with a subject of

"FixDist".

```
        IBM and AIX are registered trademarks of International Busi-
ness

        Machines Corporation.
```

The NetBSD project

NetBSD is not vulnerable to the statd buffer overflow. It does not ship with NFS locking programs (statd/lockd).

Red Hat Linux

Red Hat Linux is not vulnerable to the statd buffer overflow. No versions of Red Hat Linux include statd in any form.

Sun Microsystems

The statd vulnerability has been fixed by the following patches:

SunOS version	Patch Id
5.5.1	104166-03
5.5.1_x86	104167-02
5.5	103468-03
5.5_x86	103469-03
5.4	102769-04
5.4_x86	102770-04
4.1.4	102516-06
4.1.3_U1	101592-09

SunOS 5.6 and 5.6_x86 are not vulnerable to this problem.

The vulnerability described in this advisory is not the same as that described in Sun Security Bulletin #135.

Sun recommended and security patches (including checksums) are available from:
http://sunsolve.sun.com/sunsolve/pubpatches/patches.html.

AUSCERT maintains a local mirror of Sun recommended and security patches at:
ftp://ftp.auscert.org.au/pub/mirrors/sunsolve1.sun.com/.

AUSCERT thanks Peter Marelas (The Fulcrum Consulting Group), Tim MacKenzie (The Fulcrum Consulting Group) and CERT/CC for their assistance in the preparation of this advisory.

UPDATES

Vendor Information

Below is information we have received from vendors. If you do not see your vendor's name below, contact the vendor directly for information.

NetBSD

NetBSD 1.2.1 and prior do not ship with rpc.statd. NetBSD 1.3 ships an rpc.statd that is not vulnerable.

Silicon Graphics Inc.

Silicon Graphics Inc. has investigated the issue and has recommended steps for neutralizing the exposure. It is HIGHLY RECOMMENDED that these measures be implemented on ALL SGI systems.

For further information, please refer to Silicon Graphics Inc. Security Advisory Number: 19971201-01-P1391 "Buffer Overrun Vulnerability in statd(1M) Program"

The SGI anonymous FTP site is sgigate.sgi.com (204.94.209.1) or its mirror, ftp.sgi.com. Security information and patches can be found in the ~ftp/security and ~ftp/patches directories, respectfully.

Revision History

```
Mar. 08, 1999   Updated patch information for Sun Microsystems.

Jul. 07, 1998   Updated information for Digital Equipment Corpora-
tion.

Feb. 12, 1998   Updated information for Hewlett-Packard and Data
General Corporation.

Dec. 19, 1997   Vendor information for SGI added to the UPDATES sec-
tion.

Dec. 15, 1997   Vendor information for NetBSD has been added to the
UPDATES section.
```

27 CA-1997-27: FTP Bounce

Original issue date: December 10, 1997
Last revised: July 26, 2002
Updated links, wu-ftpd, SGI, and HP information

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

In some implementations of FTP daemons, the PORT command can be misused to open a connection to a port of the attacker's choosing on a machine that the attacker could not have accessed directly. There have been ongoing discussions about this problem (called "FTP bounce") for several years, and some vendors have developed solutions for this problem.

The CERT/CC staff urges you to install a comprehensive patch if one is available. Until then, we recommend the wu-ftpd package identified in Section III.B. as a workaround.

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

I. Description

In the past few years there have been ongoing discussions about a problem known as "FTP bounce." In its simplest terms, the problem is based on the misuse of the PORT command in the FTP protocol.

To understand the FTP bounce attack, please see the tech tip at
http://www.cert.org/tech_tips/ftp_port_attacks.html.

The core component of the problem is that by using the PORT command in active FTP mode, an attacker may be able to establish connections to arbitrary ports on machines other than the originating client. This behavior is RFC compliant, but it is also potentially a source of security problems for some sites. The example attacks described in the tech tip demonstrate the potential of this vulnerability.

