



# CVE-2015-1794

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

## Summary

<b>CVE</b>	CVE-2015-1794
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2015-12-06 20:59:00 UTC
<b>Updated</b>	2023-02-13 00:46:00 UTC
<b>Description</b>	The ssl3_get_key_exchange function in ssl/s3_clnt.c in OpenSSL 1.0.2 before 1.0.2e allows remote servers to cause a den

## Risk And Classification

**Problem Types:** CWE-189

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.2	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.2a	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.2b	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.2c	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.2d	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.2	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.2a	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.2b	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.2c	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.2d	All	All	All

## References

Reference	Source	Li
Oracle Critical Patch Update Advisory - April 2016	CONFIRM	<a href="#">wv</a>
USN-2830-1: OpenSSL vulnerabilities   Ubuntu	UBUNTU	<a href="#">wv</a>
Multiple Vulnerabilities in OpenSSL (December 2015) Affecting Cisco Products	CISCO	<a href="#">toc</a>
[security-announce] openSUSE-SU-2016:0637-1: important: Security update	SUSE	<a href="#">list</a>

<a href="https://openssl.org/news/secadv/20151203.txt">openssl.org/news/secadv/20151203.txt</a>	CONFIRM	<a href="#">op</a>
<a href="#">FortiGuard.com   OpenSSL Advisory - December 2015</a>	CONFIRM	<a href="#">for</a>
<a href="https://git.openssl.org">git.openssl.org Git - openssl.git/commit</a>	CONFIRM	<a href="#">git</a>
<a href="#">2016-10 Security Bulletin: CTPView: Multiple vulnerabilities in CTPView - Juniper Networks</a>	CONFIRM	<a href="#">kb</a>
<a href="https://cert-portal.siemens.com/productcert/pdf/ssa-412672.pdf">cert-portal.siemens.com/productcert/pdf/ssa-412672.pdf</a>	CONFIRM	<a href="#">ce</a>
<a href="https://git.openssl.org">git.openssl.org Git - openssl.git/commit</a>	MISC	<a href="#">git</a>
<a href="#">Document Display   HPE Support Center</a>	CONFIRM	<a href="#">h2</a>
<a href="#">Juniper Networks - 2016-10 Security Bulletin: OpenSSL security updates</a>	CONFIRM	<a href="#">kb</a>
<a href="#">OpenSSL Multiple Bugs Let Remote Users Deny Service and Obtain Potentially Sensitive Information - SecurityTracker</a>	SECTRACK	<a href="#">wv</a>
<a href="#">The Slackware Linux Project: Slackware Security Advisories</a>	SLACKWARE	<a href="#">wv</a>
<a href="#">CVE Program record</a>	CVE.ORG	<a href="#">wv</a>
<a href="#">NVD vulnerability detail</a>	NVD	<a href="#">nv</a>

No vendor comments have been submitted for this CVE.

#### Legacy QID Mappings

[591280](#) Siemens SCALANCE X-200RNA Switch Devices Denial of Service (DoS) Multiple Vulnerabilities (ICSA-22-349-21, SSA-412672)

© [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](#).

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