

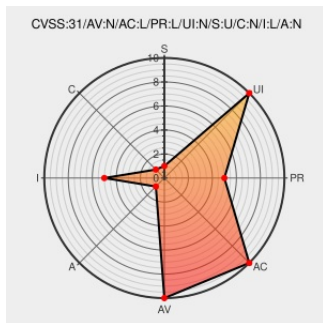


# CVE-2020-3591

Published on: 11/06/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:39 PM UTC

## CVE-2020-3591 - advisory for cisco-sa-vmanxssh-9KHEqRpM

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

Certain versions of [Sd-wan Vmanage](#) from [Cisco](#) contain the following vulnerability:

A vulnerability in the web-based management interface of the Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability exists because the web-based management interface does not properly validate user-supplied input.

An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.

CVE-2020-3591 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 SD-WAN vManage** version n/a

CVSS3 Score: **4.3 - MEDIUM**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>LOW</b>          | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>NONE</b>            | <b>LOW</b>          | <b>NONE</b>         |

CVSS2 Score: **3.5 - LOW**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>MEDIUM</b>     | <b>SINGLE</b>       |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
|                        |                   |                     |

NONE

PARTIAL

NONE

## CVE References

| Description                                             | Tags                                                                                                                                                     | Link                                                                                   |
|---------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| Cisco SD-WAN vManage Cross-Site Scripting Vulnerability | <a href="#">Patch</a><br><a href="#">Vendor Advisory</a><br><a href="https://tools.cisco.com/text/html">tools.cisco.com</a><br><a href="#">text/html</a> | <a href="#">CISCO 20201104 Cisco SD-WAN vManage Cross-Site Scripting 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 [comment@cve.report](mailto: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 |
|--------------------------------------------------|-----------------------|--------------------------------|---------|--------|---------|----------|
| Application                                      | <a href="#">Cisco</a> | <a href="#">Sd-wan Vmanage</a> | 20.3.1  | All    | All     | All      |
| Application                                      | <a href="#">Cisco</a> | <a href="#">Sd-wan Vmanage</a> | 20.3.1  | All    | All     | All      |
| Application                                      | <a href="#">Cisco</a> | <a href="#">Sd-wan Vmanage</a> | All     | All    | All     | All      |
| cpe:2.3:a:cisco:sd-wan_vmanage:20.3.1:*:*:*:*:*: |                       |                                |         |        |         |          |
| cpe:2.3:a:cisco:sd-wan_vmanage:20.3.1:*:*:*:*:*: |                       |                                |         |        |         |          |
| cpe:2.3:a:cisco:sd-wan_vmanage:*:*:*:*:*:        |                       |                                |         |        |         |          |

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](#)