



CVE-2020-3521

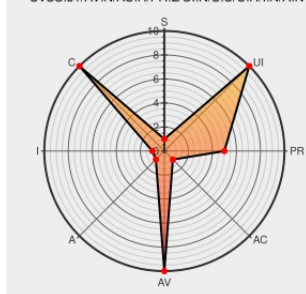
Published on: 08/26/2020 12:00:00 AM UTC

Last Modified on: 11/07/2023 03:22:00 AM UTC

CVE-2020-3521 - advisory for cisco-sa-dcnm-file-path-6PKONjHe

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

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



Certain versions of [Data Center Network Manager](#) from [Cisco](#) contain the following vulnerability:

A vulnerability in a specific REST API of Cisco Data Center Network Manager (DCNM) Software could allow an authenticated, remote attacker to conduct directory traversal attacks on an affected device. The vulnerability is due to insufficient validation of user-supplied input to the API. An attacker with a low-privileged account could exploit this

vulnerability by sending a crafted request to the API. A successful exploit could allow the attacker to read arbitrary files on the affected system.

CVE-2020-3521 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 Data Center Network Manager** 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 Data Center Network Manager Read File Path Traversal Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20200819 Cisco Data Center Network Manager Read File Path Traversal 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
Application	Cisco	Data Center Network Manager	All	All	All	All
Application	Cisco	Data Center Network Manager	All	All	All	All

cpe:2.3:a:cisco:data_center_network_manager:*:*:*:*:*:

cpe:2.3:a:cisco:data_center_network_manager:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→