



CVE-2021-1374

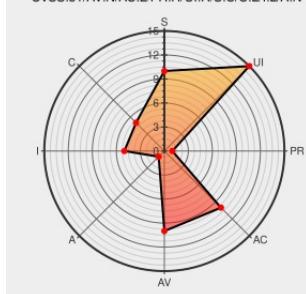
Published on: 03/24/2021 12:00:00 AM UTC

Last Modified on: 03/29/2021 07:46:00 PM UTC

CVE-2021-1374 - advisory for cisco-sa-ewlc-xss-cAfMtCzv

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

CVSS:31/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N



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

A vulnerability in the web-based management interface of Cisco IOS XE Wireless Controller software for the Catalyst 9000 Family of switches could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against another user of the web-based management interface of an affected device. The vulnerability is due to

insufficient validation of user-supplied input by the web-based management interface of an affected device. An attacker could exploit this vulnerability by authenticating to the device as a high-privileged user, adding certain configurations with malicious code in one of its fields, and persuading another user to click on it. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or to access sensitive, browser-based information.

CVE-2021-1374 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 - Cisco IOS XE Software** version **n/a**

CVSS3 Score: **4.8 - MEDIUM**

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

CVSS2 Score: **3.5 - LOW**

Access Vector	Access Complexity	Authentication
---------------	-------------------	----------------

NETWORK	MEDIUM	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Cisco IOS XE Wireless Controller Software for the Catalyst 9000 Family Stored Cross-Site Scripting Vulnerability	tools.cisco.com text/html	CISCO 20210324 Cisco IOS XE Wireless Controller Software for the Catalyst 9000 Family Stored 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.

Related QID Numbers

316913 Cisco IOS XE Wireless Controller Software for the Catalyst 9000 Family Stored Cross-Site Scripting Vulnerability(cisco-sa-ewlc-xss-cAfMtGzv)

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	16.10.1c	All	All	All
Operating System	Cisco	Ios Xe	16.10.1d	All	All	All
Operating System	Cisco	Ios Xe	16.10.1e	All	All	All
Operating System	Cisco	Ios Xe	16.10.1f	All	All	All
Operating System	Cisco	Ios Xe	16.10.1g	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	16.10.3	All	All	All
Operating System	Cisco	Ios 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 System	Cisco	los Xe	16.11.1s	All	All	All
Operating System	Cisco	los Xe	16.11.2	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	16.12.1x	All	All	All
Operating System	Cisco	los Xe	16.12.1y	All	All	All
Operating System	Cisco	los Xe	16.12.1z	All	All	All
Operating System	Cisco	los Xe	16.12.2	All	All	All
Operating System	Cisco	los Xe	16.12.2a	All	All	All
Operating System	Cisco	los Xe	16.12.2s	All	All	All
Operating System	Cisco	los Xe	16.12.2t	All	All	All
Operating System	Cisco	los Xe	16.12.3	All	All	All
Operating System	Cisco	los Xe	16.12.3a	All	All	All
Operating System	Cisco	los Xe	16.12.3s	All	All	All
Operating System	Cisco	los Xe	16.12.4	All	All	All
Operating System	Cisco	los Xe	16.12.4a	All	All	All

