

Cisco Security Advisory

Cisco Unified Communications Manager Cross-Site Scripting Vulnerability



Advisory ID: cisco-sa-20170118-cucm
Published: 2017 January 18 16:00 GMT
Version 1.0: Final
CVSS Score: [Base - 6.1](#)
Workarounds: No workarounds available
Cisco Bug IDs: [CSCvb97237](#)

[CVE-2017-3798](#) [Download CVRF](#)
[CWE-79](#) [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

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

A standalone copy or paraphrase of the text of this document that omits the distribution URL is an uncontrolled copy and may lack important information or contain factual errors. The information in this document is intended for end users of Cisco products.

<p>Information For</p> <ul style="list-style-type: none"> Small Business Midsized Business Service Provider Executives <p>Industries ></p> <p>Marketplace</p> <p>Contacts</p> <ul style="list-style-type: none"> Contact Cisco Find a Reseller 	<p>News & Alerts</p> <ul style="list-style-type: none"> Newsroom Blogs Field Notices Security Advisories <p>Technology Trends</p> <ul style="list-style-type: none"> Cloud Internet of Things (IoT) Mobility Software Defined Networking (SDN) 	<p>Support</p> <ul style="list-style-type: none"> Downloads Documentation <p>Communities</p> <ul style="list-style-type: none"> DevNet Learning Network Support Community <p>Video Portal ></p>	<p>About Cisco</p> <ul style="list-style-type: none"> Investor Relations Corporate Social Responsibility Environmental Sustainability Tomorrow Starts Here Our People <p>Careers</p> <ul style="list-style-type: none"> Search Jobs Life at Cisco <p>Programs</p> <ul style="list-style-type: none"> Cisco Designated VIP Program Cisco Powered Financing Options
---	--	--	--