CVE-2020-11666

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

Summary

CVE	CVE-2020-11666
State	PUBLIC
Assigner	vuln@ca.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-04-15 20:15:00 UTC
Updated	2021-07-21 11:39:00 UTC
Description	CA API Developer Portal 4.3.1 and earlier contains an access control flaw that allows malicious users to elevate privileges.

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Broadcom	Ca Api Developer Portal	All	All	All	All

References

Reference	Source	Link	Tags
Broadcom Support Portal	MISC	techdocs.broadcom.com	Vendo
Full Disclosure: CA20200414-01: Security Notice for CA API Developer Portal	FULLDISC	seclists.org	Mailing
CA API Developer Portal 4.2.x / 4.3.1 Access Bypass / Privilege Escalation ≈ Packet Storm	MISC	packetstormsecurity.com	Third F
CA API Developer Portal 4.2.x / 4.3.1 Access Bypass / Privilege Escalation ≈ Packet Storm	MISC	packetstormsecurity.com	Third F
CVE Program record	CVE.ORG	www.cve.org	canoni
NVD vulnerability detail	NVD	nvd.nist.gov	canoni

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