



# CVE-2017-3732

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

## Summary

<b>CVE</b>	CVE-2017-3732
<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>	2022-08-29 20:43:00 UTC
<b>Description</b>	There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL 1.0.2 before 1.0.2k and 1.1.0

## Risk And Classification

**Problem Types:** CWE-200

## 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>	1.1.0a	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>	1.1.0a	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>
FreeBSD-SA-17:02	FREEBSD	<a href="#">secu</a>
<a href="http://www.openssl.org/news/secadv/20170126.txt">www.openssl.org/news/secadv/20170126.txt</a>	CONFIRM	<a href="#">www</a>
Oracle Critical Patch Update - January 2018	CONFIRM	<a href="#">www</a>
Red Hat Customer Portal	REDHAT	<a href="#">acce</a>
[R5] SecurityCenter 5.4.3 Fixes Multiple Vulnerabilities - Security Advisory   Tenable Network Security	CONFIRM	<a href="#">www</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>
Red Hat Customer Portal	REDHAT	<a href="#">acce</a>
Document Display   HPE Support Center	CONFIRM	<a href="#">supp</a>
Red Hat Customer Portal	REDHAT	<a href="#">acce</a>
OpenSSL CVE-2017-3732 Information Disclosure Vulnerability	BID	<a href="#">www</a>
Red Hat Customer Portal	REDHAT	<a href="#">acce</a>
Red Hat Customer Portal	REDHAT	<a href="#">acce</a>
OpenSSL CVE-2017-3732 Information Disclosure Vulnerability	CONFIRM	

Oracle Critical Patch Update - July 2017	CONFIRM	<a href="#">www</a>
Oracle Critical Patch Update - October 2017	CONFIRM	<a href="#">www</a>
bn/asm/x86_64-mont5.pl: fix carry bug in bn_sqr8x_internal. · openssl/openssl@a59b90b · GitHub	MISC	<a href="#">github</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:** OSS-Fuzz project

### Legacy QID Mappings

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

[710243](#) Gentoo Linux MySQL Multiple Vulnerabilities (GLSA 201802-04)

© [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](#)