Cisco Security Advisory

Cisco Unified Communications Manager Session Initiation Protocol Denial of Service Vulnerabilities

Severity

Advisory ID: cisco-sa-20100922-cucmsip
Published: 2010 September 22 16:00 GMT
Version1.0: Final
Workarounds: See below
Cisco Bug IDs: CSCta20040 CSCtf72678

CVE-2010-2834
CVE-2010-2835

Download CVRF

Download PDF

Email

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

SA Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerabilities

IS Cisco IOS Software and Unified Communications Manager Session Initiation Protocol Packet Processing Denial of Service Vulnerability

Subscribe to Cisco Security Notifications

Subscribe

Summary

Cisco Unified Communications Manager contains two denial of service (DoS) vulnerabilities that affect the processing of Session Initiation Protocol (SIP) messages. Exploitation of these vulnerabilities could cause an interruption of voice services.

To address these vulnerabilities, Cisco has released free software updates. There is a workaround for these vulnerabilities.

This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-cucmsip.

Note: Cisco IOS® Software is also affected by the vulnerabilities described in this advisory. A companion advisory for Cisco IOS software is available at:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-sip

Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-bundle

Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

Affected Products

Vulnerable Products

The following products are affected by the vulnerabilities that are described in this advisory:

- Cisco Unified Communications Manager 6.x
- Cisco Unified Communications Manager 7.x
- Cisco Unified Communications Manager 8.x

Administrators of systems that are running Cisco Unified Communications Manager versions 6.x, 7.x and 8.x can determine the software version by viewing the main page of the Cisco Unified Communications Manager Administration interface. The software version can also be determined by running the **show version active** command via the command-line interface.

Products Confirmed Not Vulnerable

Cisco Unified Communications Manager version 4.x is not affected by these vulnerabilities. No other Cisco products are currently known to be affected by these vulnerabilities.

Details

Cisco Unified Communications Manager 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, VoIP gateways, and multimedia applications.

Cisco Unified Communications Manager contains two DoS vulnerabilities that involve the processing of SIP messages. Each vulnerability is triggered by a malformed SIP message that could cause a critical process to fail, which could result in the disruption of voice services. All SIP ports (TCP ports 5060 and 5061 and UDP ports 5060 and 5061) are affected.

The first SIP DoS vulnerability is documented in Cisco Bug ID CSCta31358 (registered customers only) and has been assigned the CVE identifier CVE-2010-2835. This vulnerability is fixed in Cisco Unified Communications Manager versions 6.1(5), 7.0(2a)su3, 7.1(3b)su2, 7.1(5) and 8.0(1). The corresponding IOS defect is CSCta20040.

The second SIP DoS vulnerability is documented in Cisco Bug ID CSCtf14987 (registered customers only) and has been assigned the CVE identifier CVE-2010-2834. The second vulnerability is fixed in Cisco Unified Communications Manager versions 6.1(5)SU1, 7.1(5) and 8.0(2). The corresponding IOS defect is CSCtf72678.

Workarounds

For customers who do not use SIP in their environment, there is a workaround for these vulnerabilities. Cisco Unified Communication Manager versions 6.1(4), 7.1(2) and 8.0(1) introduced the ability to disable SIP processing. SIP processing is enabled by default. Use the following instructions to disable SIP processing:

Step 1: Log into the Cisco Unified CM Administration web interface.

Step 2: Navigate to **System Service Parameters** and select the appropriate Cisco Unified Communications Manager server and the "Cisco CallManager" service.

Step 3: Change the "SIP Interoperability Enabled" parameter to False, and click **Save.**

Note: For a SIP processing change to take effect, the Cisco CallManager Service must be restarted. For information on how to restart the service, refer to the "Restarting the Cisco CallManager Service" section of the document at:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/7_1_2/ccmcfg/b03dpi.html#wp1075124

It is possible to mitigate these vulnerabilities by implementing filtering on screening devices and permitting access to TCP ports 5060 and 5061 and UDP ports 5060 and 5061 only from networks that require SIP access to Cisco Unified Communications Manager servers.

Additional mitigations that can be deployed on Cisco devices in the network are available in the companion document "Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Multiple Vulnerabilities in Cisco Voice Products", which is available at the following location:

http://tools.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20100922-voice

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.

Cisco Unified Communication Manager Version	Recommended Release
6.x	6.1(5)SU1
7.x	7.1(5b)SU2
8.x	8.0(3a)

Note: The recommended releases listed in the table above are the latest Cisco Unified Communications Manager versions available at the publication of this advisory, and each release includes software fixes for all the vulnerabilities described in this advisory.

Cisco Unified Communications Manager software can be downloaded at the following link:

http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=268439621

Exploitation and Public Announcements

The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerabilities described in this advisory.

All vulnerabilities described in this advisory were discovered as a result of internal testing conducted by Cisco.

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-cucmsip

---

Revision History

Revision 1.0	2010-September-22	Initial public release

Legal Disclaimer