CVE-2020-1967

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-1967
State	PUBLIC
Assigner	openssl-security@openssl.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-04-21 14:15:00 UTC
Updated	2023-11-07 03:19:00 UTC
Description	Server or client applications that call the SSL_check_chain() function during or after a TLS 1.3 handshake may crash due to

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Broadcom	Fabric Operating System	-	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
Operating System	Freebsd	Freebsd	12.1	-	All	All
Operating System	Freebsd	Freebsd	12.1	-	All	All
Application	Jdedwards	Enterpriseone	All	All	All	All
Application	Jdedwards	Enterpriseone	All	All	All	All
Application	Netapp	Active Iq Unified Manager	All	All	All	All
Application	Netapp	Active Iq Unified Manager	All	All	All	All

Application	Netapp	Active Iq Unified Manager	All	All	All	All
Application	Netapp	Active Iq Unified Manager	All	All	All	All
Operating System	Netapp	Brocade Fabric Operating System Firmware	-	All	All	All
Operating System	Netapp	Brocade Fabric Operating System Firmware	-	All	All	All
Application	Netapp	E-series Performance Analyzer	-	All	All	All
Application	Netapp	E-series Performance Analyzer	-	All	All	All
Application	Netapp	Oncommand Insight	-	All	All	All
Application	Netapp	Oncommand Insight	-	All	All	All
Application	Netapp	Oncommand Workflow Automation	-	All	All	All
Application	Netapp	Oncommand Workflow Automation	-	All	All	All
Application	Netapp	Smi-s Provider	-	All	All	All
Application	Netapp	Smi-s Provider	-	All	All	All
Application	Netapp	Snapcenter	-	All	All	All
Application	Netapp	Snapcenter	-	All	All	All
Application	Netapp	Steelstore Cloud Integrated Storage	-	All	All	All
Application	Netapp	Steelstore Cloud Integrated Storage	-	All	All	All
Application	Openssl	Openssl	All	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All
Application	Oracle	Application Server	12.1.3	All	All	All
Application	Oracle	Enterprise Manager Base Platform	13.4.0.0	All	All	All
Application	Oracle	Enterprise Manager For Storage Management	13.3.0.0	All	All	All
Application	Oracle	Enterprise Manager For Storage Management	13.4.0.0	All	All	All
Application	Oracle	Enterprise Manager For Storage Management	13.3.0.0	All	All	All
Application	Oracle	Enterprise Manager For Storage Management	13.4.0.0	All	All	All
Application	Oracle	Enterprise Manager Ops Center	12.4.0	All	All	All
Application	Oracle	Enterprise Manager Ops Center	12.4.0	All	All	All
Application	Oracle	Http Server	12.2.1.4.0	All	All	All
Application	Oracle	Http Server	12.2.1.4.0	All	All	All
Application	Oracle	Jd Edwards World Security	a9.4	All	All	All
Application	Oracle	Mysql	All	All	All	All
Application	Oracle	Mysql	All	All	All	All
Application	Oracle	Mysql	All	All	All	All

Application	Oracle	Mysql Connectors	All	All	All	All
Application	Oracle	Mysql Enterprise Monitor	All	All	All	All
Application	Oracle	Mysql Enterprise Monitor	All	All	All	All
Application	Oracle	Mysql Workbench	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	8.59	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
OpenSSL: Multiple vulnerabilities (GLSA 202004-10) — Gentoo security	GENTOO
[SECURITY] Fedora 32 Update: openssl-1.1.1g-1.fc32 - package-announce - Fedora Mailing-Lists	
[SECURITY] Fedora 31 Update: openssl-1.1.1g-1.fc31 - package-announce - Fedora Mailing-Lists	FEDORA
Pony Mail!	MLIST
[SECURITY] Fedora 31 Update: openssl-1.1.1g-1.fc31 - package-announce - Fedora Mailing-Lists	
July 2020 MySQL Vulnerabilities in NetApp Products | NetApp Product Security	CONFIRM
Oracle Critical Patch Update Advisory - July 2020	MISC
[security-announce] openSUSE-SU-2020:0945-1: moderate: Security update f	SUSE
Pony Mail!	
Oracle Critical Patch Update Advisory - October 2020	MISC
Oracle Critical Patch Update Advisory - July 2021	N/A
[R1] Tenable.sc 5.17.0 Fixes Multiple Vulnerabilities - Security Advisory | Tenable®	CONFIRM
[SECURITY] Fedora 30 Update: openssl-1.1.1g-1.fc30 - package-announce - Fedora Mailing-Lists	FEDORA
Oracle Critical Patch Update Advisory - October 2021	MISC
[R1] LCE 6.0.9 Fixes Multiple Third-party Vulnerabilities - Security Advisory | Tenable®	CONFIRM
OpenSSL signature_algorithms_cert Denial Of Service ≈ Packet Storm	MISC
Pony Mail!	
www.openssl.org/news/secadv/20200421.txt	CONFIRM
CVE-2020-1967 OpenSSL Vulnerability in NetApp Products | NetApp Product Security	CONFIRM
Full Disclosure: CVE-2020-1967: proving sigalg != NULL	FULLDISC
Pony Mail!	

[R1] Nessus Agent 7.6.3 Fixes Multiple Third-party Vulnerabilities - Security Advisory | Tenable®	CONFIRM
FreeBSD-SA-20:11	FREEBSD
git.openssl.org Git - openssl.git/commitdiff	CONFIRM
[SECURITY] Fedora 30 Update: openssl-1.1.1g-1.fc30 - package-announce - Fedora Mailing-Lists	
Synology Inc.	CONFIRM
GitHub - irsl/CVE-2020-1967: Proof of concept exploit about OpenSSL signature_algorithms_cert DoS flaw (CVE-2020-1967)	MISC
Synology Inc.	CONFIRM
[SECURITY] Fedora 32 Update: openssl-1.1.1g-1.fc32 - package-announce - Fedora Mailing-Lists	FEDORA
[R1] Nessus Network Monitor 5.11.1 Fixes One Third-party Vulnerability - Security Advisory | Tenable®	CONFIRM
Public KB - SA44440 - April 21 2020 OpenSSL Security Advisory	CONFIRM
[security-announce] openSUSE-SU-2020:0933-1: moderate: Security update f	SUSE
Pony Mail!	MLIST
oss-security - [CVE-2020-1967] OpenSSL 1.1.1d+ Segmentation fault in SSL_check_chain	MLIST
Oracle Critical Patch Update Advisory - April 2021	MISC
git.openssl.org Git - openssl.git/commitdiff	
Oracle Critical Patch Update Advisory - January 2021	MISC
Debian -- Security Information -- DSA-4661-1 openssl	DEBIAN
Pony Mail!	MLIST
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

LEGACY: Bernd Edlinger

Legacy QID Mappings

296072 Oracle Solaris 11.4 Support Repository Update (SRU) 25.75.3 Missing (CPUJUL2020)

375970 Oracle PeopleSoft Enterprise PeopleTools Product Multiple Vulnerabilities (CPUOCT2021)

500495 Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)

500563 Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)

500762 Alpine Linux Security Update for openssl

501162 Alpine Linux Security Update for openssl

501981 Alpine Linux Security Update for Open Secure Sockets Layer3 (OpenSSL3)

502900 Alpine Linux Security Update for openssl1.1-compat

504254 Alpine Linux Security Update for openssl

690571 Free Berkeley Software Distribution (FreeBSD) Security Update for Open Secure Sockets Layer (OpenSSL) remote Denial of Service (DoS) Vulnerability (012809ce-83f3-11ea-92ab-00163e433440)