Yocto Project Security - Now and the Future

Marta Rybczynska, Syslinbit
marta.rybczynska@syslinbit.com

Yocto Project Summit, 2023.11

Who is Marta?

- **PhD** in Telecommunications (Network Security)
- **20+ years in Open Source**, former Vice-President & Treasurer of KDE e.V., guest author at LWN.net
- Currently focusing on **Open Source Supply chain**
- Founder of **Syslinbit**, a OSS-focus company offering development and training, including **embedded security**
- YP contributions: JSON output of the cve-check, NVD API2 format fetcher, and more

State of early 2023

What you might know

Security-focus features (1)

- **Compiler hardening options**

```
openembedded-core/meta/conf/distro/include/security_flags.inc
```

- **“cve-check” to be enabled in your local.conf**

```
INHERIT += “cve-check”
```

  - Based on package version name
  - Support for patches applied in YP if they follow a naming scheme (see a presentation earlier today)

Security-focus features (2)

- **CVE handling and LTS workflow**
  - Backporting security fixes to older branches (dunfell, kirkstone)
- **Security-focus layers**
  - In `meta-security`
- **YP layer-compatible program**
  - Enforcing various best practices with security impact

Security-focus features (3)

- Documentation
  - **Making Images More Secure**
    https://docs.yoctoproject.org/dev-manual/securing-images.html
  - **What I wish I'd known about Yocto Project**
    https://docs.yoctoproject.org/what-i-wish-id-known.html

Weaknesses

- **Frequent use of “debug-tweaks”**
  - Root login without password
  - Should be testing only, but…
- **Defaults in poky could be different**
- **Lack of formal security processes**

State of late 2023

What you might have heard about

New funding from the Sovereign Tech Fund will help the Yocto Project drive significant transformation

The Yocto Project is a powerful and versatile open source initiative that offers a comprehensive set of tools and metadata, enabling developers to easily construct custom operating systems. With recently announced financial support from the Sovereign Tech Fund (STF), Yocto Project will drive significant transformation in the open source community. nstead of relying on pre-compiled binaries, the Yocto Project allows for creating tailored Linux images easily targeted to a specific device's hardware architecture. This flexibility makes it an invaluable resource for a wide range of applications, from embedded systems to Internet of Things (IoT) devices.

"Without fanfare, Yocto Project touches most people's lives without their knowledge," notes Richard Purdie, lead Architect at Yocto Project. "At least half the world's internet traffic passes through routers built using Yocto. Add in mobile phone masts, software in cars, software inside core server components, and there are billions of devices all around us that are relied upon every day, making it a key piece of easily overlooked critical infrastructure software."

The Significance of the Yocto Project and openembedded

While the Yocto Project may not be visible to end-users, its importance is undeniable. It is the foundational software infrastructure for numerous industries, including automotive, medical technology, consumer electronics, and telecommunications. Companies like BMW Group, OpenBMC, and many operating system vendors depend on the Yocto Project to build their products. This underscores its critical role in developing connected cars, servers, communication base stations, and more.

From: https://www.yoctoproject.org/blog/2023/10/10/sovereign-tech-fund-boosts-yocto-project/

Meet the Yocto Project Security Team

- **Team to handle potential security reports**
  - Issue reporting either to one of:
    - https://bugzilla.yoctoproject.org/enter_bug.cgi?product=Security
    - security AT yoctoproject DOT org
  - All fixes go through the usual review process
- **SECURITY.md in a layer is now recommended**
  - Redirecting to the YP security team, or the layer team
- **Process documentation:**
  https://docs.yoctoproject.org/dev/dev-manual/security-subjects.html

Unknown vulnerability handling in a nutshell

- **Security team receives the issue**
- **Option 1: Core issue upstream**
  - (Private) Communicate with the affected upstream
  - (Public) Backport the fix when ready
- **Option 2: Core issue in YP**
  - (Private) Find people to prepare the fix
  - (Private) Communicate with the reporter
  - (Private) First testing of the fix
  - (Public) Fix submission and backports as usual

YP Security documentation

- Vulnerability reporting
  - https://docs.yoctoproject.org/dev-manual/security-subjects.html
- CVE fixes
  - https://docs.yoctoproject.org/dev/dev-manual/vulnerabilities.html#fixing-vulnerabilities-in-recipes
- More coming

Various initiatives - WORK IN PROGRESS

- **Proposal:**
  - Discuss at **yocto-security@lists.yoctoproject.org**
- **Choosen threads from MLs:**
  - [PATCH v2] cve-check.bbclass: support embedded SW components with different version number
  - Need comments or plan on User- group guidelines

CVE work synchronization - WORK IN PROGRESS

- **Observation:**
  - Two persons (or team) working on the same fix without knowing about each other
  - Waste of everyone's time
- **Proposal:**
  - Use a single synchronization point
    - Who is working on which one
    - Share information (eg. upstream fix not ready yet)
  - See https://wiki.yoctoproject.org/wiki/Synchronization_CVEs

“Is YP affected by…” - WORK IN PROGRESS

- **Observation:**
  - cve-check gives information on issues affecting/not affecting YP
  - What about all other CVEs? ~1100/week
- **Proposal:**
  - SRTool update by David Reyna & team
    - See another presentation
  - Discussion calls open to join (ask Marta or David)

SPDX3 - WORK IN PROGRESS

- **New SPDX version in the works:**
  - Better handling of composition
  - Modular
- **PoC work:**
  - Available https://git.yoctoproject.org/poky-contrib/log/?h=mrybczyn/spdx3
  - SPDX3 not published yet, still changing
  - Discussions including Joshua W et al in progress (contact us if interested)

What can happen next?

What WE want to do next

NVD feed update - December 15th, 2023

- **NVD data feed**
  - Used by cve-check
  - Old version goes down (replaced by API 2.0)
- **If you're up to date with YP**
  - Up-to-date: master or LTS
  - Nothing to do!
- **If on old version**
  - cve-check will stop working!
- **See https://nvd.nist.gov/General/News/change-timeline**

What will happen next?

- It depends on YOU

Interested by/benefiting from an existing initiative?

- **Convince your company to join:**
  - Development time
  - Expert time (CVE triage etc)
- **Contribute individually**

Before you will be forced to…

- Legislation is coming (CRA and others)
- Embedded Linux security has a bad opinion

The European Cyber Resilience Act

September 19, 2023
This article was contributed by Marta Rybczyńska

The security of digital products has become a topic of regulation in recent years. Currently, the European Union is moving forward with another new law, which, if it comes into effect in a form close to the current draft, will affect software developers worldwide. This new proposal, called the "Cyber Resilience Act" (CRA), brings mandatory security requirements on all digital products, both software and hardware, that are available in Europe. While it aims at a worthy goal, the proposal is causing a stir among open-source communities.

There is a reason why the open-source world has concerns: the legislation indirectly defines who is responsible for the security of open source and who should pay to improve the current state. In addition, it puts the responsibility on individual developers and foundations hosting open-source projects instead of the manufacturers of goods embedding the software. It could have important consequences for open source across the globe.

LWN.net: https://lwn.net/Articles/944300/

Yocto Project Security - Now and the Future

Marta Rybczynska, Syslinbit
marta.rybczynska@syslinbit.com

Yocto Project Summit, 2023.11

yocto PROJECT | THE LINUX FOUNDATION