Cisco Security Advisory

Cisco Unified Communications Manager Overflow Vulnerabilities

Advisory ID: cisco-sa-20070711-cucm
Published: 2007 July 11 16:00 GMT
Version1.0: Final
CVSS Score: Base - 10.0
Workarounds: See below

CVE-2006-5277
CVE-2006-5278
CWE-119

Download CVRF
Download PDF
Email

Summary

Cisco Unified Communications Manager (CUCM), formerly CallManager, contains two overflow vulnerabilities that could allow a remote, unauthenticated user to cause a denial of service (DoS) condition or execute arbitrary code.

A workaround exists for one of the vulnerabilities.

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

This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070711-cucm.

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 3.3 versions prior to 3.3(5)SR3
- Cisco Unified CallManager 4.1 versions prior to 4.1(3)SR5
- Cisco Unified CallManager 4.2 versions prior to 4.2(3)SR2
- Cisco Unified Communications Manager 4.3 versions prior to 4.3(1)SR1
- Cisco Unified CallManager 5.0 and Communications Manager 5.1 versions prior to 5.1(2)

Administrators of systems running CUCM version 3.x and 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 running CUCM version 5.0 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 version 6.0 and Cisco CallManager Express are not affected by these vulnerabilities. No other Cisco products are currently known to be affected by these vulnerabilities.

Details

Cisco Unified Communications Manager (CUCM), formerly CallManager, 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.

- **CTL Provider Service Overflow**
  The Certificate Trust List (CTL) Provider service of 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 is user-configurable. This vulnerability is corrected in CUCM versions 4.1(3)SR5, 4.2(3)SR2, 4.3(1)SR1 and 5.1(2). CUCM 3.x versions are not affected by this vulnerability. This issue is documented in Cisco Bug ID CSCsi03042.
- **RIS Data Collector Heap Overflow**
  The Real-Time Information Server (RIS) Data Collector service of CUCM contains a heap overflow vulnerability that could allow a remote, unauthenticated user to cause a DoS condition or execute arbitrary code. The RIS Data Collector process listens on TCP port 2556 by default, but the port is user-configurable. This vulnerability is corrected in CUCM versions 3.3(5)SR2b, 4.1(3)SR5, 4.2(3)SR2, 4.3(1)SR1 and 5.1(2). This issue is documented in Cisco Bug ID CSCsi10509.

Vulnerability Scoring Details

Cisco is providing 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 1.0.

Cisco will provide a base and temporal score. Customers can then compute environmental scores to assist in determining the impact of the vulnerability in individual networks.

Cisco PSIRT will set the bias in all cases to normal. Customers are encouraged to apply the bias parameter when determining the environmental impact of a particular vulnerability.

CVSS is a standards based scoring method that conveys vulnerability severity and helps determine urgency and priority of response.

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://tools.cisco.com/security/center/cvssCalculator.x.

CSCsi03042 (registered customers only) - CallManager CTL Provider Service Overflow and Password Bypass

Calculate the environmental score of CSCsi03042

CVSS Base Score - 10

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Remote	Low	Not Required	Complete	Complete	Complete	Normal

CVSS Temporal Score - 8.3

Exploitability	Remediation Level	Report Confidence
Functional	Official-Fix	Confirmed

CSCsi10509 (registered customers only) - CallManager RISDC Heap Overflow

Calculate the environmental score of CSCsi10509

CVSS Base Score - 10

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias

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 Certificate Trust List Provider Service Buffer Overflow Vulnerability

IS Cisco Unified Communications Manager Real-Time Information Server Data Collector Service Buffer Overflow Vulnerability

AMB Identifying and Mitigating Exploitation of the Multiple Cisco Unified Communications Manager and Presence Server Vulnerabilities

IPS RIS Data Collector Heap Overflow

Subscribe to Cisco Security Notifications

Subscribe

Remote	**Low**	**Not Required**	**Complete**	**Complete**	**Complete**	**Normal**
CVSS Temporal Score - 8.3						
Exploitability		**Remediation Level**		**Report Confidence**		
Functional		**Official-Fix**		**Confirmed**		

Workarounds

It is possible to workaround the CTL Provider Service Overflow vulnerability by disabling the CTL Provider Service if it is not needed. Access to the CTL Provider Service is usually only required during the initial configuration of CUCM authentication and encryption features. For CUCM 4.x systems, please consult the following documentation for details on how to disable CUCM services:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/service/4_2_3/ccmsrva/sasrvact.html

For CUCM 5.x systems, please consult the following documentation for details on how to disable CUCM services:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/service/5_0_1/ccmsrva/sasrvact.html#wp1048220

Filtering traffic to affected CUCM systems on screening devices can be used as a mitigation technique for both vulnerabilities:

- Permit access to TCP port 2444 only between the CUCM systems where the CTL Provider service is active and the CTL Client, usually on the administrator's workstation, to mitigate the CTL Provider service overflow.
- Permit access to TCP port 2556 only from other CUCM cluster systems to mitigate the RIS Data Collector overflow.

It is possible to change the default ports of the CTL Provider (2444/TCP) and RIS Data Collector (2556/TCP) services. If changed, filtering should be based on the values used. The values of the ports can be viewed in CUCM Administration interface by following the **System Service Parameters** menu and selecting the appropriate service.

There is currently no method to configure filtering directly on a CUCM system.

Although it is often difficult to block traffic transiting your network, it is possible to identify traffic that should never be allowed to target your infrastructure devices and block that traffic at the border of your network. Infrastructure ACLs are considered a network security best practice and should be considered as a long-term addition to good network security, as well as a workaround for this specific vulnerability. The filters shown above should be included as part of an infrastructure access list which will protect all devices with IP addresses in the infrastructure IP address range.

The white paper entitled "Protecting Your Core: Infrastructure Protection Access Control Lists" presents guidelines and recommended deployment techniques for infrastructure protection access lists. This document is available at the following link:

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml

Filters blocking access to TCP/2444 and TCP/2556 should be deployed at the network edge as part of a transit access list which will protect the router where the ACL is configured, as well as other devices behind it. Further information about transit ACLs 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-20070711-cucm

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.

These vulnerabilities were reported to Cisco by the IBM Internet Security Systems X-Force team.

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070711-cucm

---

Revision History

Revision 1.0	2007-June-11	Initial public release.

Legal Disclaimer