CVE-2019-1549

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2019-1549
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	OpenSSL 1.1.1 introduced a rewritten random number generator (RNG). This was intended to include protection in the eve

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

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