Operating System	Cisco	ios Xe	16.6.1	All	All	All
Operating System	Cisco	ios Xe	16.6.2	All	All	All
Operating System	Cisco	ios Xe	16.6.3	All	All	All
Operating System	Cisco	ios Xe	16.6.4	All	All	All
Operating System	Cisco	ios Xe	16.6.4a	All	All	All
Operating System	Cisco	ios Xe	16.6.4s	All	All	All
Operating System	Cisco	ios Xe	16.6.5	All	All	All
Operating System	Cisco	ios Xe	16.6.5a	All	All	All
Operating System	Cisco	ios Xe	16.6.5b	All	All	All
Operating System	Cisco	ios Xe	16.6.6	All	All	All
Operating System	Cisco	ios Xe	16.6.7	All	All	All
Operating System	Cisco	ios Xe	16.6.7a	All	All	All
Operating System	Cisco	ios Xe	16.6.8	All	All	All
Operating System	Cisco	ios Xe	16.7.1	All	All	All
Operating System	Cisco	ios Xe	16.7.1a	All	All	All
Operating System	Cisco	ios Xe	16.7.1b	All	All	All
Operating System	Cisco	ios Xe	16.7.2	All	All	All
Operating System	Cisco	ios Xe	16.7.3	All	All	All
Operating System	Cisco	ios Xe	16.7.4	All	All	All
Operating System	Cisco	ios Xe	16.8.1	All	All	All
Operating System	Cisco	ios Xe	16.8.1a	All	All	All
Operating System	Cisco	ios Xe	16.8.1b	All	All	All
Operating System	Cisco	ios Xe	16.8.1c	All	All	All

System						
Operating System	Cisco	ios Xe	16.8.1d	All	All	All
Operating System	Cisco	ios Xe	16.8.1e	All	All	All
Operating System	Cisco	ios Xe	16.8.1s	All	All	All
Operating System	Cisco	ios Xe	16.8.2	All	All	All
Operating System	Cisco	ios Xe	16.8.3	All	All	All
Operating System	Cisco	ios Xe	16.9.1	All	All	All
Operating System	Cisco	ios Xe	16.9.1a	All	All	All
Operating System	Cisco	ios Xe	16.9.1b	All	All	All
Operating System	Cisco	ios Xe	16.9.1c	All	All	All
Operating System	Cisco	ios Xe	16.9.1d	All	All	All
Operating System	Cisco	ios Xe	16.9.1s	All	All	All
Operating System	Cisco	ios Xe	16.9.2	All	All	All
Operating System	Cisco	ios Xe	16.9.2a	All	All	All
Operating System	Cisco	ios Xe	16.9.2s	All	All	All
Operating System	Cisco	ios Xe	16.9.3	All	All	All
Operating System	Cisco	ios Xe	16.9.3a	All	All	All
Operating System	Cisco	ios Xe	16.9.3h	All	All	All
Operating System	Cisco	ios Xe	16.9.3s	All	All	All
Operating System	Cisco	ios Xe	16.9.4	All	All	All
Operating System	Cisco	ios Xe	16.9.4c	All	All	All
Operating System	Cisco	ios Xe	16.9.5	All	All	All
Operating System	Cisco	ios Xe	16.9.5f	All	All	All
Operating System	Cisco	ios Xe	17.1.1	All	All	All

System						
Operating System	Cisco	ios Xe	17.1.1a	All	All	All
Operating System	Cisco	ios Xe	17.1.1s	All	All	All
Operating System	Cisco	ios Xe	17.1.1t	All	All	All
Operating System	Cisco	ios Xe	17.1.2	All	All	All
Operating System	Cisco	ios Xe	17.2.1	All	All	All
Operating System	Cisco	ios Xe	17.2.1a	All	All	All
Operating System	Cisco	ios Xe	17.2.1r	All	All	All
Operating System	Cisco	ios Xe	17.2.1v	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:16.10.3:*****:						
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:16.11.2:*****:						
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:16.12.1x:*****:
cpe:2.3:o:cisco:ios_xe:16.12.1y:*****:
cpe:2.3:o:cisco:ios_xe:16.12.1z:*****:
cpe:2.3:o:cisco:ios_xe:16.12.2:*****:
cpe:2.3:o:cisco:ios_xe:16.12.2a:*****:
cpe:2.3:o:cisco:ios_xe:16.12.2s:*****:
cpe:2.3:o:cisco:ios_xe:16.12.2t:*****:
cpe:2.3:o:cisco:ios_xe:16.12.3:*****:
cpe:2.3:o:cisco:ios_xe:16.12.3a:*****:
cpe:2.3:o:cisco:ios_xe:16.12.3s:*****:
cpe:2.3:o:cisco:ios_xe:16.12.4:*****:
cpe:2.3:o:cisco:ios_xe:16.12.4a:*****:
cpe:2.3:o:cisco:ios_xe:16.6.1:*****:
cpe:2.3:o:cisco:ios_xe:16.6.2:*****:
cpe:2.3:o:cisco:ios_xe:16.6.3:*****:
cpe:2.3:o:cisco:ios_xe:16.6.4:*****:
cpe:2.3:o:cisco:ios_xe:16.6.4a:*****:
cpe:2.3:o:cisco:ios_xe:16.6.4s:*****:
cpe:2.3:o:cisco:ios_xe:16.6.5:*****:
cpe:2.3:o:cisco:ios_xe:16.6.5a:*****:
cpe:2.3:o:cisco:ios_xe:16.6.5b:*****:
cpe:2.3:o:cisco:ios_xe:16.6.6:*****:
cpe:2.3:o:cisco:ios_xe:16.6.7:*****:
cpe:2.3:o:cisco:ios_xe:16.6.7a:*****:

