arm

Trusted Firmware TSC

2025-09-18

Agenda

- Progressing the TF.org "Guidance on AI-assisted contributions"
  - Opportunity for maintainer feedback
- More info on the Arm proposed bug bounty program for TF.org
- Debrief on OSFC call regarding EU-CRA impacts on boot managers

TF.org "Guidance on AI-assisted contributions"

- TF.org board had a vote to approve proceeding with creating such guidance
- Policy proposed at TF.org board based on Linux Foundation and Apache Software Foundation guidance
- Previously discussed at board and TSC (last minutes here)
- Eric Finco @ ST had feedback
  - Would like all contributions that use AI assistants to explicitly attribute the tool(s) used in the contribution for transparency reasons
  - Would like the policy to apply to all TrustedFirmware.org projects, rather allowing projects to develop their own project-specific guidance
- Some pushback from others on these modifications
- Dan sent this to representative list of maintainers for wider feedback
  - Some further pushback received
- How do we proceed?

Arm proposed bug bounty program for TF.org

- Arm already has a bug bounty program based on Intigriti platform
  - Current scope is:
    - Arm GPU Firmware using Command Stream Frontend (CSF) – Tier2
    - Arm Mali GPU Kernel Driver (Kbase) – Tier 3
  - Bounty values depend on Tier and Severity

- Arm PSIRT propose extending this to cover TF.org projects
- Bounty values TBD
- Project requirements:
  - Must have a valid threat model
  - TF.org security incident handling process must be active for that project

- Currently qualifying projects: TF-A, TF-M, OP-TEE, Mbed TLS

Proposed bug bounty scope

- In scope vulnerabilities must…
  - … be reproducible by Arm using either main branch or a currently supported LTS branch
  - … exist in code intended for production deployment
  - … have a Proof of Concept demonstrating the issue is exploitable with a meaningful security impact

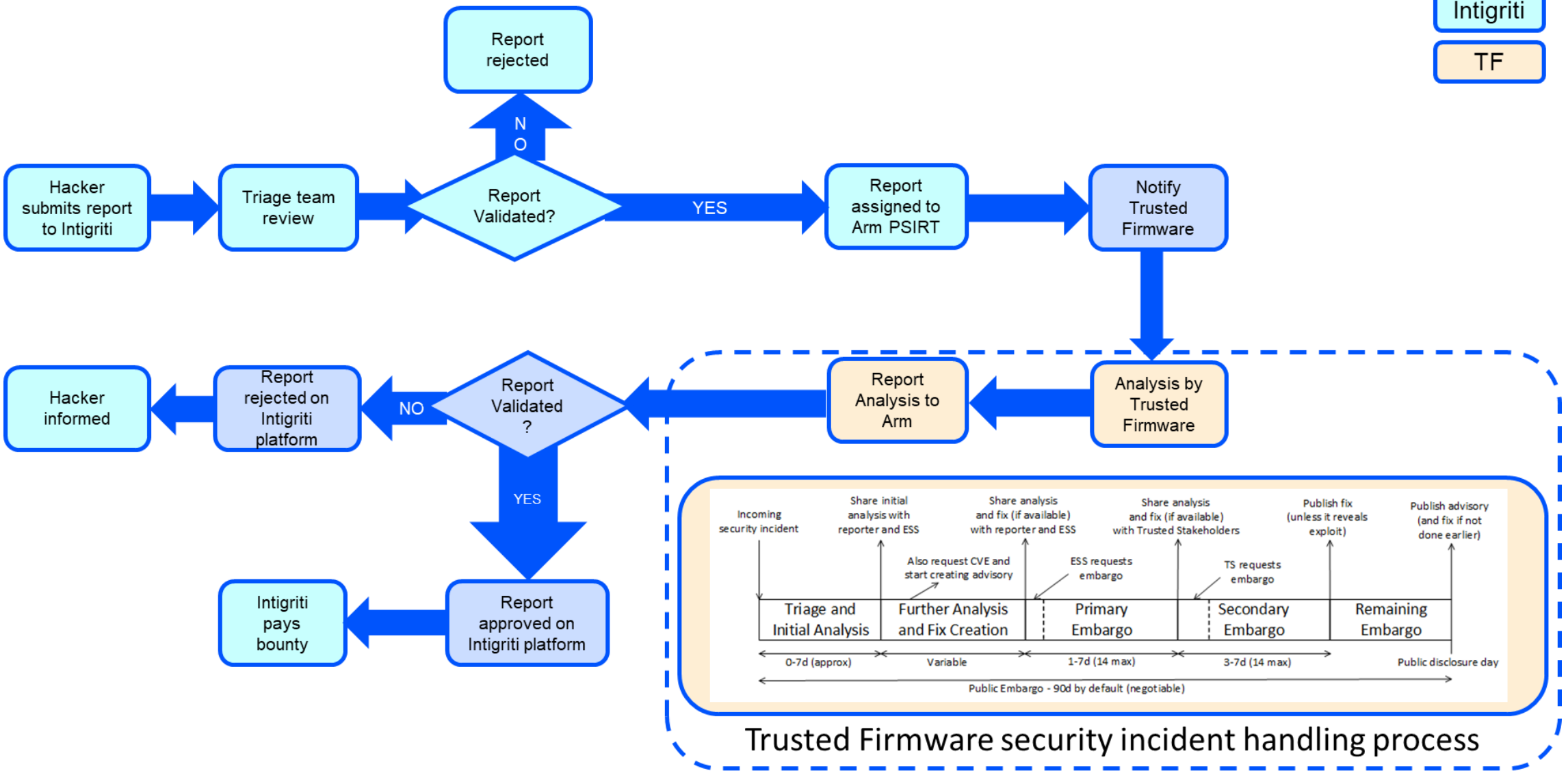
- Out of scope
  - Vulnerabilities in Trusted Firmware's web estate
  - Vulnerabilities identified in test code or other non-production code e.g. support tooling
  - Vulnerabilities in platform-specific code for non-Arm products

General policy info (inherited from existing program)

- Other restrictions
  - Researchers must be at least 18 years old
  - Researchers must not be a resident of, or submit issues from, a country the US, UK or EU has embargoed, or be employed by or affiliated with an embargoed entity
  - Employees of Trusted Firmware members and relatives of employees of Trusted Firmware members are not eligible for bounty rewards from the program
  - Employees of Trusted Firmware members should report suspected vulnerabilities directly to the Trusted Firmware security aliases
- Rules of engagement
  - Must respect the Intigrity Community Code of Conduct and Terms and Conditions
  - Must respect the TF.org Code of Conduct
- Safe harbor for ethical hacking activities of researchers is provided

Intigriti / Arm / TF Process Flow

Key: Arm | Intigriti | TF



Debrief on OSFC call regarding EU-CRA impacts on boot managers

- …

arm

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