Cisco Security Advisory

Cisco Unified Communications Manager iFrame Data Clickjacking Vulnerability

Advisory ID:	cisco-sa-20161012-ucm
Published:	2016 October 12 16:00 GMT
Version1.0:	Final
CVSS Score:	Base - 4.3
Workarounds:	No workarounds available
Cisco Bug IDs:	CSCuz64683 CSCuz64698

CVE-2016-6440
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

The Cisco Unified Communications Manager (CUCM) may be vulnerable to data that can be displayed inside an *iframe* within a web page, which in turn could lead to a clickjacking attack. Protection mechanisms should be used to prevent this type of attack.

The vulnerability is due to a lack of proper input sanitization of *iframe* data within the HTTP requests sent to the device. An attacker could exploit this vulnerability by sending crafted HTTP packets with malicious *iframe* data. An exploit could allow the attacker to perform a clickjacking or phishing attack where the user is tricked into clicking on a malicious link. Protection mechanisms should be used to prevent this type of attack.

Cisco has released software updates that address this vulnerability. Workarounds that address this vulnerability are not available.

This advisory is available at the following link:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161012-ucm

Affected Products

Vulnerable Products

Cisco Unified Communications Manager (CUCM) is affected.

Products Confirmed Not Vulnerable

No other Cisco products are currently known to be affected by this vulnerability.

Workarounds

Workarounds that address this vulnerability are not available.

Fixed Software

Cisco provides information about fixed software in Cisco bugs, which are accessible through the Cisco Bug Search Tool.

When considering software upgrades, customers are advised to consult the Cisco Security Advisories and Responses archive at http://www.cisco.com/go/psirt and review subsequent advisories to determine exposure and a complete upgrade solution.

In all cases, customers should ensure that the devices to be upgraded contain sufficient memory and confirm that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, customers are advised to contact the Cisco Technical Assistance Center (TAC) or their contracted maintenance providers.

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-20161012-ucm

---

Revision History

Version	Description	Section	Status	Date
1.0	Initial public release.	-	Final	2016-October-12

Legal Disclaimer