



CVE-2016-6329

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

Summary

CVE	CVE-2016-6329
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-01-31 22:59:00 UTC
Updated	2019-07-09 13:15:00 UTC
Description	OpenVPN, when using a 64-bit block cipher, makes it easier for remote attackers to obtain cleartext data via a birthday attack.

Risk And Classification

Problem Types: CWE-310 | CWE-200

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference
OpenVPN CVE-2016-6329 Information Disclosure Vulnerability
OpenVPN Blowfish Cipher Block Collision Weakness Lets Remote Users Decrypt Data in Certain Cases - SecurityTracker
OpenVPN: Multiple vulnerabilities (GLSA 201611-02) — Gentoo Security
IBM Security Bulletin: OpenSSL and OpenVPN vulnerabilities affect IBM Rational Team Concert (CVE-2016-2183, CVE-2016-6329) - United States
SWEET32 – OpenVPN Community
cert-portal.siemens.com/productcert/pdf/ssa-556833.pdf
Sweet32: Birthday attacks on 64-bit block ciphers in TLS and OpenVPN
HPE Support document - HPE Support Center
IBM Security Bulletin: Vulnerabilities in OpenSSL, OpenVPN and GNU glibc affect IBM Security Virtual Server Protection for VMware - United States
IBM Security Bulletin: IBM i is affected by several vulnerabilities (CVE-2016-2183 and CVE-2016-6329) - United States
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.

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)