



CVE-2022-25166

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

Summary

CVE	CVE-2022-25166
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-04-14 16:15:00 UTC
Updated	2022-04-23 02:35:00 UTC
Description	An issue was discovered in Amazon AWS VPN Client 2.0.0. It is possible to include a UNC path in the OpenVPN configuration

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Amazon	Aws Client Vpn	2.0.0	All	All	All

References

Reference
CVE-2022-25165: Privilege Escalation to SYSTEM in AWS VPN Client - Rhino Security Labs
GitHub - RhinoSecurityLabs/CVEs: A collection of proof-of-concept exploit scripts written by the team at Rhino Security Labs for various CVEs
CVE Program record
NVD vulnerability detail

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](#)