

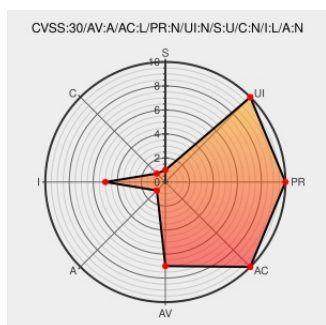


CVE-2020-3222

Published on: 06/03/2020 12:00:00 AM UTC

Last Modified on: 09/22/2021 07:55:00 PM UTC

CVE-2020-3222 - advisory for cisco-sa-webui-unauthprxy-KXXsbWh

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of **ios Xe** from **Cisco** contain the following vulnerability:

A vulnerability in the web-based user interface (web UI) of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to bypass access control restrictions on an affected device. The vulnerability is due to the presence of a proxy service at a specific endpoint of the web UI. An attacker could exploit this vulnerability by

connecting to the proxy service. An exploit could allow the attacker to bypass access restrictions on the network by proxying their access request through the management network of the affected device. As the proxy is reached over the management virtual routing and forwarding (VRF), this could reduce the effectiveness of the bypass.

CVE-2020-3222 has been assigned by [Cisco](#) 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 IOS XE Software 16.10.1** version **n/a**

CVSS3 Score: **4.3 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
ADJACENT_NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	LOW	NONE

CVSS2 Score: **3.3 - LOW**

Access Vector	Access Complexity	Authentication
ADJACENT_NETWORK	LOW	NONE
Confidentiality	Integrity	Availability

Impact	Impact	Impact				
NONE	PARTIAL	NONE				
CVE References						
Description	Tags	Link				
Cisco IOS XE Software Web UI Unauthenticated Proxy Service Vulnerability	Patch Vendor Advisory tools.cisco.com text/html	 CISCO 20200603 Cisco IOS XE Software Web UI Unauthenticated Proxy Service 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
Operating System	Cisco	los Xe	16.10.1	All	All	All
Operating System	Cisco	los Xe	16.10.1a	All	All	All
Operating System	Cisco	los Xe	16.10.1b	All	All	All
Operating System	Cisco	los Xe	16.10.1c	All	All	All
Operating System	Cisco	los Xe	16.10.1d	All	All	All
Operating System	Cisco	los Xe	16.10.1e	All	All	All
Operating System	Cisco	los Xe	16.10.1f	All	All	All
Operating System	Cisco	los Xe	16.10.1g	All	All	All
Operating System	Cisco	los Xe	16.10.1s	All	All	All
Operating System	Cisco	los Xe	16.10.2	All	All	All
Operating System	Cisco	los Xe	16.11.1	All	All	All
Operating System	Cisco	los Xe	16.11.1a	All	All	All
Operating System	Cisco	los Xe	16.11.1b	All	All	All
Operating	Cisco	los Xe	16.11.1c	All	All	All

System						
Operating System	Cisco	los Xe	16.11.1s	All	All	All
Operating System	Cisco	los Xe	16.12.1	All	All	All
Operating System	Cisco	los Xe	16.12.1a	All	All	All
Operating System	Cisco	los Xe	16.12.1c	All	All	All
Operating System	Cisco	los Xe	16.12.1s	All	All	All
Operating System	Cisco	los Xe	16.12.1t	All	All	All
Operating System	Cisco	los Xe	16.12.1w	All	All	All
Operating System	Cisco	los Xe	16.12.1y	All	All	All
Operating System	Cisco	los Xe	16.10.1	All	All	All
Operating System	Cisco	los Xe	16.10.1a	All	All	All
Operating System	Cisco	los Xe	16.10.1b	All	All	All
Operating System	Cisco	los Xe	16.10.1c	All	All	All
Operating System	Cisco	los Xe	16.10.1d	All	All	All
Operating System	Cisco	los Xe	16.10.1e	All	All	All
Operating System	Cisco	los Xe	16.10.1f	All	All	All
Operating System	Cisco	los Xe	16.10.1g	All	All	All
Operating System	Cisco	los Xe	16.10.1s	All	All	All
Operating System	Cisco	los Xe	16.10.2	All	All	All
Operating System	Cisco	los Xe	16.11.1	All	All	All
Operating System	Cisco	los Xe	16.11.1a	All	All	All
Operating System	Cisco	los Xe	16.11.1b	All	All	All
Operating System	Cisco	los Xe	16.11.1c	All	All	All
Operating	Cisco	los Xe	16.11.1s	All	All	All

