



# CVE-2017-3731

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

## Summary

<b>CVE</b>	CVE-2017-3731
<b>State</b>	PUBLIC
<b>Assigner</b>	openssl-security@openssl.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-05-04 19:29:00 UTC
<b>Updated</b>	2022-08-16 13:16:00 UTC
<b>Description</b>	If an SSL/TLS server or client is running on a 32-bit host, and a specific cipher is being used, then a truncated packet can c

## Risk And Classification

### Problem Types: CWE-125

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nodejs	Node.js	All	All	All	All
Application	Nodejs	Node.js	All	All	All	All
Application	Nodejs	Node.js	All	All	All	All
Application	Nodejs	Node.js	All	All	All	All
Application	Nodejs	Node.js	All	All	All	All
Application	Openssl	Openssl	1.0.2	All	All	All
Application	Openssl	Openssl	1.0.2	beta1	All	All
Application	Openssl	Openssl	1.0.2	beta2	All	All
Application	Openssl	Openssl	1.0.2	beta3	All	All
Application	Openssl	Openssl	1.0.2a	All	All	All
Application	Openssl	Openssl	1.0.2b	All	All	All
Application	Openssl	Openssl	1.0.2c	All	All	All
Application	Openssl	Openssl	1.0.2d	All	All	All
Application	Openssl	Openssl	1.0.2e	All	All	All
Application	Openssl	Openssl	1.0.2f	All	All	All
Application	Openssl	Openssl	1.0.2h	All	All	All
Application	Openssl	Openssl	1.0.2i	All	All	All

Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.2j	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.1.0a	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.1.0b	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.1.0c	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>	1.0.2	beta1	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.2	beta2	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.2	beta3	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>	1.0.2e	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.2f	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.2h	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.2i	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.2j	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.1.0a	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.1.0b	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.1.0c	All	All	All

## References

Reference	Source	Link
OpenSSL: Multiple vulnerabilities (GLSA 201702-07) — Gentoo Security	GENTOO	<a href="#">secu</a>
Red Hat Customer Portal	REDHAT	<a href="#">rhn.r</a>
Debian -- Security Information -- DSA-3773-1 openssl	DEBIAN	<a href="#">www</a>
FreeBSD-SA-17:02	FREEBSD	<a href="#">secu</a>
<a href="#">www.openssl.org/news/secadv/20170126.txt</a>	CONFIRM	<a href="#">www</a>
Oracle Critical Patch Update - January 2018	CONFIRM	<a href="#">www</a>
OpenSSL CVE-2017-3731 Denial of Service Vulnerability	BID	<a href="#">www</a>
[R5] SecurityCenter 5.4.3 Fixes Multiple Vulnerabilities - Security Advisory   Tenable Network Security	CONFIRM	<a href="#">www</a>
crypto/evp: harden AEAD ciphers. · openssl/openssl@00d9654 · GitHub	MISC	<a href="#">githu</a>
OpenSSL Multiple Bugs Let Remote Users Deny Service and Obtain Potentially Sensitive Information - SecurityTracker	SECTRACK	<a href="#">www</a>
Red Hat Customer Portal	REDHAT	<a href="#">acce</a>
Document Display   HPE Support Center	CONFIRM	<a href="#">supp</a>
Red Hat Customer Portal	REDHAT	

Hed Hat Customer Portal	REDHAT	<a href="#">acce</a>
October 2017 MySQL Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="#">secul</a>
Red Hat Customer Portal	REDHAT	<a href="#">acce</a>
Pixel&nbsp;/&nbsp;Nexus Security Bulletin—November 2017   Android Open Source Project	CONFIRM	<a href="#">sour</a>
CVE-2017-3731 OpenSSL Vulnerability	CONFIRM	<a href="#">secul</a>
Oracle Critical Patch Update - July 2017	CONFIRM	<a href="#">www</a>
Oracle Critical Patch Update - October 2017	CONFIRM	<a href="#">www</a>
Oracle Critical Patch Update Advisory - April 2019	MISC	<a href="#">www</a>
CVE Program record	CVE.ORG	<a href="#">www</a>
NVD vulnerability detail	NVD	<a href="#">nvd.</a>

### Vendor Comments And Credit

#### Discovery Credit

**LEGACY:** Robert Świącki of Google

### Legacy QID Mappings

[378210](#) Virtuozzo Linux Security Update for openssl-perl (VZLSA-2017:0286)

[390226](#) Oracle Managed Virtualization (VM) Server for x86 Security Update for Open Secure Sockets Layer (OpenSSL) (OVMSA-2021-0011)

[390284](#) Oracle Managed Virtualization (VM) Server for x86 Security Update for Open Secure Sockets Layer (OpenSSL) (OVMSA-2023-0013)

[43835](#) HPE Switches And Routers Open Secure Sockets Layer (OpenSSL) Multiple Remote Vulnerabilities (HPESBHF03838)

© [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](#)