CVE-2017-7520

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

Summary

CVE	CVE-2017-7520
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-06-27 13:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	OpenVPN versions before 2.4.3 and before 2.3.17 are vulnerable to denial-of-service and/or possibly sensitive memory leal

Risk And Classification

Problem Types: CWE-125

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	2.4.2	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	2.4.2	All	All	All
Application	Openvpn	Openvpn	All	All	All	All

References

Reference
OpenVPN Multiple Flaws Let Remote Users Obtain Potentially Sensitive Information, Deny Service, and Execute Arbitrary Code - SecurityTra
OpenVPN Multiple Security Vulnerabilities
VulnerabilitiesFixedInOpenVPN243 – OpenVPN Community
Debian -- Security Information -- DSA-3900-1 openvpn
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.