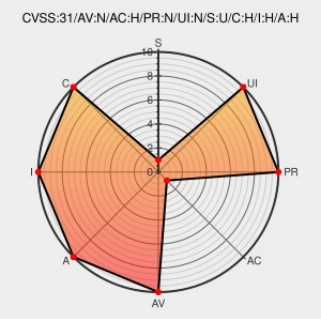
CVE-2021-1433

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

Last Modified on: 03/29/2021 08:04:00 PM UTC

CVE-2021-1433 - advisory for cisco-sa-iosxe-buffover-CqdRWLc

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 in Cisco IOS XE SD-WAN Software could allow an unauthenticated, remote attacker to cause a buffer overflow on an affected device. This vulnerability is due to insufficient bounds checking when the device processes traffic. An attacker could exploit this vulnerability by sending crafted traffic to the device. The attacker must have a man-in-the-middle position between Cisco vManage and an associated device that is running an affected version of Cisco IOS XE SD-WAN Software. An exploit could allow the attacker to conduct a controllable buffer overflow attack (and possibly execute arbitrary commands as the root user) or cause a device reload, resulting in a denial of service (DoS) condition.

CVE-2021-1433 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: 8.1 - HIGH

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

CVSS2 Score: 9.3 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE

Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

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

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	16.12.1	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	16.12.1za	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

System						
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	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	3.15.1xbs	All	All	All
Operating System	Cisco	Ios Xe	3.15.2xbs	All	All	All

cpe:2.3:o:cisco:ios_xe:16.12.1:*:*:*:*:*:*:*:

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:16.12.1za:*:*:*:*:*:*:*:

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: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: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→