Security updates in styhead

And beyond

Marta Rybczynska

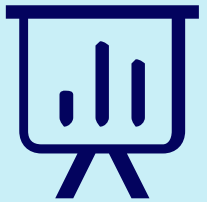
What has changed in the world around us

- Regulations
  - The Cyber Resilience Act has been published
  - Three years to make your products compatible
- Attacks
  - Even more attacks on embedded
  - More requests for security features
- Events
  - The NVD (National Vulnerability Database) crisis and its aftermath

Technical features

- Cve-check rework
  - Vex-style output
  - External tooling (including multiple vulnerability databases)
- Default configuration
  - The effort to harden default YP configurations continues
- SPDX changes and SPDX3
  - SPDX2 still available, SPDX3 by default
- SECURITY.md
  - Informing security researchers how to report vulnerabilities

YGREKY



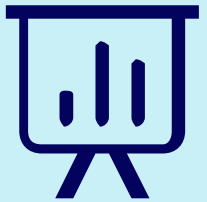
Breaking news: Poky is not for production!

Poky’s motd

```
$ cat
meta-poky/recipes-core/base-files/files/poky/motd
WARNING: Poky is a reference Yocto Project
distribution that should be used for
testing and development purposes only. It is
recommended that you create your
own distribution for production use.

(from meta-yocto
2e0cec1e9d97f78ba015da8812fd1888c47debcb
in February 2024)
```

YGREKY



Cve-check changes

Cve-check changes

YGREKY

- **Removal of the text output format**
- **CPE tagging**
- **External tooling for CVE checking**

Cve-check Text mode removal

YGREKY

- Why
  - Hard to parse
  - Duplication of functionalities and code
- If you still use it
  - scripts/cve-json-to-text.py -i <cve-summary.json> -o my-summary.txt
- But really…
  - Migrate to the JSON format

CVE_STATUS tagging

YGREKY

- Problem
  - The vex requires sometimes changes in the CVE classification
    - Also needed with multiple databases
  - CVE_STATUS had no way to specify which package it applies to
    - If you have a general include, the CVE will show up for ALL package
    - And… we have cve-extra-exclusions.inc
- Solution
  - CPE tagging of CVE_STATUS entries
  - Format: “cause: cpe: vendor: product: description”
  - The “cpe:vendor:product” part is optional

CVE_STATUS[CVE-2000-0006] = "upstream-wontfix: cpe:*:strace: CVE is more than 20 years old \
with no resolution evident. Broken links in CVE database references make resolution impractical."

CVE_STATUS tagging: future use

YGREKY

- Per-product assessments
  - You can create an ‘include’ with specific vulnerability assessments
    - Not vulnerable because we disabled a configuration option
    - Not vulnerable because we do not use this part of the code
    - …
- Will probably require other tooling
  - From and to other formats

External tooling for CVE checking

- Why
  - How to check CVEs years after the first build ?
  - Do you REALLY keep all release builds?
    - You should keep all release packages, however
  - We do not need the complete build to do a CVE check… “just” the package list

