

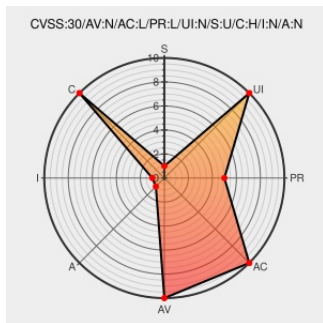


CVE-2020-3437

Published on: 07/16/2020 12:00:00 AM UTC

Last Modified on: 01/01/2022 06:45:00 PM UTC

CVE-2020-3437 - advisory for cisco-sa-vmanwebid-5QWMcCvt

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

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

A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to read arbitrary files on the underlying filesystem of the device. The vulnerability is due to insufficient file scope limiting. An attacker could exploit this vulnerability by creating a specific file reference on the

filesystem and then accessing it through the web-based management interface. A successful exploit could allow the attacker to read arbitrary files from the filesystem of the underlying operating system.

CVE-2020-3437 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: **6.5 - MEDIUM**

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

CVSS2 Score: **4 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact

PARTIAL

NONE

NONE

CVE References

Description	Tags	Link
Cisco SD-WAN vManage 19.2.2 Remote Root ≈ Packet Storm	packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/162958/Cisco-SD-WAN-vManage-19.2.2-Remote-Root.html
Cisco SD-WAN vManage Software Information Disclosure Vulnerability	Vendor Advisory tools.cisco.com text/html	 CISCO 20200715 Cisco SD-WAN vManage Software Information Disclosure 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	Sd-wan Firmware	All	All	All	All
Operating System	Cisco	Sd-wan Firmware	All	All	All	All
<code>cpe:2.3:o:cisco:sd-wan_firmware:*****:</code>						
<code>cpe:2.3:o:cisco:sd-wan_firmware:*****:</code>						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
--------	-------	--------------

[← 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](#)