

Cisco Security Advisory: Cisco Unified Communications Manager Denial of Service and Authentication Bypass Vulnerabilities

Advisory ID: cisco-sa-20080625-cucm

<http://www.cisco.com/warp/public/707/cisco-sa-20080625-cucm.shtml>

Revision 1.0

For Public Release 2008 June 25 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 (CUCM), formerly Cisco CallManager, contains a denial of service (DoS) vulnerability in the Computer Telephony Integration (CTI) Manager service that may cause an interruption in voice services and an authentication bypass vulnerability in the Real-Time Information Server (RIS) Data Collector that may expose information that is useful for reconnaissance.

Cisco has released free software updates 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-20080625-cucm.shtml>.

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

☐ Affected Products

☐ Vulnerable Products

The following products are vulnerable:

- Cisco Unified CallManager 4.1 versions
- Cisco Unified Communications Manager 4.2 versions prior to 4.2(3)SR4
- Cisco Unified Communications Manager 4.3 versions prior to 4.3(2)SR1
- Cisco Unified Communications Manager 5.x versions prior to 5.1(3c)
- Cisco Unified Communications Manager 6.x versions prior to 6.1(2)

Administrators of systems running Cisco Unified Communications Manager (CUCM) version 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 that are running CUCM versions 5.x and 6.x 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 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 (CUCM) 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.

Computer Telephony Integration Manager Related Vulnerability

The Computer Telephony Integration (CTI) Manager service of CUCM versions 5.x and 6.x contains a vulnerability when handling malformed input that may result in a DoS condition. The CTI Manager service listens by default on TCP port 2748 and is not user-configurable. There is no workaround for this vulnerability. This vulnerability is fixed in CUCM versions 5.1(3c) and 6.1(2). This vulnerability is documented in Cisco Bug ID CSCso75027 and has been assigned Common Vulnerabilities and Exposures (CVE) identifier [CVE-2008-2061](#).

Real-Time Information Server Data Collector Related Vulnerability

The Real-Time Information Server (RIS) Data Collector service of CUCM versions 4.x, 5.x, and 6.x contains an authentication bypass vulnerability that may result in the unauthorized disclosure of certain CUCM cluster information. In normal operation, Real-Time Monitoring Tool (RTMT) clients gather CUCM cluster statistics by authenticating to a Simple Object Access Protocol (SOAP) based web interface. The SOAP interface proxies authenticated connections to the RIS Data Collector process. The RIS Data Collector service listens on TCP port 2556 by default and is user configurable. By connecting directly to the port that the RIS Data Collector process listens on, it may be possible to bypass authentication checks and gain read-only access to information about a CUCM cluster. The information available includes performance statistics, user names, and configured IP phones. This information may be used to mount further attacks. No passwords or other sensitive CUCM configuration may be obtained via this vulnerability. No CUCM configuration changes can be made.

There is no workaround for this vulnerability. This vulnerability is fixed in CUCM versions 4.2(3)SR4, 4.3(2)SR1, 5.1(3), and 6.1(1). For CUCM 4.x versions, this vulnerability is documented in Cisco Bug ID CSCsq35151 and has been assigned CVE identifier [CVE-2008-2062](#). For CUCM 5.x and 6.x versions, this vulnerability is documented in Cisco Bug ID CSCsj90843 and has been assigned CVE identifier [CVE-2008-2730](#).

☐ 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> .

<u>CSCso75027 - CTI Manager TSP Crash</u> (<u>registered</u> customers only)					
Calculate the environmental score of <u>CSCso75027</u>					
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	

CSCsq35151 - RISDC Authentication Bypass (registered customers only)

Calculate the environmental score of CSCsq35151

CVSS Base Score - **5**

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	Partial	None	None

CVSS Temporal Score - **4.1**

Exploitability	Remediation Level	Report Confidence
Functional	Official-Fix	Confirmed

CSCsj90843 - RISDC Authentication Bypass (registered customers only)

Calculate the environmental score of CSCsj90843

CVSS Base Score - **5**

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	Partial	None	None

CVSS Temporal Score - **4.1**

Exploitability	Remediation Level	Report Confidence
Functional	Official-Fix	Confirmed

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

☐ **Impact**

Successful exploitation of the vulnerabilities in this advisory may result in the interruption of voice services or disclosure of information useful for reconnaissance.

[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 (CUCM) version 4.2(3)SR4 contains fixes for all vulnerabilities affecting CUCM version 4.2 listed in this advisory. Cisco Unified CallManager 4.1 version administrators are encouraged to upgrade to CUCM version 4.2(3)SR4 in order to obtain fixed software. Version 4.2(3)SR4 can be downloaded at the following link:

<http://tools.cisco.com/support/downloads/go/PlatformList.x?sftType=Unified%20Communications%20Manager%20Updates&mdfid=280264388&treeName=Voice%20and%20Unified%20Communications&mdfLevel=Software%20Version/Option&url=null&modelName=Cisco%20Unified%20CallManager%20Version%204.2&isPlatform=N&treeMdfId=278875240&modifmdfid=null&imname=null&hybrid=Y&imst=N>

CUCM version 4.3(2)SR1 contains fixes for all vulnerabilities affecting CUCM version 4.3 listed in this advisory and is scheduled to be released in mid-July, 2008. Version 4.3(2)SR1 will be available for download at the following link:

<http://tools.cisco.com/support/downloads/go/PlatformList.x?sftType=Unified%20Communications%20Manager%20Updates&mdfid=280771554&treeName=Voice%20and%20Unified%20Communications&mdfLevel=Software%20Version/Option&url=null&modelName=Cisco%20Unified%20Communications%20Manager%20Version%204.3&isPlatform=N&treeMdfId=278875240&modifmdfid=null&imname=null&hybrid=Y&imst=N>

CUCM version 5.1(3c) contains fixes for all vulnerabilities affecting CUCM version 5.x listed in this advisory. Version 5.1(3c) can be downloaded 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>

CUCM version 6.1(2) contains fixes for all vulnerabilities affecting CUCM version 6.x listed in this advisory. Version 6.1(2) 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>

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

☐ Workarounds

CTI Manager Related Vulnerability

It is possible to mitigate the CTI Manager vulnerability (CSCso75027) by implementing filtering on screening devices. Administrators are advised to permit access to TCP port 2748 only from networks that contain systems running CTI-enabled applications.

RIS Data Collector Related Vulnerability

It is possible to mitigate the RIS Data Collector vulnerability (CSCsq35151 and CSCsj90843) by implementing filtering on screening devices. Administrators are advised to permit access to TCP port 2556 only from other CUCM cluster systems.

It is possible to change the default port (TCP 2556) of the RIS Data Collector service. If changed, filtering should be based on the values used. The values of the ports can be viewed in the Cisco Unified Communications Manager (CUCM) administration interface by following the **System > Service Parameters** menu and selecting the appropriate service.

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-20080625-cucm.shtml>

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

☐ 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/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.

[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.

Cisco PSIRT greatly appreciates the opportunity to work with researchers on security vulnerabilities and welcomes the opportunity to review and assist in product reports. We would like to thank VoIPshield for working with us towards the goal of keeping Cisco networks and the Internet, as a whole, secure.

[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-20080625-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	2008-June-25	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.](#)