II. Impact

An attacker may be able to establish a connection between the FTP server machine and an arbitrary port on another system. This connection may be used to bypass access controls that would otherwise apply.

III. Solution

Because the core element of the attack (the FTP server can establish connections to arbitrary machines and arbitrary ports) is also a required component for RFC compliance, there is no clear-cut

solution. With this in mind, we urge you to carefully consider the type of service that your site offers.

The best solution solely from a security perspective is to ensure that your FTP server software cannot establish connections to arbitrary machines. However, sites that rely on the RFC-compliant behavior may find that implementing this solution will affect applications that they use. (We have not received any first-hand reports of such cases.) Consequently, many vendors offer solutions that allow sites offering the FTP service to make the choice that best suits them. You should check to see what type of behavior your vendor's FTP daemon adopts (Section A).

If you wish to implement an FTP service that does not allow this attack and your vendor does not offer a daemon with this functionality, consider using the wu-ftpd package described in Section B. Other steps you can take are described in Section C.

A. Vendor Information

It is our experience that vendor implementations fall into one of these groups:

1. strict conformance with RFC functionality: The PORT command may be used to connect directly to a third-party machine, and this is the only functionality allowed. Some vendors who choose to maintain strict conformance have addressed this problem by modifying all other network services to reject connections originating from the FTP data port (port 20).
2. strict suppression of the PORT command: The PORT command may be used to connect to the originating client, and this is the only functionality allowed.

3. variable PORT command behavior: The PORT command may be used in either of the above two ways, with one way being the default. Switching between them is usually achieved with a command line parameter. You should be careful to verify which is the default.

Appendix A contains a list of vendors who have provided information about this problem. We will update the appendix as we receive more information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact your vendor directly.

B. Use the wu-ftpd package as a workaround.

The wu-ftpd package addresses the FTP bounce problem by ensuring that the PORT command cannot be used to establish connections to machines other than the originating client.

The latest version of wu-ftpd is available from

http://www.wuftpd.org/

C. FTP Configuration

Some attacks rely on an intermediate file being uploaded to one or more server machines via (usually anonymous) FTP. This file is used in a later phase of the attack.

Your site should offer anonymous upload facilities only if it is absolutely necessary. Even then, you must carefully configure the incoming area. For further details, see "Anonymous

FTP Configuration Guidelines" at
http://www.cert.org/tech_tips/anonymous_ftp_config.html.

Note that these steps only repel attacks that rely on intermediate uploads. The steps are not effective against other attacks.

If your site allows file uploads, we urge your to ensure that the FTP service restricts the PORT command so that it can only be used to connect to the originating client.

Appendix A Vendor Information

Below is a list of the vendors who have provided information for this advisory. We will update this appendix as we receive additional information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact the vendor directly.

Caldera, Inc.

Caldera OpenLinux(tm) 1.2 ships with wu-ftpd-2.4.2 beta 15. For those with earlier versions of wu-ftpd, updates to this package can be obtained from:
ftp://ftp.caldera.com/pub/openlinux/updates/1.1/current/.

Other Caldera security resources are located at: http://www.caldera.com/tech-ref/security/.

Cray Research - A Silicon Graphics Company

The ftpd supplied with Unicos and Unicos/mk is currently in category 1. We are working to make it category 3.

DATA GENERAL

```
DGUX documents a "-p" switch for ftpd, which appears to prevent ex-
ploitation of the problem described. Revision R4.20MU04 and later
will be configured to include this switch in the /etc/inetd.conf
file.

Customers running earlier revisions should change the ftp line in
their inetd.conf file to the following:

ftp     stream  tcp     nowait  root    /usr/bin/ftpd        ftpd -p
-t900
```

DIGITAL EQUIPMENT CORPORATION

```
A DIGITAL EQUIPMENT CORPORATION ADVISORY  VB#SSRT0452, concerning
"DIGITAL UNIX

ftpd  V3.2g, V4.0, V4.0a, V4.0b, V4.0c" was issued APR  30,  1998.
For more information, please see the World Wide Web at the following
FTP address: http://www.service.digital.com/html/patch_service.html
```

Use the FTP access option, select DIGITAL_UNIX directory then choose the appropriate version directory and download the patch accordingly.

