



CVE-2018-0737

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

Summary

CVE	CVE-2018-0737
State	PUBLIC
Assigner	openssl-security@openssl.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-04-16 18:29:00 UTC
Updated	2023-11-07 02:51:00 UTC
Description	The OpenSSL RSA Key generation algorithm has been shown to be vulnerable to a cache timing side channel attack. An a

Risk And Classification

Problem Types: CWE-327

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	17.10	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	17.10	All	All	All
Application	Openssl	Openssl	All	All	All	All
Application	Openssl	Openssl	All	All	All	All

References

Reference
Red Hat Customer Portal
Red Hat Customer Portal
[SECURITY] Fedora 30 Update: compat-openssl10-1.0.2o-7.fc30 - package-announce - Fedora Mailing-Lists
git.openssl.org Git - openssl.git/commitdiff
[R1] Nessus 7.1.4 Fixes Multiple Third-party Vulnerabilities - Security Advisory Tenable®
[SECURITY] Fedora 31 Update: compat-openssl10-1.0.2o-8.fc31 - package-announce - Fedora Mailing-Lists

[SECURITY] Fedora 30 Update: compat-openssl10-1.0.2o-7.fc30 - package-announce - Fedora Mailing-Lists
[R1] LCE 5.1.1 Fixes Multiple Third-party Vulnerabilities - Security Advisory Tenable®
[SECURITY] Fedora 29 Update: compat-openssl10-1.0.2o-7.fc29 - package-announce - Fedora Mailing-Lists
OpenSSL RSA Key Generation BN_mod_inverse() and BN_mod_exp_mont() Cache Timing Attack Lets Local Users Recover the Private Key
[R1] SecurityCenter 5.7.1 Fixes Multiple Third-Party Vulnerabilities - Security Advisory Tenable®
Debian -- Security Information -- DSA-4348-1 openssl
PAN-SA-2018-0015 OpenSSL Vulnerabilities in PAN-OS
OpenSSL: Multiple vulnerabilities (GLSA 201811-21) — Gentoo security
[SECURITY] [DLA 1449-1] openssl security update
USN-3628-1: OpenSSL vulnerability Ubuntu security notices Ubuntu
Red Hat Customer Portal
Oracle Critical Patch Update Advisory - July 2021
USN-3628-2: OpenSSL vulnerability Ubuntu security notices
[R1] Nessus 8.0.0 Fixes Multiple Third-party Vulnerabilities - Security Advisory Tenable®
git.openssl.org Git - openssl.git/commitdiff
OpenSSL CVE-2018-0737 Side Channel Attack Information Disclosure Vulnerability
[SECURITY] Fedora 29 Update: compat-openssl10-1.0.2o-7.fc29 - package-announce - Fedora Mailing-Lists
Oracle Critical Patch Update - January 2019
Oracle Critical Patch Update - July 2019
CVE-2018-0737 OpenSSL Vulnerability in NetApp Products NetApp Product Security
Red Hat Customer Portal
git.openssl.org Git - openssl.git/commitdiff
[SECURITY] Fedora 31 Update: compat-openssl10-1.0.2o-8.fc31 - package-announce - Fedora Mailing-Lists
www.openssl.org/news/secadv/20180416.txt
August 2018 Security Releases Node.js
USN-3692-1: OpenSSL vulnerabilities Ubuntu security notices
Debian -- Security Information -- DSA-4355-1 openssl1.0
CPU Oct 2018
git.openssl.org Git - openssl.git/commitdiff
Oracle Critical Patch Update Advisory - April 2020
Red Hat Customer Portal
USN-3692-2: OpenSSL vulnerabilities Ubuntu security notices
Oracle Critical Patch Update Advisory - April 2019
CVE Program record
NVD vulnerability detail

Vendor Comments And Credit

Discovery Credit

LEGACY: Alejandro Cabrera Aldaya, Billy Brumley, Cesar Pereida Garcia and Luis Manuel Alvarez Tapia

Legacy QID Mappings

[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)

[591115](#) ABB Relion 670 series and Relion 650 series Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities (ABBVU-PGGA-1MRG032388)

[670784](#) EulerOS Security Update for shim (EulerOS-SA-2021-2542)

[670808](#) EulerOS Security Update for shim (EulerOS-SA-2021-2566)

[710214](#) Gentoo Linux Open Secure Sockets Layer Multiple Vulnerabilities (GLSA 201811-21)

© [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](#)