

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

Advisory ID: [cisco-sa-20090826-cucm](#)

<http://www.cisco.com/warp/public/707/cisco-sa-20090826-cucm.shtml>

Revision 1.0

For Public Release 2009 August 26 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 CallManager) contains multiple denial of service (DoS) vulnerabilities that if exploited could cause an interruption to voice services. The Session Initiation Protocol (SIP) and Skinny Client Control Protocol (SCCP) services are affected by these vulnerabilities.

Cisco has released free software updates for select Cisco Unified Communications Manager versions that address these vulnerabilities. There are no workarounds for these vulnerabilities.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090826-cucm.shtml>.

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

☐ **Affected Products**

☐ **Vulnerable Products**

The following products are affected by vulnerabilities described in this advisory:

- Cisco Unified Communications Manager 4.x
- Cisco Unified Communications Manager 5.x
- Cisco Unified Communications Manager 6.x
- Cisco Unified Communications Manager 7.x

☐ **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, VoIP gateways, and multimedia applications.

Malformed SIP Message Vulnerabilities

Cisco Unified Communications Manager contains two DoS vulnerabilities that involve the processing of SIP packets. Each vulnerability is triggered by a malformed SIP message that could cause a critical process to fail, resulting in the disruption of voice services. All SIP ports (TCP 5060 and 5061, UDP 5060 and 5061) are affected by these vulnerabilities.

The first SIP DoS vulnerability is documented in Cisco Bug ID CSCsi46466 and has been assigned the CVE identifier CVE-2009-2050. The first vulnerability is fixed in Cisco Unified Communications Manager versions 6.1(1) and later.

Cisco Unified Communications Manager 4.x versions are only affected by the first SIP DoS vulnerability if a SIP trunk is explicitly configured. To determine if a SIP trunk is configured on a Cisco Unified Communications Manager version 4.x system, navigate to **Device > Trunk** and choose the option **SIP Trunk** in the Cisco Unified Communications Manager administration interface. To mitigate against this vulnerability, administrators are advised to restrict access to TCP

and UDP port 5060 on vulnerable Cisco Unified Communications Manager 4.x systems that are configured to use SIP trunks with screening devices to valid SIP trunk end points.

The second SIP DoS vulnerability is documented in Cisco Bug ID CSCsz40392 and has been assigned the CVE identifier CVE-2009-2051. The second vulnerability is fixed in Cisco Unified Communications Manager versions 5.1(3g), 6.1(4), and 7.1(2).

Network Connection Tracking Vulnerability

Cisco Unified Communications Manager contains a DoS vulnerability that involves the tracking of network connections by the embedded operating system firewall. By establishing many TCP connections with a vulnerable system, an attacker could overwhelm the operating system table that is used to track network connections and prevent new connections from being established to system services. Any service that listens to a TCP port on a vulnerable system could be affected by this vulnerability, including SIP and SCCP.

This vulnerability is documented in Cisco Bug ID CSCsq22534 and has been assigned the CVE identifier CVE-2009-2052. The vulnerability is fixed in Cisco Unified Communications Manager versions 5.1(3g), 6.1(4), 7.0(2), and 7.1(2).

Related SIP and SCCP DoS Vulnerabilities

Cisco Unified Communications Manager contains two DoS vulnerabilities involving the processing of SIP and SCCP packets. By flooding a vulnerable system with many TCP packets, an attacker could exhaust operating system file descriptors that cause the SIP port (TCP 5060 and 5061) and SCCP port (TCP 2000 and 2443) to close. This action could prevent new connections from being established to the SIP and SCCP services. SIP UDP (5060 and 5061) ports are not affected.

The SCCP vulnerability is documented in Cisco Bug ID CSCsx32236 and has been assigned the CVE identifier CVE-2009-2053. The SCCP vulnerability is fixed in Cisco Unified Communications Manager versions 5.1(3g), 6.1(4), 7.0(2a)su1, and 7.1(2).

The SIP vulnerability is documented in Cisco Bug ID CSCsx23689 and has been assigned the CVE identifier CVE-2009-2054. The SIP vulnerability is fixed in Cisco Unified Communications Manager versions 5.1(3g), 6.1(4), 7.0(2a)su1, and 7.1(2a)su1.

[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>.

CSCsi46466 - CM 6.1 SDL router services dead when receiving abnormal SIP header (registered customers only)					
Calculate the environmental score of CSCsi46466					
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	

CSCsz40392 - CCM: Coredump in sipSafeStrlen from malicious INVITE (registered customers only)					
Calculate the environmental score of CSCsz40392					
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	

CSCsq22534 - IP_Contrack Fills Up During TCP Flood Attack (registered customers only)					
Calculate the environmental score of CSCsq22534					
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

CSCsx32236 - SCCP Port Closed in Response to FD Resource Exhaustion (registered customers only)					
Calculate the environmental score of CSCsx32236					
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	

CSCsx23689 - SIP Port Closed in Response to FD Resource Exhaustion (registered customers only)					
Calculate the environmental score of CSCsx23689					
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 could result in the interruption of voice services. To restore voice services, affected Cisco Unified Communications Manager services may require a manual restart.

[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	Recommended Release
5.x	5.1(3g) (Available for download in early September 2009)
6.x	6.1(4)
7.x	7.1(2a)SU1

Cisco Unified Communications Manager software version 5.1(3g) will be available for download in early September 2009 at the following link:

<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>

Cisco Unified Communications Manager software version 6.1(4) can be downloaded at the following link:

<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>

Administrators are advised to upgrade Cisco Unified Communications Manager systems running software version 7.0 to version 7.1(2a)SU1. Cisco Unified Communications Manager software version 7.1(2a)SU1 can be downloaded at the following link:

<http://tools.cisco.com/support/downloads/go/PlatformList.x?sftType=Unified+Communications+Manager+Updates&mdfid=282421166&treeName=Voice+and+20Version/Option&url=null&modelName=Cisco+Unified+Communications+Manager+Version+7.1>

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

☐ Workarounds

There are no workarounds for the vulnerabilities in this advisory. Administrators can mitigate the SCCP- and SIP-related vulnerabilities by implementing filtering on screening devices to permit access to TCP ports 2000 and 2443, and TCP and UDP ports 5060 and 5061 only from networks that need SCCP and SIP access to Cisco Unified Communications Manager servers.

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-20090826-cucm.shtml>

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

☐ **Obtaining Fixed Software**

Cisco has released free software updates for select Cisco Unified Communications Manager versions 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.

Cisco Unified Communications Manager Versions 6.x and Later

Cisco has released free software updates for all vulnerabilities described in this advisory in Cisco Unified Communications Manager versions 6.x and 7.x.

Cisco Unified Communications Manager Versions 4.x and 5.x

For Cisco Bug ID Cscsi46466, Cisco will not provide a software fix for Cisco Unified Communications Manager versions 4.x and 5.x. Customers who are concerned about the availability of fixed software for this vulnerability in these releases should contact the following email address:

cucm-august26-inquiry@cisco.com

☐ **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 vulnerabilities described in this advisory. The vulnerabilities were discovered 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-20090826-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 1.0	2009-August-26	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.](#)