CVE-2018-0734

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2018-0734
State	PUBLIC
Assigner	openssl-security@openssl.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-10-30 12:29:00 UTC
Updated	2023-11-07 02:51:00 UTC
Description	The OpenSSL DSA signature algorithm has been shown to be vulnerable to a timing side channel attack. An attacker could

Risk And Classification

Problem Types: CWE-327

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	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	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	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Netapp	Cloud Backup	-	All	All	All
Application	Netapp	Cloud Backup	-	All	All	All
Hardware	Netapp	Cn1610	-	All	All	All
Hardware	Netapp	Cn1610	-	All	All	All
Operating System	Netapp	Cn1610 Firmware	-	All	All	All
Operating System	Netapp	Cn1610 Firmware	-	All	All	All
Application	Netapp	Oncommand Unified Manager	All	All	All	All

Application	Netapp	Oncommand Unified Manager	All	All	All	All
Application	Netapp	Santricity Smi-s Provider	-	All	All	All
Application	Netapp	Santricity Smi-s Provider	-	All	All	All
Application	Netapp	Snapcenter	-	All	All	All
Application	Netapp	Snapcenter	-	All	All	All
Application	Netapp	Steelstore	-	All	All	All
Application	Netapp	Steelstore	-	All	All	All
Application	Netapp	Storage Automation Store	-	All	All	All
Application	Netapp	Storage Automation Store	-	All	All	All
Application	Nodejs	Node.js	All	All	All	All
Application	Nodejs	Node.js	All	All	All	All
Application	Nodejs	Node.js	10.13.0	All	All	All
Application	Nodejs	Node.js	All	All	All	All
Application	Nodejs	Node.js	All	All	All	All
Application	Nodejs	Node.js	All	All	All	All
Application	Nodejs	Node.js	All	All	All	All
Application	Nodejs	Node.js	All	All	All	All
Application	Nodejs	Node.js	All	All	All	All
Application	Nodejs	Node.js	All	All	All	All
Application	Openssl	Openssl	1.1.1	All	All	All
Application	Openssl	Openssl	1.1.1	All	All	All
Application	Openssl	Openssl	All	All	All	All
Application	Openssl	Openssl	All	All	All	All
Application	Oracle	Api Gateway	11.1.2.4.0	All	All	All
Application	Oracle	Api Gateway	11.1.2.4.0	All	All	All
Application	Oracle	E-business Suite Technology Stack	0.9.8	All	All	All
Application	Oracle	E-business Suite Technology Stack	1.0.0	All	All	All
Application	Oracle	E-business Suite Technology Stack	1.0.1	All	All	All
Application	Oracle	E-business Suite Technology Stack	0.9.8	All	All	All
Application	Oracle	E-business Suite Technology Stack	1.0.0	All	All	All
Application	Oracle	E-business Suite Technology Stack	1.0.1	All	All	All
Application	Oracle	Enterprise Manager Base Platform	12.1.0.5.0	All	All	All
Application	Oracle	Enterprise Manager Base Platform	13.2.0.0.0	All	All	All
Application	Oracle	Enterprise Manager Base Platform	13.3.0.0.0	All	All	All
Application	Oracle	Enterprise Manager Base Platform	12.1.0.5.0	All	All	All

Application	Oracle	Enterprise Manager Base Platform	13.2.0.0.0	All	All	All
Application	Oracle	Enterprise Manager Base Platform	13.3.0.0.0	All	All	All
Application	Oracle	Enterprise Manager Ops Center	12.3.3	All	All	All
Application	Oracle	Enterprise Manager Ops Center	12.3.3	All	All	All
Application	Oracle	Mysql Enterprise Backup	All	All	All	All
Application	Oracle	Mysql Enterprise Backup	All	All	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.55	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	8.55	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	Primavera P6 Professional Project Management	15.1	All	All	All
Application	Oracle	Primavera P6 Professional Project Management	15.2	All	All	All
Application	Oracle	Primavera P6 Professional Project Management	16.1	All	All	All
Application	Oracle	Primavera P6 Professional Project Management	16.2	All	All	All
Application	Oracle	Primavera P6 Professional Project Management	18.8	All	All	All
Application	Oracle	Primavera P6 Professional Project Management	8.4	All	All	All
Application	Oracle	Primavera P6 Professional Project Management	15.1	All	All	All
Application	Oracle	Primavera P6 Professional Project Management	15.2	All	All	All
Application	Oracle	Primavera P6 Professional Project Management	16.1	All	All	All
Application	Oracle	Primavera P6 Professional Project Management	16.2	All	All	All
Application	Oracle	Primavera P6 Professional Project Management	18.8	All	All	All
Application	Oracle	Primavera P6 Professional Project Management	8.4	All	All	All
Application	Oracle	Primavera P6 Professional Project Management	All	All	All	All
Application	Oracle	Tuxedo	12.1.1.0.0	All	All	All
Application	Oracle	Tuxedo	12.1.1.0.0	All	All	All

