

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

Advisory ID: cisco-sa-20080924-cucm

<http://www.cisco.com/warp/public/707/cisco-sa-20080924-cucm.shtml>

Revision 1.1

Last Updated 2008 April 09 1500 UTC (GMT)

For Public Release 2008 September 24 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](#)

Summary

Cisco Unified Communications Manager, formerly Cisco Unified CallManager, contains two denial of service (DoS) vulnerabilities in the Session Initiation Protocol (SIP) service. An exploit of these vulnerabilities may cause an interruption in voice services.

Cisco will release free software updates that address these vulnerabilities and this advisory will be updated as fixed software becomes available. There are no workarounds for these vulnerabilities.

Note: Cisco IOS software is also affected by the vulnerabilities described in this advisory. A companion advisory for Cisco IOS software is available at <http://www.cisco.com/warp/public/707/cisco-sa-20080924-sip.shtml>.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080924-cucm.shtml>.

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

☐ Affected Products

The vulnerabilities described in this document apply to the Cisco Unified Communications Manager.

☐ Vulnerable Products

The following Cisco Unified Communications Manager versions are affected:

- Cisco Unified CallManager 4.1 versions prior to 4.1.3SR8
- Cisco Unified CallManager 4.2 versions prior to 4.2(3)SR4b
- Cisco Unified CallManager 4.3 versions prior to 4.3(2)SR1a
- Cisco Unified Communications Manager 5.x versions prior to 5.1(3d)
- Cisco Unified Communications Manager 6.x versions prior to 6.1(2)su1

Administrators of systems running Cisco Unified CallManager 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.

In Cisco Unified CallManager version 4.x, the use of SIP as a call signaling protocol is *not enabled* by default, and for the Cisco Unified CallManager server to start listening for SIP messages on TCP and UDP ports 5060 and 5061 a SIP trunk needs to be configured.

In Cisco Unified Communications Manager versions 5.x and later, the use of SIP as a call signaling protocol is enabled by default in Cisco Unified Communications Manager and cannot be disabled.

Cisco IOS software is also affected by these vulnerabilities, although they are tracked by different Cisco bug IDs. A companion security advisory for Cisco IOS software is available at <http://www.cisco.com/warp/public/707/cisco-sa-20080924-sip.shtml>.

☐ **Products Confirmed Not Vulnerable**

With the exception of Cisco IOS software, no other Cisco products are currently known to be vulnerable to the issues described in this advisory.

Cisco Unified Communications Manager version 7.x is not affected by these vulnerabilities.

Cisco Unified CallManager version 4.x is not affected by these vulnerabilities if it does not have any SIP trunks configured.

[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 is used to manage 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 to accommodate for other applications that require call setup and termination. SIP call signaling can

use UDP (port 5060), TCP (port 5060), or TLS (TCP port 5061) as the underlying transport protocol.

Two DoS vulnerabilities exist in the SIP implementation of the Cisco Unified Communications Manager. These vulnerabilities can be triggered while processing specific and valid SIP messages and can lead to a reload of the main Cisco Unified Communications Manager process.

Version 4.x of Cisco Unified CallManager does not have SIP enabled by default unless a SIP trunk is configured. Versions 5.x and later of the Cisco Unified Communications Manager have SIP enabled by default and cannot be disabled.

The vulnerabilities are being tracked by the following Cisco bug IDs:

- [CSCsu38644](#) ([registered](#) customers only) , assigned CVE ID CVE-2008-3800
- [CSCsm46064](#) ([registered](#) customers only) , assigned CVE ID CVE-2008-3801

[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>.

CSCsu38644

Calculate the environmental score of CSCsu38644

CVSS Base Score - **7.1**

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

CVSS Temporal Score - **5.9**

Exploitability	Remediation Level	Report Confidence
Functional	Official-Fix	Confirmed

CSCsm46064

Calculate the environmental score of CSCsm46064

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

Major Release	First Fixed Release	Recommended Release
4.1.x	4.1(3)SR8	4.1(3)SR8a
4.2.x	4.2(3)SR4b	4.2(3)SR4b
4.3.x	4.3(2)SR1a	4.3(2)SR1b
5.1.x	5.1(3d)	5.1(3e)
6.1.x	6.1(2)SU1	6.1(3b)SU1

Downloading Cisco Unified Communications Manager Software

To download Cisco Unified Communications Manager Software go to the Voice Software Downloads section of the Software Center on cisco.com at <http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=278875240>, then navigate to **IP Telephony > Call Control > Cisco Unified Communications Manager (CallManager)** and select the appropriate version of Cisco Unified Communications Manager.

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

☐ Workarounds

There are no workarounds for these vulnerabilities.

It is possible to mitigate the 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.

If the Cisco Unified Communications Manager does not need to provide SIP services, the ports on which the Cisco Unified Communications Manager listens for SIP messages can be moved to non-standard ports. To change the ports from their default values, log into the Cisco Unified CallManager Administration web interface, go to **System > Cisco Unified CM**, locate the appropriate Cisco Unified Communications Manager, change the fields **SIP Phone Port** and **SIP Phone Secure Port** to a non-standard port, then click **Save**. **SIP Phone Port**, by default 5060, 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 and UDP ports 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 change of the SIP ports to take effect, the Cisco CallManager Service needs to be restarted. For information on how to accomplish this, refer to "Restarting the Cisco CallManager Service" 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 within the network are available in the Cisco Applied Mitigation Bulletin companion document for this advisory, which is available at the following link: <http://www.cisco.com/warp/public/707/cisco-amb-20080924-sip.shtml>.

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

☐ **Obtaining Fixed Software**

Cisco will release free software updates that address these vulnerabilities and this advisory will be updated as fixed software becomes available. 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.

☐ **Exploitation and Public Announcements**

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

These vulnerabilities were discovered by Cisco internal testing and during handling of customer service requests.

[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-20080924-cucm.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 1.1	2009-April-09	Updated table of fixed software to indicate fixed software availability and current recommended releases. Changed advisory status from <i>INTERIM</i> to <i>FINAL</i> .
Revision 1.0	2008-September-24	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.](#)