The FreeBSD Project

FreeBSD 2.2.0 and all later releases do not allow the FTP bounce attack (unless explicitly allowed by the -R option). FreeBSD 2.1.7 and earlier releases can be abused by the bounce attack.

Hewlett-Packard Company

This problem is addressed HP Security Bulletin 028. This bulletin can be found at one of these URLs:

http://us-support.external.hp.com (for US, Canada, Asia-Pacific, & Latin-America)

http://europe-support.external.hp.com (for Europe)

```
**********************************************************************

Current patches for SB#28 as of 11/5/97 from security patch matrix

**********************************************************************

Security Bulletin 028: Security Vulnerability in FTP

                Current                              Original

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

          s300  8.00: None                     s300  8.00: None

          s300  9.00: PHNE_6146                s300  9.00: PHNE_6146

          s300  9.03: PHNE_6146                s300  9.03: PHNE_6146

          s300  9.10: PHNE_6146                s300  9.10: PHNE_6146

          s700  8.05: None                     s700  8.05: None

          s700  8.07: None                     s700  8.07: None

          s700  9.01: PHNE_10008               s700  9.01: PHNE_6013

          s700  9.03: PHNE_10008               s700  9.03: PHNE_6013

          s700  9.05: PHNE_10008               s700  9.05: PHNE_6013

          s700  9.07: PHNE_10008               s700  9.07: PHNE_6013

          s700  9.09: PHNE_6169                s700  9.09: PHNE_6169

                       PHNE_6170                            PHNE_6170
```

```
            s700 10.00: PHNE_10009              s700 10.00: PHNE_6014
            s700 10.01: PHNE_10009              s700 10.01: PHNE_6014
            s700 10.09: PHNE_5965               s700 10.09: PHNE_5965
            s700 10.10: PHNE_10009              s700 10.10: None
            s700 10.16: None                    s700 10.16: None
            s700 10.20: None                    s700 10.20: None
            s700 10.24: None                    s700 10.24: None
            s700 10.30: None                    s700 10.30: None
            s800  8.00: None                    s800  8.00: None
            s800  8.02: None                    s800  8.02: None
            s800  8.06: None                    s800  8.06: None
            s800  9.00: PHNE_10008              s800  9.00: PHNE_6013
            s800  9.04: PHNE_10008              s800  9.04: PHNE_6013
            s800  9.08: PHNE_6171               s800  9.08: PHNE_6171
            s800 10.00: PHNE_10009              s800 10.00: PHNE_6014
            s800 10.01: PHNE_10009              s800 10.01: PHNE_6014
            s800 10.09: None                    s800 10.09: None
            s800 10.10: PHNE_10009              s800 10.10: None
            s800 10.16: None                    s800 10.16: None
            s800 10.20: None                    s800 10.20: None
            s800 10.24: None                    s800 10.24: None
            s800 10.30: None                    s800 10.30: None

*****************************************************************

   Accessing the HP ESC

 *****************************************************************

   Hewlett Packard's HP-UX patches/Security Bulletins/Security

   patches are available via email and/or WWW (via the browser
```

of your choice) on HP Supportline (HPSL).

To subscribe to automatically receive future NEW HP Security Bulletins from

the HP SupportLine Digest service via electronic mail, do the following:

1) From your Web browser, access the URL:

http://us-support.external.hp.com (US,Canada,Asia-Pacific,

and Latin-America)

http://europe-support.external.hp.com (Europe)

Login with your user ID and password, or register for one (remember

to save the User ID assigned to you, and your password). Once you are on the Main Menu, Click on the Technical Knowledge Database, and it will connect to a HP Search Technical Knowledge DB page. Near the bottom is a hyperlink to our Security Bulletin archive. Once in the archive there is another link to our current security patch matrix.

