



CVE-2019-15983

Published on: 01/06/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:45 PM UTC

CVE-2019-15983 - advisory for cisco-sa-20200102-dcnm-xml-ext-entity

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

CVSS:30/AV:N/AC:L/PR:H/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 the SOAP API of Cisco Data Center Network Manager (DCNM) could allow an authenticated, remote attacker to gain read access to information that is stored on an affected system. To exploit this vulnerability, an attacker would need administrative privileges on the DCNM application. The vulnerability exists because

the SOAP API improperly handles XML External Entity (XXE) entries when parsing certain XML files. An attacker could exploit this vulnerability by inserting malicious XML content in an API request. A successful exploit could allow the attacker to read arbitrary files from the affected device. Note: The severity of this vulnerability is aggravated by the vulnerabilities described in the Cisco Data Center Network Manager Authentication Bypass Vulnerabilities advisory, published simultaneously with this one.

CVE-2019-15983 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: **4.9 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	HIGH	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 XML External Entity Read Access Vulnerability

Vendor Advisory

tools.cisco.com

text/html

CISCO 2020102

Cisco Data Center Network Manager XML External Entity Read Access 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 →