arm

Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Gilles Peskine

2024-05-06

Recent community activity (thank you!)

- Valerio Setti @Nordic
  - #9017 - Improve generate_test_keys.py
  - #9073 - Undefined reference to mbedtls_md_error_from_psa() function
  - #9090 - [Backport 3.6] Undefined reference to mbedtls_md_error_from_psa() function

- Misc
  - #9055 Kal42 - Add pragma for bcrypt.lib - Fix win build with cmake
  - #8983 Troy-Butler - Fix NULL argument handling in mbedtls_xxx_free() functions
  - #9045 Troy-Butler - [Backport 3.6] Fix NULL argument handling in mbedtls_xxx_free() functions
  - #9082 andre-rosa - Add invalid padding_len check in get_pkcs_padding
  - #8896 ascillato - Fix compilation when -Werror=maybe-uninitialized is enabled
  - #9085 nileshkale123 - Fixed issue of redefinition warning messages for _GNU_SOURCE
  - #9086 nileshkale123 - Fixed issue of redefinition warning messages for _GNU_SOURCE
  - #9026 nileshkale123 - Fixed redefination warning messages for _GNU_SOURCE
  - #8949 rojer - x509_crt: Add LWIP implementation of inet_pton

arm

Major activities within core team

https://github.com/orgs/Mbed-TLS/projects/1

- Mbed TLS 4.0
  - PSA_CRYPTO_C / CLIENT always on
  - Consume TF-PSA-Crypto repository as source of PSA and crypto code
  - Remove some legacy interfaces & features
- TF-PSA-Crypto
  - https://github.com/Mbed-TLS/TF-PSA-Crypto
  - Will become upstream source for crypto in Mbed TLS
  - Paused to focus on 3.6, resume in Q2
- CI
  - Testing on Arm coming soon

Release Timeline

- 4.0 currently aiming for first half of 2025
- 3.6 LTS supported until early 2027
- 2.28 LTS ends supported life end of 2024

arm

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