The KDE Security Team

What is it?

- An email alias security@kde.org
- We handle security issues in software created by KDE
- **WE DO NOT** handle security issues in software used by KDE, for that you want sysadmin@kde.org (e.g: If there's some vulnerability in gitlab, wordpress, etc.)

Who are we?

- A group of people (9+Adam) with quite some KDE history *
  - It’s important that there’s trust in us since we handle things that could be potentially used maliciously
  - „People with quite some history“ are usually super busy, maybe we should try to add some new folks

[*] 3 people whose account creation date is lost in history, the rest not older than 2010

What do we do?

- Mostly reactive (due to lack of people/time)
- Oss-fuzz
  - kimageformats
  - kcodecs
  - karchive

How do we work?

- Someone sends a potential vulnerability
- Answer very quickly with a „Thanks we'll look into it“
- Check if it has any merit or not
- Potentially contact with someone external to the team to get the issue fixed
- Get a CVE
- Publish an advisory (potential a heads-up to distributors)

How can you help?

- There’s more things to add to oss-fuzz
  - kfilemetadata
  - baloo
  - kmime
  - etc.
- Audit Kauth uses
- Experiment rewriting some stuff in „safe“ languages

Thanks!

Questions?