



# CVE-2021-1431

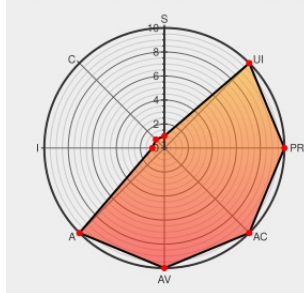
Published on: 03/24/2021 12:00:00 AM UTC

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](#)

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H



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 [Cisco PSIRT](#) 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    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>NONE</b>         | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>NONE</b>            | <b>NONE</b>         | <b>HIGH</b>         |

CVSS2 Score: **7.8 - HIGH**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>LOW</b>        | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>NONE</b>            | <b>NONE</b>       | <b>COMPLETE</b>     |

CVE References

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Tags                                                         | Link                                                                                                |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| Cisco IOS XE SD-WAN Software vDaemon Denial of Service Vulnerability                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | <a href="#">tools.cisco.com</a><br><a href="#">text/html</a> | <a href="#">CISCO 20210324 Cisco IOS XE SD-WAN Software vDaemon Denial of Service Vulnerability</a> |
| 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 <a href="mailto:comment@cve.report">comment@cve.report</a> . |                                                              |                                                                                                     |

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 | <a href="#">Cisco</a> | <a href="#">ios Xe</a> | 16.11.1  | All    | All     | All      |
| Operating System | <a href="#">Cisco</a> | <a href="#">ios Xe</a> | 16.11.1a | All    | All     | All      |
| Operating System | <a href="#">Cisco</a> | <a href="#">ios Xe</a> | 16.11.1b | All    | All     | All      |
| Operating System | <a href="#">Cisco</a> | <a href="#">ios Xe</a> | 16.11.1c | All    | All     | All      |
| Operating System | <a href="#">Cisco</a> | <a href="#">ios Xe</a> | 16.11.1s | All    | All     | All      |
| Operating System | <a href="#">Cisco</a> | <a href="#">ios Xe</a> | 16.11.2  | All    | All     | All      |
| Operating System | <a href="#">Cisco</a> | <a href="#">ios Xe</a> | 16.12.1  | All    | All     | All      |
| Operating System | <a href="#">Cisco</a> | <a href="#">ios Xe</a> | 16.12.1a | All    | All     | All      |
| Operating System | <a href="#">Cisco</a> | <a href="#">ios Xe</a> | 16.12.1c | All    | All     | All      |
| Operating System | <a href="#">Cisco</a> | <a href="#">ios Xe</a> | 16.12.1s | All    | All     | All      |
| Operating System | <a href="#">Cisco</a> | <a href="#">ios Xe</a> | 16.12.1t | All    | All     | All      |
| Operating System | <a href="#">Cisco</a> | <a href="#">ios Xe</a> | 16.12.1w | All    | All     | All      |
| Operating System | <a href="#">Cisco</a> | <a href="#">ios Xe</a> | 16.12.1x | All    | All     | All      |
| Operating System | <a href="#">Cisco</a> | <a href="#">ios Xe</a> | 16.12.1y | All    | All     | All      |
| Operating System | <a href="#">Cisco</a> | <a href="#">ios Xe</a> | 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:16.12.1a:~::~::~:  |
| 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)             |
|-------------------------------|-------|--------------------------|
| <a href="#">← Previous ID</a> |       | <a href="#">Next ID→</a> |

© [CVE.report](#) 2024   |

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](#)