CVE-2021-44732

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-44732
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-12-20 08:15:00 UTC
Updated	2023-02-24 00:09:00 UTC
Description	Mbed TLS before 3.0.1 has a double free in certain out-of-memory conditions, as demonstrated by an mbedtls_ssl_set_ses

Risk And Classification

Problem Types: CWE-415

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Arm	Mbed Tls	All	All	All	All
Application	Arm	Mbed Tls	3.0.0	-	All	All
Application	Arm	Mbed Tls	3.0.0	preview1	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All

References

Reference	Source	Link	Tags
Release Mbed TLS 2.16.12 · ARMmbed/mbedtls · GitHub	CONFIRM	github.com	
Release Mbed TLS 3.1.0 · ARMmbed/mbedtls · GitHub	CONFIRM	github.com	
Release Mbed TLS 2.28.0 · ARMmbed/mbedtls · GitHub	CONFIRM	github.com	
Releases · ARMmbed/mbedtls · GitHub	MISC	github.com	
Potential double-free after an out of memory error - Tech Updates - Mbed TLS (Previously PolarSSL)	CONFIRM	tls.mbed.org	
829660 – (CVE-2021-44732) net-libs/mbedtls: multiple vulnerabilities	CONFIRM	bugs.gentoo.org	
[SECURITY] [DLA 3249-1] mbedtls security update	MLIST	lists.debian.org	
CVE Program record	CVE.ORG	www.cve.org	canor
NVD vulnerability detail	NVD	nvd.nist.gov	canor

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

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

184355 Debian Security Update for mbedtls (CVE-2021-44732)

500394 Alpine Linux Security Update for mbedtls

504152 Alpine Linux Security Update for mbedtls

690761 Free Berkeley Software Distribution (FreeBSD) Security Update for mbed Transport Layer Security (TLS) (c1b2b492-6999-11ec-a50c-001cc0382b2f)

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

904896 Common Base Linux Mariner (CBL-Mariner) Security Update for fluent-bit (12328)