Cisco Security Advisory

Cisco Unified Communications Manager Authentication Denial of Service Vulnerability

Advisory ID: Cisco-SA-20130515-CVE-2013-1188
Published: 2013 May 15 20:12 GMT
Version1.0: Final
CVSS Score: Base - 5.0
Workarounds: See below
Cisco Bug IDs: CSCud39515

CVE-2013-1188
CWE-399

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 device authentication of Cisco Unified Communications Manager (CUCM) could allow an unauthenticated, remote attacker to impact application response.

The vulnerability is due to incomplete throttling of authentication requests. An attacker could exploit this vulnerability by sending multiple authentication requests in a short period of time. An exploit could allow the attacker to degrade the performance of the CUCM application.

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

To exploit this vulnerability, an attacker may require access to a trusted, internal network to send authentication requests to the targeted system. This access requirement could limit the likelihood of a successful exploit.

Customers are advised to review the bug report in the "Vendor Announcements" section for a current list of affected versions.

Affected Products

Cisco has released a security notice for bug ID CSCud39515 at the following link: CVE-2013-1188

Vulnerable Products

At the time this alert was first published, Cisco CUCM versions 9.1(1) and prior were vulnerable. Later versions of Cisco CUCM may also be affected.

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.

It is critical to prevent unauthorized direct communication to network devices. Restrict network traffic destined for the network infrastructure to protect against reconnaissance and DoS attacks. For configuration details, see Protecting Your Core: Infrastructure Protection Access Control Lists.

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 e-mail 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-20130515-CVE-2013-1188

Revision History

Version	Description	Section	Status	Date
1.0	Initial Release	NA	Final	2013-May-15

Legal Disclaimer