CVE-2019-1543

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2019-1543
State	PUBLIC
Assigner	openssl-security@openssl.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-03-06 21:29:00 UTC
Updated	2023-11-07 03:08:00 UTC
Description	ChaCha20-Poly1305 is an AEAD cipher, and requires a unique nonce input for every encryption operation. RFC 7539 spec

Risk And Classification

Problem Types: CWE-327 | CWE-330

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

References

Reference
[SECURITY] Fedora 30 Update: compat-openssl10-1.0.2o-7.fc30 - package-announce - Fedora Mailing-Lists
[SECURITY] Fedora 30 Update: compat-openssl10-1.0.2o-7.fc30 - package-announce - Fedora Mailing-Lists
[SECURITY] Fedora 29 Update: compat-openssl10-1.0.2o-7.fc29 - package-announce - Fedora Mailing-Lists
Bugtraq: [SECURITY] [DSA 4475-1] openssl security update
[security-announce] openSUSE-SU-2019:1814-1: important: Security update
git.openssl.org Git - openssl.git/commitdiff
Security Bulletin - Policy Auditor update fixes multiple vulnerabilities in third-party libraries (CVE-2016-0718, CVE-2016-4472, CVE-2016-5300
git.openssl.org Git - openssl.git/commitdiff
[SECURITY] Fedora 29 Update: compat-openssl10-1.0.2o-7.fc29 - package-announce - Fedora Mailing-Lists
git.openssl.org Git - openssl.git/commitdiff
Oracle Critical Patch Update - July 2019
Debian -- Security Information -- DSA-4475-1 openssl

Oracle Critical Patch Update - October 2019
git.openssl.org Git - openssl.git/commitdiff
Oracle Critical Patch Update Advisory - April 2020
Red Hat Customer Portal
www.openssl.org/news/secadv/20190306.txt
CVE Program record
NVD vulnerability detail

Vendor Comments And Credit

Discovery Credit

LEGACY: Joran Dirk Greef of Ronomon

Legacy QID Mappings

500182	Alpine Linux Security Update for file
500492	Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)
500560	Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)
500759	Alpine Linux Security Update for openssl
501159	Alpine Linux Security Update for openssl
501978	Alpine Linux Security Update for Open Secure Sockets Layer3 (OpenSSL3)
502897	Alpine Linux Security Update for openssl1.1-compat
503921	Alpine Linux Security Update for file
504251	Alpine Linux Security Update for openssl