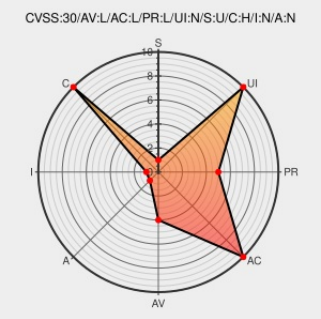
CVE-2021-1235

Published on: 01/20/2021 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:55 PM UTC

CVE-2021-1235 - advisory for cisco-sa-sdwan-vinfdis-MC8L58dj

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



Certain versions of Sd-wan Vmanage from Cisco contain the following vulnerability:

A vulnerability in the CLI of Cisco SD-WAN vManage Software could allow an authenticated, local attacker to read sensitive database files on an affected system. The vulnerability is due to insufficient user authorization. An attacker could exploit this vulnerability by accessing the vshell of an affected system. A successful exploit could allow the attacker to read database files from the filesystem of the underlying operating system.

CVE-2021-1235 has been assigned by 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: 5.5 - MEDIUM

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

CVSS2 Score: 4.9 - MEDIUM

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

CVE References

Description	Tags	Link
Cisco SD-WAN vManage Information Disclosure Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20210120 Cisco SD-WAN vManage 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

Exploit/POC from Github

CVE-2021-1235

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Sd-wan Vmanage	All	All	All	All
Application	Cisco	Sd-wan Vmanage	All	All	All	All

cpe:2.3:a:cisco:sd-wan_vmanage:*:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:sd-wan_vmanage:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report