

Cisco Security Advisory: Cisco Unified Communications Manager Denial of Service Vulnerabilities

Advisory ID: cisco-sa-20080514-cucmdos

<http://www.cisco.com/warp/public/707/cisco-sa-20080514-cucmdos.shtml>

Revision 1.0

For Public Release 2008 May 14 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 multiple denial of service (DoS) vulnerabilities that may cause an interruption in voice services, if exploited. These vulnerabilities were discovered internally by Cisco. The following Cisco Unified Communications Manager services are affected:

- Certificate Trust List (CTL) Provider
- Certificate Authority Proxy Function (CAPF)
- Session Initiation Protocol (SIP)
- Simple Network Management Protocol (SNMP) Trap

Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate some of these vulnerabilities are available.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080514-cucmdos.shtml>.

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

☐ Affected Products

☐ Vulnerable Products

These products are vulnerable:

- Cisco Unified CallManager 4.1 versions prior to 4.1.3SR7
- Cisco Unified Communications Manager 4.2 versions prior to 4.2(3)SR4
- Cisco Unified Communications Manager 4.3 versions prior to 4.3(2)
- Cisco Unified Communications Manager 5.x versions prior to 5.1(3)
- Cisco Unified Communications Manager 6.x versions prior to 6.1(1)

Administrators of systems running Cisco Unified Communications Manager version 4.x can determine the software version by navigating to **Help > About Cisco Unified CallManager** and selecting the **Details** button via the Cisco Unified Communications Manager Administration interface.

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** via the command line interface (CLI).

☐ **Products Confirmed Not Vulnerable**

Cisco Unified Communications Manager Express is not affected by these vulnerabilities. No other Cisco products are currently known to be affected by these vulnerabilities.

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

☐ **Details**

Cisco Unified Communications Manager is the call processing component of the Cisco IP Telephony solution that extends enterprise telephony features and functions to packet telephony network devices, such as IP phones, media processing devices, voice-over-IP (VoIP) gateways, and multimedia applications.

Certificate Trust List Provider Related Vulnerabilities

The Certificate Trust List (CTL) Provider service of Cisco Unified Communications Manager version 5.x contains a memory consumption vulnerability that occurs when a series of malformed TCP packets are received by a vulnerable Cisco Unified Communications Manager system and may result in a DoS condition. The CTL Provider service listens by default on TCP port 2444 and is user configurable. The CTL Provider service is enabled by default. There is a workaround for this vulnerability. The vulnerability is fixed in Cisco Unified Communications Manager version 5.1(3). The vulnerability is documented in Cisco Bug ID [CSCsj80609](#) ([registered](#) customers only) and has been assigned the CVE identifier [CVE-2008-1742](#).

The CTL Provider service of Cisco Unified Communications Manager versions 5.x and 6.x contain a memory consumption vulnerability that occurs when a series of malformed TCP packets are received by a vulnerable Cisco Unified Communications Manager system and may result in a DoS condition. The CTL Provider service listens by default on TCP port 2444 and is user configurable. There is a workaround for this vulnerability. The vulnerability is fixed in Cisco Unified Communications Manager versions 5.1(3) and 6.1(1). This vulnerability is documented in Cisco Bug ID [CSCsi98433](#) ([registered](#) customers only) and has been assigned the CVE identifier [CVE-2008-1743](#).

Certificate Authority Proxy Function Related Vulnerability

The Certificate Authority Proxy Function (CAPF) service of Cisco Unified Communications Manager versions 4.1, 4.2 and 4.3 contain a vulnerability when handling malformed input that may result in a DoS condition. The CAPF service listens by default on TCP port 3804 and is user configurable. The CAPF service is disabled by default. There is a workaround for this vulnerability. This vulnerability is fixed in Cisco Unified Communications Manager versions 4.1(3)SR7, 4.2(3)SR4 and 4.3(2). This vulnerability is documented in Cisco Bug ID [CSCsk46770](#) ([registered](#) customers only) and has been assigned the CVE identifier [CVE-2008-1744](#).

