Cisco Security Advisory

Cisco Unified Communications Manager Multiple Vulnerabilities

Advisory ID: Cisco-SA-20150522-CVE-2015-0749
Published: 2015 May 22 16:07 GMT
Version1.0: Final
CVSS Score: Base - 4.3
Workarounds: See below
Cisco Bug IDs: CSCut66725

CVE-2015-0749
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

Multiple vulnerabilities in Cisco Unified Communications Manager could allow an unauthenticated, remote attacker to conduct cross-site scripting (XSS), cross-site request forgery (XSRF), and phishing attacks on the affected software.

The vulnerabilities are due to improper input validation of certain parameters passed to the affected software. An attacker could exploit these vulnerabilities by convincing a user to follow a malicious link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected site or allow the attacker to access sensitive browser-based information.

Cisco has confirmed these vulnerabilities and software updates are available.

To exploit these vulnerabilities, the attacker may provide a link that directs a user to a malicious site and use misleading language or instructions to persuade the user to follow the link.

Affected Products

Cisco has released bug ID CSCut66725 for registered users, which contains additional details and an up-to-date list of affected product versions.

Vulnerable Products

At the time this alert was first published, Cisco Unified Communications Manager 10.5(2.10000.5) was vulnerable. Later versions of Cisco Unified Communications Manager 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.

Users should verify that unsolicited links are safe to follow.

For additional information about XSS attacks and the methods used to exploit these vulnerabilities, see the Cisco Applied Mitigation Bulletin Understanding Cross-Site Scripting (XSS) Threat Vectors.

For additional information about CSRF 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

Cisco customers with active contracts can obtain updates through the Software Center at the following link: Cisco. Cisco customers without contracts can obtain upgrades by contacting the Cisco Technical Assistance Center at 1-800-553-2447 or 1-408-526-7209 or via email at *tac@cisco.com*.

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-20150522-CVE-2015-0749

Revision History

Version	Description	Section	Status	Date
1.0	Initial Release	NA	Final	2015-May-22

Legal Disclaimer