

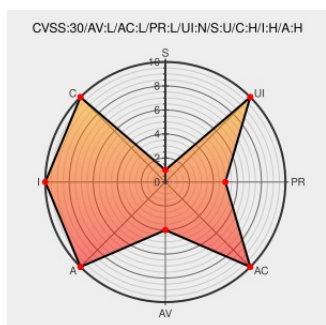


CVE-2020-3380

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

Last Modified on: 03/23/2021 11:23:38 PM UTC

CVE-2020-3380 - advisory for cisco-sa-dcnm-privescal-zxfCH7Dg

[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 CLI of Cisco Data Center Network Manager (DCNM) could allow an authenticated, local attacker to elevate privileges to root and execute arbitrary commands on the underlying operating system. The vulnerability is due to insufficient restrictions during the execution of an affected CLI command. An attacker could

exploit this vulnerability by authenticating as the fmserver user and submitting malicious input to a specific command. A successful exploit could allow the attacker to elevate privileges to root and execute arbitrary commands on the underlying operating system.

CVE-2020-3380 has been assigned by [Cisco](#) 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 - Cisco Data Center Network Manager** version n/a

CVSS3 Score: **7.8 - HIGH**

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

CVSS2 Score: **7.2 - HIGH**

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

COMPLETE

COMPLETE

COMPLETE

CVE References

Description

Tags

Link

Cisco Data Center Network Manager Privilege Escalation Vulnerability

Vendor Advisory
tools.cisco.com
text/html

 [CISCO 20200715 Cisco Data Center Network Manager Privilege Escalation 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 →](#)

© 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](#)