CVE-2017-3731

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2017-3731
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	2022-08-16 13:16:00 UTC
Description	If an SSL/TLS server or client is running on a 32-bit host, and a specific cipher is being used, then a truncated packet can c

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	1.0.2	All	All	All
Application	Openssl	Openssl	1.0.2	beta1	All	All
Application	Openssl	Openssl	1.0.2	beta2	All	All
Application	Openssl	Openssl	1.0.2	beta3	All	All
Application	Openssl	Openssl	1.0.2a	All	All	All
Application	Openssl	Openssl	1.0.2b	All	All	All
Application	Openssl	Openssl	1.0.2c	All	All	All
Application	Openssl	Openssl	1.0.2d	All	All	All
Application	Openssl	Openssl	1.0.2e	All	All	All
Application	Openssl	Openssl	1.0.2f	All	All	All
Application	Openssl	Openssl	1.0.2h	All	All	All
Application	Openssl	Openssl	1.0.2i	All	All	All

Application	Openssl	Openssl	1.0.2j	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	1.0.2	All	All	All
Application	Openssl	Openssl	1.0.2	beta1	All	All
Application	Openssl	Openssl	1.0.2	beta2	All	All
Application	Openssl	Openssl	1.0.2	beta3	All	All
Application	Openssl	Openssl	1.0.2a	All	All	All
Application	Openssl	Openssl	1.0.2b	All	All	All
Application	Openssl	Openssl	1.0.2c	All	All	All
Application	Openssl	Openssl	1.0.2d	All	All	All
Application	Openssl	Openssl	1.0.2e	All	All	All
Application	Openssl	Openssl	1.0.2f	All	All	All
Application	Openssl	Openssl	1.0.2h	All	All	All
Application	Openssl	Openssl	1.0.2i	All	All	All
Application	Openssl	Openssl	1.0.2j	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

References

Reference	Source	Link
OpenSSL: Multiple vulnerabilities (GLSA 201702-07) — Gentoo Security	GENTOO	secu
Red Hat Customer Portal	REDHAT	rhn.r
Debian -- Security Information -- DSA-3773-1 openssl	DEBIAN	www
FreeBSD-SA-17:02	FREEBSD	secu
www.openssl.org/news/secadv/20170126.txt	CONFIRM	www
Oracle Critical Patch Update - January 2018	CONFIRM	www
OpenSSL CVE-2017-3731 Denial of Service Vulnerability	BID	www
[R5] SecurityCenter 5.4.3 Fixes Multiple Vulnerabilities - Security Advisory | Tenable Network Security	CONFIRM	www
crypto/evp: harden AEAD ciphers. · openssl/openssl@00d9654 · GitHub	MISC	githu
OpenSSL Multiple Bugs Let Remote Users Deny Service and Obtain Potentially Sensitive Information - SecurityTracker	SECTRACK	www
Red Hat Customer Portal	REDHAT	acce
Document Display | HPE Support Center	CONFIRM	supp

Red Hat Customer Portal	REDHAT	acce
October 2017 MySQL Vulnerabilities in NetApp Products | NetApp Product Security	CONFIRM	secu
Red Hat Customer Portal	REDHAT	acce
Pixel / Nexus Security Bulletin—November 2017 | Android Open Source Project	CONFIRM	sour
CVE-2017-3731 OpenSSL Vulnerability	CONFIRM	secu
Oracle Critical Patch Update - July 2017	CONFIRM	www
Oracle Critical Patch Update - October 2017	CONFIRM	www
Oracle Critical Patch Update Advisory - April 2019	MISC	www
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd.

Vendor Comments And Credit

Discovery Credit

LEGACY: Robert Święcki of Google

Legacy QID Mappings

378210 Virtuozzo Linux Security Update for openssl-perl (VZLSA-2017:0286)

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)

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