CVE-2020-36382

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-36382
State	PUBLIC
Assigner	security@openvpn.net
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-06-04 11:15:00 UTC
Updated	2022-09-20 19:28:00 UTC
Description	OpenVPN Access Server 2.7.3 to 2.8.7 allows remote attackers to trigger an assert during the user authentication phase via

Risk And Classification

Problem Types: CWE-617

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openvpn	Openvpn Access Server	All	All	All	All

References

Reference	Source	Link	Tags
Access Server Release Notes | OpenVPN	MISC	openvpn.net	
Access Server Security Update (CVE-2020-15077, CVE-2020-36382) | OpenVPN	MISC	openvpn.net	
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.

Legacy QID Mappings

375867 Open Virtual Private Network (OpenVPN) Access Server Multiple Security Vulnerabilities

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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