

# Cisco Security Advisory: Cisco Unified Communications Manager CTL Provider Heap Overflow

Advisory ID: cisco-sa-20080116-cucmctl

<http://www.cisco.com/warp/public/707/cisco-sa-20080116-cucmctl.shtml>

## Revision 1.0

For Public Release 2008 January 16 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 CallManager, contains a heap overflow vulnerability in the Certificate Trust List (CTL) Provider service that could allow a remote, unauthenticated user to cause a denial of service (DoS) condition or execute arbitrary code. There is a workaround for this vulnerability.

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

Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-0027 has been assigned to this vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080116-cucmctl.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 4.0
- Cisco Unified CallManager 4.1 Versions prior to 4.1(3)SR5c
- Cisco Unified Communications Manager 4.2 Versions prior to 4.2(3)SR3
- Cisco Unified Communications Manager 4.3 Versions prior to 4.3(1)SR1

The version of software running on a CUCM 4.x system can be determined by navigating to **Help > About Cisco Unified CallManager** and selecting the **Details** button via the CUCM Administration interface.

### ☐ Products Confirmed Not Vulnerable

CUCM Versions 3.3, 5.0, 5.1, 6.0, 6.1 and Cisco CallManager Express are not affected by this vulnerability. No other Cisco products are currently known to be affected by this vulnerability.

[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, voice-over-IP (VoIP) gateways, and multimedia applications.

When a CUCM server is deployed in secure mode, a Certificate Trust List (CTL) is used by Cisco Unified IP Phone devices to verify the identity of CUCM servers. The CTL contains public keys and other information to allow the Cisco IP Phone devices to establish a trusted relationship with a CUCM server. The CTL is provisioned using the CTL Provider service on a CUCM server and with the CTL Provider client on an administrator workstation. The CTL Provider service needs to be enabled during the initial configuration of a CUCM server/cluster or when changes are required to the CTL. Please consult the Workarounds section of this advisory for information on how to determine if the CTL Provider service is enabled on a CUCM server.

The CTL Provider service of the 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 can be modified by the user. This issue is documented in Cisco Bug ID CSCsj22605.

[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> .

<b><u>CSCsj22605 - CUCM CTL Provider Heap Overflow Vulnerability</u></b> ( <u>registered</u> customers only)					
<b>Calculate the environmental score of <u>CSCsj22605</u></b>					
<b>CVSS Base Score - 10</b>					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	Complete	Complete	Complete
<b>CVSS Temporal Score - 8.3</b>					
Exploitability	Remediation Level		Report Confidence		
Functional	Official-Fix		Confirmed		

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

## ☐ Impact

Successful exploitation of this vulnerability may result in a DoS condition or the execution of arbitrary code.

[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.

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

## ☐ Workarounds

It is possible to workaround the vulnerability by disabling the CTL Provider service when not in use. Access to the CTL Provider service is required for the initial configuration of the CUCM authentication and encryption features, or during configuration updates. For the CUCM 4.x systems, please consult the following documentation for details on how to disable the CUCM services:

[http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/cucm/service/4\\_2\\_3/ccmsrva/sasrvact.html](http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/service/4_2_3/ccmsrva/sasrvact.html)

Filtering traffic to the affected CUCM systems on screening devices can be used as a mitigation technique for this vulnerability. To mitigate the CTL Producer service overflow, access to TCP port 2444 should be permitted only between the CUCM servers and administrator workstations running the CTL Provider client. There is currently no supported method to configure filtering directly on a CUCM system.

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

Filters blocking access to TCP port 2444 should be deployed at the network edge as part of a transit access control list (tACL). Further information about transit access control lists 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](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-20080116-cucmctl.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](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](mailto:psirt@cisco.com) or [security-alert@cisco.com](mailto:security-alert@cisco.com) for software upgrades.

Fixed software for CUCM can be obtained here:

<b>CUCM Version</b>	<b>Fixed Release</b>	<b>Recommended Release</b>	<b>Download Location</b>
CUCM 4.0	N/A	Upgrade to a fixed Version of CUCM 4.1 or later	N/A
CUCM 4.1	CUCM 4.1(3) SR5c	CUCM 4.1(3)SR6 or later	<a href="http://www.cisco.com/cgi-bin/tablebuild.pl/callmgr-41?psrtdcat20e2">http://www.cisco.com/cgi-bin/tablebuild.pl/callmgr-41?psrtdcat20e2</a>
CUCM 4.2	CUCM 4.2(3) SR3	CUCM 4.2(3)SR3 or later	<a href="http://www.cisco.com/cgi-bin/tablebuild.pl/callmgr-42?psrtdcat20e2">http://www.cisco.com/cgi-bin/tablebuild.pl/callmgr-42?psrtdcat20e2</a>

CUCM 4.3	CUCM 4.3(1) SR1	CUCM 4.3(1) SR1a or later	<a href="http://www.cisco.com/cgi-bin/tablebuild.pl/callmgr-43?psrtdcat20e2">http://www.cisco.com/ cgi-bin/ tablebuild.pl/ callmgr-43? psrtdcat20e2</a>
-------------	-----------------------	------------------------------	---

## ☐ 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](mailto: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.

This vulnerability was reported to Cisco by TippingPoint. Cisco would like to thank TippingPoint for reporting this vulnerability and working with us towards resolution of this problem.

[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-20080116-cucmctl.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](mailto:cust-security-announce@cisco.com)
- [first-teams@first.org](mailto:first-teams@first.org)
- [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)
- [vulnwatch@vulnwatch.org](mailto:vulnwatch@vulnwatch.org)
- [cisco@spot.colorado.edu](mailto:cisco@spot.colorado.edu)
- [cisco-nsp@puck.nether.net](mailto:cisco-nsp@puck.nether.net)
- [full-disclosure@lists.grok.org.uk](mailto:full-disclosure@lists.grok.org.uk)
- [comp.dcom.sys.cisco@newsgate.cisco.com](mailto: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-January-16	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](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.](#)