CVE-2018-0735

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2018-0735
State	PUBLIC
Assigner	openssl-security@openssl.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-10-29 13:29:00 UTC
Updated	2023-11-07 02:51:00 UTC
Description	The OpenSSL ECDSA signature algorithm has been shown to be vulnerable to a timing side channel attack. An attacker co

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	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	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	Element Software	-	All	All	All
Application	Netapp	Element Software	-	All	All	All
Application	Netapp	Oncommand Unified Manager	All	All	All	All
Application	Netapp	Oncommand Unified Manager	All	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	Smi-s Provider	-	All	All	All
Application	Netapp	Smi-s Provider	-	All	All	All
Application	Netapp	Snapdrive	-	All	All	All
Application	Netapp	Snapdrive	-	All	All	All
Application	Netapp	Snapdrive	-	All	All	All
Application	Netapp	Snapdrive	-	All	All	All
Application	Netapp	Steelstore	-	All	All	All
Application	Netapp	Steelstore	-	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	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	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	Application Server	0.9.8	All	All	All
Application	Oracle	Application Server	1.0.0	All	All	All
Application	Oracle	Application Server	1.0.1	All	All	All
Application	Oracle	Application Server	0.9.8	All	All	All
Application	Oracle	Application Server	1.0.0	All	All	All
Application	Oracle	Application Server	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	All	All	All	All
Application	Oracle	Mysql	All	All	All	All
Application	Oracle	Mysql	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 Enterprise Project Portfolio Management	15.1	All	All	All
Application	Oracle	Primavera P6 Enterprise Project Portfolio Management	15.2	All	All	All
Application	Oracle	Primavera P6 Enterprise Project Portfolio Management	16.1	All	All	All
Application	Oracle	Primavera P6 Enterprise Project Portfolio Management	16.2	All	All	All
Application	Oracle	Primavera P6 Enterprise Project Portfolio Management	18.8	All	All	All
Application	Oracle	Primavera P6 Enterprise Project Portfolio Management	8.4	All	All	All
Application	Oracle	Primavera P6 Enterprise Project Portfolio Management	15.1	All	All	All
Application	Oracle	Primavera P6 Enterprise Project Portfolio Management	15.2	All	All	All
Application	Oracle	Primavera P6 Enterprise Project Portfolio Management	16.1	All	All	All
Application	Oracle	Primavera P6 Enterprise Project Portfolio Management	16.2	All	All	All
Application	Oracle	Primavera P6 Enterprise Project Portfolio Management	18.8	All	All	All
Application	Oracle	Primavera P6 Enterprise Project Portfolio Management	8.4	All	All	All
Application	Oracle	Primavera P6 Enterprise Project Portfolio Management	All	All	All	All
Application	Oracle	Secure Global Desktop	5.4	All	All	All
Application	Oracle	Secure Global Desktop	5.4	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
Application	Oracle	Vm Virtualbox	All	All	All	All
Application	Oracle	Vm Virtualbox	All	All	All	All

References

Reference	Sou

OpenSSL CVE-2018-0735 Side Channel Attack Information Disclosure Vulnerability	BID
git.openssl.org Git - openssl.git/commitdiff	
www.openssl.org/news/secadv/20181029.txt	CO
Debian -- Security Information -- DSA-4348-1 openssl	DE
git.openssl.org Git - openssl.git/commitdiff	CO
November 2018 Security Releases | Node.js	CO
Oracle Critical Patch Update - January 2019	CO
OpenSSL ECDSA Signature Algorithm Lets Remote Users Obtain Passwords on the Target System in Certain Cases - SecurityTracker	SE
Oracle Critical Patch Update - July 2019	MIS
[SECURITY] [DLA 1586-1] openssl security update	ML
git.openssl.org Git - openssl.git/commitdiff	CO
October 2018 OpenSSL Vulnerabilities in NetApp Products | NetApp Product Security	CO
Oracle Critical Patch Update Advisory - January 2020	MIS
USN-3840-1: OpenSSL vulnerabilities | Ubuntu security notices	UB
Red Hat Customer Portal	RE
git.openssl.org Git - openssl.git/commitdiff	
Oracle Critical Patch Update Advisory - April 2019	MIS
CVE Program record	CV
NVD vulnerability detail	NV

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)

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)