CVE-2017-3732

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2017-3732
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	2022-08-29 20:43:00 UTC
Description	There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL 1.0.2 before 1.0.2k and 1.1.0

Risk And Classification

Problem Types: CWE-200

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	1.1.0a	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	1.1.0a	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
FreeBSD-SA-17:02	FREEBSD	secu
www.openssl.org/news/secadv/20170126.txt	CONFIRM	www
Oracle Critical Patch Update - January 2018	CONFIRM	www
Red Hat Customer Portal	REDHAT	acce
[R5] SecurityCenter 5.4.3 Fixes Multiple Vulnerabilities - Security Advisory | Tenable Network Security	CONFIRM	www
OpenSSL Multiple Bugs Let Remote Users Deny Service and Obtain Potentially Sensitive Information - SecurityTracker	SECTRACK	www
Red Hat Customer Portal	REDHAT	acce
Red Hat Customer Portal	REDHAT	acce
Document Display | HPE Support Center	CONFIRM	supp
Red Hat Customer Portal	REDHAT	acce
OpenSSL CVE-2017-3732 Information Disclosure Vulnerability	BID	www
Red Hat Customer Portal	REDHAT	acce
Red Hat Customer Portal	REDHAT	acce

Oracle Critical Patch Update - July 2017	CONFIRM	www
Oracle Critical Patch Update - October 2017	CONFIRM	www
bn/asm/x86_64-mont5.pl: fix carry bug in bn_sqr8x_internal. · openssl/openssl@a59b90b · GitHub	MISC	githu
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: OSS-Fuzz project

Legacy QID Mappings

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

710243 Gentoo Linux MySQL Multiple Vulnerabilities (GLSA 201802-04)