References

Reference	Source	Link
Red Hat Customer Portal	REDHAT	access.redhat.co
git.openssl.org Git - openssl.git/commitdiff		git.openssl.org
[security-announce] openSUSE-SU-2019:1547-1: important: Security update	SUSE	lists.opensuse.or
January 2019 MySQL Vulnerabilities in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.c
[SECURITY] Fedora 30 Update: compat-openssl10-1.0.2o-7.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraprojec
git.openssl.org Git - openssl.git/commitdiff		git.openssl.org

[R1] Nessus 7.1.4 Fixes Multiple Third-party Vulnerabilities - Security Advisory | Tenable®	CONFIRM	www.tenable.com
[SECURITY] Fedora 31 Update: compat-openssl10-1.0.2o-8.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject
[SECURITY] Fedora 30 Update: compat-openssl10-1.0.2o-7.fc30 - package-announce - Fedora Mailing-Lists		lists.fedoraproject
[SECURITY] Fedora 29 Update: compat-openssl10-1.0.2o-7.fc29 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject
[R1] Nessus 8.1.1 Fixes Multiple Third-party Vulnerabilities - Security Advisory | Tenable®	CONFIRM	www.tenable.com
Debian -- Security Information -- DSA-4348-1 openssl	DEBIAN	www.debian.org
[security-announce] openSUSE-SU-2019:1814-1: important: Security update	SUSE	lists.opensuse.or
git.openssl.org Git - openssl.git/commitdiff	CONFIRM	git.openssl.org
Red Hat Customer Portal	REDHAT	access.redhat.co
November 2018 Security Releases | Node.js	CONFIRM	nodejs.org
[SECURITY] Fedora 29 Update: compat-openssl10-1.0.2o-7.fc29 - package-announce - Fedora Mailing-Lists		lists.fedoraproject
Oracle Critical Patch Update - January 2019	CONFIRM	www.oracle.com
Oracle Critical Patch Update - July 2019	MISC	www.oracle.com
Red Hat Customer Portal	REDHAT	access.redhat.co
www.openssl.org/news/secadv/20181030.txt	CONFIRM	www.openssl.org
[SECURITY] Fedora 31 Update: compat-openssl10-1.0.2o-8.fc31 - package-announce - Fedora Mailing-Lists		lists.fedoraproject
git.openssl.org Git - openssl.git/commitdiff		git.openssl.org
OpenSSL CVE-2018-0734 Side Channel Attack Information Disclosure Vulnerability	BID	www.securityfocu
April 2019 MySQL Vulnerabilities in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.c
October 2018 OpenSSL Vulnerabilities in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.c
Debian -- Security Information -- DSA-4355-1 openssl1.0	DEBIAN	www.debian.org
Oracle Critical Patch Update Advisory - January 2020	MISC	www.oracle.com
USN-3840-1: OpenSSL vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com
Oracle Critical Patch Update Advisory - April 2020	N/A	www.oracle.com
Red Hat Customer Portal	REDHAT	access.redhat.co
git.openssl.org Git - openssl.git/commitdiff	CONFIRM	git.openssl.org
Red Hat Customer Portal	REDHAT	access.redhat.co
git.openssl.org Git - openssl.git/commitdiff	CONFIRM	git.openssl.org
Oracle Critical Patch Update Advisory - April 2019	MISC	www.oracle.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

LEGACY: Samuel Weiser

Legacy QID Mappings

296075 Oracle Solaris 11.4 Support Repository Update (SRU) 21.69.0 Missing (CPUAPR2020)

296087 Oracle Solaris 11.4 Support Repository Update (SRU) 8.1.5 Missing (CPUAPR2019)

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

377473 Alibaba Cloud Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ALINUX2-SA-2019:0086)

500432 Alpine Linux Security Update for nodejs

500491 Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)

500559 Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)

500758 Alpine Linux Security Update for openssl

501095 Alpine Linux Security Update for nodejs-current

501158 Alpine Linux Security Update for openssl

501977 Alpine Linux Security Update for Open Secure Sockets Layer3 (OpenSSL3)

502896 Alpine Linux Security Update for openssl1.1-compat

504195 Alpine Linux Security Update for nodejs

504250 Alpine Linux Security Update for openssl

690638 Free Berkeley Software Distribution (FreeBSD) Security Update for Open Secure Sockets Layer (OpenSSL) (238ae7de-dba2-11e8-b713-b499baebfeaf)

900064 CBL-Mariner Linux Security Update for nodejs 8.11.4

903261 Common Base Linux Mariner (CBL-Mariner) Security Update for nodejs (4295)