Cisco Security Advisory

Cisco Unified Communications Manager Cross-Site Scripting Vulnerability

Advisory ID: cisco-sa-20170118-cucm
Published: 2017 January 18 16:00 GMT
Version1.0: Final
CVSS Score: Base - 6.1
Workarounds: No workarounds available
Cisco Bug IDs: CSCvb97237

CVE-2017-3798
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 cross-site scripting (XSS) filter bypass vulnerability in the web-based management interface of Cisco Unified Communications Manager could allow an unauthenticated, remote attacker to mount XSS attacks against a user of an affected device.

The vulnerability is due to a failure to properly call XSS filter subsystems when a URL contains a certain parameter. An attacker who can persuade an authenticated user of an affected device to follow an attacker-provided link or visit an attacker-controlled website could exploit this vulnerability to execute arbitrary code in the context of the affected site in the user's browser.

There are no workarounds that address this vulnerability.

This advisory is available at the following link:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170118-cucm

Affected Products

Vulnerable Products

This vulnerability affects Cisco Unified Communications Manager. For information about affected software releases, consult the Cisco bug ID(s) at the top of this advisory.

Products Confirmed Not Vulnerable

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

Workarounds

There are no workarounds that address this vulnerability.

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

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170118-cucm

---

Revision History

Version	Description	Section	Status	Date
1.0	Initial public release.	-	Final	2017-January-18

Legal Disclaimer