Cisco Security Advisory

Cisco Unified Communications Manager Stack Trace Web Disclosure Vulnerability

Advisory ID: Cisco-SA-20130802-CVE-2013-3442
Published: 2013 August 2 18:56 GMT
Version1.0: Final
CVSS Score: Base - 4.0
Workarounds: See below
Cisco Bug IDs: CSCug34854

CVE-2013-3442
CWE-200

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

An issue in the web portal of Cisco Unified Communications Manager (Unified CM) could allow an authenticated, remote attacker to view exception stack trace details.

The issue is due to disclosure of exception stack trace details. An attacker could exploit this issue by generating a stack exception in the Cisco Unified CM web portal. An exploit could allow the attacker to gain additional insight into the functioning of the underlying Cisco Unified CM components.

Cisco has confirmed this vulnerability in a security notice and software updates are available.

To exploit the vulnerability, the attacker must authenticate to the targeted system. This access requirement may limit the likelihood of a successful exploit.

Affected Products

Customers should refer to Cisco bug ID CSCug34854 for the most complete list of affected product versions.

Vulnerable Products

At the time this alert was first published, Cisco Unified CM versions 9.1(1) and prior were vulnerable. Later versions of Cisco Unified CM 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.

Administrators may consider using IP-based access control lists (ACLs) to allow only trusted systems to access the affected systems.

Administrators are advised to allow only privileged users to access administration or management systems.

Administrators are advised to monitor affected system

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-20130802-CVE-2013-3442

Revision History

Version	Description	Section	Status	Date
1.0	Initial Release	NA	Final	2013-Aug-02

Legal Disclaimer