

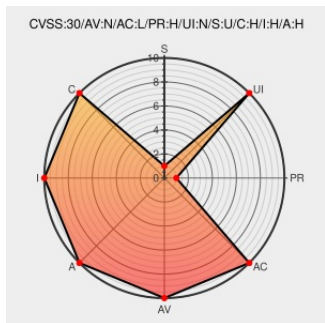


CVE-2020-3212

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

Last Modified on: 03/23/2021 11:23:39 PM UTC

CVE-2020-3212 - advisory for cisco-sa-web-cmdinj3-44st5CcA

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

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 could exploit this vulnerability by uploading a crafted file to the web UI

of an affected device. A successful exploit could allow the attacker to inject and execute arbitrary commands with root privileges on the device.

CVE-2020-3212 has been assigned by [Cisco PSIRT](#) 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 16.11.1** 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 Impact	Integrity Impact	Availability 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	16.11.1	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	16.12.1y	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	16.12.1y	All	All	All

```
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:16.12.1y:~::~::~:
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:16.12.1y:~::~::~:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)