SIP-Related Vulnerabilities

Cisco Unified Communications Manager versions 5.x and 6.x contain a vulnerability in the handling of malformed SIP JOIN messages that may result in a DoS condition. SIP processing cannot be disabled in Cisco Unified Communications Manager. There is no workaround for this vulnerability. This vulnerability is fixed in Cisco Unified Communications Manager versions 5.1(2) and 6.1(1). This vulnerability is documented in Cisco Bug ID [CSCsi48115](#) ([registered](#) customers only) and has been assigned the CVE identifier [CVE-2008-1745](#).

Cisco Unified Communications Manager versions 4.1, 4.2, 4.3, 5.x and 6.x contain a vulnerability in the handling of SIP INVITE messages that may result in a DoS condition. SIP processing cannot be disabled in Cisco Unified Communications Manager. There is no workaround for this vulnerability. Cisco Unified Communications Manager version 4.x systems not configured to use SIP are not vulnerable. The vulnerability is fixed in Cisco Unified Communications Manager versions 4.1(3)SR6, 4.2(3)SR3, 4.3(2), 5.1(3) and 6.1(1). This vulnerability is documented in Cisco Bug ID [CSCsk46944](#) ([registered](#) customers only) and has been assigned the CVE identifier [CVE-2008-1747](#).

Cisco Unified Communications Manager versions 4.1, 4.2, 4.3, 5.x and 6.x contain a vulnerability in the handling of SIP INVITE messages that may result in a DoS condition. SIP processing cannot be disabled in Cisco Unified Communications Manager. There is no workaround for this vulnerability. Cisco Unified Communications Manager version 4.x systems not configured to use SIP are not vulnerable. This vulnerability is fixed in Cisco Unified Communications Manager versions 4.1(3)SR7, 4.2(3)SR4, 4.3(2), 5.1(3) and 6.1(1). This vulnerability is documented in Cisco Bug ID [CSCsl22355](#) ([registered](#) customers only) and has been assigned the CVE identifier [CVE-2008-1748](#).

SNMP Trap-Related Vulnerability

The SNMP Trap Agent service of Cisco Unified Communications Manager versions 4.1, 4.2, 4.3, 5.x and 6.x contain a vulnerability that occurs when a series of malformed UDP packets are received by a vulnerable Cisco Unified Communications Manager system and may result in a DoS condition. The SNMP Trap Agent service listens by default on UDP port 61441. There is a workaround for this vulnerability. This vulnerability is fixed in Cisco Unified Communications Manager versions 4.1(3)SR6, 4.2(3)SR3, 4.3(2), 5.1(3) and 6.1(1). This vulnerability is documented in Cisco Bug ID

[CSCsj24113](#) ([registered](#) customers only) and has been assigned the CVE identifier [CVE-2008-1746](#).

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

☐ 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> .

CSCsj80609 - Memory Leak Due to TCPFUZZ on Port 2444

(CTLProvider) ([registered](#) customers only)

Calculate the environmental score of [CSCsj80609](#)

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
------------	--------------	-----------

CSCsi98433 - CTLProvider leaks memory in certain scenarios (registered customers only)

Calculate the environmental score of CSCsi98433

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

CSCsk46770 - CAPF crash with network traffic (registered customers only)

Calculate the environmental score of CSCsk46770

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

CSCsi48115 - CM 6.1 stops providing service when receiving malformed Join sip-header (registered customers only)

Calculate the environmental score of CSCsi48115

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	

CSCsk46944 - CCM service restarts on receiving a valid SIP Packet
(registered customers only)

Calculate the environmental score of CSCsk46944

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	

CSCsl22355 - CCM does not validate SIP URL input properly (registered
customers only)

Calculate the environmental score of CSCsl22355

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

CSCsj24113 - CCM Process Coredump/Restart During ISIC Execution
Against Port 61441 (registered customers only)

Calculate the environmental score of CSCsj24113

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 vulnerabilities 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 CallManager version 4.1(3)SR7 contains fixes for all vulnerabilities affecting Cisco Unified CallManager version 4.1 listed in this advisory. It can be downloaded at the following link:

