



CVE-2023-20011

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

Summary

| | |
|------------------------|------------------------------------------------------------------------------------------------------------------------------|
| CVE | CVE-2023-20011 |
| State | PUBLIC |
| Assigner | psirt@cisco.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2023-02-23 20:15:00 UTC |
| Updated | 2023-11-07 04:05:00 UTC |
| Description | A vulnerability in the web-based management interface of Cisco Application Policy Infrastructure Controller (APIC) and Cisco |

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|--------|----------------------------------------------|---------|--------|---------|----------|
| Application | Cisco | Application Policy Infrastructure Controller | All | All | All | All |
| Application | Cisco | Cloud Network Controller | All | All | All | All |

References

| Reference | Source |
|--------------------------------------------------------------------------------------------------------------------------------|---------|
| Cisco Application Policy Infrastructure Controller and Cisco Cloud Network Controller Cross-Site Request Forgery Vulnerability | CISCO |
| CVE Program record | CVE.ORG |
| NVD vulnerability detail | NVD |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

317301 Cisco Application Policy Infrastructure Controller (APIC) Cross-Site Request Forgery (CSRF) Vulnerability (cisco-sa-capic-csrfv-DMx6KSwV)

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