



CVE-2023-20034

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

Summary

CVE	CVE-2023-20034
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-09-27 18:15:00 UTC
Updated	2024-01-25 17:15:00 UTC
Description	Vulnerability in the Elasticsearch database used in the of Cisco SD-WAN vManage software could allow an unauthenticated

Risk And Classification

Problem Types: NVD-CWE-noinfo

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	20.6	All	All	All
Application	Cisco	Sd-wan	20.7	All	All	All

References

Reference	Source	Link	Tags
Cisco Catalyst SD-WAN Manager Vulnerabilities	MISC	sec.cloudapps.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

317361 Cisco SD-WAN vManage Information Disclosure Vulnerability (cisco-sa-sdwan-vman-sc-LRLfu2z)

completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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