Cisco Security Advisory

Cisco Unified Communications Manager Web Interface Cross-Site Scripting Vulnerability

Medium

Advisory ID: cisco-sa-20161116-ucm
Published: 2016 November 16 16:00 GMT
Version1.0: Final
CVSS Score: Base - 4.3
Workarounds: No workarounds available
Cisco Bug IDs: CSCvb37121

CVE-2016-6472
CWE-79

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 several parameters of the ccmivr page of Cisco Unified Communication Manager (CallManager) could allow an unauthenticated, remote attacker to launch a cross-site scripting (XSS) attack against a user of the web interface on the affected system.

The vulnerability is due to insufficient input validation of some parameters used by that page. An attacker could exploit this vulnerability by convincing the user of the system to follow an attacker-supplied link. An exploit could allow the attacker to cause arbitrary script or HTML code to be executed on the user's browser within the context of the affected application.

Cisco has not released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

This advisory is available at the following link:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161116-ucm

Affected Products

Vulnerable Products

This vulnerability affects Cisco Unified Communications Manager.

Products Confirmed Not Vulnerable

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

Workarounds

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

Fixed Software

For information about fixed software releases, consult the Cisco bug ID(s) at the top of this advisory.

When considering software upgrades, customers are advised to regularly consult the advisories for Cisco products, which are available from the Cisco Security Advisories and Alerts page, 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-20161116-ucm

---

Revision History

Version	Description	Section	Status	Date
1.0	Initial public release.	-	Final	2016-November-16

Legal Disclaimer