



CVE-2019-12716

Published on: 10/02/2019 12:00:00 AM UTC

Last Modified on: 02/16/2023 02:41:00 AM UTC

CVE-2019-12716 - advisory for cisco-sa-20191002-cucm-xss-12716

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Unified Communications Manager](#) from [Cisco](#) contain the following vulnerability:

A vulnerability in the web-based interface of Cisco Unified Communications Manager and Cisco Unified Communications Manager Session Management Edition (SME) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based interface. The

vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected software. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-based information.

CVE-2019-12716 has been assigned by [psirt@cisco.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

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.

Affected Vendor/Software: [Cisco](#) - **Cisco Unified Communications Manager** version n/a

CVSS3 Score: **6.1 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE

Confidentiality Impact	Integrity Impact	Availability Impact				
NONE	PARTIAL	NONE				
CVE References						
Description	Tags	Link				
Cisco Unified Communications Manager Cross-Site Scripting Vulnerability	Vendor Advisory tools.cisco.com text/html	 CISCO 20191002 Cisco Unified Communications Manager Cross-Site Scripting Vulnerability				
By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.						
There are currently no QIDs associated with this CVE						
Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Unified Communications Manager	10.5(2.10000.5)	All	All	All
Application	Cisco	Unified Communications Manager	10.5\2.10000.5\	All	All	All
Application	Cisco	Unified Communications Manager	11.5(1.10000.6)	All	All	All
Application	Cisco	Unified Communications Manager	11.5\1.10000.6\	All	All	All
Application	Cisco	Unified Communications Manager	12.0(1.10000.10)	All	All	All
Application	Cisco	Unified Communications Manager	12.0\1.10000.10\	All	All	All
Application	Cisco	Unified Communications Manager	12.5(1.10000.22)	All	All	All
Application	Cisco	Unified Communications Manager	12.5\1.10000.22\	All	All	All
Application	Cisco	Unified Communications Manager	10.5\2.10000.5\	All	All	All
Application	Cisco	Unified Communications Manager	11.5\1.10000.6\	All	All	All
Application	Cisco	Unified Communications Manager	12.0\1.10000.10\	All	All	All
Application	Cisco	Unified Communications Manager	12.5\1.10000.22\	All	All	All
cpe:2.3:a:cisco:unified_communications_manager:10.5(2.10000.5):*****:						
cpe:2.3:a:cisco:unified_communications_manager:10.5\2.10000.5\):*****:						
cpe:2.3:a:cisco:unified_communications_manager:11.5(1.10000.6):*****:						
cpe:2.3:a:cisco:unified_communications_manager:11.5\1.10000.6\):*****:						
cpe:2.3:a:cisco:unified_communications_manager:12.0(1.10000.10):*****:						
cpe:2.3:a:cisco:unified_communications_manager:12.0\1.10000.10\):*****:						
cpe:2.3:a:cisco:unified_communications_manager:12.5(1.10000.22):*****:						

cpe:2.3:a:cisco:unified_communications_manager:12.5(1.10000.22\):*.~.*~.*~.*~.*~.*~.*:
cpe:2.3:a:cisco:unified_communications_manager:10.5(2.10000.5\):*.~.*~.*~.*~.*~.*~.*:
cpe:2.3:a:cisco:unified_communications_manager:11.5(1.10000.6\):*.~.*~.*~.*~.*~.*~.*:
cpe:2.3:a:cisco:unified_communications_manager:12.0(1.10000.10\):*.~.*~.*~.*~.*~.*~.*:
cpe:2.3:a:cisco:unified_communications_manager:12.5(1.10000.22\):*.~.*~.*~.*~.*~.*~.*:

cpe:2.3:a:cisco:unified_communications_manager:12.5(1.10000.22\):*.~.*~.*~.*~.*~.*~.*:
cpe:2.3:a:cisco:unified_communications_manager:10.5(2.10000.5\):*.~.*~.*~.*~.*~.*~.*:
cpe:2.3:a:cisco:unified_communications_manager:11.5(1.10000.6\):*.~.*~.*~.*~.*~.*~.*:
cpe:2.3:a:cisco:unified_communications_manager:12.0(1.10000.10\):*.~.*~.*~.*~.*~.*~.*:
cpe:2.3:a:cisco:unified_communications_manager:12.5(1.10000.22\):*.~.*~.*~.*~.*~.*~.*:

cpe:2.3:a:cisco:unified_communications_manager:12.5(1.10000.22\):*.~.*~.*~.*~.*~.*~.*:
cpe:2.3:a:cisco:unified_communications_manager:10.5(2.10000.5\):*.~.*~.*~.*~.*~.*~.*:
cpe:2.3:a:cisco:unified_communications_manager:11.5(1.10000.6\):*.~.*~.*~.*~.*~.*~.*:
cpe:2.3:a:cisco:unified_communications_manager:12.0(1.10000.10\):*.~.*~.*~.*~.*~.*~.*:
cpe:2.3:a:cisco:unified_communications_manager:12.5(1.10000.22\):*.~.*~.*~.*~.*~.*~.*:

cpe:2.3:a:cisco:unified_communications_manager:12.5(1.10000.22\):*.~::~.*:
cpe:2.3:a:cisco:unified_communications_manager:10.5(2.10000.5\):*.~::~.*:
cpe:2.3:a:cisco:unified_communications_manager:11.5(1.10000.6\):*.~::~.*:
cpe:2.3:a:cisco:unified_communications_manager:12.0(1.10000.10\):*.~::~.*:
cpe:2.3:a:cisco:unified_communications_manager:12.5(1.10000.22\):*.~::~.*:

cpe:2.3:a:cisco:unified_communications_manager:12.5(1.10000.22\):*.~.*~.*~.*~.*~.*~.*:
cpe:2.3:a:cisco:unified_communications_manager:10.5(2.10000.5\):*.~.*~.*~.*~.*~.*~.*:
cpe:2.3:a:cisco:unified_communications_manager:11.5(1.10000.6\):*.~.*~.*~.*~.*~.*~.*:
cpe:2.3:a:cisco:unified_communications_manager:12.0(1.10000.10\):*.~.*~.*~.*~.*~.*~.*:
cpe:2.3:a:cisco:unified_communications_manager:12.5(1.10000.22\):*.~.*~.*~.*~.*~.*~.*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

© CVE.report 2023 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report