CVE-2017-3738

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2017-3738
State	PUBLIC
Assigner	openssl-security@openssl.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-12-07 16:29:00 UTC
Updated	2022-08-19 11:49:00 UTC
Description	There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	9.0	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	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	1.0.2g	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	1.0.2k	All	All	All
Application	Openssl	Openssl	1.0.2l	All	All	All
Application	Openssl	Openssl	1.0.2m	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	Openssl	Openssl	1.1.0d	All	All	All
Application	Openssl	Openssl	1.1.0e	All	All	All
Application	Openssl	Openssl	1.1.0f	All	All	All
Application	Openssl	Openssl	1.1.0g	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	1.0.2g	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	1.0.2k	All	All	All
Application	Openssl	Openssl	1.0.2l	All	All	All
Application	Openssl	Openssl	1.0.2m	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	Openssl	Openssl	1.1.0d	All	All	All
Application	Openssl	Openssl	1.1.0e	All	All	All
Application	Openssl	Openssl	1.1.0f	All	All	All
Application	Openssl	Openssl	1.1.0g	All	All	All

References

Reference
OpenSSL: Multiple vulnerabilities (GLSA 201712-03) — Gentoo security
Document Display | HPE Support Center
Debian -- Security Information -- DSA-4065-1 openssl1.0
Oracle Critical Patch Update - January 2018
CPU July 2018
Oracle Critical Patch Update - April 2018
FreeBSD-SA-17:12
www.openssl.org/news/secadv/20180327.txt
Red Hat Customer Portal
OpenSSL CVE-2017-3738 Information Disclosure Vulnerability
[R1] Nessus Network Monitor 5.5.0 Fixes One Third-party Vulnerability - Security Advisory | Tenable®
Oracle Critical Patch Update - January 2019
Debian -- Security Information -- DSA-4157-1 openssl
December 2017 OpenSSL Vulnerabilities in NetApp Products | NetApp Product Security
Oracle Critical Patch Update - July 2019
[R1] Industrial Security 1.1.0 Fixes One Third-party Vulnerability - Security Advisory | Tenable®
[R2] SecurityCenter 5.6.1 Fixes Multiple Third-party Vulnerabilities - Security Advisory | Tenable®
Red Hat Customer Portal
Red Hat Customer Portal
CPU Oct 2018
Red Hat Customer Portal
Data Confidentiality/Integrity Vulnerability, December 2017 | Node.js
OpenSSL Overflow in rsaz_1024_mul_avx2() Lets Remote Users Obtain Potentially Sensitive Information in Certain Cases and SSL_read()/S
bn/asm/rsaz-avx2.pl: fix digit correction bug in rsaz_1024_mul_avx2. · openssl/openssl@e502cc8 · GitHub
www.openssl.org/news/secadv/20171207.txt
[R1] OpenSSL Stand-alone Patch Available for SecurityCenter versions 5.0 or Later - Security Advisory | Tenable®
Oracle Critical Patch Update Advisory - April 2019

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

710507 Gentoo Linux Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities (GLSA 201712-03)