CVE-2018-0732

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2018-0732
State	PUBLIC
Assigner	openssl-security@openssl.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-06-12 13:29:00 UTC
Updated	2023-11-07 02:51:00 UTC
Description	During key agreement in a TLS handshake using a DH(E) based ciphersuite a malicious server can send a very large prime

Risk And Classification

Problem Types: CWE-320

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	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	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	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	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Nodejs	Node.js	All	All	All	All
Application	Nodejs	Node.js	All	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.red
January 2019 MySQL Vulnerabilities in NetApp Products | NetApp Product Security	CONFIRM	security.ne
[SECURITY] Fedora 30 Update: compat-openssl10-1.0.2o-7.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedora
Red Hat Customer Portal	REDHAT	access.red
git.openssl.org Git - openssl.git/commitdiff		git.openssl
[R1] Nessus 7.1.4 Fixes Multiple Third-party Vulnerabilities - Security Advisory | Tenable®	CONFIRM	www.tenab
Red Hat Customer Portal	REDHAT	access.red
[SECURITY] Fedora 31 Update: compat-openssl10-1.0.2o-8.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedora
[SECURITY] Fedora 30 Update: compat-openssl10-1.0.2o-7.fc30 - package-announce - Fedora Mailing-Lists		lists.fedora
[R1] LCE 5.1.1 Fixes Multiple Third-party Vulnerabilities - Security Advisory | Tenable®	CONFIRM	www.tenab
[SECURITY] Fedora 29 Update: compat-openssl10-1.0.2o-7.fc29 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedora
[R1] SecurityCenter 5.7.1 Fixes Multiple Third-Party Vulnerabilities - Security Advisory | Tenable®	CONFIRM	www.tenab
www.openssl.org/news/secadv/20180612.txt	CONFIRM	www.opens
Debian -- Security Information -- DSA-4348-1 openssl	DEBIAN	www.debia
PAN-SA-2018-0015 OpenSSL Vulnerabilities in PAN-OS	CONFIRM	securityadv
[SECURITY] [DLA 1449-1] openssl security update	MLIST	lists.debian
Red Hat Customer Portal	REDHAT	access.red
Red Hat Customer Portal	REDHAT	access.red
OpenSSL DH Parameter Processing Lets Remote Servers Deny Service on Connected Clients - SecurityTracker	SECTRACK	www.secur
[R1] Nessus 8.0.0 Fixes Multiple Third-party Vulnerabilities - Security Advisory | Tenable®	CONFIRM	www.tenab
git.openssl.org Git - openssl.git/commitdiff	CONFIRM	git.openssl
[SECURITY] Fedora 29 Update: compat-openssl10-1.0.2o-7.fc29 - package-announce - Fedora Mailing-Lists		lists.fedora
Oracle Critical Patch Update - January 2019	CONFIRM	www.oracle
OpenSSL CVE-2018-0732 Denial of Service Vulnerability	BID	www.secur
Red Hat Customer Portal	REDHAT	access.red
Oracle Critical Patch Update - July 2019	MISC	www.oracle
CVE-2018-0732 OpenSSL Vulnerability in NetApp Products | NetApp Product Security	CONFIRM	security.ne
git.openssl.org Git - openssl.git/commitdiff	CONFIRM	git.openssl
git.openssl.org Git - openssl.git/commitdiff		git.openssl
cert-portal.siemens.com/productcert/pdf/ssa-419820.pdf	CONFIRM	cert-portal.s
[SECURITY] Fedora 31 Update: compat-openssl10-1.0.2o-8.fc31 - package-announce - Fedora Mailing-Lists		lists.fedora
August 2018 Security Releases | Node.js	CONFIRM	nodejs.org
USN-3692-1: OpenSSL vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu

Debian -- Security Information -- DSA-4355-1 openssl1.0	DEBIAN	www.debia
CPU Oct 2018	CONFIRM	www.oracle
OpenSSL: Denial of Service (GLSA 201811-03) — Gentoo security	GENTOO	security.ge
Oracle Critical Patch Update - October 2019	MISC	www.oracle
Red Hat Customer Portal	REDHAT	access.red
Oracle Critical Patch Update Advisory - April 2020	N/A	www.oracle
Oracle Critical Patch Update Advisory - January 2021	MISC	www.oracle
USN-3692-2: OpenSSL vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu
Oracle Critical Patch Update Advisory - April 2019	MISC	www.oracle
CVE Program record	CVE.ORG	www.cve.o
NVD vulnerability detail	NVD	nvd.nist.go

Vendor Comments And Credit

Discovery Credit

LEGACY: Guido Vranken

Legacy QID Mappings

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)

500368 Alpine Linux Security Update for libressl

590699 Siemens TIM 1531 IRC Vulnerability (ICSA-21-159-08)

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)

690588 Free Berkeley Software Distribution (FreeBSD) Security Update for Open Secure Sockets Layer (OpenSSL) (c82ecac5-6e3f-11e8-8777-b499baebfeaf)

710295 Gentoo Linux Open Secure Sockets Layer Denial of service Vulnerability (GLSA 201811-03)

CVE.report and Source URL Uptime Status status.cve.report