



CVE-2020-3211

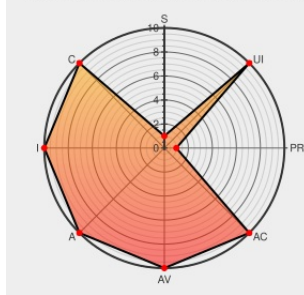
Published on: 06/03/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:40 PM UTC

CVE-2020-3211 - advisory for cisco-sa-web-cmdinj4-S2TmH7GA

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

CVSS:30/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H



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

A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to execute arbitrary commands with root privileges on the underlying operating system of an affected device. The vulnerability is due to improper input sanitization. An attacker who has valid administrative access to an affected device could exploit this

vulnerability by supplying a crafted input parameter on a form in the web UI and then submitting that form. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device, which could lead to complete system compromise.

CVE-2020-3211 has been assigned by [Cisco psirt@cisco.com](#) to track the vulnerability - currently rated as **HIGH** 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: **7.2 - HIGH**

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

CVSS2 Score: **9 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality	Integrity	Availability

Impact	Impact	Impact				
COMPLETE	COMPLETE	COMPLETE				
CVE References						
Description	Tags	Link				
Cisco IOS XE Software Web UI Command Injection Vulnerability	Patch Vendor Advisory tools.cisco.com text/html	 CISCO 20200603 Cisco IOS XE Software Web UI Command Injection 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	ios Xe	16.10.1	All	All	All
Operating System	Cisco	ios Xe	16.10.1a	All	All	All
Operating System	Cisco	ios Xe	16.10.1b	All	All	All
Operating System	Cisco	ios Xe	16.10.1e	All	All	All
Operating System	Cisco	ios Xe	16.10.1s	All	All	All
Operating System	Cisco	ios Xe	16.10.2	All	All	All
Operating System	Cisco	ios Xe	16.11.1	All	All	All
Operating System	Cisco	ios Xe	16.11.1a	All	All	All
Operating System	Cisco	ios Xe	16.11.1b	All	All	All
Operating System	Cisco	ios Xe	16.11.1c	All	All	All
Operating System	Cisco	ios Xe	16.11.1s	All	All	All
Operating System	Cisco	ios Xe	16.12.1	All	All	All
Operating System	Cisco	ios Xe	16.12.1a	All	All	All
Operating	Cisco	ios Xe	16.12.1c	All	All	All

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:16.10.1:~::~::~:
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:16.10.1e:~::~::~:
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:~::~::~:

No vendor comments have been submitted for this CVE

© [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](#)