

Cisco Security Advisory: Heap Overflow in Solaris cachefs Daemon

Document ID: 25718

Advisory ID: cisco-sa-20020724-solaris-cachefs

<http://www.cisco.com/warp/public/707/cisco-sa-20020724-solaris-cachefs.shtml>

Revision 1.1

Last Updated 2002 July 25 1600 UTC (GMT)

For Public Release 2002 July 24 1600 UTC (GMT)

Please provide your feedback on this document.

Summary
Affected Products
Details
Impact
Software Versions and Fixes
Workarounds
Obtaining Fixed Software
Exploitation and Public Announcements
Status of This Notice: INTERIM
Distribution
Revision History
Cisco Security Procedures

Summary

This advisory describes a vulnerability that affects Cisco products and applications that are installed on the Solaris operating system, and is based on the vulnerability of a common service within the Solaris operating system, not due to a defect of the Cisco product or application. A vulnerability in the "cachefs" program was discovered that enables an attacker to execute arbitrary code under Solaris OS. This vulnerability was publicly announced in the CERT Advisory CA-2002-11. All Cisco products and applications that are installed on Solaris OS are considered vulnerable to the underlying operating system vulnerability, unless the workaround was applied. This vulnerability is described in details in Sun(sm) Alert Notification at <http://sunsolve.sun.com/search/document.do?assetkey=1-26-44309-1>.

No other Cisco product is vulnerable.

Sun is working on a patch. Until the patch is released all affected customers are advised to apply the workaround described in the workaround section.

This advisory is available at
<http://www.cisco.com/warp/public/707/cisco-sa-20020724-solaris-cachefs.shtml>.

Cisco Security Advisory: Heap Overflow in Solaris cachefs Daemon

Affected Products

This section provides details on affected products.

Vulnerable Products

All products that are based on the following Solaris releases are affected:

- Solaris 2.5.1
- Solaris 2.6
- Solaris 7
- Solaris 8

The following products are affected:

- **Media Gateway Controller (MGC) and Related Products**

- ◆ Products running on Solaris 2.5.1 are vulnerable unless CSCOh013.pkg release 1.0(9) or later has been installed. The product that is based on this version of Solaris is Signaling Controller 2200 (SC2200).
- ◆ Products running on Solaris 2.6 are vulnerable unless CSCOh013.pkg release 1.0(9) or later has been installed. Products running on Solaris 8 are vulnerable unless CSCOh013.pkg release 2.0(2) or later has been installed. The products that are based on these versions of Solaris are:
 - ◇ SC2200
 - ◇ Cisco Virtual Switch Controller (VSC3000)
 - ◇ Cisco PGW2200 Public Switched Telephone Network (PSTN) Gateway
 - ◇ Cisco Billing and Management Server (BAMS)
 - ◇ Cisco Voice Services Provisioning Tool (VSPT)

- **Cisco Element Management Framework (CEMF) and Related Products**

All releases of CEMF are vulnerable. The related products are:

- ◆ Cisco 12000 Manager
- ◆ Cisco DSL Manager
- ◆ Element Manager Software for the Cisco 7200 and 7400 Series Routers
- ◆ Element Manager Software for the Catalyst 6500 Series & Cisco 7600 Series Routers
- ◆ Universal Gateway Manager
- ◆ Cisco Cable Manager
- ◆ Cisco Media Gateway Manager
- ◆ Cisco MGC (Media Gateway Controller) Node Manager

- **Cisco IP Manager**

All releases.

- **Cisco Secure ACS for Unix**

All releases.

Products Confirmed Not Vulnerable

The following products are not affected:

- BTS10200
- Cisco IDS

No other Cisco products are currently known to be affected by these vulnerabilities.

Cisco Security Advisory: Heap Overflow in Solaris cachefs Daemon

Details

This vulnerability is described in the following advisories/notifications:

- Sun Alert Notification at <http://sunsolve.sun.com/search/document.do?assetkey=1-26-44309-1> .
- CERT Advisory CA-2002-11 at <http://www.cert.org/advisories/CA-2002-11.html> .
- This issue is also being referenced as CAN-2002-0033 (see <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0033>).

A remotely exploitable heap overflow exists in the cachefsd program. It is installed by default on the Sun Solaris OS. Cachefsd caches requests for operations on remote file systems mounted via the use of NFS protocol. An attacker can send a crafted RPC request to the cachefsd program to exploit the vulnerability.

According to Sun Microsystems, failed attempts to exploit this vulnerability may leave a core dump file in the root directory. Note that the core file may be created by some other process and that its presence is not a certain sign of a compromise. Additionally, if the file /etc/cachefstab exists, it may contain entries other than a known cache directories (e.g., /cachefs/cache0).

Impact

It is possible to execute an arbitrary code on the vulnerable computer. That can lead to a full OS compromise where an attacker can gain root privileges.

Software Versions and Fixes

Sun Microsystem is working on a patch. Their latest status on this vulnerability is available at <http://sunsolve.sun.com/search/document.do?assetkey=1-26-44309-1> .

