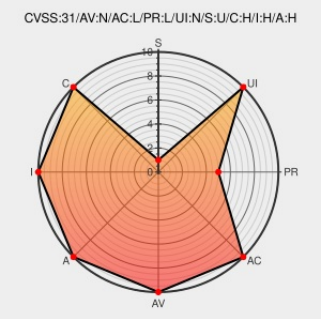
CVE-2020-3383

Published on: 07/30/2020 12:00:00 AM UTC

Last Modified on: 08/06/2021 06:59:00 PM UTC

CVE-2020-3383 - advisory for cisco-sa-dcnm-path-trav-2xZOnJdR

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



Certain versions of Data Center Network Manager from Cisco contain the following vulnerability:

A vulnerability in the archive utility of Cisco Data Center Network Manager (DCNM) could allow an authenticated, remote attacker to conduct directory traversal attacks on an affected device. The vulnerability is due to a lack of proper input validation of paths that are embedded within archive files. An attacker could exploit this vulnerability by sending a crafted request to an affected device. A successful exploit could allow the attacker to write arbitrary files in the system with the privileges of the logged-in user.

CVE-2020-3383 has been assigned by psirt@cisco.com 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 Data Center Network Manager** version **n/a**

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 9 - HIGH

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

CVE References

Description	Tags	Link
Cisco Data Center Network Manager Path Traversal Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20200729 Cisco Data Center Network Manager 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

Exploit/POC from Github

PoC for exploiting CVE-2020-3383 : A vulnerability in the archive utility of Cisco Data Center Network Manager (DCNM)…

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

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→