Updated daily, this matrix is categorized by platform/OS release, and by bulletin topic.

This is resolved on HP-e3000 MPE/iX systems - fix: 8606-204841 in the following patches to FTP Server:

- FTPGD62 for C.60.00
- FTPGD63 for C.65.00
- FTPGD49 for C.70.00

IBM Corporation

All AIX ftp servers are vulnerable to the FTP bounce attack. The following fixes are in progress:

AIX 3.2: upgrade to v4
AIX 4.1: IX73075
AIX 4.2: IX73076
AIX 4.3: IX73077

To Order

APARs may be ordered using Electronic Fix Distribution (via FixDist) or from the IBM Support Center. For more information on FixDist, reference URL:

http://www.ibm.com/support/ or send e-mail to aixserv@austin.ibm.com with a subject of "FixDist".

MadGoat

This problem is fixed in MGFTP V2.2-2, which was released several months ago. That version restricts the port numbers to ports above 1024. However, it does not block access to third-party machines. V2.2-4, scheduled for release next week, will do that as well.

Microsoft Corporation

We prevent this attack by disallowing "third party" transfers. This is done via a modification to our implementation of the PORT command. When the FTP server receives a PORT command, the specified IP address *must* match the client's source IP address for the control channel.

In other words, then the client sends a PORT command to the FTP server, giving the server an IP address & port number to connect back to the client for the data transfer, the IP address *must* be the client's original IP address.

We have one other fix in which we disallow the PORT command from specifying reserved ports (those less than 1024) except port 20 (the default data port). By default, any client attempt to issue a port command with (port < 1024 && port != 20) will cause the PORT command to fail. This check can be disabled setting the EnablePortAttack registry value.

NEC Corporation

Several NEC Unix systems have proven vulnerable. Work is currently underway to identify all affected systems. Patches are forthcoming.

NCR Corporation

NCR is delivering a set of operating system dependent patches which contain an update for this problem. Accompanying each patch is a README file which discusses the general purpose of the patch and describes how to apply it to your system.

Recommended solution: Apply one of the following patches depending on the revision of the inet package installed on your system. To check its version execute:

```
pkginfo -x inet
```

For inet 5.01.xx.xx: - PINET501 (Version later than 05.01.01.64)
For inet 6.01.xx.xx: - PINET601 (Version later than 06.01.00.24)
For inet 6.02.xx.xx: - PINET602 (Version later than 06.02.00.05)

After installation of the respective patch, the default behavior will be to protect from this vulnerability. A new ftpd man-page describe how to enable the old RFC compliant behavior.

The NetBSD Project

There are no patches for NetBSD 1.2.1 or prior, however the ftpd sources available from:
ftp.netbsd.org:/pub/NetBSD/NetBSD-current/src/libexec/ftpd
should work on a NetBSD 1.2.1 machine.

The OpenBSD project

FTP bounce can be fixed in the operating system by fixing all vulnerable services by checking for connections from port 20. Since this has been done in OpenBSD, OpenBSD is not vulnerable and does NOT NEED the variable port command. The solution applies since OpenBSD 2.1 (ie. it applies for both 2.1 and for 2.2).

Red Hat Software

We ship wu-ftpd, so this isn't a problem for us.

The Santa Cruz Operation, Inc.

SCO has determined that the following Operating systems are vulnerable to the ftp-bounce attack :-

OpenServer	5.0.4
UnixWare	2.1
ODT	3.0
CMW+	

We are currently working on a fix to this problem.

Siemens-Nixdorf Informationssysteme AG

ReliantUNIX is vulnerable.

The problem has been corrected in the current sources.
Patches will be developed (as necessary) and made available via your Siemens-Nixdorf customers service.

Silicon Graphics Inc.

Silicon Graphics Inc. has released SGI Security Advisory 20020305-01-I:
ftp://patches.sgi.com/support/free/security/advisories/20020305-02-I.