System						
Operating System	Cisco	ios Xe	16.12.1	All	All	All
Operating System	Cisco	ios Xe	16.12.1a	All	All	All
Operating System	Cisco	ios Xe	16.12.1c	All	All	All
Operating System	Cisco	ios Xe	16.12.1s	All	All	All
Operating System	Cisco	ios Xe	16.12.1t	All	All	All
Operating System	Cisco	ios Xe	16.12.1w	All	All	All
Operating System	Cisco	ios Xe	16.12.1y	All	All	All
cpe:2.3:o:cisco:ios_xe:16.10.1:*****:						
cpe:2.3:o:cisco:ios_xe:16.10.1a:*****:						
cpe:2.3:o:cisco:ios_xe:16.10.1b:*****:						
cpe:2.3:o:cisco:ios_xe:16.10.1c:*****:						
cpe:2.3:o:cisco:ios_xe:16.10.1d:*****:						
cpe:2.3:o:cisco:ios_xe:16.10.1e:*****:						
cpe:2.3:o:cisco:ios_xe:16.10.1f:*****:						
cpe:2.3:o:cisco:ios_xe:16.10.1g:*****:						
cpe:2.3:o:cisco:ios_xe:16.10.1s:*****:						
cpe:2.3:o:cisco:ios_xe:16.10.2:*****:						
cpe:2.3:o:cisco:ios_xe:16.11.1:*****:						
cpe:2.3:o:cisco:ios_xe:16.11.1a:*****:						
cpe:2.3:o:cisco:ios_xe:16.11.1b:*****:						
cpe:2.3:o:cisco:ios_xe:16.11.1c:*****:						
cpe:2.3:o:cisco:ios_xe:16.11.1s:*****:						
cpe:2.3:o:cisco:ios_xe:16.12.1:*****:						
cpe:2.3:o:cisco:ios_xe:16.12.1a:*****:						
cpe:2.3:o:cisco:ios_xe:16.12.1c:*****:						
cpe:2.3:o:cisco:ios_xe:16.12.1s:*****:						

cpe:2.3:o:cisco:ios_xe:16.12.1t:*****:
cpe:2.3:o:cisco:ios_xe:16.12.1w:*****:
cpe:2.3:o:cisco:ios_xe:16.12.1y:*****:
cpe:2.3:o:cisco:ios_xe:16.10.1:*****:
cpe:2.3:o:cisco:ios_xe:16.10.1a:*****:
cpe:2.3:o:cisco:ios_xe:16.10.1b:*****:
cpe:2.3:o:cisco:ios_xe:16.10.1c:*****:
cpe:2.3:o:cisco:ios_xe:16.10.1d:*****:
cpe:2.3:o:cisco:ios_xe:16.10.1e:*****:
cpe:2.3:o:cisco:ios_xe:16.10.1f:*****:
cpe:2.3:o:cisco:ios_xe:16.10.1g:*****:
cpe:2.3:o:cisco:ios_xe:16.10.1s:*****:
cpe:2.3:o:cisco:ios_xe:16.10.2:*****:
cpe:2.3:o:cisco:ios_xe:16.11.1:*****:
cpe:2.3:o:cisco:ios_xe:16.11.1a:*****:
cpe:2.3:o:cisco:ios_xe:16.11.1b:*****:
cpe:2.3:o:cisco:ios_xe:16.11.1c:*****:
cpe:2.3:o:cisco:ios_xe:16.11.1s:*****:
cpe:2.3:o:cisco:ios_xe:16.12.1:*****:
cpe:2.3:o:cisco:ios_xe:16.12.1a:*****:
cpe:2.3:o:cisco:ios_xe:16.12.1c:*****:
cpe:2.3:o:cisco:ios_xe:16.12.1s:*****:
cpe:2.3:o:cisco:ios_xe:16.12.1t:*****:
cpe:2.3:o:cisco:ios_xe:16.12.1w:*****:
cpe:2.3:o:cisco:ios_xe:16.12.1y:*****:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
--------	-------	--------------

© [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](#)