YGREKY

Distribution Builders Meet VEX

Marta Rybczynska

Who am I?

YGREKY

- PhD in Telecommunications
  - On anonymity systems
- 20+ years in open source
  - Contributions to the Linux kernel, Yocto Project, various other projects
  - Security team member of Eclipse Foundation and the Yocto Project
- Strong security focus
  - Security processes
  - Tooling (Yocto Project's cve-check)
  - Those days also: subject around the CRA implementation
- Founder of Ygreky, an open source security company

ALL OPINIONS HERE ARE MY OWN

What is Yocto Project?

YGREKY

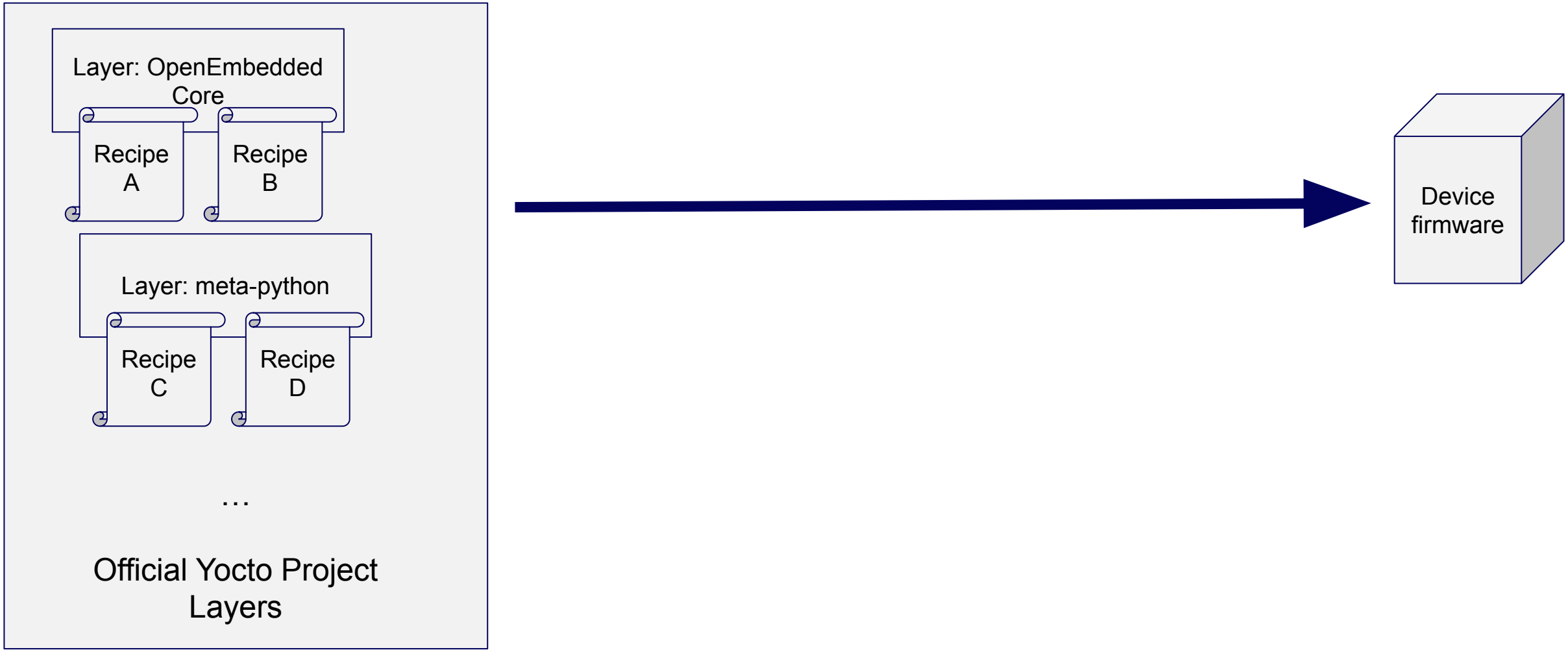
- A (Linux) distribution creation framework
  - Mostly used in embedded systems
  - Easy to extend and modify by hardware vendors
  - The “de-facto” standard for building custom Linux distributions
- Open source
  - A mix of licences, mostly MIT & GPL 2.0
  - A Linux Foundation project
- Usage
  - Automotive, set top boxes, robotics, routers, home appliances…
  - You (very likely) own devices with firmware built using the Yocto Project

