CVE-2018-0739

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2018-0739
State	PUBLIC
Assigner	openssl-security@openssl.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-03-27 21:29:00 UTC
Updated	2023-11-07 02:51:00 UTC
Description	Constructed ASN.1 types with a recursive definition (such as can be found in PKCS7) could eventually exceed the stack giv

Risk And Classification

Problem Types: CWE-674

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	17.10	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	17.10	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Openssl	Openssl	All	All	All	All
Application	Openssl	Openssl	All	All	All	All

References

Reference	Source	Link

Red Hat Customer Portal	REDHAT	access.re
Red Hat Customer Portal	REDHAT	access.re
OpenSSL CVE-2018-0739 Denial of Service Vulnerability	BID	www.sec
Red Hat Customer Portal	REDHAT	access.re
PAN-SA-2018-0015 OpenSSL Vulnerabilities in PAN-OS	CONFIRM	securitya
OpenSSL: Multiple vulnerabilities (GLSA 201811-21) — Gentoo security	GENTOO	security.g
git.openssl.org Git - openssl.git/commitdiff		git.opens
CPU July 2018	CONFIRM	www.ora
Oracle Critical Patch Update - April 2018	CONFIRM	www.ora
Red Hat Customer Portal	REDHAT	access.re
March 2018 OpenSSL Vulnerabilities in NetApp Products | NetApp Product Security	CONFIRM	security.n
Oracle Critical Patch Update Advisory - July 2021	N/A	www.ora
Red Hat Customer Portal	REDHAT	access.re
Oracle PeopleSoft Enterprise PeopleTools Multiple Remote Security Vulnerabilities	BID	www.sec
July 2018 MySQL Vulnerabilities in NetApp Products | NetApp Product Security	CONFIRM	security.n
www.openssl.org/news/secadv/20180327.txt	CONFIRM	www.ope
USN-3611-2: OpenSSL vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubun
[R1] Nessus Network Monitor 5.5.0 Fixes One Third-party Vulnerability - Security Advisory | Tenable®	CONFIRM	www.tena
Oracle Critical Patch Update - January 2019	CONFIRM	www.ora
Debian -- Security Information -- DSA-4157-1 openssl	DEBIAN	www.deb
March 2018 Security Releases | Node.js	CONFIRM	nodejs.or
[SECURITY] [DLA 1330-1] openssl security update	MLIST	lists.debi
Dropbear: Multiple vulnerabilities (GLSA 202007-53) — Gentoo security	GENTOO	security.g
Oracle Critical Patch Update - July 2019	MISC	www.ora
[R1] Industrial Security 1.1.0 Fixes One Third-party Vulnerability - Security Advisory | Tenable®	CONFIRM	www.tena
Red Hat Customer Portal	REDHAT	access.re
USN-3611-1: OpenSSL vulnerability | Ubuntu security notices | Ubuntu	UBUNTU	usn.ubun
OpenSSL Bugs Let Users Deny Service and Bypass Authentication in Certain Cases - SecurityTracker	SECTRACK	www.sec
git.openssl.org Git - openssl.git/commitdiff		git.opens
Red Hat Customer Portal	REDHAT	access.re
CPU Oct 2018	CONFIRM	www.ora
Debian -- Security Information -- DSA-4158-1 openssl1.0	DEBIAN	www.deb
git.openssl.org Git - openssl.git/commitdiff	CONFIRM	git.opens
git.openssl.org Git - openssl.git/commitdiff	CONFIRM	git.opens
[R1] OpenSSL Stand-alone Patch Available for SecurityCenter versions 5.0 or Later - Security Advisory | Tenable®	CONFIRM	www.tena
Oracle Critical Patch Update Advisory - April 2019	MISC	

Oracle Critical Patch Update Advisory - April 2019	MISC	www.ora
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.g

Vendor Comments And Credit

Discovery Credit

LEGACY: OSS-fuzz

Legacy QID Mappings

296090 Oracle Solaris 11.4 Support Repository Update (SRU) 5.1.3 Missing (CPUJAN2019)

390226 Oracle Managed Virtualization (VM) Server for x86 Security Update for Open Secure Sockets Layer (OpenSSL) (OVMSA-2021-0011)

390284 Oracle Managed Virtualization (VM) Server for x86 Security Update for Open Secure Sockets Layer (OpenSSL) (OVMSA-2023-0013)

43888 Huawei Router Open Secure Sockets Layer (OpenSSL) Vulnerability Vulnerability (Huawei-SA-20180613-01-openssl-en)

591115 ABB Relion 670 series and Relion 650 series Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities (ABBVU-PGGA-1MRG032388)

670784 EulerOS Security Update for shim (EulerOS-SA-2021-2542)

670808 EulerOS Security Update for shim (EulerOS-SA-2021-2566)

690582 Free Berkeley Software Distribution (FreeBSD) Security Update for mysql (909be51b-9b3b-11e8-add2-b499baebfeaf)

710214 Gentoo Linux Open Secure Sockets Layer Multiple Vulnerabilities (GLSA 201811-21)