CVE-2018-0427

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

Summary

CVE	CVE-2018-0427
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-08-15 20:29:00 UTC
Updated	2020-08-31 16:15:00 UTC
Description	A vulnerability in the CronJob scheduler API of Cisco Digital Network Architecture (DNA) Center could allow an authenticate

Risk And Classification

Problem Types: CWE-78

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Application Policy Infrastructure Controller Enterprise Module	dnac1.1	All	All	All
Application	Cisco	Application Policy Infrastructure Controller Enterprise Module	dnac1.1	All	All	All

References

Reference	Source	Link	Tags
Cisco Digital Network Architecture Center Command Injection Vulnerability	CISCO	tools.cisco.com	Vendor Advisory
Malformed Request	BID	www.securityfocus.com	Third Party Advisory, VDI
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.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

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