CVE-2023-20098

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2023-20098
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-05-09 18:15:00 UTC
Updated	2024-01-25 17:15:00 UTC
Description	A vulnerability in the CLI of Cisco SDWAN vManage Software could allow an authenticated, local attacker to delete arbitrary

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Catalyst Sd-wan Manager	20.11	All	All	All
Application	Cisco	Sd-wan Vmanage	All	All	All	All
Application	Cisco	Sd-wan Vmanage	20.11	All	All	All

References

Reference	Source	Link
Cisco vManage - Unauthorized data access (CVE-2023-20098) · Advisory · orangecertcc/security-research · GitHub	MISC	github.co
Cisco SD-WAN vManage Software Arbitrary File Deletion Vulnerability	MISC	sec.cloud
CVE Program record	CVE.ORG	www.cve.
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

317322 Cisco SD-WAN vManage Software Arbitrary File Deletion Vulnerability (cisco-sa-sdwan-vmanage-wfnqmYhN)

Free CVE JSON API cve.report/api

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