CERT Advisory CA-2002-11 Heap Overflow in Cachefs Daemon (cachefsd)

Original release date: May 06, 2002
Last revised: May 14, 2002
Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

- Sun Solaris 2.5.1, 2.6, 7, and 8 (SPARC and Intel architectures)

Overview

Sun's NFS/RPC file system cachefs daemon (cachefsd) is shipped and installed by default with Sun Solaris 2.5.1, 2.6, 7, and 8 (SPARC and Intel architectures). A remotely exploitable vulnerability exists in cachefsd that could permit a remote attacker to execute arbitrary code with the privileges of the cachefsd, typically root. The CERT/CC has received credible reports of scanning and exploitation of Solaris systems running cachefsd.

I. Description

A remotely exploitable heap overflow exists in the cachefsd program shipped and installed by default with Sun Solaris 2.5.1, 2.6, 7, and 8 (SPARC and Intel architectures). Cachefsd caches requests for operations on remote file systems mounted via the use of NFS protocol. A remote attacker can send a crafted RPC request to the cachefsd program to exploit the vulnerability.

Logs of exploitation attempts may resemble the following:

```
May 16 22:46:08 victim-host inetd[600]: /usr/lib/fs/cachefs/cachefsd: Segmentation Fault - core dumped
May 16 22:46:21 victim-host last message repeated 7 times
May 16 22:46:22 victim-host inetd[600]: /usr/lib/fs/cachefs/cachefsd: Bus Error - core dumped
May 16 22:46:24 victim-host inetd[600]: /usr/lib/fs/cachefs/cachefsd: Segmentation Fault - core dumped
May 16 22:46:56 victim-host inetd[600]: /usr/lib/fs/cachefs/cachefsd: Bus Error - core dumped
May 16 22:46:59 victim-host last message repeated 1 time
May 16 22:47:02 victim-host inetd[600]: /usr/lib/fs/cachefs/cachefsd: Segmentation Fault - core dumped
May 16 22:47:07 victim-host last message repeated 3 times
May 16 22:47:09 victim-host inetd[600]: /usr/lib/fs/cachefs/cachefsd: Hangup
May 16 22:47:11 victim-host inetd[600]: /usr/lib/fs/cachefs/cachefsd: Segmentation Fault - core dumped
```

Sun Microsystems has released a
Sun Alert Notification which addresses this issue as well as the issue described in VU#161931.

According to the Sun Alert Notification, failed attempts to exploit this vulnerability may leave a core dump file in the root directory. The presence of the *core* file does not preclude the success of subsequent attacks. Additionally, if the file */etc/cachefstab* exists, it may contain unusual entries.

This issue is also being referenced as CAN-2002-0033:

> *http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0033*

II. Impact

A remote attacker may be able to execute code with the privileges of the cachefsd process, typically root.

III. Solution

Apply a patch from your vendor

Appendix A contains information provided by vendors for this advisory.

If a patch is not available, disable cachefsd in *inetd.conf* until a patch can be applied.

If disabling the cachefsd is not an option, follow the suggested workaround in the Sun Alert Notification.

Appendix A. - Vendor Information

This appendix contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below, please check the Vulnerability Note (VU#635811) or contact your vendor directly.

Cray, Inc.

> *Cray, Inc. is not vulnerable since cachefs is not supported under Unicos and Unicos/mk.*

Fujitsu

> *UXP/V is not vulnerable, because it does not have Cachefs and similar functionalities.*

Hewlett-Packard

> *HP-UX is not vulnerable because it does not use cachefsd.*

IBM

> *IBM's AIX operating system, all versions, is not vulnerable.*

Nortel Networks

> *Nortel Networks products and solutions using the affected Sun Solaris operating systems do not utilize the NFS/RPC file system cachefs daemon. Nortel Networks recommends following the mitigating practices in Sun Microsystems Inc.'s Alert Notification.; this will not impact these Nortel Networks products and solutions.*
> *For more information please contact Nortel at:*
>
> > *North America: 1-8004NORTEL or 1-800-466-7835*
> > *Europe, Middle East and Africa: 00800 8008 9009, or +44 (0) 870 907 9009*
>
> *Contacts for other regions are available at*
>
> > *www.nortelnetworks.com/help/contact/global/*

SGI

> *SGI does not ship with SUN cachefsd, so IRIX is not vulnerable.*

Sun

> *See the Sun Alert Notification available at http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F44309.*

The CERT/CC acknowledges the Last Stage of Delirium Team for discovering and reporting on this vulnerability and thanks Sun Microsystems for their technical assistance.

Feedback can be directed to the authors:
Jason A. Rafail and Jeffrey S. Havrilla

Revision History

```
May 06, 2002:  Initial release
May 06, 2002:  Corrected CVE number and links
May 07, 2002:  Added Hewlett-Packard vendor statement
May 07, 2002:  Corrected credit statement
May 09, 2002:  Corrected credit statement
May 09, 2002:  Corrected CVE number and links
May 09, 2002:  Removed AusCERT Advisory
May 13, 2002:  Added Cray vendor statement
May 13, 2002:  Added Nortel Networks vendor statement
May 14, 2002:  Added Fujitsu vendor statement
```