

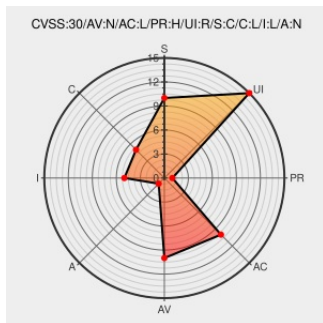


CVE-2020-3354

Published on: 06/17/2020 12:00:00 AM UTC

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

CVE-2020-3354 - advisory for cisco-sa-dcnm-stored-xss-VyE4bNAh

[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 web-based management interface of Cisco Data Center Network Manager (DCNM) could allow an authenticated, remote attacker with administrative credentials to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient input validation by the web-based management

interface. An attacker could exploit this vulnerability by inserting malicious data into a specific data field in the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker would need administrative credentials on the affected device.

CVE-2020-3354 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 - Cisco Data Center Network Manager** version n/a

CVSS3 Score: **4.8 - MEDIUM**

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

CVSS2 Score: **3.5 - LOW**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE

CVE References

DescriptionTagsLink

Cisco Data Center Network Manager Stored Cross-Site Scripting VulnerabilityVendor Advisorytools.cisco.comtext/htmlCISCO 20200617 Cisco Data Center Network Manager Stored Cross-Site Scripting 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)

TypeVendorProductVersionUpdateEditionLanguage

ApplicationCiscoData Center Network ManagerAllAllAllAll

ApplicationCiscoData Center Network ManagerAllAllAllAll

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 IDNext ID >