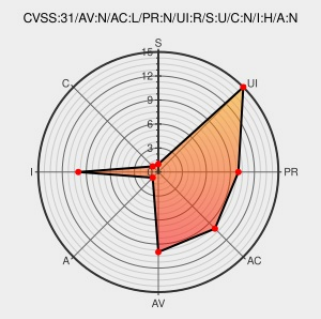
CVE-2022-20735

Published on: Not Yet Published

Last Modified on: 05/13/2022 07:05:00 PM UTC

CVE-2022-20735 - advisory for cisco-sa-sdwan-vmanage-csrf-rxQL4tXR

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Sd-wan Vmanage from Cisco contain the following vulnerability:

A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. This vulnerability is due to insufficient CSRF protections for the web-based management interface on an affected system. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the affected user. These actions could include modifying the system configuration and deleting accounts.

CVE-2022-20735 has been assigned by psirt@cisco.com to track the vulnerability - currently rated as MEDIUM severity.

The Cisco 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	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	HIGH	NONE

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**

NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
No Description Provided	tools.cisco.com text/html	CISCO 20220413 Cisco SD-WAN vManage Software Cross-Site Request Forgery 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.

Related QID Numbers

317152 Cisco SD-WAN vManage Software Cross-Site Request Forgery (CSRF) Vulnerability (cisco-sa-sdwan-vmanage-csrf-rxQL4tXR)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Sd-wan Vmanage	All	All	All	All
Application	Cisco	Sd-wan Vmanage	20.7	All	All	All

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

cpe:2.3:a:cisco:sd-wan_vmanage:20.7:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-20735 : A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could all… twitter.com/i/web/status/1…	2022-04-15 14:36:31
/r/netcve	CVE-2022-20735	2022-04-15 15:38:31

← Previous ID

Next ID→