Cisco Security Advisory

Cisco Unified Communications Manager SIP Subsystem Vulnerability

Advisory ID: Cisco-SA-20140811-CVE-2014-3337
Published: 2014 August 11 20:36 GMT
Version1.0: Final
CVSS Score: Base - 6.8
Workarounds: See below
Cisco Bug IDs: CSCtq76428

CVE-2014-3337
CWE-20

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.

Subscribe to Cisco Security Notifications

Subscribe

Summary

A vulnerability in the Session Initiation Protocol (SIP) subsystem of Cisco Unified Communications Manager (Cisco Unified CM) could allow an authenticated, remote attacker to trigger a denial of service condition.

The vulnerability is due to a failure by the SIP subsystem to properly sanitize Extensible Markup Language (XML) prior to passing it to the XML processing engine. An attacker could exploit this vulnerability by submitting a crafted SIP message from a registered endpoint to an affected Cisco Unified CM. Successful exploitation could allow the attacker to cause a process crash that results in a denial of service condition.

Cisco has confirmed the vulnerability in a security notice and released software updates.

To exploit this vulnerability, an attacker must authenticate to the targeted system or to a registered endpoint to a targeted system. This access requirement may reduce the likelihood of a successful exploit.

Cisco indicates through the CVSS score that functional exploit code exists; however, the code is not known to be publicly available.

Affected Products

Customers are advised to consult Cisco bug ID CSCtq76428 for the most complete list of affected product versions.

Vulnerable Products

At the time this alert was first published, Cisco Unified CM version 8.6(.2) and prior were vulnerable. Later releases of Cisco Unified CM may also be vulnerable.

Products Confirmed Not Vulnerable

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

Workarounds

Administrators are advised to apply the appropriate updates.

Administrators are advised to allow only trusted users to have network access.

Administrators are advised to monitor affected systems.

Fixed Software

Cisco customers with active contracts should contact their Cisco support team for assistance in upgrading to a software version that includes fixes for this vulnerability. Cisco customers without contracts may contact the Cisco Technical Assistance Center at 1-800-553-2447 or 1-408-526-7209 or via email at *tac@cisco.com* for assistance.

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.

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-SA-20140811-CVE-2014-3337

Revision History

Version	Description	Section	Status	Date
1.0	Initial Release	NA	Final	2014-Aug-11

Legal Disclaimer