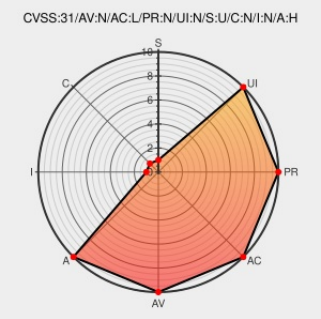
CVE-2021-1431

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

Last Modified on: 11/07/2023 03:28:00 AM UTC

CVE-2021-1431 - advisory for cisco-sa-iosxe-sdwdos-4zeEeC9w

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Ios Xe from Cisco contain the following vulnerability:

A vulnerability in the vDaemon process of Cisco IOS XE SD-WAN Software could allow an unauthenticated, remote attacker to cause a device to reload, resulting a denial of service (DoS) condition. This vulnerability is due to insufficient handling of malformed packets. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition.

CVE-2021-1431 has been assigned by 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: 7.5 - HIGH

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

CVSS2 Score: 7.8 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
Cisco IOS XE SD-WAN Software vDaemon Denial of Service Vulnerability	tools.cisco.com text/html	CISCO 20210324 Cisco IOS XE SD-WAN Software vDaemon Denial of Service Vulnerability

Related QID Numbers

317133 Cisco Internetwork Operating System (IOS) XE SD-WAN Software vDaemon Denial of Service (DoS) Vulnerability (cisco-sa-iosxe-sdwdos-4zeEeC9w)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	16.11.2	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	16.12.1x	All	All	All
Operating System	Cisco	Ios Xe	16.12.1y	All	All	All
Operating System	Cisco	Ios Xe	16.12.1z	All	All	All

Operating System	Cisco	Ios Xe	16.12.1z	All	All	All
Operating System	Cisco	Ios Xe	16.12.2	All	All	All
Operating System	Cisco	Ios Xe	16.12.2a	All	All	All
Operating System	Cisco	Ios Xe	16.12.2s	All	All	All
Operating System	Cisco	Ios Xe	16.12.2t	All	All	All
Operating System	Cisco	Ios Xe	16.12.3	All	All	All
Operating System	Cisco	Ios Xe	16.12.3a	All	All	All
Operating System	Cisco	Ios Xe	16.12.3s	All	All	All
Operating System	Cisco	Ios Xe	16.12.4	All	All	All
Operating System	Cisco	Ios Xe	16.12.4a	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
Operating System	Cisco	Ios Xe	17.2.2	All	All	All
Operating System	Cisco	Ios Xe	17.2.3	All	All	All
Operating System	Cisco	Ios Xe	3.15.1xbs	All	All	All
Operating System	Cisco	Ios Xe	3.15.2xbs	All	All	All

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:16.12.1:*:*:*:*:*:*:*

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: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:*:*:*:*:*:*:*

cpe:2.3:o:cisco:ios_xe:17.2.2:*:*:*:*:*:*:*

cpe:2.3:o:cisco:ios_xe:17.2.3:*:*:*:*:*:*:*

cpe:2.3:o:cisco:ios_xe:3.15.1xbs:*:*:*:*:*:*:*

cpe:2.3:o:cisco:ios_xe:3.15.2xbs:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→