



CVE-2021-34726

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

Summary

CVE	CVE-2021-34726
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-09-23 03:15:00 UTC
Updated	2022-10-24 14:25:00 UTC
Description	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to inject arbitrary commands.

Risk And Classification

Problem Types: CWE-78

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
Cisco SD-WAN Software Command Injection Vulnerability	CISCO	tools.cisco.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[317056](#) Cisco SD-WAN Software Command Injection Vulnerability (cisco-sa-sdwan-maapi-cmdinjec-znUYTuC)

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)