Sun Microsystems, Inc.

Sun's FTP server software in SunOS 4.1.x and 5.x allow PORT requests to make data connections to arbitrary hosts. Prior to SunOS 5.6, Sun's FTP server software also allows data connections to arbitrary ports.

In SunOS 5.6, the FTP server software does not accept PORT requests to make data connections to well-known (privileged) ports. Sun has also released the following patches that prevent Sun's FTP server software from accepting PORT requests to make data connections to well-known ports for the following SunOS releases:

103603-05 SunOS 5.5.1
103604-05 SunOS 5.5.1_x86
103577-06 SunOS 5.5
103578-06 SunOS 5.5_x86
101945-51 SunOS 5.4
101946-45 SunOS 5.4_x86
104938-01 SunOS 5.3
104477-03 SunOS 4.1.4
104454-03 SunOS 4.1.3_U1

Sun recommends that sites that do not require their FTP server make connections to arbitrary hosts consider using wu-ftpd as a workaround.

The CERT Coordination Center thanks AUSCERT and DFN-CERT for helping develop this advisory. We also thank Steve Bellovin, and the vendors who offered valuable comments on the problem and solutions: BSDI, Caldera, Hewlett-Packard, Livingston, NetBSD, OpenBSD, Sun Microsystems.

Revision History

```
Dec 11, 1997: Vendor updates for Caldera, Digital Equipment Corpora-
tion, and NEC Corporation.

Dec 16, 1997: Vendor updates for Sun Microsystems, Inc.

Dec 19, 1997: Updates to Section III-B and Acknowledgments.

Jan 07, 1998: Updated vendor information for NCR. Updates to Section
III.B.

Jan 08, 1998: Updates to Section III.B.

Jul 09, 1998: Updated information for Digital Equipment Corporation
```

Mar 08, 1999: Added vendor information for Data General.

Feb 28, 2002: Updated invalid IBM link

Feb 28, 2002: Updated broken ftp links

Apr 03, 2002: Updated wu-ftpd information, added HP MPE and SGI information

Jul 26, 2002: Corrected spelling errors in SGI vendor statement

28 CA-1997-28: IP Denial-of-Service Attacks

Original issue date: December 16, 1997
Last revised: May 26, 1998
Updated vendor information for Sun Microsystems, Inc.

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

The CERT Coordination Center has received reports of two attack tools (Teardrop and Land) that are being used to exploit two vulnerabilities in the TCP/IP protocol. Both tools enable a remote user to cause a denial of service.

The CERT/CC team recommends installing patches from your vendor. Until you are able to do so, we urge you to use the workaround described in Section III.B. to reduce the likelihood of a successful attack using Land. There is no workaround for Teardrop.

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

I. Description

In recent weeks there has been discussion on public mailing lists about two denial-of-service attack tools, Teardrop and Land. These attack tools have similar effects on some systems (namely, causing the victim machine to crash), but the tools exploit different vulnerabilities.

The CERT Coordination Center has received several reports of sites being attacked by either one or both of these tools. It is important to note that it may be necessary for a system administrator to apply separate patches, if they exist, for each attack tool.

Topic 1 - Teardrop

Some implementations of the TCP/IP IP fragmentation re-assembly code do not properly handle overlapping IP fragments. Teardrop is a widely available attack tool that exploits this vulnerability.

Topic 2 - Land

Some implementations of TCP/IP are vulnerable to packets that are crafted in a particular way (a SYN packet in which the source address and port are the same as the destination--i.e., spoofed). Land is a widely available attack tool that exploits this vulnerability.

II. Impact

Topic 1 - Teardrop

Any remote user can crash a vulnerable machine.

Topic 2 - Land

Any remote user that can send spoofed packets to a host can crash or "hang" that host.

III. Solution

CERT/CC urges you to immediately apply vendor patches if they are available. You may have to apply different patches for each attack tool.

You may want to use the workaround for Land, so please review both Sections A and B below.

