CERT Advisory 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 Business
        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 Corporation.

Feb. 12, 1998   Updated information for Hewlett-Packard and Data General Corporation.

Dec. 19, 1997   Vendor information for SGI added to the UPDATES section.

Dec. 15, 1997   Vendor information for NetBSD has been added to the UPDATES section.
```