

Cisco Security Advisory: Cisco Unified Communications Manager Overflow Vulnerabilities

Advisory ID: cisco-sa-20070711-cucm

<http://www.cisco.com/warp/public/707/cisco-sa-20070711-cucm.shtml>

Revision 1.0

For Public Release 2007 July 11 1600 UTC (GMT)

Please provide your [feedback](#) on this document.

Contents

[Summary](#)

[Affected Products](#)

[Details](#)

[Vulnerability Scoring Details](#)

[Impact](#)

[Software Version 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 (CUCM), formerly CallManager, contains two overflow vulnerabilities that could allow a remote, unauthenticated user to cause a denial of service (DoS) condition or execute arbitrary code.

A workaround exists for one of the vulnerabilities.

Cisco has made free software available to address these vulnerabilities for affected customers.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20070711-cucm.shtml>.

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

☐ Affected Products

Note: Cisco Unified CallManager versions 4.2, 4.3, 5.1 and 6.0 have been renamed as Cisco Unified Communications Manager. CUCM versions 3.3, 4.0, 4.1 and 5.0 retain the Cisco Unified CallManager name.

☐ Vulnerable Products

These products are vulnerable:

- Cisco Unified CallManager 3.3 versions prior to 3.3(5)SR3
- Cisco Unified CallManager 4.1 versions prior to 4.1(3)SR5
- Cisco Unified CallManager 4.2 versions prior to 4.2(3)SR2
- Cisco Unified Communications Manager 4.3 versions prior to 4.3(1)SR1
- Cisco Unified CallManager 5.0 and Communications Manager 5.1 versions prior to 5.1(2)

Administrators of systems running CUCM version 3.x and 4.x can determine the software version by navigating to **Help > About Cisco Unified CallManager** and selecting the **Details** button via the CUCM Administration interface.

Administrators of systems running CUCM version 5.0 can determine the software version by viewing the main page of the CUCM 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 version 6.0 and Cisco CallManager 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 (CUCM), formerly CallManager, 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.

- **CTL Provider Service Overflow**
The Certificate Trust List (CTL) Provider service of CUCM contains a heap overflow vulnerability that could allow a remote, unauthenticated user to cause a DoS condition or execute arbitrary code. The CTL Provider service listens on TCP port 2444 by default, but the port is user-configurable. This vulnerability is corrected in CUCM versions 4.1(3)SR5, 4.2(3)SR2, 4.3(1)SR1 and 5.1(2). CUCM 3.x versions are not affected by this vulnerability. This issue is documented in Cisco Bug ID CSCsi03042.
- **RIS Data Collector Heap Overflow**
The Real-Time Information Server (RIS) Data Collector service of CUCM contains a heap overflow vulnerability that could allow a remote, unauthenticated user to cause a DoS condition or execute arbitrary code. The RIS Data Collector process listens on TCP port 2556 by default, but the port is user-configurable. This vulnerability is corrected in CUCM versions 3.3(5)SR2b, 4.1(3)SR5, 4.2(3)SR2, 4.3(1)SR1 and 5.1(2). This issue is documented in Cisco Bug ID CSCsi10509.

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

☐ Vulnerability Scoring Details

Cisco is providing 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 1.0.

Cisco will provide a base and temporal score. Customers can then compute environmental scores to assist in determining the impact of the vulnerability in individual networks.

Cisco PSIRT will set the bias in all cases to normal. Customers are encouraged to apply the bias parameter when determining the environmental impact of a particular vulnerability.

CVSS is a standards based scoring method that conveys vulnerability severity and helps determine urgency and priority of response.

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>.

**CSCsi03042 (registered customers only) - CallManager CTL Provider Service
Overflow and Password Bypass**

Calculate the environmental score of CSCsi03042

CVSS Base Score - 10

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Remote	Low	Not Required	Complete	Complete	Complete	Normal

CVSS Temporal Score - 8.3

Exploitability	Remediation Level	Report Confidence
Functional	Official-Fix	Confirmed

CSCsi10509 (registered customers only) - CallManager RISDC Heap Overflow

Calculate the environmental score of CSCsi10509

CVSS Base Score - 10						
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Remote	Low	Not Required	Complete	Complete	Complete	Normal
CVSS Temporal Score - 8.3						
Exploitability		Remediation Level		Report Confidence		
Functional		Official-Fix		Confirmed		

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

Impact

Successful exploitation of these vulnerabilities may result in a DoS condition or the execution of arbitrary code.

