Cisco Security Advisory

Cisco Unified Communications Manager CTL Provider Heap Overflow

Advisory ID: cisco-sa-20080116-cucmctl
Published: 2008 January 16 16:00 GMT
Version1.0: Final
CVSS Score: Base - 10.0
Workarounds: See below

CVE-2008-0027
CWE-119

Download CVRF
Download PDF
Email

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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080116-cucmctl.

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.

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.

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

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

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://tools.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20080116-cucmctl

Fixed Software

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.

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.

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080116-cucmctl

---

Revision History

Revision 1.0	2008-January-16	Initial public release.

Legal Disclaimer

Cisco Security Vulnerability Policy

To learn about Cisco security vulnerability disclosure policies and publications, see the Security Vulnerability Policy. This document also contains instructions for obtaining fixed software and receiving security vulnerability information from Cisco.

Related Resources

IS Cisco Unified Communications Manager CTL Provider Buffer Overflow Vulnerability

AMB Identifying and Mitigating Exploitation of the Cisco Unified Communications Manager CTL Provider Heap Overflow

ST 13363

IPS Cisco Unified Communications Manager CTL Provider Heap Overflow

Subscribe to Cisco Security Notifications

Subscribe