Cisco Security Advisory

Cisco Unified Communications Manager User Web Dialer Cross-Site Request Forgery Vulnerability

Advisory ID: Cisco-SA-20130802-CVE-2013-3450
Published: 2013 August 2 18:55 GMT
Version1.0: Final
CVSS Score: Base - 4.3
Workarounds: See below
Cisco Bug IDs: CSCui13028

CVE-2013-3450
CWE-352

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 User WebDialer page of Cisco Unified Communications Manager (Unified CM) could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack.

The vulnerability is due to insufficient CSRF protections. An attacker could exploit this vulnerability by convincing the user of the affected system to follow a malicious link or visit an attacker-controlled website. A successful exploit could allow the attacker to dial calls on behalf of the affected user.

Cisco has confirmed this vulnerability in a security notice; however, software updates are not available.

To exploit the vulnerability, the attacker may provide a link to a malicious site and persuade the user to follow the link by using misleading language and instructions.

Affected Products

Customers should refer to Cisco bug ID CSCui13028 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 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 contact the vendor regarding future updates and releases.

Users are advised not to open email messages from suspicious or unrecognized sources. If users cannot verify that links or attachments included in email messages are safe, they are advised not to open them.

For additional information about cross-site request forgery attacks and potential mitigation methods, see the Cisco Applied Mitigation Bulletin Understanding Cross-Site Request Forgery Threat Vectors.

Administrators are advised to monitor affected systems.

Fixed Software

Software updates are not available.

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-2013-3450

Revision History

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

Legal Disclaimer