CVE-2017-3730

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2017-3730
State	PUBLIC
Assigner	openssl-security@openssl.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-05-04 19:29:00 UTC
Updated	2019-04-25 13:59:00 UTC
Description	In OpenSSL 1.1.0 before 1.1.0d, if a malicious server supplies bad parameters for a DHE or ECDHE key exchange then thi

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openssl	Openssl	1.1.0	All	All	All
Application	Openssl	Openssl	1.1.0a	All	All	All
Application	Openssl	Openssl	1.1.0b	All	All	All
Application	Openssl	Openssl	1.1.0c	All	All	All
Application	Openssl	Openssl	1.1.0	All	All	All
Application	Openssl	Openssl	1.1.0a	All	All	All
Application	Openssl	Openssl	1.1.0b	All	All	All
Application	Openssl	Openssl	1.1.0c	All	All	All
Application	Oracle	Agile Engineering Data Management	6.1.3	All	All	All
Application	Oracle	Agile Engineering Data Management	6.2.0	All	All	All
Application	Oracle	Agile Engineering Data Management	6.1.3	All	All	All
Application	Oracle	Agile Engineering Data Management	6.2.0	All	All	All
Application	Oracle	Communications Application Session Controller	3.7.1	All	All	All
Application	Oracle	Communications Application Session Controller	3.8.0	All	All	All
Application	Oracle	Communications Application Session Controller	3.7.1	All	All	All
Application	Oracle	Communications Application Session Controller	3.8.0	All	All	All
Application	Oracle	Communications Eagle Lnp Application Processor	10.0	All	All	All

Application	Oracle	Communications Eagle Lnp Application Processor	10.1	All	All	All
Application	Oracle	Communications Eagle Lnp Application Processor	10.2	All	All	All
Application	Oracle	Communications Eagle Lnp Application Processor	10.0	All	All	All
Application	Oracle	Communications Eagle Lnp Application Processor	10.1	All	All	All
Application	Oracle	Communications Eagle Lnp Application Processor	10.2	All	All	All
Application	Oracle	Communications Operations Monitor	3.4	All	All	All
Application	Oracle	Communications Operations Monitor	4.0	All	All	All
Application	Oracle	Communications Operations Monitor	3.4	All	All	All
Application	Oracle	Communications Operations Monitor	4.0	All	All	All
Application	Oracle	Jd Edwards Enterpriseone Tools	9.2	All	All	All
Application	Oracle	Jd Edwards Enterpriseone Tools	9.2	All	All	All
Application	Oracle	Jd Edwards World Security	a9.1	All	All	All
Application	Oracle	Jd Edwards World Security	a9.2	All	All	All
Application	Oracle	Jd Edwards World Security	a9.3	All	All	All
Application	Oracle	Jd Edwards World Security	a9.4	All	All	All
Application	Oracle	Jd Edwards World Security	a9.1	All	All	All
Application	Oracle	Jd Edwards World Security	a9.2	All	All	All
Application	Oracle	Jd Edwards World Security	a9.3	All	All	All
Application	Oracle	Jd Edwards World Security	a9.4	All	All	All

References

Reference	Source	Lin
OpenSSL: Multiple vulnerabilities (GLSA 201702-07) — Gentoo Security	GENTOO	sec
Fix missing NULL checks in CKE processing · openssl/openssl@efbe126 · GitHub	MISC	gith
www.openssl.org/news/secadv/20170126.txt	CONFIRM	ww
Oracle Critical Patch Update - January 2018	CONFIRM	ww
OpenSSL Multiple Bugs Let Remote Users Deny Service and Obtain Potentially Sensitive Information - SecurityTracker	SECTRACK	ww
OpenSSL 1.1.0 - Remote Client Denial of Service - Multiple dos Exploit	EXPLOIT-DB	ww
OpenSSL CVE-2017-3730 NULL Pointer Dereference Denial of Service Vulnerability	BID	ww
Document Display | HPE Support Center	CONFIRM	sup
Oracle Critical Patch Update - October 2017	CONFIRM	ww
Oracle Critical Patch Update Advisory - April 2019	MISC	ww
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nvc

Vendor Comments And Credit

Discovery Credit

LEGACY: Guido Vranken

Legacy QID Mappings

43835 HPE Switches And Routers Open Secure Sockets Layer (OpenSSL) Multiple Remote Vulnerabilities (HPESBHF03838)