A. Consult your vendor

Appendix A contains information from vendors who provided input for this advisory. We will update the appendix as we receive more information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact your vendor directly.

It is important to note that you may have to apply different patches for each attack tool.

B. Apply the following workaround (Land only)

A workaround for the Land attack tool is to block IP-spoofed packets. This workaround does not apply to the Teardrop attack tool because the Teardrop attack does not rely on IP-spoofed packets.

Attacks like those of the Land tool rely on the use of forged packets, that is, packets where the attacker deliberately falsifies the origin address. With the current IP protocol technology, it is impossible to eliminate IP-spoofed packets. However, you can reduce the likelihood of your site's networks being used to initiate forged packets by filtering outgoing packets that have a source address different from that of your internal network.

Currently, the best method to reduce the number of IP-spoofed packets exiting your network is to install filtering on your routers that requires packets leaving your network to have a source address from your internal network. This type of filter prevents a source IP spoofing attack from your site by filtering all outgoing packets that contain a source address from a different network.

A detailed description of this type of filtering is available in RFC 2267, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing" by Paul Ferguson of Cisco Systems, Inc. and Daniel Senie of Blazenet, Inc. We recommend it to both Internet Service Providers and sites that manage their own routers. The document is currently available at ftp://ftp.isi.edu/in-notes/rfc2267.txt.

Appendix A Vendor Information

Below is a list of the vendors who have provided information for this advisory. We will update this appendix as we receive additional information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact the vendor directly.

Berkeley Software Design, Inc. (BSDI)

No version of BSD/OS is vulnerable to Teardrop.

Patched versions of 2.1 and all 3.0 and 3.1 versions are also not vulnerable to Land.

Caldera Corporation

Topic 1 - Teardrop

Unless patched, Linux 2.0.x kernels prior to 2.0.32 are vulnerable. With the application of the kernel update described in Caldera Security Advisory SA-1997.29 (dated 3-Dec-1997), Caldera OpenLinux is not vulnerable. This Caldera advisory describes how to obtain and install the update and can be found at: http://www.caldera.com/tech-ref/security/SA-1997.29.html.

Other Caldera Security Advisories can be found at: http://www.caldera.com/tech-ref/security/.

Topic 2 - Land

There are no known reports of any version of the Linux kernel, including those shipping with Caldera OpenLinux, being vulnerable to this exploit.

Cisco Systems

Topic 1 - Teardrop

Not vulnerable.

Topic 2 - Land

IOS/7000 software, Catalyst 5xxx and 29xx LAN switches, BPX and IGX WAN switches and AXIS shelf appear to be vulnerable. PIX firewall and Centri firewall are not vulnerable.

For more information reference URL: http://www.cisco.com/warp/public/770/land-pub.shtml

Digital Equipment Corporation

This reported problem is not present for Digital's ULTRIX or Digital UNIX Operating Systems Software.

The FreeBSD Project

Topic 1 - Teardrop

CSRG 4.4 is not vulnerable.

Topic 2 - Land

No feedback.