External tooling for CVE checking

YGREKY

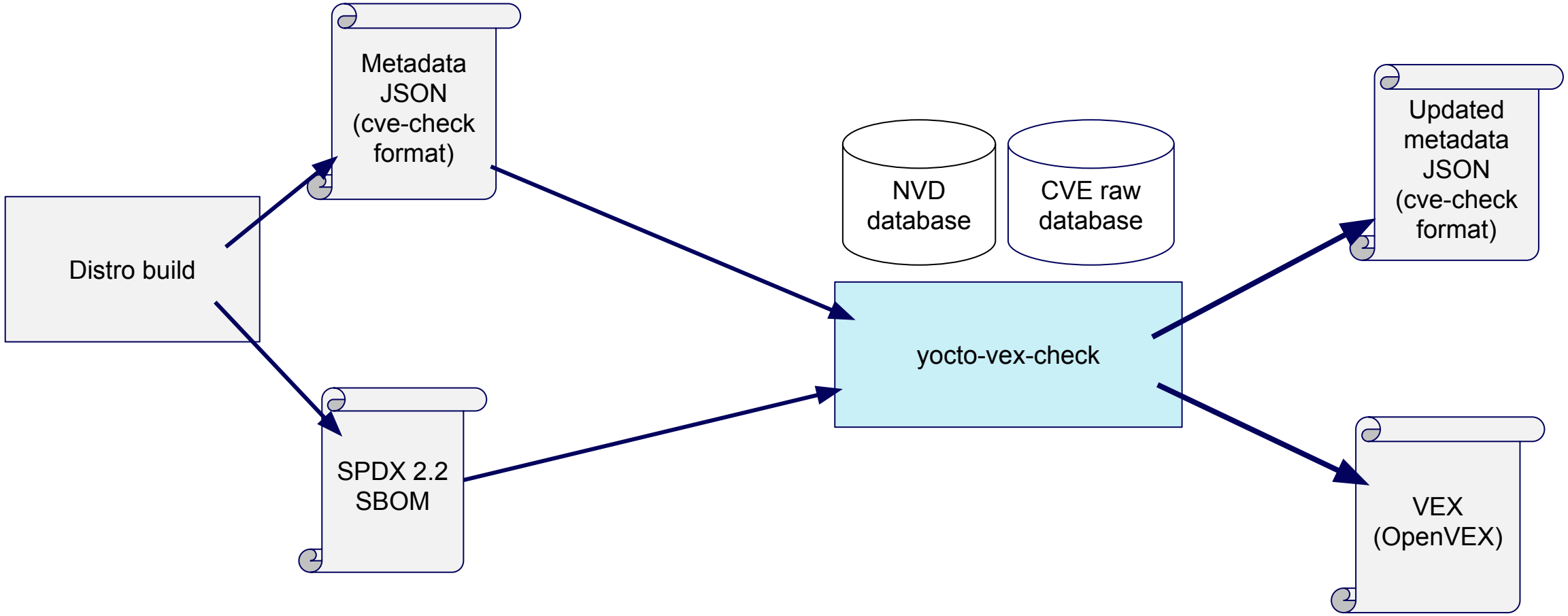
- Why
  - How to check CVEs years after the first build ?
  - Do you REALLY keep all release builds?
    - You should keep all release packages, however
  - We do not need the complete build to do a CVE check… “just” the package list
- Difficulties on the road
  - SPDX(2.2) does not contain all data needed
  - VEX formats neither
  - NVD crisis and a need for an alternative database
  - What we need to keep: ignores and overrides, patch file list with their CVEs

External tooling for CVE checking

- Current solution
  - Vex.bbclass with files using augmented cve-check format
  - Yocto-vex-check processing using NVD or raw CVE database
    - https://gitlab.com/syslinbit/public/yocto-vex-check
  - Overrides in a separate repository
    - Currently: https://github.com/mrybczyn/cvelistV5-overrides

External tooling for CVE checking: yocto-vex-check

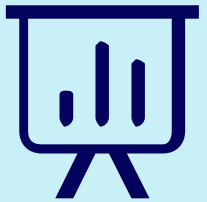
YGREKY



What does it mean?

- You can save all data needed for cve-check from a build
- You can cve-check the same status with 2 databases
  - NVD and raw CVE
  - Solution is modular, possible to add more
  - External hosting for now
  - The plan is to move them to YP repositories

YGREKY



Future directions

(Marta’s opinion,
Not an official YP plan)

Solve the NVD situation (URGENT)

YGREKY

- Use an alternative feed
  - PoC kind-of-working
- Long term: the external tooling will help
  - Database download is a separate process

Committed work

- Cve-check & VEX & friends
  - Move of yocto-vex-check to the YP infrastructure
    - Work on overrides to finish first
- Document styhead changes
  - Docs are heavily out-of-date, sadly
- Secure defaults
  - (DONE) “debug-tweaks” gone
    - Misleading option name
  - Rework the “hardening” distribution from meta-security
    - As a DISTRO_FEATURE
    - Production-level security options including permissions

More ideas: vulnerabilities

YGREKY

- Merge results from multiple databases
  - Automatically merge NVD and CVE results
  - Note: NVD has ~20k entries backlog
  - Use different databases for different packages?
- Additional databases
  - OSV support
- VEX encoding of metadata
  - Stacking of VEXes
  - Discussions with VEX people needed
- Vex integration with SPDX3
  - In external tooling and data post processing
  - SPDX3 has a _different_ VEX format ;(
- Integration and validation with other tools
  - Simulate composition YP + host + RTOS + ...
- Better synchronization on backporting fixes

More ideas: secure defaults

- Running services as separate users
  - Automatic and easy-to use (a single include)
- Best practices blueprints
  - Secure boot
  - System update
  - Alternatives to “debug-tweaks”: SSH key enrollment etc
- Secure-by-default options
  - Review configuration for secure-by-default options

Questions?