CVE-2017-3737

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2017-3737
State	PUBLIC
Assigner	openssl-security@openssl.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-12-07 16:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occu

Risk And Classification

Problem Types: CWE-125 | CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	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	1.0.2g	All	All	All
Application	Openssl	Openssl	1.0.2h	All	All	All
Application	Openssl	Openssl	1.0.2i	All	All	All
Application	Openssl	Openssl	1.0.2j	All	All	All
Application	Openssl	Openssl	1.0.2k	All	All	All
Application	Openssl	Openssl	1.0.2l	All	All	All
Application	Openssl	Openssl	1.0.2m	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	1.0.2g	All	All	All
Application	Openssl	Openssl	1.0.2h	All	All	All
Application	Openssl	Openssl	1.0.2i	All	All	All
Application	Openssl	Openssl	1.0.2j	All	All	All
Application	Openssl	Openssl	1.0.2k	All	All	All
Application	Openssl	Openssl	1.0.2l	All	All	All
Application	Openssl	Openssl	1.0.2m	All	All	All

References

Reference
CVE-2017-3737: OpenSSL Security Bypass Vulnerability - DigitalMunition
OpenSSL: Multiple vulnerabilities (GLSA 201712-03) — Gentoo security
Debian -- Security Information -- DSA-4065-1 openssl1.0
Oracle Critical Patch Update - January 2018
CPU July 2018
Oracle Critical Patch Update - April 2018
FreeBSD-SA-17:12
cert-portal.siemens.com/productcert/pdf/ssa-179516.pdf
Red Hat Customer Portal
January 2018 MySQL vulnerabilities in NetApp Products | NetApp Product Security
December 2017 OpenSSL Vulnerabilities in NetApp Products | NetApp Product Security
Oracle Critical Patch Update - July 2019
[R2] SecurityCenter 5.6.1 Fixes Multiple Third-party Vulnerabilities - Security Advisory | Tenable®
Red Hat Customer Portal
OpenSSL CVE-2017-3737 Security Bypass Vulnerability
Red Hat Customer Portal
April 2018 MySQL Vulnerabilities in NetApp Products | NetApp Product Security
Red Hat Customer Portal
OpenSSL Overflow in rsaz_1024_mul_avx2() Lets Remote Users Obtain Potentially Sensitive Information in Certain Cases and SSL_read()/S
www.openssl.org/news/secadv/20171207.txt
Don't allow read/write after fatal error · openssl/openssl@898fb88 · GitHub
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

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

591201 Siemens WinCC (TIA Portal), IPC Diagbase and Simatic Step 7 (TIA Portal) Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities (SSA-179516)

591261 Siemens MindConnect, S7-1200/1500 CPU family, ET 200SP Open Controller Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities (ICSA-18-226-02, SSA-179516)

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

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

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 registred 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