<http://www.cisco.com/cgi-bin/tablebuild.pl/callmgr-41?psrtdcat20e2>

Cisco Unified Communications Manager version 4.2(3)SR4 contains fixes for all vulnerabilities affecting Cisco Unified Communications Manager version 4.2 listed in this advisory and is scheduled to be released in early June, 2008. It will be available for download at the following link:

<http://www.cisco.com/cgi-bin/tablebuild.pl/callmgr-42?psrtdcat20e2>

Cisco Unified Communications Manager version 4.3(2) contains fixes for all vulnerabilities affecting Cisco Unified Communications Manager version 4.2 listed in this advisory. It can be downloaded at the following link:

<http://www.cisco.com/cgi-bin/tablebuild.pl/callmgr-43?psrtdcat20e2>

Cisco Unified Communications Manager version 5.1(3) contains fixes for all vulnerabilities affecting Cisco Unified Communications Manager version 5.x listed in this advisory. It can be downloaded at the following link:

<http://www.cisco.com/cgi-bin/tablebuild.pl/callmgr-51?psrtdcat20e2>

Cisco Unified Communications Manager version 6.1(1) contains fixes for all vulnerabilities affecting Cisco Unified Communications Manager version 6.x listed in this advisory. It can be downloaded at the following link:

<http://www.cisco.com/cgi-bin/tablebuild.pl/callmgr-61?psrtdcat20e2>

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

☐ Workarounds

CTL Provider Related Vulnerabilities

To mitigate against the CTL Provider service vulnerabilities (CSCsj80609 and CSCsi98433), system administrators can disable the CTL Provider service if it is not needed. Access to the CTL Provider Service is usually only required during the initial configuration of Cisco Unified Communications Manager authentication and encryption features. The CTL Provider service is controlled via the *Cisco CTL Provider* menu selection.

It is possible to mitigate the CTL Provider vulnerabilities by implementing filtering on screening devices. If the CTL Provider service is enabled, permit access to TCP port 2444 only between the Cisco Unified Communications Manager systems where the CTL Provider service is active and the CTL Client, usually on the administrator's workstation, to mitigate the CTL Provider service overflow.

Note: It is possible to change the default port of the CTL Provider service (TCP port 2444). If changed, filtering should be based on the values used. The values of the ports can be viewed in Cisco Unified Communications Manager Administration interface by following the **System > Service Parameters** menu and selecting the appropriate service.

CAPF Related Vulnerability

To mitigate against the CAPF service vulnerability (CSCsk46770), system administrators can disable the CAPF service if it is not needed. 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 enabled, permit access to TCP port 3804 only from networks that contain IP phone devices needing to utilize the CAPF service.

SIP-Related Vulnerabilities

It is possible to mitigate the SIP vulnerabilities by implementing filtering on screening devices. Permit TCP/UDP access to ports 5060 and 5061 from only networks that need SIP access to Cisco Unified Communications Manager servers.

SNMP Trap-Related Vulnerability

To mitigate against the SNMP Trap service vulnerability (CSCsj24113), system administrators can disable the SNMP Trap service. For Cisco Unified Communications Manager 4.x systems, the SNMP Trap service is controlled by the embedded Windows SNMP service. To disable the Windows SNMP service, navigate to **Start > Programs > Administrative Tools > Services**, and stop the **SNMP Service**.

Note: The SNMP Trap Service listed in the Windows Service configuration screen is not applicable to this vulnerability and disabling it does not provide any benefit as a workaround for this vulnerability. For Cisco Unified Communications Manager 5.x and 6.x systems, the SNMP Trap

service is controlled via the **Cisco CallManager SNMP Service** selection on the Control Center Feature Services screen.

It is possible to mitigate the SNMP Trap service vulnerability by implementing filtering on screening devices. Permit access to UDP port 61441 only from management systems that need access to the SNMP Trap service.

For Cisco Unified Communications Manager 4.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/4_2_3/ccmsrva/sasrvact.html

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-20080514-cucmdos.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/warp/public/687/Directory/DirTAC.shtml> 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 vulnerabilities described in this advisory.

These vulnerabilities were discovered internally by Cisco.

[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-20080514-cucmdos.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-teams@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	2008-May-14	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.](#)