Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Janos Follath
2024-04-22
Recent community activity (thank you!)

Valerio Setti @Nordic

Misc
- #8983 Troy-Butler - Fix NULL argument handling in mbedtls_xxx_free() functions
- #9026 nileshkale123 - Fixed redefinition warning messages for __GNU_SOURCE
- #9001 raymo200915 - Add PKCS#7 parser features for integrating MbedTLS with U-Boot
- #8907 szsam - Backport 2.28: ssl_mail_client: Fix unbounded write of sprintf()
- #8897 szsam - ssl_mail_client: Fix unbounded write of sprintf()
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](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
Thank You  
Danke  
Gracias  
Grazie  
谢谢  
ありがとう  
Asante  
Merci  
감사합니다  
धन्यवाद  
Kiitos  
شكرًا  
ধন্যবাদ  
ناودה  
ధంశుడ్మడ