

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

Advisory ID: cisco-sa-20100303-cucm

<http://www.cisco.com/warp/public/707/cisco-sa-20100303-cucm.shtml>

Revision 1.0

For Public Release 2010 March 3 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 if exploited could cause an interruption of voice services. The Session Initiation Protocol (SIP), Skinny Client Control Protocol (SCCP) and Computer Telephony Integration (CTI) Manager services are affected by these vulnerabilities.

To address these vulnerabilities, Cisco has released free software updates for select Cisco Unified Communications Manager versions. There is a workaround for one of the vulnerabilities.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20100303-cucm.shtml>.

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

☐ **Affected Products**

☐ **Vulnerable Products**

The following products are affected by vulnerabilities that are 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

Note: Cisco Unified Communications Manager version 5.1 reached the End of Software Maintenance on February 13, 2010. For customers using Cisco Unified Communications Manager 5.x versions, please contact your Cisco support team for assistance in upgrading to a supported version of Cisco Unified Communications Manager.

☐ **Products Confirmed Not Vulnerable**

Cisco Unified Communications Manager version 8.0(1) and Cisco Unified Communications Manager Express are 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 SCCP Message Vulnerabilities

Cisco Unified Communications Manager contains two DoS vulnerabilities that involve the processing of SCCP packets. Each vulnerability is triggered by a malformed SCCP message that could cause a critical process to fail, which could result in the disruption of voice services. All SCCP ports (TCP ports 2000 and 2443) are affected.

The first SCCP DoS vulnerability is documented in Cisco Bug ID [CSCtc38985](#) ([registered](#) customers only) and has been assigned the CVE identifier CVE-2010-0587. This vulnerability is fixed in Cisco Unified Communications Manager versions 4.3(2)SR2, 6.1(5), 7.1(3a)su1 and 8.0(1).

The second SCCP DoS vulnerability is documented in Cisco Bug ID [CSCtc47823](#) ([registered](#) customers only) and has been assigned the CVE identifier CVE-2010-0588. This vulnerability is fixed in Cisco Unified Communications Manager versions 6.1(5), 7.1(3a)su1 and 8.0(1). Cisco Unified Communications Manager 4.x versions are not affected.

Malformed SIP Message Vulnerabilities

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

The first SIP DoS vulnerability is documented in Cisco Bug ID [CSCtc37188](#) ([registered](#) customers only) and has been assigned the CVE identifier CVE-2010-0590. This vulnerability is fixed in Cisco Unified Communications Manager versions 7.1(3a)su1 and 8.0(1). Cisco Unified Communications Manager 4.x and 6.x versions are not affected.

The second SIP DoS vulnerability is documented in Cisco Bug ID [CSCtc62362](#) ([registered](#) customers only) and has been assigned the CVE identifier CVE-2010-0591. The second vulnerability is fixed in Cisco Unified Communications Manager versions 6.1(5), 7.1(3b)SU2 and 8.0(1). Cisco Unified Communications Manager 4.x versions are not affected.

Malformed CTI Manager Message Vulnerability

The CTI Manager service of Cisco Unified Communications Manager contains a DoS vulnerability. A malformed message sent to the CTI Manager service port (TCP 2748) could cause the CTI Manager service to fail, which could result in the interruption of CTI applications. The CTI Manager service is disabled by default.

The CTI Manager vulnerability is documented in Cisco Bug ID [CSCsu31800](#) ([registered](#) customers only) and has been assigned the CVE identifier CVE-2010-0592. This vulnerability is fixed in Cisco Unified Communications Manager versions 4.3(2)sr1a, 6.1(3), 7.0(2), 7.1(2) and 8.0(1).

[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>

CSCtc38985 - CCM Coredump on SCCP StationCapabilitiesRes Message with MaxCap Exceeded (registered customers only)					
Calculate the environmental score of CSCtc38985					
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	

CSCtc47823 - CCM Core at invalid Line# in SCCP RegAvailableLines and FwdStatReq (registered customers only)					
Calculate the environmental score of CSCtc47823					
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	

CSCtc37188 - CMSIPUtility Coredump on Fuzzed Register Message (registered customers only)					
Calculate the environmental score of CSCtc37188					
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

[CSCtc62362 - CCM Coredump on Overflow of Field Telephone-URL in REG Msg](#) (**registered customers only)**

Calculate the environmental score of [CSCtc62362](#)

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

[CSCsu31800 - CTI crash with invalid packet](#) (**registered customers only)**

Calculate the environmental score of [CSCsu31800](#)

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 that are described in this advisory could result in the interruption of voice services. An affected Cisco Unified Communications Manager services may require a manual restart to restore 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	Recommended Release
4.x	4.3(2)SR2
5.x	Cisco Unified Communications Manager version 5.1 reached the End of Software Maintenance on February 13, 2010.
6.x	6.1(5)
7.x	7.1(3b)SU2
8.x	Cisco Unified Communications Manager version 8.0(1) was distributed with software fixes for all the vulnerabilities that are described in this advisory.

Cisco Unified Communications Manager software version 4.3(2)SR2 can be downloaded at the following link:

<http://tools.cisco.com/support/downloads/go/PlatformList.x?sftType=Unified+Communications+Manager+Updates&mdfid=280771554&treeName=Voice+and+Unified+Communications&mdfLevel=Software%20Version/Option&url=null&modelName=Cisco+Unified+Communications+Manager+Version+4.3&isPlatform=N&treeMdfId=278875240&modifmdfid=null&imname=&hybrid=Y&imst=N>

Cisco Unified Communications Manager software version 6.1(5) can be downloaded at the following link:

<http://tools.cisco.com/support/downloads/go/ReleaseType.x?optPlat=&isPlatform=Y&mdfid=281023410&sftType=Unified+Communications+Manager+Updates&treeName=Voice+and+Unified+Communications&modelName=Cisco+Unified+Communications+Manager+Version+6.1&mdfLevel=Software%20Version/Option&treeMdfId=278875240&modifmdfid=null&imname=&hybrid=Y&imst=N>

Cisco Unified Communications Manager software version 7.1(3b)SU2 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+Unified+Communications&mdfLevel=Software%20Version/Option&url=null&modelName=Cisco+Unified+Communications+Manager+Version+7.1&isPlatform=N&treeMdfId=278875240&modifmdfid=null&imname=&hybrid=Y&imst=N>

☐ Workarounds

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 require SCCP and SIP access to Cisco Unified Communications Manager appliances.

It is possible to mitigate the CTI Manager vulnerability by disabling the CTI Manager service t is not necessary; however, this workaround will interrupt applications that reply on the CTI Manager service. Administrators can also mitigate the vulnerability by implementing filtering on screening devices to permit access to TCP port 2748 only from networks that require access to the CTI Manager service. Please consult the following documentation for details on disabling Cisco Unified Communications Manager services:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/service/6_0_1/admin/sasrvact.html#wp1048390

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-20100303-cucm.shtml>

☐ 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 vulnerabilities described in this advisory.

The vulnerability documented in Cisco Bug ID [CSCtc38985](#) ([registered](#) customers only) was reported to Cisco by the Siperia VIPER Lab. Cisco would like to thank Siperia VIPER Lab team for reporting this vulnerability to us and for working with us on a coordinated disclosure.

All other vulnerabilities described in this advisory were discovered as a result of internal testing conducted 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-20100303-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	2010-March-03	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 in

structions 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](#)

© 2009 - 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)