CVE-2021-43666

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-43666
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-03-24 18:15:00 UTC
Updated	2023-07-20 15:06:00 UTC
Description	A Denial of Service vulnerability exists in mbed TLS 3.0.0 and earlier in the mbedtls_pkcs12_derivation function when an in

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
mbedtls_pkcs12_derivation() can't exit when the input password length is 0. · Issue #5136 · ARMmbed/mbedtls · GitHub	MISC	github
[SECURITY] [DLA 3249-1] mbedtls security update	MLIST	lists.d
CVE Program record	CVE.ORG	www.c
NVD vulnerability detail	NVD	nvd.ni

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

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

184161 Debian Security Update for mbedtls (CVE-2021-43666)

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