Yocto Project Security

Discussion 26th September 2023

Context

- Yocto Project RFQ https://www.yoctoproject.org/community/yocto-project-engineering-request-for-quotation/
- Two axes
  - **Processes** (will discuss today)
  - SPDX 3.0 POC (another discussion pending)

What are the goals of the RFQ (Marta’s understanding)

- Identify and define security processes
- Document and implement them
- Provide training (developers, maintainers etc)

What happened so far?

- Direct discussions with people (Richard, Ross, Steve S, Khem, Joshua, Mark H)
- Email discussion thread https://lists.yoctoproject.org/g/yocto/message/60983
- Tooling testing
  - SRTool (still working)
  - Manual fetch of CVE v5 JSON data

Directions

- Synchronization of the CVE work
- Security team and private reporting
- Complete CVE reports (SRTool et al)
- Development initiatives (eg. static analysis)
- Documentation & training
- Visibility

Direction: Synchronization of the CVE work

- Regular CVE check reports
- Fixes submitted to the ML
- Who works on what?
- Proposal: https://wiki.yoctoproject.org/wiki/Synchronization_CVEs

Direction: Security team and private reporting

- Need a place to get private (not published yet) reports
- Ready for multi-distro embargoes (in the future)
- Proposal: https://wiki.yoctoproject.org/wiki/Security_private_reporting

Direction: Complete CVE reports

- Outcome: a file/web page with a list of all CVEs and information if YP is affected
- Various technical solutions
  - SRTool
  - New custom tooling
- Challenges
  - Requires work to fill
  - Requires time to maintain (every day, every week)
- Proposal: do a test and estimate what would be needed

Rough stats: ~1100 CVEs per week (most not-YP related)

Direction: Development initiatives

- Enable collaboration to work on features
  - Static analysis
  - Code signing
  - Hardening…
- Proposal: ML? Ask for initiatives?

Documentation and Training

- Identified targets
  - Submitting CVE fixes for security researchers and/or non-YP developers
- Related to new processes
  - How to handle a private report?
  - How to make a private report?
  - How to synchronize CVE work?
  - …

Visibility

- Documentation will be one step
  - A new Security page with links? A category?
- Process outcome(s)
  - SECURITY.md file
  - Security advisories
  - Release notes rework
- Talks/presentations at events
  - What would you like to see at YP DevDays 2023.11?

Summary and wrapping up

- Many ideas
  - Engagement needed if we implement them
  - .. but the workload is not equal
- This is work in progress
  - Patches welcome!
- Workflow proposal
  - Write on the wiki, announce on the ML
  - Move to YP documentation when a process is ready