



CVE-2020-3374

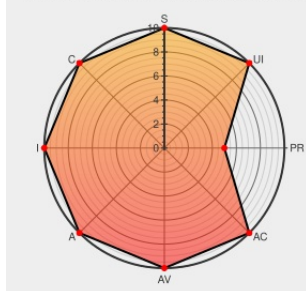
Published on: 07/30/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:39 PM UTC

CVE-2020-3374 - advisory for cisco-sa-uabvman-SYGzt8Bv

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

CVSS:30/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H



Certain versions of **Sd-wan** 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, enabling them to access sensitive information, modify the system configuration, or impact the availability of the affected system. The vulnerability is due to insufficient authorization

checking on the 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. The attacker may be able to access sensitive information, modify the system configuration, or impact the availability of the affected system.

CVE-2020-3374 has been assigned by [cisco](#) psirt@cisco.com to track the vulnerability - currently rated as **CRITICAL** 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 SD-WAN vManage** version **n/a**

CVSS3 Score: **9.9 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	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 SD-WAN vManage Software Authorization Bypass Vulnerability

Vendor Advisory

tools.cisco.com

text/html

CISCO 20200729 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

Sd-wan

All

All

All

All

Application

Cisco

Sd-wan

All

All

All

All

Application

Cisco

Sd-wan

All

All

All

All

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

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →