



CVE-2020-17365

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

Summary

CVE	CVE-2020-17365
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-09-24 23:15:00 UTC
Updated	2020-10-09 16:28:00 UTC
Description	Improper directory permissions in the Hotspot Shield VPN client software for Windows 10.3.0 and earlier may allow an auth

Risk And Classification

Problem Types: CWE-59 | CWE-732

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pango	Hotspot Shield	All	All	All	All

References

Reference	Source	Link	Tags
Security Updates Pango	MISC	www.pango.co	Vendor Advisory
CVE-2020-17365 - Hotspot Shield VPN New Privilege Escalation Vulnerability - Cymptom	MISC	cymptom.com	Third Party Adviso
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.

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](#)