

Cisco Security Advisory: Cisco Unified Communications Manager Session Initiation Protocol Denial of Service Vulnerability

Advisory ID: cisco-sa-20090923-cm

<http://www.cisco.com/warp/public/707/cisco-sa-20090923-cm.shtml>

Revision 1.0

For Public Release 2009 September 23 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, which was formerly Cisco Unified CallManager, contains a denial of service (DoS) vulnerability in the Session Initiation Protocol (SIP) service. An exploit of this vulnerability may cause an interruption in voice services.

Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090923-cm.shtml>.

Note: Cisco IOS® Software is also affected by the vulnerability described in this advisory. A companion advisory for Cisco IOS software is available at <http://www.cisco.com/warp/public/707/cisco-sa-20090923-sip.shtml>.

Note: The September 23, 2009, Cisco IOS Security Advisory bundled publication includes eleven Security Advisories. Ten of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses a vulnerability in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory.

Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Advisory Bundled Publication" at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep09.html

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

☐ Affected Products

The vulnerability described in this document applies to the Cisco Unified Communications Manager.

☐ Vulnerable Products

The following Cisco Unified Communications Manager versions are affected:

- Cisco Unified Communications Manager 5.x versions prior to 5.1(3g)
- Cisco Unified Communications Manager 6.x versions prior to 6.1(4)

- Cisco Unified Communications Manager 7.0.x versions prior to 7.0(2a)su1
- Cisco Unified Communications Manager 7.1.x versions prior to 7.1(2)

Cisco Unified CallManager versions 4.x are not affected by this vulnerability. Administrators of systems that are running Cisco Unified Communications Manager versions 5.x, 6.x and 7.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 **show version active** command via the command-line interface.

A SIP trunk must be configured for the Cisco Unified CallManager server to begin listening for SIP messages on TCP and UDP port 5060 and TCP/5061. However, in Cisco Unified Communications Manager versions 5.x and later, the use of SIP as a call signaling protocol is enabled by default and cannot be disabled.

Cisco IOS Software is also affected by this vulnerability, but it is associated with different Cisco bug IDs. A companion security advisory for Cisco IOS Software is available at: <http://www.cisco.com/warp/public/707/cisco-sa-20090923-sip.shtml>

☐ **Products Confirmed Not Vulnerable**

Cisco Unified CallManager versions 4.x are not affected by this vulnerability. With the exception of Cisco IOS software, no other Cisco products are currently known to be affected by this vulnerability.

[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 gateways, and multimedia applications.

SIP is a popular signaling protocol that manages voice and video calls across IP networks such as the Internet. SIP is responsible for handling all aspects of call setup and termination. Voice and video are the most popular types of sessions that SIP handles, but the protocol is flexible enough to accommodate other applications that require call setup and termination. SIP call signaling can use UDP (port 5060), TCP (port 5060), or Transport Layer Security (TLS; TCP port 5061) as the underlying transport protocol.

A DoS vulnerability exists in the SIP implementation of the Cisco Unified Communications

Manager. This vulnerability could be triggered when Cisco Unified Communications Manager processes crafted SIP messages. An exploit could lead to a reload of the main Cisco Unified Communications Manager process.

This vulnerability is documented in Cisco bug ID [CSCsz95423](#) ([registered](#) customers only) and has been assigned Common Vulnerabilities and Exposures (CVE) ID CVE-2009-2864.

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

☐ Vulnerability Scoring Details

Cisco has provided scores for the vulnerability 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>.

CSCsz95423 - Crafted SIP packet may cause CM process to crash

Calculate the environmental score of [CSCsz95423](#)

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 that is described in this advisory could result in a reload of the Cisco Unified Communications Manager process, which 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.

The following table contains the first fixed software release for this vulnerability. A device running a version of the given release in a specific row (less than the First Fixed Release) is known to be vulnerable.

Release	First Fixed Version
4.x	Not Vulnerable
5.x	5.1(3g)
6.x	6.1(4)
7.0.x	7.0(2a)su1
7.1.x	7.1(2)

☐ Workarounds

There are no workarounds for this vulnerability.

It is possible to mitigate this vulnerability by implementing filtering on screening devices and permitting TCP/UDP access to ports 5060 and TCP/5061 only from networks that require SIP access to Cisco Unified Communications Manager servers.

If Cisco Unified Communications Manager does not need to provide SIP services, administrators can configure the Cisco Unified Communications Manager to listen for SIP messages on non standard ports. Use the following instructions to change the ports from their default values:

Step 1 Log into the Cisco Unified CallManager Administration web interface.

Step 2 Navigate to **System > Cisco Unified CM** and locate the appropriate Cisco Unified Communications Manager.

Step 3 Change the fields **SIP Phone Port** and **SIP Phone Secure Port** fields to a non standard port and click **Save**.

SIP Phone Port, which is 5060 by default, refers to the TCP and UDP ports where the Cisco Unified Communications Manager listens for normal SIP messages, and SIP Phone Secure Port, by default 5061, refers to the TCP port where the Cisco Unified Communications Manager listens for SIP over TLS messages. For additional information about this procedure, refer to the "Updating a Cisco Unified Communications Manager" section of the "Cisco Unified Communications Manager Administration Guide" at http://www.cisco.com/en/US/docs/voice_ip_comm/cucmbe/admin/7_0_1/ccmcfg/b02ccm.html#wp1057513.

Note: For a SIP port change to take effect, the Cisco CallManager Service must be restarted. For information on how to restart the service, refer to the "Restarting the Cisco CallManager Service" section of the document at http://www.cisco.com/en/US/docs/voice_ip_comm/cucmbe/admin/7_0_1/ccmcfg/b03dpi.html#wp1075124.

Additional mitigations that can be deployed on Cisco devices in the network are available in the companion document "Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Denial of Service Vulnerabilities in Cisco Unified Communications Manager and Cisco IOS Software", which is available at the following location: <http://www.cisco.com/warp/public/707/cisco-amb-20090923-voice.shtml>.

☐ **Obtaining Fixed Software**

Cisco has released free software updates that address this vulnerability. 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 discovered during internal testing.

[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-20090923-cm.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-September-23	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>.

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](#)