Hewlett-Packard Corporation

HPSBUX9801-076
SECURITY BULLETIN: #00076, 21 January 1998

Description: Security Vulnerability with land on HP-UX

The problem can be fixed by applying the appropriate cumulative ARPA Transport patch mentioned below.

```
HP-UX release 11.00 HP9000 Series 700/800     PHNE_14017
HP-UX release 10.30 HP9000 Series 700/800     PHNE_13671
HP-UX release 10.20 HP9000 Series 800         PHNE_13468
HP-UX release 10.24 HP9000 Series 700         PHNE_13888
HP-UX release 10.24 HP9000 Series 800         PHNE_13889
HP-UX release 10.20 HP9000 Series 800         PHNE_13468
HP-UX release 10.20 HP9000 Series 700         PHNE_13469
HP-UX release 10.16 HP9000 Series 700         PHKL_14242
HP-UX release 10.16 HP9000 Series 800         PHKL_14243
HP-UX release 10.10 HP9000 Series 800         PHNE_13470
HP-UX release 10.10 HP9000 Series 700         PHNE_13471
HP-UX release 10.01 HP9000 Series 800         PHNE_13472
HP-UX release 10.01 HP9000 Series 700         PHNE_13473
HP-UX release 10.00 HP9000 Series 800         PHNE_13474
HP-UX release 10.00 HP9000 Series 700         PHNE_13475
HP-UX release  9.04 HP9000 Series 800         PHNE_13476
HP-UX release  9.0[3,5,7] HP9000 Series 700   PHNE_13477
HP-UX release  9.01 HP9000 Series 700         PHNE_13478
HP-UX release  9.00 HP9000 Series 800         PHNE_13479
```

IBM Corporation

Topic 1 - Teardrop

AIX is not vulnerable.

Topic 2 - Land

AIX is not vulnerable.

Microsoft Corporation

Topic 1 - Teardrop

Windows NT 4.0 with SP 3 and post SP 3 fixes applied and Windows 95 with the appropriate patch are not vulnerable. Patch information is available at URL: ftp://ftp.microsoft.com/bussys/winnt/kb/Q154/1/74.TXT.

Topic 2 - Land

Windows NT 4.0 with the appropriate patch is not vulnerable. Patch information is available at URL: ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/land-fix/Q165005.txt.

Windows 95 without the WinSock 2.0 Update is not vulnerable. Patch information is available at URL: ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/land-fix/Q177539.TXT.

NCR Corporation

Topic 1 - Teardrop

NCR MP-RAS TCP/IP implementation is not vulnerable.

Topic 2 - Land

Apply a patch for your MP-RAS UNIX TCP/IP depending on the revision of the inet package installed on your system. To check its version execute:

```
pkginfo -x inet
```

For inet 5.01.xx.xx: - PINET501 (Version later than 05.01.01.08)
For inet 6.01.xx.xx. - Not vulnerable.
For inet 6.02.xx.xx. - Not vulnerable.

The NetBSD Project

Topic 1 - Teardrop

Versions 1.2 and above are not vulnerable.

Topic 2 - Land

Versions prior to 1.3_BETA will hang. 1.3_BETA and later versions are not vulnerable.

Red Hat Software

Topic 1 - Teardrop

Linux is not vulnerable.

Topic 2 - Land

Linux is not vulnerable.

Sun Microsystems, Inc.

Topic 1 - Teardrop

All releases of Solaris are not vulnerable. All supported versions of SunOS 4.1.x (4.1.3_U1 and 4.1.4) are not vulnerable.

Topic 2 - Land

```
All releases of Solaris are not vulnerable. SunOS 4.1.3_U1 and 4.1.4
are vulnerable. The following patches should be installed:

        SunOS version   Patch Id

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

        4.1.4           102517-05

        4.1.3_U1        102010-06

Sun recommended and security patches (including checksums) are
available from: http://sunsolve.sun.com/sunsolve/pub-
patches/patches.html.
```

The CERT Coordination Center thanks Paul Ferguson and Daniel Senie for providing information on network ingress filtering.

Revision History

```
May 26, 1998  Updated vendor information for Sun Microsystems, Inc.

Apr. 28, 1998 Corrected URL for obtaining RFCs.

Mar. 10, 1998 Updated vendor information for Hewlett-Packard.
```

Jan. 29, 1998 Updated reference to the filtering document (now an RFC) in Section III.B.

Jan. 22, 1998 Updated vendor information for Hewlett-Packard.

Jan. 15, 1998 Updated vendor information for Cisco Systems (Teardrop topic).

Jan. 5, 1998 Updated vendor information for NetBSD.

Dec. 17, 1997 Added or updated vendor information for Caldera, NCR, BSDI, and Sun.

Dec. 16, 1997 Added vendor information for Digital Equipment Corporation and Hewlett-Packard.