CVE-2021-36647

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-36647
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-01-17 21:15:00 UTC
Updated	2023-01-27 17:56:00 UTC
Description	Use of a Broken or Risky Cryptographic Algorithm in the function mbedtls_mpi_exp_mod() in lignum.c in Mbed TLS Mbed T

Risk And Classification

Problem Types: CWE-327

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Arm	Mbed Tls	All	All	All	All

References

Reference	Source	Link	Tags
Local side channel attack on RSA - Tech Updates - Mbed TLS (Previously PolarSSL)	MISC	tls.mbed.org	
kouzili.com/Load-Step.pdf	MISC	kouzili.com	
Releases · ARMmbed/mbedtls · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

183968 Debian Security Update for mbedtls (CVE-2021-36647)

905280 Common Base Linux Mariner (CBL-Mariner) Security Update for fluent-bit (13023)

906522 Common Base Linux Mariner (CBL-Mariner) Security Update for fluent-bit (13023-1)

906626 Common Base Linux Mariner (CBL-Mariner) Security Update for fluent-bit (13023-3)