CVE-2019-1547

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2019-1547
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	Normally in OpenSSL EC groups always have a co-factor present and this is used in side channel resistant code paths. Ho

Risk And Classification

Problem Types: NVD-CWE-noinfo

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
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
myF5
git.openssl.org Git - openssl.git/commitdiff
Oracle Critical Patch Update Advisory - July 2020
[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
[R1] Nessus Network Monitor 5.11.0 Fixes Multiple Third-party Vulnerabilities - Security Advisory | Tenable®
[1909.01785] Certified Side Channels
April 2020 MySQL Vulnerabilities in NetApp Products | NetApp Product Security
[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
January 2020 MySQL Vulnerabilities in NetApp Products | NetApp Product Security
[security-announce] openSUSE-SU-2019:2189-1: moderate: Security update f
git.openssl.org Git - openssl.git/commitdiff
Bugtraq: [SECURITY] [DSA 4539-1] openssl security update
Debian -- Security Information -- DSA-4540-1 openssl1.0
Slackware Security Advisory - openssl Updates ≈ Packet Storm
support.f5.com/csp/article/K73422160
[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
git.openssl.org Git - openssl.git/commitdiff
Oracle Critical Patch Update Advisory - April 2020
USN-4504-1: OpenSSL vulnerabilities | Ubuntu security notices | Ubuntu
[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: Cesar Pereida García, Sohaib ul Hassan, Nicola Tuveri, Iaroslav Gridin, Alejandro Cabrera Aldaya, and Billy Brumley

Cabrera Aldaya, and Billy Brumley

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)

379452 IBM Cognos Analytics Multiple Vulnerabilities (7123154)

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

710119 Gentoo Linux Open Secure Sockets Layer Multiple Vulnerabilities (GLSA 201911-04)