CVE-2020-36424

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-36424
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-07-19 17:15:00 UTC
Updated	2023-01-11 17:02:00 UTC
Description	An issue was discovered in Arm Mbed TLS before 2.24.0. An attacker can recover a private key (for RSA or static Diffie-He

Risk And Classification

Problem Types: CWE-203

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Arm	Mbed Tls	All	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All

References

Reference
740108 – (CVE-2020-16150, CVE-2020-36424, CVE-2020-36425, CVE-2020-36426) <net-libs/mbedtls-{2.16.8,2.24.0}: Multiple vulnerabilities
Local side channel attack on RSA and static Diffie-Hellman - Tech Updates - Mbed TLS (Previously PolarSSL)
Release Mbed TLS 2.16.8 · ARMmbed/mbedtls · GitHub
Release Mbed TLS 2.24.0 · ARMmbed/mbedtls · GitHub
Release Mbed TLS 2.7.17 · ARMmbed/mbedtls · GitHub
[SECURITY] [DLA 3249-1] mbedtls security update
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

180705 Debian Security Update for mbedtls (CVE-2020-36424)

181446 Debian Security Update for mbedtls (DLA 3249-1)

710702 Gentoo Linux Mbed Transport Layer Security (TLS) Multiple Vulnerabilities (GLSA 202301-08)