CVE-2017-7479

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

Summary

CVE	CVE-2017-7479
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-05-15 18:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	OpenVPN versions before 2.3.15 and before 2.4.2 are vulnerable to reachable assertion when packet-ID counter rolls over

Risk And Classification

Problem Types: CWE-617

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openvpn	Openvpn	2.4.0	All	All	All
Application	Openvpn	Openvpn	2.4.0	alpha2	All	All
Application	Openvpn	Openvpn	2.4.0	beta1	All	All
Application	Openvpn	Openvpn	2.4.0	beta2	All	All
Application	Openvpn	Openvpn	2.4.0	rc1	All	All
Application	Openvpn	Openvpn	2.4.0	rc2	All	All
Application	Openvpn	Openvpn	2.4.1	All	All	All
Application	Openvpn	Openvpn	2.4.0	All	All	All
Application	Openvpn	Openvpn	2.4.0	alpha2	All	All
Application	Openvpn	Openvpn	2.4.0	beta1	All	All
Application	Openvpn	Openvpn	2.4.0	beta2	All	All
Application	Openvpn	Openvpn	2.4.0	rc1	All	All
Application	Openvpn	Openvpn	2.4.0	rc2	All	All
Application	Openvpn	Openvpn	2.4.1	All	All	All
Application	Openvpn	Openvpn	All	All	All	All

References

Reference	Source	Link
OpenVPN Packet Processing Flaws Let Remote Users Cause the Target Service to Crash - SecurityTracker	SECTRACK	www.securitytra
QuarkslabAndCryptographyEngineerAudits – OpenVPN Community	CONFIRM	community.oper
Debian -- Security Information -- DSA-3900-1 openvpn	DEBIAN	www.debian.org
OpenVPN CVE-2017-7479 Denial of Service Vulnerability	BID	www.securityfoc
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.