

Cisco Security Advisory: Cisco Unified Communications Manager CAPF Denial of Service Vulnerability

Advisory ID: cisco-sa-20090121-cucmcapf

<http://www.cisco.com/warp/public/707/cisco-sa-20090121-cucmcapf.shtml>

Revision 1.0

For Public Release 2009 January 21 1600 UTC (GMT)

Please provide your [feedback](#) on this document.

Contents

[Summary](#)

[Affected Products](#)

[Details](#)

[Vulnerability Scoring Details](#)

[Impact](#)

[Software Versions and Fixes](#)

[Workarounds](#)

[Obtaining Fixed Software](#)

[Exploitation and Public Announcements](#)

[Status of this Notice: FINAL](#)

[Distribution](#)

[Revision History](#)

[Cisco Security Procedures](#)

Summary

Cisco Unified Communications Manager, formerly Cisco CallManager, contains a denial of service (DoS) vulnerability in the Certificate Authority Proxy Function (CAPF) service. Exploitation of this vulnerability could cause an interruption in voice services. The CAPF service is disabled by default.

Cisco has released free software updates that address this vulnerability. Workarounds available that mitigate this vulnerability are available.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090121-cucmcapf.shtml>.

[\[Expand all sections\]](#) [\[Collapse all sections\]](#)

☐ Affected Products

☐ Vulnerable Products

These products are vulnerable:

- Cisco Unified Communications Manager 5.x versions prior to 5.1(3e)
- Cisco Unified Communications Manager 6.x versions prior to 6.1(3)

Administrators of systems that are running Cisco Unified Communications Manager versions 5.x and 6.x can determine the software version by viewing the main page of the Cisco Unified Communications Manager Administration interface. The software version can also be determined by running the command **show version active** by way of the command line interface (CLI).

☐ Products Confirmed Not Vulnerable

Cisco Unified Communications Manager version 4.x and Cisco Unified Communications Manager Express are not affected by this vulnerability. No other Cisco products are currently known to be affected by this vulnerability.

Note: Cisco Unified Communications Manager 7.0(1) shipped with the software fix for this vulnerability and is not affected.

☐ Details

The CAPF service of Cisco Unified Communications Manager versions 5.x and 6.x contain a vulnerability when handling malformed input that may result in a DoS condition. The CAPF service is disabled by default; however, if it is enabled, the CAPF service listens by default on TCP port 3804 and the listening port is configurable by the user. There is a workaround for this vulnerability. This vulnerability is fixed in Cisco Unified Communications Manager versions 5.1(3e) and 6.1(3). This vulnerability is documented in Cisco Bug ID CSCsq32032 and has been assigned Common Vulnerabilities and Exposures (CVE) identifier CVE-2009-0057.

☐ Vulnerability Scoring Details

Cisco has provided scores for the vulnerabilities in this advisory based on the Common Vulnerability Scoring System (CVSS). The CVSS scoring in this Security Advisory is done in accordance with CVSS version 2.0.

CVSS is a standards-based scoring method that conveys vulnerability severity and helps determine urgency and priority of response.

Cisco has provided a base and temporal score. Customers can then compute environmental scores to assist in determining the impact of the vulnerability in individual networks.

Cisco has provided an FAQ to answer additional questions regarding CVSS at:

<http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html>

Cisco has also provided a CVSS calculator to help compute the environmental impact for individual networks at:

<http://intellishield.cisco.com/security/alertmanager/cvss>

CSCsq32032 - CAPF DoS when client terminates prematurely (registered customers only)

Calculate the environmental score of CSCsq32032

CVSS Base Score - 7.8

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete

CVSS Temporal Score - 6.4

Exploitability	Remediation Level	Report Confidence
Functional	Official-Fix	Confirmed

[Top of the section](#) [Close Section](#)

[-] **Impact**

Successful exploitation of the vulnerability described in this advisory may result in the interruption of voice services.

[Top of the section](#) [Close Section](#)

[-] **Software Versions and Fixes**

When considering software upgrades, also consult <http://www.cisco.com/go/psirt> and any subsequent advisories to determine exposure and a complete upgrade solution.

In all cases, customers should exercise caution to be certain the devices to be upgraded contain sufficient memory and that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, contact the Cisco Technical Assistance Center (TAC) or your contracted maintenance provider for assistance.

