CVE-2020-25200

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

Summary

CVE	CVE-2020-25200
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-10-01 18:15:00 UTC
Updated	2023-11-07 03:20:00 UTC
Description	** DISPUTED ** Pritunl 1.29.2145.25 allows attackers to enumerate valid VPN usernames via a series of /auth/session logi

Risk And Classification

Problem Types: CWE-203

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pritunl	Pritunl	1.29.2145.25	All	All	All
Application	Pritunl	Pritunl	1.29.2145.25	All	All	All

References

Reference	Source	Link	Tags
Pritunl - Advanced Security	MISC	pritunl.com	Vendor Advi
Pritunl - Enterprise Cloud Networking	MISC	pritunl.com	Vendor Advi
pritunl-CVE-2020-25200/CVE-2020-25200 at master · lukaszstu/pritunl-CVE-2020-25200 · GitHub	MISC	github.com	Third Party A
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

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