



CVE-2021-1589

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

Summary

CVE	CVE-2021-1589
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-09-23 03:15:00 UTC
Updated	2023-11-07 03:28:00 UTC
Description	A vulnerability in the disaster recovery feature of Cisco SD-WAN vManage Software could allow an authenticated, remote a

Risk And Classification

Problem Types: CWE-522

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 vManage Software Disaster Recovery Feature Password Exposure Vulnerability	CISCO	tools.cisco.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, e

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

317058 Cisco SD-WAN vManage Software Disaster Recovery Feature Password Exposure Vulnerability (cisco-sa-sd-wan-credentials-ydYfskzZ)

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](#).

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