Cisco Unified Communications Manager version 5.1(3e) contains the fix for this vulnerability and can be downloaded here:

<http://tools.cisco.com/support/downloads/go/ReleaseType.x?>

[optPlat=null&isPlatform=Y&mdfid=280735907&sftType=Unified%20Communications%20Manager%20Updates&treeName=Voice%20and%20Unified%20Communications&modelName=Cisco%20Unified%20Communications%20Manager%20Version%205.1&mdfLevel=Software%20Version/Option&treeMdfId=278875240&modifmdfid=null&imname=null&hybrid=Y&imst=N](http://tools.cisco.com/support/downloads/go/PlatformList.x?sftType=Unified%20Communications%20Manager%20Updates&mdfid=280735907&treeName=Voice%20and%20Unified%20Communications&modelName=Cisco%20Unified%20Communications%20Manager%20Version%205.1&mdfLevel=Software%20Version/Option&treeMdfId=278875240&modifmdfid=null&imname=null&hybrid=Y&imst=N) ([registered customers only](#))

Cisco Unified Communications Manager version 6.1(3) contains the fix for this vulnerability can downloaded here:

<http://tools.cisco.com/support/downloads/go/PlatformList.x?sftType=Unified%20Communications%20Manager%20Updates&mdfid=281023410&treeName=Voice%20and%20Unified%20Communications&mdfLevel=Software%20Version/Option&url=null&modelName=Cisco%20Unified%20Communications%20Manager%20Version%206.1&isPlatform=N&treeMdfId=278875240&modifmdfid=null&imname=null&hybrid=Y&imst=N> ([registered customers only](#))

[Top of the section](#) [Close Section](#)

☐ Workarounds

To mitigate against this vulnerability, system administrators can disable the CAPF service if it is not necessary for business operations. Access to the CAPF service is only required if Cisco Unified Communications Manager systems and IP phone devices are configured to use certificates for a secure deployment. If phones are not configured to use certificates, then the CAPF service can be disabled. The CAPF service is controlled by the *Cisco Certificate Authority Proxy Function* menu selection.

It is possible to mitigate the CAPF vulnerability by implementing filtering on screening devices if the CAPF service is required. If the CAPF service is enabled, allow access to TCP port 3804 only from networks that contain IP phone devices that require the CAPF service. The CAPF port is user configurable, and if modified, filtering on screening devices should be based on the TCP port that is used.

For Cisco Unified Communications Manager 5.x and 6.x systems, please consult the following documentation for details on how to disable Cisco Unified Communications Manager services:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/service/5_0_1/ccmsrva/sasrvact.html#wp1048220

Additional mitigation techniques that can be deployed on Cisco devices within the network are available in the Cisco Applied Mitigation Bulletin companion document for this advisory:

<http://www.cisco.com/warp/public/707/cisco-amb-20090121-cucmcapf.shtml>

[Top of the section](#) [Close Section](#)

☐ **Obtaining Fixed Software**

Cisco has released free software updates that address these vulnerabilities. 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/en/US/docs/general/warranty/English/EU1KEN_.html, or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml> .

Do not contact 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 agreements 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 do not hold a Cisco service contract, and customers who purchase through third-party vendors but are unsuccessful in obtaining fixed software through their point of sale should acquire 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

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

Refer to http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html for additional TAC contact information, including localized telephone numbers, and instructions and e-mail addresses for use in various languages.

[Top of the section](#) [Close Section](#)

☐ Exploitation and Public Announcements

The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerability described in this advisory.

This vulnerability was reported to Cisco by VoIPshield.

[Top of the section](#) [Close Section](#)

☐ Status of this Notice: FINAL

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.

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.

[Top of the section](#) [Close Section](#)

☐ **Distribution**

This advisory is posted on Cisco's worldwide website at :

<http://www.cisco.com/warp/public/707/cisco-sa-20090121-cucmcapf.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
- first-bulletins@lists.first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk
- comp.dcom.sys.cisco@newsgate.cisco.com

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

[Top of the section](#) [Close Section](#)

☐ **Revision History**

Revision 1.0	2009-January-21	Initial public release
--------------	-----------------	------------------------

[Top of the section](#) [Close Section](#)

☐ **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 website 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>.

[Top of the section](#) [Close Section](#)

Help us help you.

Please rate this document.

- Excellent
- Good
- Average
- Fair
- Poor

This document solved my problem.

- Yes
- No
- Just browsing

Suggestions for improvement:

(256 character limit)



[Home](#)

[How to Buy](#)

[Login](#)

[Profile](#)

[Feedback](#)

[Site Map](#)

[Help](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 - 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) |

[Trademarks of Cisco Systems, Inc.](#)