



# CVE-2021-1580

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

## Summary

<b>CVE</b>	CVE-2021-1580
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@cisco.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-08-25 20:15:00 UTC
<b>Updated</b>	2023-11-07 03:28:00 UTC
<b>Description</b>	Multiple vulnerabilities in the web UI and API endpoints of Cisco Application Policy Infrastructure Controller (APIC) or Cisco

## Risk And Classification

**Problem Types:** CWE-77

## 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 Application Policy Infrastructure Controller	All	All	All	All

## References

Reference	Source	Link	Tags
Cisco Application Policy Infrastructure Controller Command Injection and File Upload Vulnerabilities	CISCO	<a href="https://tools.cisco.com">tools.cisco.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

317030 Cisco Application Policy Infrastructure Controller (APIC) Command Injection Vulnerability (cisco-sa-capic-mdvul-HBsJBuW)

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](#).

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