

Cisco Security Advisory: Multiple Cisco Unified CallManager Vulnerabilities

Advisory ID: [cisco-sa-20060712-cucm](#)

<http://www.cisco.com/warp/public/707/cisco-sa-20060712-cucm.shtml>

Revision 1.0

For Public Release 2006 July 12 1600 UTC (GMT)

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

Contents

- [Summary](#)
- [Affected Products](#)
- [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 CallManager (CUCM) 5.0 has Command Line Interface (CLI) and Session Initiation Protocol (SIP) related vulnerabilities. There are potential privilege escalation vulnerabilities in the CLI which may allow an authenticated administrator to access the base operating system with root privileges. There is also a buffer overflow vulnerability in the processing of hostnames contained in a SIP request which may result in arbitrary code execution or cause a denial of service. These vulnerabilities only affect Cisco Unified CallManager 5.0.

Cisco has made free software available to address these vulnerabilities for affected customers. There are no workarounds available to mitigate the effects of these vulnerabilities.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20060712-cucm.shtml>.

Affected Products

This section provides details on affected products.

Vulnerable Products

Only Cisco Unified CallManager versions 5.0(1), 5.0(2), 5.0(3) and 5.0(3a) are affected.

The version of CallManager software running can be determined navigating to **Show > Software** in the CUCM IPT Platform administration interface or by running the command **show version active** in the CLI.

Products Confirmed Not Vulnerable

No other Cisco products are currently known to be affected by these vulnerabilities, including all previous versions of Cisco Unified CallManager.

Details

Cisco Unified CallManager is the software-based call-processing component of the Cisco IP telephony solution which 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.

The CallManager CLI provides a backup management interface to the system in order to diagnose and troubleshoot the primary HTTPS-based management interfaces. The CLI, which runs as the root user, contains two vulnerabilities in the parsing of commands. The first vulnerability may allow an authenticated CUCM administrator to execute arbitrary operating system programs as the root user. The second vulnerability may allow output redirection of a command to a file or a folder specified on the command line.

Cisco Unified CallManager supports the coexistence of both SCCP and SIP phones, allowing for migration to SIP while protecting investments in existing devices. CUCM contains a buffer overflow vulnerability in the processing of excessively long hostnames which may be included in a SIP request.

These issues are documented by the following Cisco bug IDs:

- [CSCse11005](#) ([registered](#) customers only) Certain CLI commands allow execution of arbitrary Linux commands
- [CSCse31704](#) ([registered](#) customers only) User able to redirect command output to a file folder
- [CSCsd96542](#) ([registered](#) customers only) SD-GA: CCM cores when SIP request line host name has ASCII overflow

Impact

Successful exploitation of the CLI vulnerability documented in Cisco bug ID CSCse11005 may allow

authenticated CLI users to execute arbitrary operating system commands with root privileges. Exploitation of the CLI vulnerability documented in Cisco bug ID CSCse31704 may allow an authenticated CLI user to modify or overwrite any file on the filesystem as the root user.

Exploitation of the SIP vulnerability documented in Cisco bug ID CSCsd96542 may result in arbitrary code execution or a denial of service.

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.

Workarounds

There are no workarounds for these vulnerabilities.

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 may be obtained at <http://www.cisco.com/cgi-bin/tablebuild.pl/callmgr-50>.

Affected Releases	Fixed Releases
Cisco Unified CallManager 5.0 (1)	Cisco Unified CallManager 5.0(4) and later
Cisco Unified CallManager 5.0 (2)	
Cisco Unified CallManager 5.0 (3)	

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.

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.

Distribution

This advisory is posted on Cisco's worldwide website at:

<http://www.cisco.com/warp/public/707/cisco-sa-20060712-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.

Revision History

Revision 1.0	2006-July-12 1600 UTC (GMT)	Initial public release
-----------------	--------------------------------	---------------------------

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>.

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
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------