CVE-2015-7744

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2015-7744
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-01-22 15:59:00 UTC
Updated	2022-08-29 20:52:00 UTC
Description	wolfSSL (formerly CyaSSL) before 3.6.8 does not properly handle faults associated with the Chinese Remainder Theorem (

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mariadb	Mariadb	All	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Application	Wolfssl	Wolfssl	All	All	All	All
Application	Wolfssl	Wolfssl	All	All	All	All

References

Reference
people.redhat.com/~fweimer/rsa-crt-leaks.pdf
Oracle Solaris Bulletin - April 2016
MySQL Multiple Bugs Let Remote Users Access Data and Deny Service, Remote Authenticated Users Modify Data, and Local Users Gain Ele
[security-announce] openSUSE-SU-2016:0367-1: important: Security update
Two Vulnerabilities Recently Found, An Attack on RSA using CRT and DoS Vulnerability With DTLS
[security-announce] openSUSE-SU-2016:0377-1: important: Security update

Docs-wolfssl-changelog
Factoring RSA Keys With TLS Perfect Forward Secrecy | Red Hat Security
Oracle Critical Patch Update - January 2016
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.