CVE-2020-11810

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-11810
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-04-27 15:15:00 UTC
Updated	2023-11-07 03:15:00 UTC
Description	An issue was discovered in OpenVPN 2.4.x before 2.4.9. An attacker can inject a data channel v2 (P_DATA_V2) packet us

Risk And Classification

Problem Types: CWE-362

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Application	Openvpn	Openvpn	All	All	All	All
Application	Openvpn	Openvpn	All	All	All	All

References

Reference	Source
#1272 (One client kills other client session via false client floating) – OpenVPN Community	CONFIRM
[SECURITY] Fedora 30 Update: openvpn-2.4.9-1.fc30 - package-announce - Fedora Mailing-Lists	

Fix illegal client float (CVE-2020-11810) · OpenVPN/openvpn@37bc691 · GitHub	CONFIRM
[SECURITY] Fedora 32 Update: openvpn-2.4.9-1.fc32 - package-announce - Fedora Mailing-Lists	FEDORA
Bug 1169925 – VUL-1: CVE-2020-11810: openvpn: race condition between allocating peer-id and initializing data channel key	CONFIRM
CVE-2020-11810	MISC
[SECURITY] Fedora 30 Update: openvpn-2.4.9-1.fc30 - package-announce - Fedora Mailing-Lists	FEDORA
[SECURITY] [DLA 2992-1] openvpn security update	MLIST
[Openvpn-devel,v2] Fix illegal client float - Patchwork	CONFIRM
[SECURITY] Fedora 32 Update: openvpn-2.4.9-1.fc32 - package-announce - Fedora Mailing-Lists	
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 174999 SUSE Enterprise Linux Security Update for openvpn (SUSE-SU-2021:1577-1)
- 179259 Debian Security Update for Open Virtual Private Network (OpenVPN) (DLA 2992-1)
- 198352 Ubuntu Security Notification for OpenVPN vulnerabilities (USN-4933-1)
- 500504 Alpine Linux Security Update for Open Virtual Private Network (OpenVPN)
- 500572 Alpine Linux Security Update for Open Virtual Private Network (OpenVPN)
- 500771 Alpine Linux Security Update for openvpn
- 501171 Alpine Linux Security Update for openvpn
- 504261 Alpine Linux Security Update for openvpn
- 750210 OpenSUSE Security Update for openvpn (openSUSE-SU-2021:0734-1)