



CVE-2019-1551

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

Summary

CVE	CVE-2019-1551
State	PUBLIC
Assigner	openssl-security@openssl.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-12-06 18:15:00 UTC
Updated	2023-11-07 03:08:00 UTC
Description	There is an overflow bug in the x64_64 Montgomery squaring procedure used in exponentiation with 512-bit moduli. No EC

Risk And Classification

Problem Types: CWE-190

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.10	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.10	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Application	Openssl	Openssl	All	All	All	All

Application	Openssl	Openssl	All	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Application	Oracle	Enterprise Manager Ops Center	12.4.0.0	All	All	All
Application	Oracle	Enterprise Manager Ops Center	12.4.0.0	All	All	All
Application	Oracle	Mysql Enterprise Monitor	All	All	All	All
Application	Oracle	Mysql Enterprise Monitor	All	All	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.56	All	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.57	All	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.58	All	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.56	All	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.57	All	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.58	All	All	All
Application	Tenable	Log Correlation Engine	All	All	All	All

References

Reference	Source	Link
OpenSSL: Multiple vulnerabilities (GLSA 202004-10) — Gentoo security	GENTOO	security.gentoo.org
[SECURITY] Fedora 32 Update: openssl-1.1.1g-1.fc32 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[SECURITY] Fedora 31 Update: openssl-1.1.1g-1.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 31 Update: openssl-1.1.1g-1.fc31 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
git.openssl.org Git - openssl.git/commitdiff	CONFIRM	git.openssl.org
Oracle Critical Patch Update Advisory - July 2020	MISC	www.oracle.com
[R1] Tenable.sc 5.13.0 Fixes Multiple Third-Party Vulnerabilities - Security Advisory Tenable®	CONFIRM	www.tenable.com
[R1] Tenable.sc 5.17.0 Fixes Multiple Vulnerabilities - Security Advisory Tenable®	CONFIRM	www.tenable.com
USN-4376-1: OpenSSL vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com
CVE-2019-1551 OpenSSL Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com
git.openssl.org Git - openssl.git/commitdiff		git.openssl.org
[SECURITY] Fedora 30 Update: openssl-1.1.1g-1.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[R1] LCE 6.0.9 Fixes Multiple Third-party Vulnerabilities - Security Advisory Tenable®	CONFIRM	www.tenable.com
Debian -- Security Information -- DSA-4594-1 openssl1.0	DEBIAN	www.debian.org
Slackware Security Advisory - openssl Updates ~ Packet Storm	MISC	packetstormsecurity.com
Bugtraq: [SECURITY] [DSA 4594-1] openssl1.0 security update	BUGTRAQ	seclists.org
Bugtraq: [slackware-security] openssl (SSA:2019-354-01)	BUGTRAQ	seclists.org
git.openssl.org Git - openssl.git/commitdiff		git.openssl.org
[SECURITY] Fedora 31 Update: openssl-1.1.1g-1.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org

[SECURITY] [DLA 2952-1] openssl security update	MLIS I	lists.debian.org
[R1] Nessus Agent 7.6.3 Fixes Multiple Third-party Vulnerabilities - Security Advisory Tenable®	CONFIRM	www.tenable.com
git.openssl.org Git - openssl.git/commitdiff	CONFIRM	git.openssl.org
[SECURITY] Fedora 30 Update: openssl-1.1.1g-1.fc30 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[SECURITY] Fedora 32 Update: openssl-1.1.1g-1.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
USN-4504-1: OpenSSL vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com
www.openssl.org/news/secadv/20191206.txt	CONFIRM	www.openssl.org
Oracle Critical Patch Update Advisory - April 2021	MISC	www.oracle.com
Oracle Critical Patch Update Advisory - January 2021	MISC	www.oracle.com
[security-announce] openSUSE-SU-2020:0062-1: moderate: Security update f	SUSE	lists.opensuse.org
Debian -- Security Information -- DSA-4855-1 openssl	DEBIAN	www.debian.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

LEGACY: OSS-Fuzz and Guido Vranken

Legacy QID Mappings

[179132](#) Debian Security Update for Open Secure Sockets Layer (OpenSSL) (DLA 2952-1)

[296075](#) Oracle Solaris 11.4 Support Repository Update (SRU) 21.69.0 Missing (CPUAPR2020)

[352487](#) Amazon Linux Security Advisory for openssl: ALAS2-2021-1687

[500494](#) Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)

[500562](#) Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)

[500761](#) Alpine Linux Security Update for openssl

[501161](#) Alpine Linux Security Update for openssl

[501980](#) Alpine Linux Security Update for Open Secure Sockets Layer3 (OpenSSL3)

[502899](#) Alpine Linux Security Update for openssl1.1-compat

[504253](#) Alpine Linux Security Update for openssl

[670251](#) EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2021-1825)

[770068](#) Red Hat OpenShift Container Platform 4.6 Security Update (RHSA-2021:0436)

© [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](#)