



CVE-2017-3736

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2017-3736
State	PUBLIC
Assigner	openssl-security@openssl.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-11-02 17:29:00 UTC
Updated	2019-04-23 19:30:00 UTC
Description	There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference

OpenSSL: Multiple vulnerabilities (GLSA 201712-03) — Gentoo security

www.openssl.org/news/secadv/201711102.txt

Document Display | HPE Support Center

Oracle Critical Patch Update - January 2018

CPU July 2018

Red Hat Customer Portal

Oracle Critical Patch Update - April 2018

OpenSSL CVE-2017-3736 Information Disclosure Vulnerability

Red Hat Customer Portal

Red Hat Customer Portal

Oracle Critical Patch Update - January 2019

January 2018 MySQL vulnerabilities in NetApp Products | NetApp Product Security

Oracle Critical Patch Update - July 2019

OpenSSL bn_sqr8x_internal() Carry Bug Lets Remote Users Obtain Potentially Sensitive Information on the Target System in Certain Cases

FreeBSD-SA-17:11

Debian -- Security Information -- DSA-4018-1 openssl

Red Hat Customer Portal

Debian -- Security Information -- DSA-4017-1 openssl1.0

bn/asm/x86_64-mont5.pl: fix carry bug in bn_sqr8x_internal. · openssl/openssl@4443cf7 · GitHub

Red Hat Customer Portal

CPU Oct 2018

CVE-2017-3736 OpenSSL Vulnerability in NetApp Products | NetApp Product Security

[R1] Nessus 6.11.3 Fixes Multiple Third-party Vulnerabilities - Security Advisory | Tenable®

Red Hat Customer Portal

Red Hat Customer Portal

[R1]SecurityCenter 5.6.0.1 Fixes Multiple Third-party Vulnerabilities - Security Advisory | Tenable™

Oracle Critical Patch Update Advisory - April 2019

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

Legacy QID Mappings

710507 Gentoo Linux Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities (GLSA 201712-03)

© 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](#)