

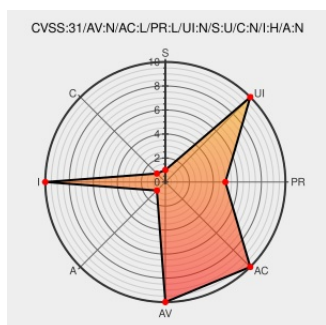


CVE-2020-3592

Published on: 11/06/2020 12:00:00 AM UTC

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

CVE-2020-3592 - advisory for cisco-sa-vmanuafw-ZHkdGGEy

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

Certain versions of [Catalyst Sd-wan Manager](#) from [Cisco](#) contain the following vulnerability:

A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to bypass authorization and modify the configuration of an affected system. The vulnerability is due to insufficient authorization checking on an affected system. An attacker could exploit this vulnerability by

sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to gain privileges beyond what would normally be authorized for their configured user authorization level. This could allow the attacker to modify the configuration of an affected system.

CVE-2020-3592 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 SD-WAN vManage** 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	NONE	HIGH	NONE

CVSS2 Score: **4 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality	Integrity	Availability
.....		

Impact

Impact

Impact

NONE

PARTIAL

NONE

CVE References

Description

Tags

Link

Cisco SD-WAN vManage Software Authorization Bypass Vulnerability

Patch

Vendor Advisory

tools.cisco.com

text/html

 CISCO 20201104 Cisco SD-WAN vManage Software Authorization Bypass 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

Catalyst Sd-wan Manager

20.3.1

All

All

All

Application

Cisco

Sd-wan Vmanage

20.3.1

All

All

All

Application

Cisco

Sd-wan Vmanage

20.3.1

All

All

All

Application

Cisco

Sd-wan Vmanage

All

All

All

All

cpe:2.3:a:cisco:catalyst_sd-wan_manager:20.3.1:*****:

cpe:2.3:a:cisco:sd-wan_vmanage:20.3.1:*****:

cpe:2.3:a:cisco:sd-wan_vmanage:20.3.1:*****:

cpe:2.3:a:cisco:sd-wan_vmanage:*****:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →