CVE-2021-35523

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

Summary

CVE	CVE-2021-35523
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-06-28 17:15:00 UTC
Updated	2021-07-02 16:26:00 UTC
Description	Securepoint SSL VPN Client v2 before 2.0.32 on Windows has unsafe configuration handling that enables local privilege es

Risk And Classification

Problem Types: CWE-269

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Securepoint	Openvpn-client	All	All	All	All

References

Reference	Source	Link
Securepoint SSL VPN v2 vulnerability - Local privilege escalation · Advisory · Securepoint/openvpn-client · GitHub	MISC	github.com
Page not found » #bogner.sh	MISC	bogner.sh
Full Disclosure: CVE-2021-35523: Local Privilege Escalation in Securepoint SSL VPN Client 2.0.30	FULLDISC	seclists.org
Securepoint SSL VPN Client 2.0.30 Local Privilege Escalation ≈ Packet Storm	MISC	packetstorm
CVE Program record	CVE.ORG	www.cve.o
NVD vulnerability detail	NVD	nvd.nist.go

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