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

Software Version 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.

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

Workarounds

It is possible to workaround the CTL Provider Service Overflow vulnerability by disabling the CTL Provider Service if it is not needed. Access to the CTL Provider Service is usually only required during the initial configuration of CUCM authentication and encryption features. For CUCM 4.x systems, please consult the following documentation for details on how to disable CUCM services:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/service/4_2_3/ccmsrva/sasrvact.html

For CUCM 5.x systems, please consult the following documentation for details on how to disable CUCM services:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/service/5_0_1/ccmsrva/sasrvact.html#wp1048220

Filtering traffic to affected CUCM systems on screening devices can be used as a mitigation technique for both vulnerabilities:

- Permit access to TCP port 2444 only between the CUCM 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.
- Permit access to TCP port 2556 only from other CUCM cluster systems to mitigate the RIS Data Collector overflow.

It is possible to change the default ports of the CTL Provider (2444/TCP) and RIS Data Collector (2556/TCP) services. If changed, filtering should be based on the values used. The values of the ports can be viewed in CUCM Administration interface by following the **System > Service Parameters** menu and selecting the appropriate service.

There is currently no method to configure filtering directly on a CUCM system.

Although it is often difficult to block traffic transiting your network, it is possible to identify traffic that should never be allowed to target your infrastructure devices and block that traffic at the border of your network. Infrastructure ACLs are considered a network security best practice and should be considered as a long-term addition to good network security, as well as a workaround for this specific vulnerability. The filters shown above should be included as part of an infrastructure access list which will protect all devices with IP addresses in the infrastructure IP address range.

The white paper entitled "Protecting Your Core: Infrastructure Protection Access Control Lists" presents guidelines and recommended deployment techniques for infrastructure protection access lists. This document is available at the following link:

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml

Filters blocking access to TCP/2444 and TCP/2556 should be deployed at the network edge as part of a transit access list which will protect the router where the ACL is configured, as well as other devices behind it. Further information about transit ACLs is available in the white paper "Transit Access Control Lists: Filtering at Your Edge," which is available at the following link:

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801afc76.shtml

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:

<http://www.cisco.com/warp/public/707/cisco-amb-20070711-cucm.shtml>

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

☐ Obtaining Fixed Software

Cisco will make free software available to address this vulnerability for affected customers. 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/public/sw-license-agreement.html>, or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact either "psirt@cisco.com" or "security-alert@cisco.com" for software upgrades.

Fixed software for CUCM can be obtained here:

CUCM Version	Fixed Release	Download Location
CUCM 3.3	CUCM 3.3(5) SR2b (Expected Availability July 18)	http://www.cisco.com/pcgi-bin/tablebuild.pl/callmgr-33?psrtdcat20e2
CUCM 4.0	N/A	Upgrade to 4.1(3) SR5b or 4.2(3)SR2b

CUCM 4.1	CUCM 4.1(3)SR5b	http://www.cisco.com/cgi-bin/tablebuild.pl/callmgr-41?psrtdcat20e2
CUCM 4.2	CUCM 4.2(3)SR2b	http://www.cisco.com/cgi-bin/tablebuild.pl/callmgr-42?psrtdcat20e2
CUCM 4.3	CUCM 4.3(1)SR1	http://www.cisco.com/cgi-bin/tablebuild.pl/callmgr-43?psrtdcat20e2
CUCM 5.0	N/A	Upgrade to CUCM 5.1(2a) *
CUCM 5.1	CUCM 5.1(2a) *	http://www.cisco.com/cgi-bin/tablebuild.pl/callmgr-51?psrtdcat20e2

* The vulnerabilities contained in this advisory were first fixed in CUCM version 5.1(2). Users are encouraged to upgrade to CUCM 5.1(2a) or later to obtain fixes for security vulnerabilities described in Cisco security advisory:

<http://www.cisco.com/warp/public/707/cisco-sa-20070711-voip.shtml>

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

☐ 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 agreement 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 who do not hold a Cisco service contract and customers who purchase through third-party vendors but are unsuccessful at obtaining fixed software through their point of sale should get their 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

Have your product serial number available and give the URL of this notice as evidence of your 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 special 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 reported to Cisco by the IBM Internet Security Systems X-Force team.

[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-20070711-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-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	2007-June-11	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.](#)