

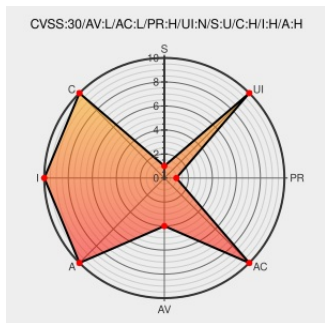


CVE-2020-3403

Published on: 09/24/2020 12:00:00 AM UTC

Last Modified on: 10/27/2022 03:47:00 PM UTC

CVE-2020-3403 - advisory for cisco-sa-iosxe-cmdinj-2MzhjM6K

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

Certain versions of [Catalyst 9800-40](#) from [Cisco](#) contain the following vulnerability:

A vulnerability in the CLI of Cisco IOS XE Software could allow an authenticated, local attacker to inject a command to the underlying operating system that will execute with root privileges upon the next reboot of the device. The authenticated user must have privileged EXEC permissions on the device. The vulnerability is due to insufficient

protection of values passed to a script that executes during device startup. An attacker could exploit this vulnerability by writing values to a specific file. A successful exploit could allow the attacker to execute commands with root privileges each time the affected device is restarted.

CVE-2020-3403 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** version n/a

CVSS3 Score: **7.8 - HIGH**

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

CVSS2 Score: **7.2 - HIGH**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact

CVE References

Description	Tags	Link
Cisco IOS XE Software Command Injection Vulnerability	Vendor Advisory tools.cisco.com text/html	🌐 CISCO 20200924 Cisco IOS XE Software 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
Hardware  	Cisco	Catalyst 9800-40	-	All	All	All
Hardware  	Cisco	Catalyst 9800-40	-	All	All	All
Hardware  	Cisco	Catalyst 9800-80	-	All	All	All
Hardware  	Cisco	Catalyst 9800-80	-	All	All	All
Hardware  	Cisco	Catalyst 9800-cl	-	All	All	All
Hardware  	Cisco	Catalyst 9800-cl	-	All	All	All
Hardware  	Cisco	Catalyst 9800-l	-	All	All	All
Hardware  	Cisco	Catalyst 9800-l	-	All	All	All
Hardware  	Cisco	Catalyst 9800-l-c	-	All	All	All
Hardware  	Cisco	Catalyst 9800-l-c	-	All	All	All
Hardware  	Cisco	Catalyst 9800-l-f	-	All	All	All
Hardware  	Cisco	Catalyst 9800-l-f	-	All	All	All
Application	Cisco	ios Xe	17.2.1	All	All	All
Operating System	Cisco	ios Xe	17.2.1	All	All	All
Application	Cisco	ios Xe	17.2.1	All	All	All

```
cpe:2.3:h:cisco:catalyst_9800-40:-:*~
```

```
cpe:2.3:h:cisco:catalyst_9800-40:-:*:*:*:*:*:
```

```
cpe:2.3:h:cisco:catalyst_9800-80:-:*:*:*:*:*:
```

```
cpe:2.3:h:cisco:catalyst_9800-80:-:*:*:*:*:*:
```

cpe:2.3:h:cisco:catalyst_9800-cl:-:*:*:*:*:*:
cpe:2.3:h:cisco:catalyst_9800-cl:-:*:*:*:*:*:
cpe:2.3:h:cisco:catalyst_9800-l:-:*:*:*:*:*:
cpe:2.3:h:cisco:catalyst_9800-l:-:*:*:*:*:*:
cpe:2.3:h:cisco:catalyst_9800-l-c:-:*:*:*:*:*:
cpe:2.3:h:cisco:catalyst_9800-l-c:-:*:*:*:*:*:
cpe:2.3:h:cisco:catalyst_9800-l-f:-:*:*:*:*:*:
cpe:2.3:h:cisco:catalyst_9800-l-f:-:*:*:*:*:*:
cpe:2.3:a:cisco:ios_xe:17.2.1:*:*:*:*:*:
cpe:2.3:o:cisco:ios_xe:17.2.1:*:*:*:*:*:
cpe:2.3:a:cisco:ios_xe:17.2.1:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
← 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