



# CVE-2019-1549

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2019-1549
<b>State</b>	PUBLIC
<b>Assigner</b>	openssl-security@openssl.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-09-10 17:15:00 UTC
<b>Updated</b>	2023-11-07 03:08:00 UTC
<b>Description</b>	OpenSSL 1.1.1 introduced a rewritten random number generator (RNG). This was intended to include protection in the event

## Risk And Classification

**Problem Types:** CWE-330

## NVD Known Affected Configurations (CPE 2.3)

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

## References

Reference	Source	Link	Ta
git.openssl.org Git - openssl.git/commitdiff		<a href="https://git.openssl.org">git.openssl.org</a>	
support.f5.com/csp/article/K44070243	CONFIRM	<a href="https://support.f5.com">support.f5.com</a>	
Debian -- Security Information -- DSA-4539-1 openssl	DEBIAN	<a href="https://www.debian.org">www.debian.org</a>	
[SECURITY] Fedora 30 Update: openssl-1.1.1d-1.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
Oracle Critical Patch Update Advisory - July 2020	MISC	<a href="https://www.oracle.com">www.oracle.com</a>	
Oracle Critical Patch Update Advisory - October 2020	MISC	<a href="https://www.oracle.com">www.oracle.com</a>	
USN-4376-1: OpenSSL vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>	
www.openssl.org/news/secadv/20190910.txt	CONFIRM	<a href="https://www.openssl.org">www.openssl.org</a>	Ve
[SECURITY] Fedora 29 Update: openssl-1.1.1d-1.fc29 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
September 2019 OpenSSL Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>	
Bugtraq: [SECURITY] [DSA 4539-1] openssl security update	BUGTRAQ	<a href="https://seclists.org">seclists.org</a>	
git.openssl.org Git - openssl.git/commitdiff	CONFIRM	<a href="https://git.openssl.org">git.openssl.org</a>	Ma
myF5		<a href="https://support.f5.com">support.f5.com</a>	

support.f5.com/csp/article/K44070243	CONFIRM	support.f5.com	
[SECURITY] Fedora 30 Update: openssl-1.1.1d-1.fc30 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
Oracle Critical Patch Update - October 2019	MISC	www.oracle.com	
Oracle Critical Patch Update Advisory - January 2020	MISC	www.oracle.com	
Oracle Critical Patch Update Advisory - April 2020	N/A	www.oracle.com	
[SECURITY] Fedora 29 Update: openssl-1.1.1d-1.fc29 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

## Vendor Comments And Credit

Discovery Credit

**LEGACY:** Matt Caswell

## 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

© [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](#)