



CVE-2018-7544

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2018-7544
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-03-16 15:29:00 UTC
Updated	2023-11-07 03:01:00 UTC
Description	** DISPUTED ** A cross-protocol scripting issue was discovered in the management interface in OpenVPN through 2.4.5. V

Risk And Classification

Problem Types: CWE-134

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
0xlabs Blog: OpenVPN: Remote Information Disclosure and Denial Of Service (CVE-2018-7544)	MISC	blog.0xlabs.com	Exploit, T
CVE Program record	CVE.ORG	www.cve.org	canonica
NVD vulnerability detail	NVD	nvd.nist.gov	canonica

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[174998](#) SUSE Enterprise Linux Security Update for openvpn (SUSE-SU-2021:1576-1)

[174999](#) SUSE Enterprise Linux Security Update for openvpn (SUSE-SU-2021:1577-1)

[750210](#) OpenSUSE Security Update for openvpn (openSUSE-SU-2021:0734-1)

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered 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](#)