



CVE-2020-3220

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

Last Modified on: 03/23/2021 11:23:38 PM UTC

CVE-2020-3220 - advisory for cisco-sa-iosxe-vpn-dos-edOmW28Z

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

CVSS:30/AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:N/A:H



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

A vulnerability in the hardware crypto driver of Cisco IOS XE Software for Cisco 4300 Series Integrated Services Routers and Cisco Catalyst 9800-L Wireless Controllers could allow an unauthenticated, remote attacker to disconnect legitimate IPsec VPN sessions to an affected device. The vulnerability is due to insufficient verification of authenticity

of received Encapsulating Security Payload (ESP) packets. An attacker could exploit this vulnerability by tampering with ESP cleartext values as a man-in-the-middle.

CVE-2020-3220 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 IOS XE Software 16.4.1** version n/a

CVSS3 Score: **6.8 - MEDIUM**

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

CVSS2 Score: **7.1 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	COMPLETE

CVE References						
Description	Tags			Link		
Cisco IOS XE Software IPsec VPN Denial of Service Vulnerability	Patch Vendor Advisory tools.cisco.com text/html			 CISCO 20200603 Cisco IOS XE Software IPsec VPN 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						
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	16.11.1	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	Cisco	Ios Xe	16.11.1s	All	All	All

System						
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	16.12.1y	All	All	All
Operating System	Cisco	los Xe	16.4.1	All	All	All
Operating System	Cisco	los Xe	16.4.2	All	All	All
Operating System	Cisco	los Xe	16.4.3	All	All	All
Operating System	Cisco	los Xe	16.5.1	All	All	All
Operating System	Cisco	los Xe	16.5.1a	All	All	All
Operating System	Cisco	los Xe	16.5.1b	All	All	All
Operating System	Cisco	los Xe	16.5.2	All	All	All
Operating System	Cisco	los Xe	16.5.3	All	All	All
Operating System	Cisco	los Xe	16.6.1	All	All	All
Operating System	Cisco	los Xe	16.6.2	All	All	All
Operating System	Cisco	los Xe	16.6.3	All	All	All
Operating System	Cisco	los Xe	16.6.4	All	All	All
Operating System	Cisco	los Xe	16.6.4a	All	All	All
Operating System	Cisco	los Xe	16.6.4s	All	All	All
Operating System	Cisco	los Xe	16.6.5	All	All	All
Operating	Cisco	los Xe	16.6.5a	All	All	All

System						
Operating System	Cisco	los Xe	16.6.5b	All	All	All
Operating System	Cisco	los Xe	16.6.6	All	All	All
Operating System	Cisco	los Xe	16.7.1	All	All	All
Operating System	Cisco	los Xe	16.7.1a	All	All	All
Operating System	Cisco	los Xe	16.7.1b	All	All	All
Operating System	Cisco	los Xe	16.7.2	All	All	All
Operating System	Cisco	los Xe	16.7.3	All	All	All
Operating System	Cisco	los Xe	16.7.4	All	All	All
Operating System	Cisco	los Xe	16.8.1	All	All	All
Operating System	Cisco	los Xe	16.8.1a	All	All	All
Operating System	Cisco	los Xe	16.8.1b	All	All	All
Operating System	Cisco	los Xe	16.8.1c	All	All	All
Operating System	Cisco	los Xe	16.8.1d	All	All	All
Operating System	Cisco	los Xe	16.8.1e	All	All	All
Operating System	Cisco	los Xe	16.8.1s	All	All	All
Operating System	Cisco	los Xe	16.8.2	All	All	All
Operating System	Cisco	los Xe	16.8.3	All	All	All
Operating System	Cisco	los Xe	16.9.1	All	All	All
Operating System	Cisco	los Xe	16.9.1a	All	All	All
Operating System	Cisco	los Xe	16.9.1b	All	All	All
Operating System	Cisco	los Xe	16.9.1c	All	All	All
Operating System	Cisco	los Xe	16.9.1d	All	All	All
Operating	Cisco	los Xe	16.9.1s	All	All	All

System						
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	16.10.1	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	16.11.1	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	16.12.1	All	All	All

Operating System	Cisco	Ios Xe	16.12.1	All	All	All
Operating System	Cisco	Ios Xe	16.12.1a	All	All	All
Operating System	Cisco	Ios Xe	16.12.1c	All	All	All
Operating System	Cisco	Ios Xe	16.12.1s	All	All	All
Operating System	Cisco	Ios Xe	16.12.1t	All	All	All
Operating System	Cisco	Ios Xe	16.12.1w	All	All	All
Operating System	Cisco	Ios Xe	16.12.1y	All	All	All
Operating System	Cisco	Ios Xe	16.4.1	All	All	All
Operating System	Cisco	Ios Xe	16.4.2	All	All	All
Operating System	Cisco	Ios Xe	16.4.3	All	All	All
Operating System	Cisco	Ios Xe	16.5.1	All	All	All
Operating System	Cisco	Ios Xe	16.5.1a	All	All	All
Operating System	Cisco	Ios Xe	16.5.1b	All	All	All
Operating System	Cisco	Ios Xe	16.5.2	All	All	All
Operating System	Cisco	Ios Xe	16.5.3	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	16.6.3D	All	All	All
Operating System	Cisco	IOS XE	16.6.6	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
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	los Xe	16.9.2	All	All	All
Operating System	Cisco	los Xe	16.9.2a	All	All	All
Operating System	Cisco	los Xe	16.9.2s	All	All	All
Operating System	Cisco	los Xe	16.9.3	All	All	All
Operating System	Cisco	los Xe	16.9.3a	All	All	All
Operating System	Cisco	los Xe	16.9.3h	All	All	All
Operating System	Cisco	los Xe	16.9.3s	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:16.11.1:*****:						
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:16.12.1:*****:						
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:16.12.1y:*****:
cpe:2.3:o:cisco:ios_xe:16.4.1:*****:
cpe:2.3:o:cisco:ios_xe:16.4.2:*****:
cpe:2.3:o:cisco:ios_xe:16.4.3:*****:
cpe:2.3:o:cisco:ios_xe:16.5.1:*****:
cpe:2.3:o:cisco:ios_xe:16.5.1a:*****:
cpe:2.3:o:cisco:ios_xe:16.5.1b:*****:
cpe:2.3:o:cisco:ios_xe:16.5.2:*****:
cpe:2.3:o:cisco:ios_xe:16.5.3:*****:
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:16.7.1:*****:
cpe:2.3:o:cisco:ios_xe:16.7.1a:*****:
cpe:2.3:o:cisco:ios_xe:16.7.1b:*****:
cpe:2.3:o:cisco:ios_xe:16.7.2:*****:
cpe:2.3:o:cisco:ios_xe:16.7.3:*****:
cpe:2.3:o:cisco:ios_xe:16.7.4:*****:
cpe:2.3:o:cisco:ios_xe:16.8.1:*****:
cpe:2.3:o:cisco:ios_xe:16.8.1a:*****:
cpe:2.3:o:cisco:ios_xe:16.8.1b:*****:

