Cisco Security Advisory

Cisco Unified Communications Manager Session Initiation Protocol Denial of Service Vulnerability

High

Advisory ID: cisco-sa-20120926-cucm
Published: 2012 September 26 16:00 GMT
Version1.0: Final
CVSS Score: Base - 7.8
Workarounds: See below
Cisco Bug IDs: CSCtj33003 CSCtw66721 CSCtw84664

CVE-2012-3949

Download CVRF
Download Oval
Download PDF
Email

Summary

Cisco Unified Communications Manager contains a vulnerability in its Session Initiation Protocol (SIP) implementation that could allow an unauthenticated, remote attacker to cause a critical service to fail, which could interrupt voice services. Affected devices must be configured to process SIP messages for this vulnerability to be exploitable.

Cisco has released software updates that address this vulnerability. A workaround exists for customers who do not require SIP in their environment.

This advisory is available at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-cucm.

Note: The September 26, 2012, Cisco IOS Software Security Advisory bundled publication includes nine Cisco Security Advisories. Eight of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses a vulnerability in Cisco Unified Communications Manager. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the September 2012 bundled publication.

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

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep12.html

Cisco IOS Software and Cisco IOS XE Software are affected by the vulnerability described in this advisory. A separate Cisco Security Advisory has been published to disclose the vulnerability that affects Cisco IOS Software and Cisco IOS XE Software at the following location:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-sip

Affected Products

Vulnerable Products

The following Cisco Unified Communications Manager software releases are affected:

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

Note: Cisco Unified Communications Manager version 6.1 reached the End of Software Maintenance on September 3, 2011. Customers using Cisco Unified Communications Manager 6.x versions should contact their Cisco support team for assistance in upgrading to a supported version of Cisco Unified Communications Manager.

Note: Cisco IOS Software and Cisco IOS XE Software are affected by the vulnerability described in this advisory. A separate Cisco Security Advisory has been published to disclose the vulnerability that affects Cisco IOS Software and Cisco IOS XE Software at the following location:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-sip

Products Confirmed Not Vulnerable

No other Cisco products are currently known to be affected by this vulnerability.

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.

Session Initiation Protocol (SIP) is a popular signaling protocol that is used to manage voice and video calls across IP networks such as the Internet. The protocol is responsible for handling all aspects of call setup and termination. Voice and video are the most popular types of sessions that SIP handles, but the protocol has the flexibility to accommodate other applications that require call setup and termination. SIP call signaling can use UDP (port 5060), TCP (port 5060), or Transport Layer Security (TLS; TCP port 5061) as the underlying transport protocol.

A vulnerability exists in the SIP implementation in Cisco Unified Communications Manager that could allow a remote attacker to cause a critical service to fail, which could interrupt voice services. This vulnerability is triggered when an affected device processes a crafted SIP message that contains a valid Session Description Protocol (SDP) message. Only traffic destined to the device can trigger the vulnerability; transit SIP traffic is not an exploit vector.

Note: In cases where SIP is running over TCP transport, a TCP three-way handshake is necessary to exploit this vulnerability.

This vulnerability is documented in Cisco bug IDs CSCtw66721 (registered customers only) and has been assigned Common Vulnerabilities and Exposures (CVE) ID CVE-2012-3949.

Note: This vulnerability also affects Cisco IOS Software and Cisco IOS XE Software. The corresponding Cisco bug IDs are CSCtw84664 and CSCtj33003. Refer to the separate Cisco Security Advisory for Cisco IOS Software for additional details.

Workarounds

A workaround exists for customers who do not require SIP in their environment. 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 in to the Cisco Unified CM Administration web interface.
- **Step 2:** Navigate to **System Service Parameters** and choose the appropriate Cisco Unified Communications Manager server and the Cisco CallManager service.
- **Step 3:** Change the SIP Interoperability Enabled parameter to **False** and then 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, see the "Restarting the Cisco CallManager Service" section of the "Cisco Unified Communications Manager Administration Guide" at http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/7_1_2/ccmcfg/b03dpi.html#wp1075124.

Additional mitigations that can be deployed on Cisco devices in the network are available in the companion document "Identifying and Mitigating Exploitation of the Cisco Unified Communications Manager and Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerability" at the following location:

http://tools.cisco.com/security/center/viewAMBAlert.x?alertId=26765

Fixed Software

When considering software upgrades, customers are advised to consult the Cisco Security Advisories and Responses archive at http://www.cisco.com/go/psirt and review subsequent advisories to determine exposure and a complete upgrade solution.

In all cases, customers should ensure that the devices to be upgraded contain sufficient memory and confirm that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, customers are advised to contact the Cisco Technical Assistance Center (TAC) or their contracted maintenance providers.

Cisco Unified Communication Manager Version	First Fixed Release	Recommended Release
7.x	7.1(5b)su5	7.1(5b)su5
8.x	8.5(1)su4 8.6(2a)su1 8.6(4) (BE3K-only release)	8.5(1)su4 8.6(2a)su2 8.6(4) (BE3K-only release)
9.x	Not affected	Not affected

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

BLG Cisco IOS Software Security Advisory Bundle Announced

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

AMB Identifying and Mitigating Exploitation of the Cisco Unified Communications Manager and Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerability

Subscribe to Cisco Security Notifications

Subscribe

Exploitation and Public Announcements

The Cisco Product Security Incident Response Team (PSIRT) is not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

This vulnerability was found during troubleshooting of TAC service requests.

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-cucm

---

Revision History

Revision 1.0	2012-September-26	Initial public release.

Legal Disclaimer