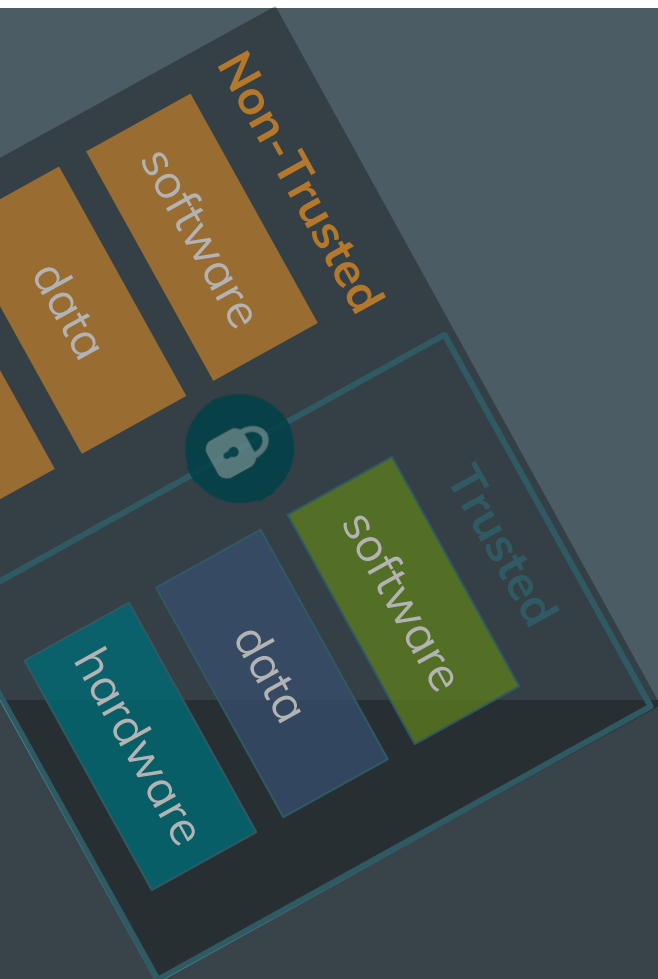




Open Source Secure World Software



SPONSORED BY:

arm

HOSTED BY:

Linaro

Overview

- Broadly based on the [kernel process](#)
 - With influence from [TF-A](#) and [OP-TEE](#) processes
 - Contrast is that this process combines vulnerability fixing and disclosure
 - kernel process only does former, leaving [distros](#) process to handle disclosure
- 2 stage disclosure process for vulnerability fixes
 - 1st stage for Especially Sensitive Stakeholders (ESSes)
 - 2nd stage for other Trusted Stakeholders
 - At each stage stakeholders can request up to 14 days embargo
 - Fix is then made public (without disclosure details)
- Disclosure details are made public as an advisory 90 days after initial report
- Single entry point security@trustedfirmwrae.com for all TF projects

ESSEs and Trusted Stakeholders

- Disclosure lists vetted and maintained by TF security team
 - Expect each TF project to have its own security team and lists
- ESSEs strictly limited to orgs with large scale, multi-tenancy deployments
 - Only relevant for TF-A currently
- Expect most organizations requiring early disclosure to be Trusted Stakeholders
- During fix embargo period, stakeholders must only share info with individuals in their organization that need it
- Propose that Arm sends a mail to all existing TF-A stakeholders to invite them to register for the new process

Disclosure details

- Prefer to release fixes ASAP
- Will only be embargoed if reporter, ESS or Trusted Stakeholder requests it
 - Within 1 calendar day for ESSes
 - Within 1 working day for Trusted Stakeholders
- Maximum vulnerability fix embargo time is 28 days (14 days at each stage)
- Disclosure times may be extended in exceptional circumstances
 - e.g. to handle Spectre/Meltdown case

Other

- Will request and use CVEs in advisories
- Reporters can optionally use PGP/GPG for communication with security team
 - Don't intend to keep communication encrypted during internal handling and disclosure
- No severity scoring in this process



Thank You

Visit www.TrustedFirmware.org or email
enquiries@TrustedFirmware.org for more information