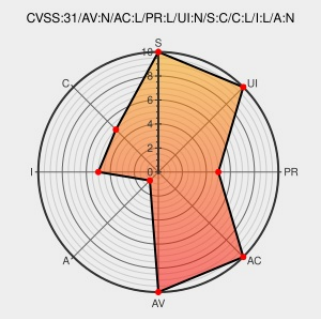
CVE-2021-1507

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

Last Modified on: 05/14/2021 02:38:00 PM UTC

CVE-2021-1507 - advisory for cisco-sa-vmanage-xss-eN75jxtW

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



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

A vulnerability in an API of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against users of the application web-based interface. This vulnerability exists because the API does not properly validate user-supplied input. An attacker could exploit this vulnerability by sending malicious input to the API. A successful exploit could allow the attacker to execute arbitrary script code in the context of the web-based interface or access sensitive, browser-based information.

CVE-2021-1507 has been assigned by 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: 5.4 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	LOW	LOW	NONE

CVSS2 Score: 3.5 - LOW

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**

NONE | PARTIAL | NONE

CVE References

Description	Tags	Link
Cisco SD-WAN vManage API Stored Cross-Site Scripting Vulnerability	tools.cisco.com text/html	CISCO 20210505 Cisco SD-WAN vManage API Stored Cross-Site Scripting 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

316987 Cisco SD-WAN vManage API Stored Cross-Site Scripting Vulnerability(cisco-sa-vmanage-xss-eN75jxtW)

Known Affected Configurations (CPE V2.3)

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

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-2021-1507 : A vulnerability in an API of Cisco SD-WAN vManage Software could allow an authenticated, remote a… twitter.com/i/web/status/1…	2021-05-06 12:57:47

← Previous ID

Next ID→