arm

TrustedFirmware TSC

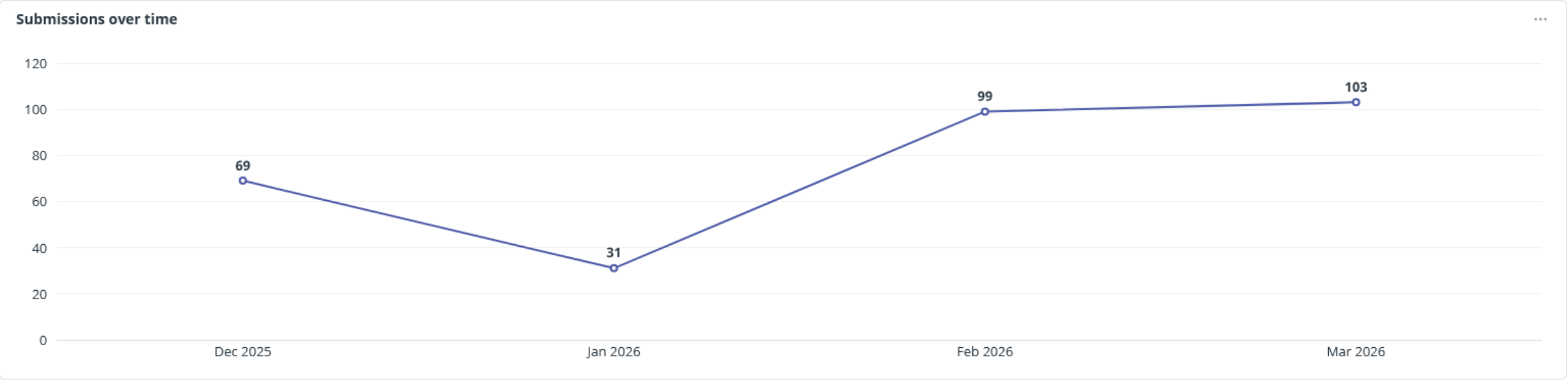
Dan Handley
2026-03-19

Platform Security Architecture (PSA) specification governance

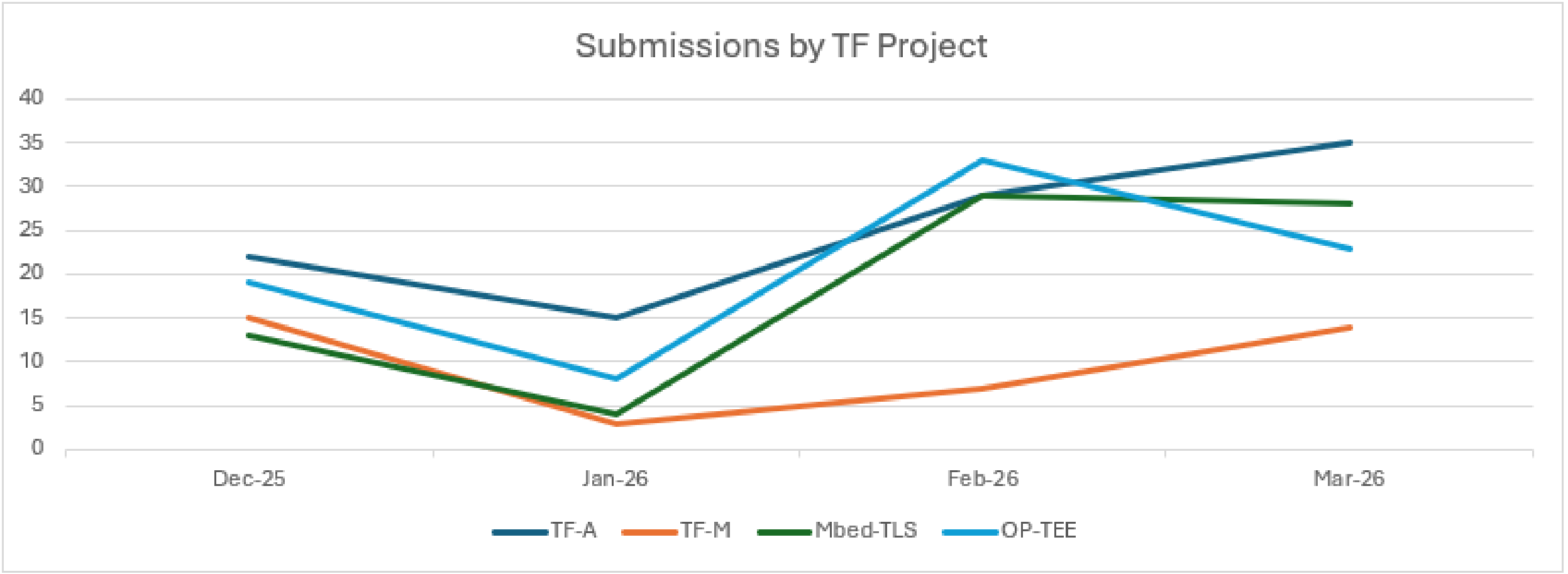
- PSA Certification scheme has already transitioned to Global Platform
  - https://newsroom.arm.com/blog/psa-certified-handover-globalplatform
- Also considering moving PSA API and FF-M specs to Global platform governance
- Specs are reasonably mature - want to sustain long term momentum with broader participation
- Propose that spec copyright/licensing remains unchanged and development continues in the open
- Arm remains committed to spec development – will nominate Arm WG leads
- No change to TF project implementations

Trusted Firmware bug bounty program

- Launched in Dec 2025
- Higher volume of reports than any of us expected
- 3 levels of triage – Intigrity, Arm PSIRT and TF security – about 10% accepted
- Program auto-suspended many times in Jan due to going over budget - see dip below
- Rules changed in Feb so that budget is only spent after vulnerability is confirmed instead of after submission - now the brakes are off
- Significant drag on the maintainers – current load not sustainable



Bug bounty submissions by project



TF CVE allocation

- With the increase in confirmed security vulnerabilities, need to request more CVEs
- Mitre becoming increasingly unresponsive (>1 month for a CVE to be allocated)
- Arm is a Certificate Numbering Authority (CNA) but TF projects are not in scope
- One option is for TF security teams to take the CNA training and absorb the admin cost
  - But already very stretched
- Have asked Linaro to look into options for providing a service, potentially spending some of the TF budget surplus

CoreCollective.dev

- Launched by Linaro in Feb 2026 with backing from Arm
- Free to join – just need to sign membership agreement
- Governance similar to TrustedFirmware but does not replace it any way

- Has a Confidential Compute Working Group (WG)
  - Not kicked off yet but expect it to in the next month or so
  - Dan Handley is joint lead
  - Linaro will assign a community manager
  - Can ”ask to join group” here (after signing membership agreement)
  - Scope TBC but likely to include:
    - Collaboration on Arm-owned CCA reference SW roadmap
    - Collaboration on activities from discontinued Linaro Deploy CCA on Arm Platforms (DCAP) project
  - Project-specific CCA firmware collaboration likely to continue in Trusted Firmware-A tech forum

arm

Tack
ಧನ್ಯವಾದಗಳು
Merci
Danke
Gracias
Grazie
谢谢
ありがとう
Asante
Thank you
감사합니다
धन्यवाद
Kiitos
شكرًا
ধন্যবাদ
תודה
ధన్యవాదములు
Köszönöm