cpe:2.3:0:cisco:ios_xe:16.6.7a:*****:
cpe:2.3:0:cisco:ios_xe:16.6.8:*****:
cpe:2.3:0:cisco:ios_xe:16.7.1:*****:
cpe:2.3:0:cisco:ios_xe:16.7.1a:*****:
cpe:2.3:0:cisco:ios_xe:16.7.1b:*****:
cpe:2.3:0:cisco:ios_xe:16.7.2:*****:
cpe:2.3:0:cisco:ios_xe:16.7.3:*****:
cpe:2.3:0:cisco:ios_xe:16.7.4:*****:
cpe:2.3:0:cisco:ios_xe:16.8.1:*****:
cpe:2.3:0:cisco:ios_xe:16.8.1a:*****:
cpe:2.3:0:cisco:ios_xe:16.8.1b:*****:
cpe:2.3:0:cisco:ios_xe:16.8.1c:*****:
cpe:2.3:0:cisco:ios_xe:16.8.1d:*****:
cpe:2.3:0:cisco:ios_xe:16.8.1e:*****:
cpe:2.3:0:cisco:ios_xe:16.8.1s:*****:
cpe:2.3:0:cisco:ios_xe:16.8.2:*****:
cpe:2.3:0:cisco:ios_xe:16.8.3:*****:
cpe:2.3:0:cisco:ios_xe:16.9.1:*****:
cpe:2.3:0:cisco:ios_xe:16.9.1a:*****:
cpe:2.3:0:cisco:ios_xe:16.9.1b:*****:
cpe:2.3:0:cisco:ios_xe:16.9.1c:*****:
cpe:2.3:0:cisco:ios_xe:16.9.1d:*****:
cpe:2.3:0:cisco:ios_xe:16.9.1s:*****:
cpe:2.3:0:cisco:ios_xe:16.9.2:*****:
cpe:2.3:0:cisco:ios_xe:16.9.2a:*****:
cpe:2.3:0:cisco:ios_xe:16.9.2s:*****:
cpe:2.3:0:cisco:ios_xe:16.9.3:*****:
cpe:2.3:0:cisco:ios_xe:16.9.3a:*****:
cpe:2.3:0:cisco:ios_xe:16.9.3h:*****:

cpe:2.3:o:cisco:ios_xe:16.9.3s:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:cisco:ios_xe:16.9.4:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:cisco:ios_xe:16.9.4c:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:cisco:ios_xe:16.9.5:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:cisco:ios_xe:16.9.5f:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:cisco:ios_xe:17.1.1:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:cisco:ios_xe:17.1.1a:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:cisco:ios_xe:17.1.1s:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:cisco:ios_xe:17.1.1t:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:cisco:ios_xe:17.1.2:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:cisco:ios_xe:17.2.1:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:cisco:ios_xe:17.2.1a:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:cisco:ios_xe:17.2.1r:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:cisco:ios_xe:17.2.1v:~::~~::~~::~~::~~::~~::~~:::

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)
← Previous ID Next ID→		