cpe:2.3:o:cisco:ios_xe:16.8.1d:*****:
cpe:2.3:o:cisco:ios_xe:16.8.1e:*****:
cpe:2.3:o:cisco:ios_xe:16.8.1s:*****:
cpe:2.3:o:cisco:ios_xe:16.8.2:*****:
cpe:2.3:o:cisco:ios_xe:16.8.3:*****:
cpe:2.3:o:cisco:ios_xe:16.9.1:*****:
cpe:2.3:o:cisco:ios_xe:16.9.1a:*****:
cpe:2.3:o:cisco:ios_xe:16.9.1b:*****:
cpe:2.3:o:cisco:ios_xe:16.9.1c:*****:
cpe:2.3:o:cisco:ios_xe:16.9.1d:*****:
cpe:2.3:o:cisco:ios_xe:16.9.1s:*****:
cpe:2.3:o:cisco:ios_xe:16.9.2:*****:
cpe:2.3:o:cisco:ios_xe:16.9.2a:*****:
cpe:2.3:o:cisco:ios_xe:16.9.2s:*****:
cpe:2.3:o:cisco:ios_xe:16.9.3:*****:
cpe:2.3:o:cisco:ios_xe:16.9.3a:*****:
cpe:2.3:o:cisco:ios_xe:16.9.3h:*****:
cpe:2.3:o:cisco:ios_xe:16.9.3s:*****:
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:16.11.1:*****:
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:16.12.1:*****:
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:16.12.1y:*****:
cpe:2.3:o:cisco:ios_xe:16.4.1:*****:
cpe:2.3:o:cisco:ios_xe:16.4.2:*****:
cpe:2.3:o:cisco:ios_xe:16.4.3:*****:
cpe:2.3:o:cisco:ios_xe:16.5.1:*****:
cpe:2.3:o:cisco:ios_xe:16.5.1a:*****:
cpe:2.3:o:cisco:ios_xe:16.5.1b:*****:
cpe:2.3:o:cisco:ios_xe:16.5.2:*****:
cpe:2.3:o:cisco:ios_xe:16.5.3:*****:
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:16.7.1:*****:
cpe:2.3:o:cisco:ios_xe:16.7.1a:*****:
cpe:2.3:o:cisco:ios_xe:16.7.1b:*****:
cpe:2.3:o:cisco:ios_xe:16.7.2:*****:
cpe:2.3:o:cisco:ios_xe:16.7.3:*****:
cpe:2.3:o:cisco:ios_xe:16.7.4:*****:
cpe:2.3:o:cisco:ios_xe:16.8.1:*****:
cpe:2.3:o:cisco:ios_xe:16.8.1a:*****:
cpe:2.3:o:cisco:ios_xe:16.8.1b:*****:
cpe:2.3:o:cisco:ios_xe:16.8.1c:*****:
cpe:2.3:o:cisco:ios_xe:16.8.1d:*****:
cpe:2.3:o:cisco:ios_xe:16.8.1e:*****:
cpe:2.3:o:cisco:ios_xe:16.8.1s:*****:
cpe:2.3:o:cisco:ios_xe:16.8.2:*****:
cpe:2.3:o:cisco:ios_xe:16.8.3:*****:
cpe:2.3:o:cisco:ios_xe:16.9.1:*****:
cpe:2.3:o:cisco:ios_xe:16.9.1a:*****:
cpe:2.3:o:cisco:ios_xe:16.9.1b:*****:
cpe:2.3:o:cisco:ios_xe:16.9.1c:*****:
cpe:2.3:o:cisco:ios_xe:16.9.1d:*****:
cpe:2.3:o:cisco:ios_xe:16.9.1s:*****:
cpe:2.3:o:cisco:ios_xe:16.9.2:*****:
cpe:2.3:o:cisco:ios_xe:16.9.2a:*****:
cpe:2.3:o:cisco:ios_xe:16.9.2s:*****:
cpe:2.3:o:cisco:ios_xe:16.9.3:*****:
cpe:2.3:o:cisco:ios_xe:16.9.3a:*****:

cpe:2.3:o:cisco:ios_xe:16.9.3h:*****:

cpe:2.3:o:cisco:ios_xe:16.9.3s:*****:

No vendor comments have been submitted for this CVE

[← 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](#)