



CVE-2019-1624

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2019-1624
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-06-20 03:15:00 UTC
Updated	2019-10-09 23:47:00 UTC
Description	A vulnerability in the vManage web-based UI (Web UI) in the Cisco SD-WAN Solution could allow an authenticated, remote

Risk And Classification

Problem Types: CWE-77

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
Cisco SD-WAN Solution Command Injection Vulnerability	CISCO	tools.cisco.com	Vendor Advisory
Cisco SD-WAN Solution CVE-2019-1624 Remote Command Injection Vulnerability	BID	www.securityfocus.com	Third Party Advis
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analys

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

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