



CVE-2019-1563

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

Summary

CVE	CVE-2019-1563
State	PUBLIC
Assigner	openssl-security@openssl.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-09-10 17:15:00 UTC
Updated	2023-11-07 03:08:00 UTC
Description	In situations where an attacker receives automated notification of the success or failure of a decryption attempt an attacker,

Risk And Classification

Problem Types: CWE-327 | CWE-203

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
Application	Openssl	Openssl	All	All	All	All

References

Reference

- [git.openssl.org Git - openssl.git/commitdiff](#)
- [Debian -- Security Information -- DSA-4539-1 openssl](#)
- [\[SECURITY\] Fedora 30 Update: openssl-1.1.1d-1.fc30 - package-announce - Fedora Mailing-Lists](#)
- [git.openssl.org Git - openssl.git/commitdiff](#)
- [Oracle Critical Patch Update Advisory - July 2020](#)
- [git.openssl.org Git - openssl.git/commitdiff](#)
- [\[security-announce\] openSUSE-SU-2019:2268-1: moderate: Security update f](#)
- [\[R1\] Tenable.sc 5.13.0 Fixes Multiple Third-Party Vulnerabilities - Security Advisory | Tenable®](#)
- [USN-4376-2: OpenSSL vulnerabilities | Ubuntu security notices | Ubuntu](#)
- [Oracle Critical Patch Update Advisory - October 2020](#)
- [OpenSSL: Multiple vulnerabilities \(GLSA 201911-04\) — Gentoo security](#)

[SECURITY] [DLA 1932-1] openssl security update

USN-4376-1: OpenSSL vulnerabilities | Ubuntu security notices | Ubuntu

Security Bulletin - Policy Auditor update fixes multiple vulnerabilities in third-party libraries (CVE-2016-0718, CVE-2016-4472, CVE-2016-5300)

[security-announce] openSUSE-SU-2019:2158-1: moderate: Security update f

www.openssl.org/news/secadv/20190910.txt

support.f5.com/csp/article/K97324400

[SECURITY] Fedora 29 Update: openssl-1.1.1d-1.fc29 - package-announce - Fedora Mailing-Lists

September 2019 OpenSSL Vulnerabilities in NetApp Products | NetApp Product Security

git.openssl.org Git - openssl.git/commitdiff

[security-announce] openSUSE-SU-2019:2189-1: moderate: Security update f

Bugtraq: [SECURITY] [DSA 4539-1] openssl security update

Debian -- Security Information -- DSA-4540-1 openssl1.0

git.openssl.org Git - openssl.git/commitdiff

Slackware Security Advisory - openssl Updates ≈ Packet Storm

[security-announce] openSUSE-SU-2019:2269-1: moderate: Security update f

Bugtraq: [slackware-security] openssl (SSA:2019-254-03)

Bugtraq: [SECURITY] [DSA 4540-1] openssl1.0 security update

git.openssl.org Git - openssl.git/commitdiff

[SECURITY] Fedora 30 Update: openssl-1.1.1d-1.fc30 - package-announce - Fedora Mailing-Lists

Oracle Critical Patch Update - October 2019

Oracle Critical Patch Update Advisory - January 2020

Oracle Critical Patch Update Advisory - April 2020

USN-4504-1: OpenSSL vulnerabilities | Ubuntu security notices | Ubuntu

myF5

[SECURITY] Fedora 29 Update: openssl-1.1.1d-1.fc29 - package-announce - Fedora Mailing-Lists

CVE Program record

NVD vulnerability detail



Vendor Comments And Credit

Discovery Credit

LEGACY: Bernd Edlinger

Legacy QID Mappings

[296078](#) Oracle Solaris 11.4 Support Repository Update (SRU) 16.4.0 Missing (CPUOCT2019)

[375626](#) IBM Cognos Analytics Multiple Vulnerabilities (6451705)

377105	Alibaba Cloud Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ALINUX3-SA-2022:0025)
38842	Open Secure Sockets Layer (OpenSSL) Security Update (OpenSSL Security Advisory 20190910)
500493	Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)
500561	Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)
500760	Alpine Linux Security Update for openssl
501160	Alpine Linux Security Update for openssl
501979	Alpine Linux Security Update for Open Secure Sockets Layer3 (OpenSSL3)
502898	Alpine Linux Security Update for openssl1.1-compat
504252	Alpine Linux Security Update for openssl
670784	EulerOS Security Update for shim (EulerOS-SA-2021-2542)
670808	EulerOS Security Update for shim (EulerOS-SA-2021-2566)
710119	Gentoo Linux Open Secure Sockets Layer Multiple Vulnerabilities (GLSA 201911-04)

© [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](#)