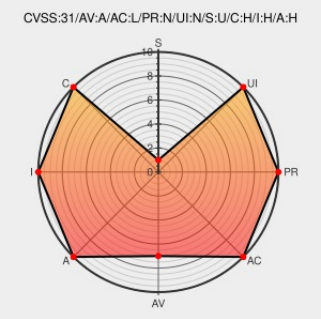
CVE-2021-1284

Published on: 05/06/2021 12:00:00 AM UTC

Last Modified on: 11/07/2023 03:27:00 AM UTC

CVE-2021-1284 - advisory for cisco-sa-sdw-auth-bypass-65aYqcS2

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 messaging service interface of Cisco SD-WAN vManage Software could allow an unauthenticated, adjacent attacker to bypass authentication and authorization and modify the configuration of an affected system. To exploit this vulnerability, the attacker must be able to access an associated Cisco SD-WAN vEdge device. This vulnerability is due to insufficient authorization checks. An attacker could exploit this vulnerability by sending crafted HTTP requests to the web-based messaging service interface of an affected system. A successful exploit could allow the attacker to gain unauthenticated read and write access to the affected vManage system. With this access, the attacker could access information about the affected vManage system, modify the configuration of the system, or make configuration changes to devices that are managed by the system.

CVE-2021-1284 has been assigned by 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 SD-WAN vManage** version **n/a**

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 5.8 - MEDIUM

Access Vector	Access Complexity	Authentication

Vector	Complexity	
ADJACENT_NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Cisco SD-WAN vManage Software Authentication Bypass Vulnerability	tools.cisco.com text/html	CISCO 20210505 Cisco SD-WAN vManage Software Authentication Bypass Vulnerability

Related QID Numbers

316970 Cisco SD-WAN vManage Software Authentication Bypass Vulnerability(cisco-sa-sdw-auth-bypass-65aYqcS2)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Catalyst Sd-wan Manager	All	All	All	All
Application	Cisco	Sd-wan Vmanage	All	All	All	All

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

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-1284 : A vulnerability in the web-based messaging service interface of Cisco SD-WAN vManage Software could… twitter.com/i/web/status/1…	2021-05-06 13:10:02

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report