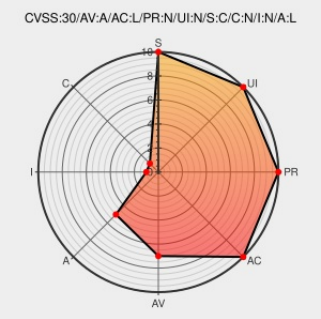
CVE-2020-3206

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 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 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	Impact	Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Cisco IOS XE Software Catalyst 9800 Series Wireless Controllers Denial of Service Vulnerability	Patch Vendor Advisory tools.cisco.com text/html	CISCO 20200603 Cisco IOS XE Software Catalyst 9800 Series Wireless Controllers Denial of Service Vulnerability

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 and Source URL Uptime Status status.cve.report