



CVE-2023-20230

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2023-20230
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-08-23 19:15:00 UTC
Updated	2024-01-25 17:15:00 UTC
Description	A vulnerability in the restricted security domain implementation of Cisco Application Policy Infrastructure Controller (APIC) c

Risk And Classification

Problem Types: CWE-732

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Application Policy Infrastructure Controller	All	All	All	All

References

Reference	Source	Link	Tags
Cisco Application Policy Infrastructure Controller Unauthorized Policy Actions Vulnerability	MISC	sec.cloudapps.cisco.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[317347](#) Cisco Application Policy Infrastructure Controller Unauthorized Policy Actions Vulnerability (cisco-sa-apic-uapa-F4TASHk)

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