

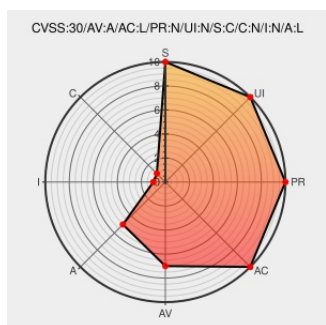


CVE-2020-3206

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

Last Modified on: 09/17/2021 06:36:00 PM UTC

CVE-2020-3206 - advisory for cisco-sa-ewlc-dos-AnvKvMxR

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

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

A vulnerability in the handling of IEEE 802.11w Protected Management Frames (PMFs) of Cisco Catalyst 9800 Series Wireless Controllers that are running Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to terminate a valid user connection to an affected device. The vulnerability exists because the affected software does not

properly validate 802.11w disassociation and deauthentication PMFs that it receives. An attacker could exploit this vulnerability by sending a spoofed 802.11w PMF from a valid, authenticated client on a network adjacent to an affected device. A successful exploit could allow the attacker to terminate a single valid user connection to the affected device.

CVE-2020-3206 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 16.10.1** version **n/a**

CVSS3 Score: **4.7 - MEDIUM**

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

CVSS2 Score: **3.3 - LOW**

Access Vector	Access Complexity	Authentication
ADJACENT_NETWORK	LOW	NONE
Confidentiality	Integrity	Availability

Impact

NONE

Impact

NONE

Impact

PARTIAL

CVE References

Description

Cisco IOS XE Software Catalyst 9800 Series Wireless Controllers Denial of Service Vulnerability

Tags

Patch

Vendor Advisory

tools.cisco.com

text/html

Link

 CISCO 20200603 Cisco IOS XE Software Catalyst 9800 Series Wireless Controllers Denial of 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

Exploit/POC from Github

PoC for exploiting CVE-2020-3206 : A vulnerability in the handling of IEEE 802.11w Protected Management Frames (PMFs)...

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	16.10.1e	All	All	All
Operating System	Cisco	ios Xe	16.10.1s	All	All	All
Operating System	Cisco	ios Xe	16.10.1	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
cpe:2.3:o:cisco:ios_xe:16.10.1:*:*:*:*:*:						
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:16.10.1:*:*:*:*:*:						
cpe:2.3:o:cisco:ios_xe:16.10.1e:*:*:*:*:*:						
cpe:2.3:o:cisco:ios_xe:16.10.1s:*:*:*:*:*:						

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](#)