Workarounds

The workaround is applicable to all Cisco products mentioned in the advisory. For MGC and related products, if you have applied the script from CSC0013.pkg you are protected and you do not have to apply this workaround.

Comment out cachefsd in /etc/inetd.conf as shown below:

- For Solaris 2.6, 7 and 8:

```
#100235/1 tli rpc/tcp wait root /usr/lib/fs/cachefs/cachefsd cachefsd
```

- Solaris 2.5.1:

```
#100235/1 stream rpc/tcp wait root /usr/lib/fs/cachefs/cachefsd cachefsd
```

Once the line is commented out either:

- Reboot, or
- Send a HUP signal to inetd(1M) and kill existing cachefsd processes, for example, on Solaris 2.5.1 and 2.6 do the following:

```
$ kill -HUP <PID of inetd>
$ kill <PIDs of any cachefsd processes>
```

Cisco Security Advisory: Heap Overflow in Solaris cachefs Daemon

Solaris 7 and 8 do the following:

```
$ pkill -HUP inetd
$ pkill cachefsd
```

Obtaining Fixed Software

Cisco has made free software available to address this vulnerability for affected customers. Prior to deploying software, customers should consult their maintenance provider or check the software for feature set compatibility and known issues specific to their environment.

Customers may only install and expect support for the feature sets they have purchased. By installing, downloading, accessing or otherwise using such software upgrades, customers agree to be bound by the terms of Cisco's software license terms found at <http://www.cisco.com/public/sw-license-agreement.html>, or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact either "psirt@cisco.com" or "security-alert@cisco.com" for software upgrades.

Customers with Service Contracts

Customers with contracts should obtain upgraded software through their regular update channels. For most customers, this means that upgrades should be obtained through the Software Center on Cisco's worldwide website at <http://www.cisco.com>.

Customers using Third-party Support Organizations

Customers whose Cisco products are provided or maintained through prior or existing agreement with third-party support organizations such as Cisco Partners, authorized resellers, or service providers should contact that support organization for guidance and assistance with the appropriate course of action in regards to this advisory.

The effectiveness of any workaround or fix is dependent on specific customer situations such as product mix, network topology, traffic behavior, and organizational mission. Due to the variety of affected products and releases, customers should consult with their service provider or support organization to ensure any applied workaround or fix is the most appropriate for use in the intended network before it is deployed.

Customers without Service Contracts

Customers who purchase direct from Cisco but who do not hold a Cisco service contract and customers who purchase through third-party vendors but are unsuccessful at obtaining fixed software through their point of sale should get their upgrades by contacting the Cisco Technical Assistance Center (TAC). TAC contacts are as follows.

- +1 800 553 2447 (toll free from within North America)
- +1 408 526 7209 (toll call from anywhere in the world)
- e-mail: tac@cisco.com

Have your product serial number available and give the URL of this notice as evidence of your entitlement to a free upgrade. Free upgrades for non-contract customers must be requested through the TAC.

Refer to <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml> for additional TAC contact information, including special localized telephone numbers and instructions and e-mail addresses for use in various languages.

Exploitation and Public Announcements

According to CERT/CC the exploit program for this vulnerability is publicly available and there are credible reports that this vulnerability is actively being exploited.

Status of This Notice: INTERIM

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME. CISCO EXPECTS TO UPDATE THIS DOCUMENT AS NEW INFORMATION BECOMES AVAILABLE.

A stand-alone copy or Paraphrase of the text of this document that omits the distribution URL in the following section is an uncontrolled copy, and may lack important information or contain factual errors.

Distribution

This notice will be posted on Cisco's Worldwide Web site at <http://www.cisco.com/warp/public/707/cisco-sa-20020724-solaris-cachefs.shtml>. In addition to Worldwide Web posting, a text version of this notice is clear-signed with the Cisco PSIRT PGP key and is posted to the following e-mail and Usenet news recipients:

- cust-security-announce@cisco.com
- bugtraq@securityfocus.com
- first-teams@first.org (includes CERT/CC)
- cisco@spot.colorado.edu
- comp.dcom.sys.cisco
- firewalls@lists.gnac.com
- Various internal Cisco mailing lists

Future updates of this notice, if any, will be placed on Cisco's Worldwide Web server, but may or may not be actively announced on mailing lists or newsgroups. Users concerned about this problem are encouraged to check the URL given above for any updates.

Revision History

Revision 1.1	2002-July-25	Update to Details section
Revision 1.0	2002-July-24	Initial public release

Cisco Security Procedures

Complete information on reporting security vulnerabilities in Cisco products, obtaining assistance with security incidents, and registering to receive security information from Cisco, is available on Cisco's

Worldwide Web site at http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html.
This includes instructions for press inquiries regarding Cisco security notices.

All Cisco Security Advisories are available at <http://www.cisco.com/go/psirt>.

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: May 03, 2007

Document ID: 25718
