arm

Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Janos Follath

2026-06-01

Recent community activity (thank you!)

- tls#10762 Nadav0077 - Backport to 3.6: harden serialized data deserialization
- tls#10761 Nadav0077 - Backport to 4.1: harden serialized data deserialization
- tls#10715 Nadav0077 - Harden TLS 1.3 serialized session loading
- tls#10765 Night-Traders-Dev - refactor: remove mbedtls third-party library from kernel build directory
- tls#10731 AmyChan-Intel - library/alignment.h: Fix 'MBEDTLS_GCC_VERSION' is not defined error
- tls#10758 wkhadgar - ssl: size _pms_ecdh against PSA_RAW_KEY_AGREEMENT_OUTPUT_MAX_SIZE
- tls#10646 rado17 - Add support for wildcard hostname checks
- merged: docs#204 DerDakon - CVE-2026-34872: unbreak summary table
- crypto#538 ruiliio - Add support for AES-XTS·
- merged: crypto#778 Nadav0077 - Fix ML-DSA signing error propagation
- crypto#793 dmitriy-bty - Forward error from mldsa87_signature_internal in sign_message

Recent community activity (thank you!)

Valerio @Nordic

- tls#10764 valeriosetti - Allow TF-PSA-Crypto path to be specified in CMake and Makefiles
- merged: tls#10741 valeriosetti - mbedtls_config.c missing mbedtls_platform_requirements.h
- merged: tls#10742 valeriosetti - [backport 4.1] mbedtls_config.c missing mbedtls_platform_requirements.h
- merged: crypto#785 valeriosetti - [backport 1.1] include tf_psa_crypto_platform_requirements.h in tf_psa_crypto_config.c
- merged: crypto#777 valeriosetti - include tf_psa_crypto_platform_requirements.h in tf_psa_crypto_config.c

Major activities within core team

https://github.com/orgs/Mbed-TLS/projects/18

- ML-DSA integration
  - Priority to bootloader/firmware use cases
- Bug bounty program
- Mbed TLS 4.2/TF-PSA-Crypto 1.2 preparations
  - Minor improvements for driver integration

Release Timeline

- 1.x/4.x development
- 1.1.x/4.1.x LTS supported until March 2029
  - 1.1.0/4.1.0 released on 2026-03-31
- 3.6 LTS supported until early 2027
  - 3.6.6 (2026-03-31): Security fixes and bugfixes

arm

Thank You
Danke
Gracias
Grazie
谢谢
ありがとう
Asante
Merci
감사합니다
धन्यवाद
Kiitos
شكرًا
ধন্যবাদ
תודה
ధన్యవాదములు