Table of Contents

Cisco Security Advisory: Cisco Call Manager Privilege Escalation

Document ID: 68792

Advisory ID: cisco−sa−20060118−ccmpe

http://www.cisco.com/warp/public/707/cisco−sa−20060118−ccmpe.shtml

Revision 1.0

For Public Release 2006 January 18 1600 UTC (GMT)

Please provide your feedback on this document.

Summary

Cisco CallManager (CCM) 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. Cisco CallManager versions with Multi Level Administration (MLA) enabled may be vulnerable to privilege escalations, which may result in read−only users gaining administrative access.

Cisco has made free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco−sa−20060118−ccmpe.shtml.

Affected Products

Vulnerable Products

These Cisco CallManager versions with Multi Level Administration (MLA) enabled are vulnerable:

- Cisco CallManager 3.2 and earlier
- Cisco CallManager 3.3, versions earlier than 3.3(5)SR1
- Cisco CallManager 4.0, versions earlier than 4.0(2a)SR2c
- Cisco CallManager 4.1, versions earlier than 4.1(3)SR2

No other Cisco products are currently known to be affected by these vulnerabilities.

Complete this procedure to check if Multi Level Administration is enabled:

1. Access CCM Administration with this URL: http://<CCMServer>/ccmadmin, where <CCMServer> specifies the IP address or name of the Cisco CallManager server.
2. Choose **User > Access Rights > Configure MLA Parameters**. The MLA Enterprise Parameter Configuration page displays.
3. MLA is enabled if the Enable MultiLevelAdmin enterprise parameter is set to True.

Details

An administrative user with read−only permission can use a crafted URL on the CCMAdmin web page to escalate privileges to a full administrative level. This vulnerability applies to users who are authenticated to the read−only administrative level. Users with no administrative access and users with full administrative permissions continue to work as expected.

Administrative users with access privilege Read Only should not be confused with the standard User Group named "Read Only" which is created at installation. For further details on user groups and assigning access privileges, please refer to this URL:
http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_administration_guide_chapter09186a00803ed6ea.h

- **CSCef75361, CSCsb12765, CSCsb88649, CSCsc26275** CCMAdmin Read Only User Can Escalate Privileges

Impact

Successful exploitation of the vulnerability may result in privilege escalation where read−only administrative users can gain full administrative privileges and create, delete, or reset devices.

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.

Each row of the Cisco CallManager software table (below) describes a release train which will address all of the vulnerabilities mentioned in this advisory. If a given release train is vulnerable, then the earliest possible releases that contain the fixes (the "First Fixed Release") and the anticipated date of availability for each are listed in the "Engineering Special," "Service Release," and "Maintenance Release" columns. A device running a Cisco CallManager release in the given train that is earlier than the release in a specific column (less than the First Fixed Release listed in the Engineering Special or Special Release column) is known to be vulnerable

to one or more issues. The Cisco CallManager should be upgraded at least to the indicated release or a later version (greater than or equal to the First Fixed Release label).

Version	Engineering Special	Service Release	Maintenance Release
3.2 and earlier			migrate to 3.3 or later
3.3	3.3(5)ES30	3.3(5)SR1a	no release planned
4.0	4.0(2a)ES62	4.0(2a)SR2c	no release planned
4.1	4.1(2)ES55 4.1(3)ES32	4.1(3)SR2	no release planned

Workarounds

It is possible to eliminate the ability for an attacker to escalate privileges from Read Only to Full Access without applying the service release by not using the Read Only access privilege, but instead only using the No Access or Full Access privileges. This is not an ideal solution, but can provide a temporary workaround.

For detailed instructions on configuring the privileges for a User Group within Cisco CallManager 4.1(3) see the Multilevel Administration Access Configuration (http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_administration_guide_chapter09186a00803ed6ea.
section of the Cisco CallManager Administration Guide (http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_administration_guide_book09186a00803be4ec.htm

Obtaining Fixed Software

Cisco has made free software available to address this vulnerability for affected customers. 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.

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.

This vulnerability was reported to Cisco by CNLabs of Switzerland.

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−20060118−ccmpe.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−voip@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−January−18	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.

Updated: Jan 18, 2006 Document ID: 68792