Recipes and layers

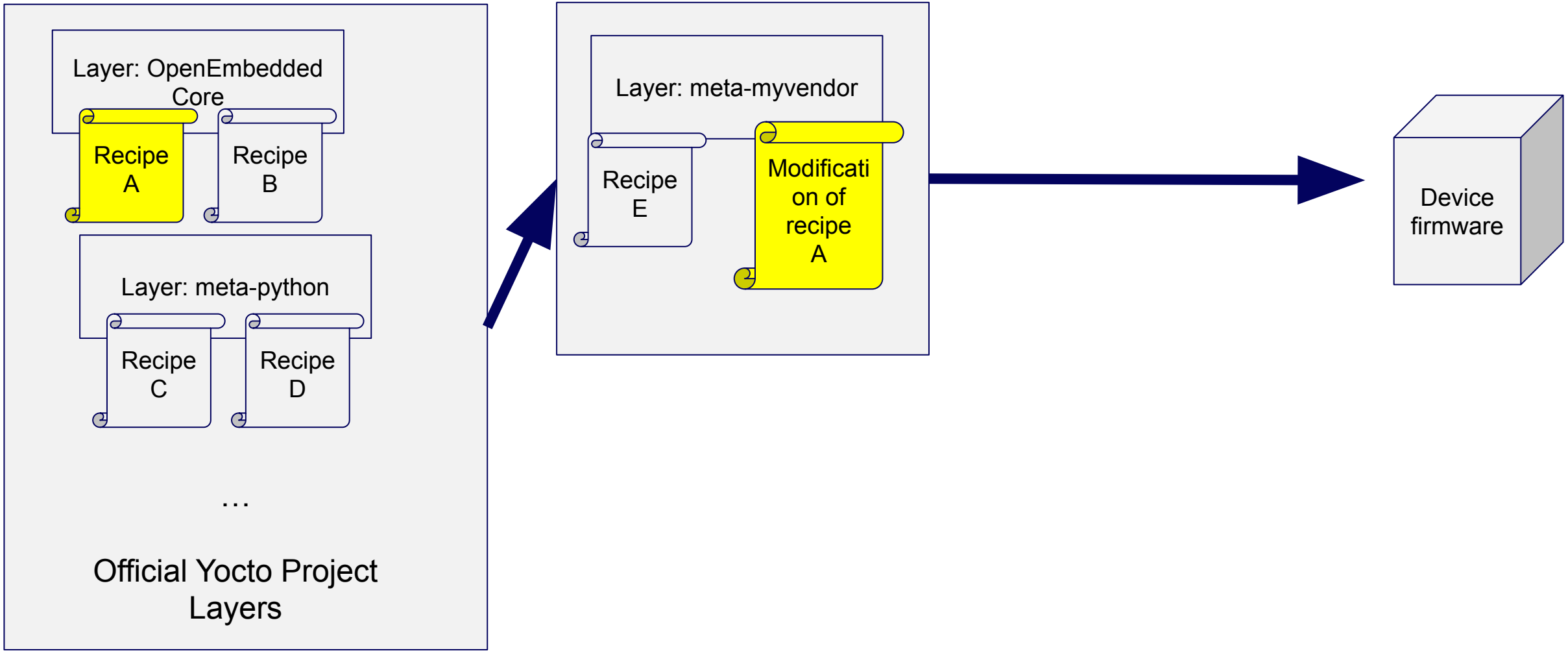
YGREKY

- A recipe
  - Instructions to build one software package
  - Points to source code
  - Runs the package's native build system
  - All technologies supported: from assembly and C, to Java, Go, Rust and Python
- A layer (meta-*)
  - A collection of recipes with a common purpose
  - Examples:
    - A layer to support specific hardware
    - A layer around a specific functionality, eg. meta-security

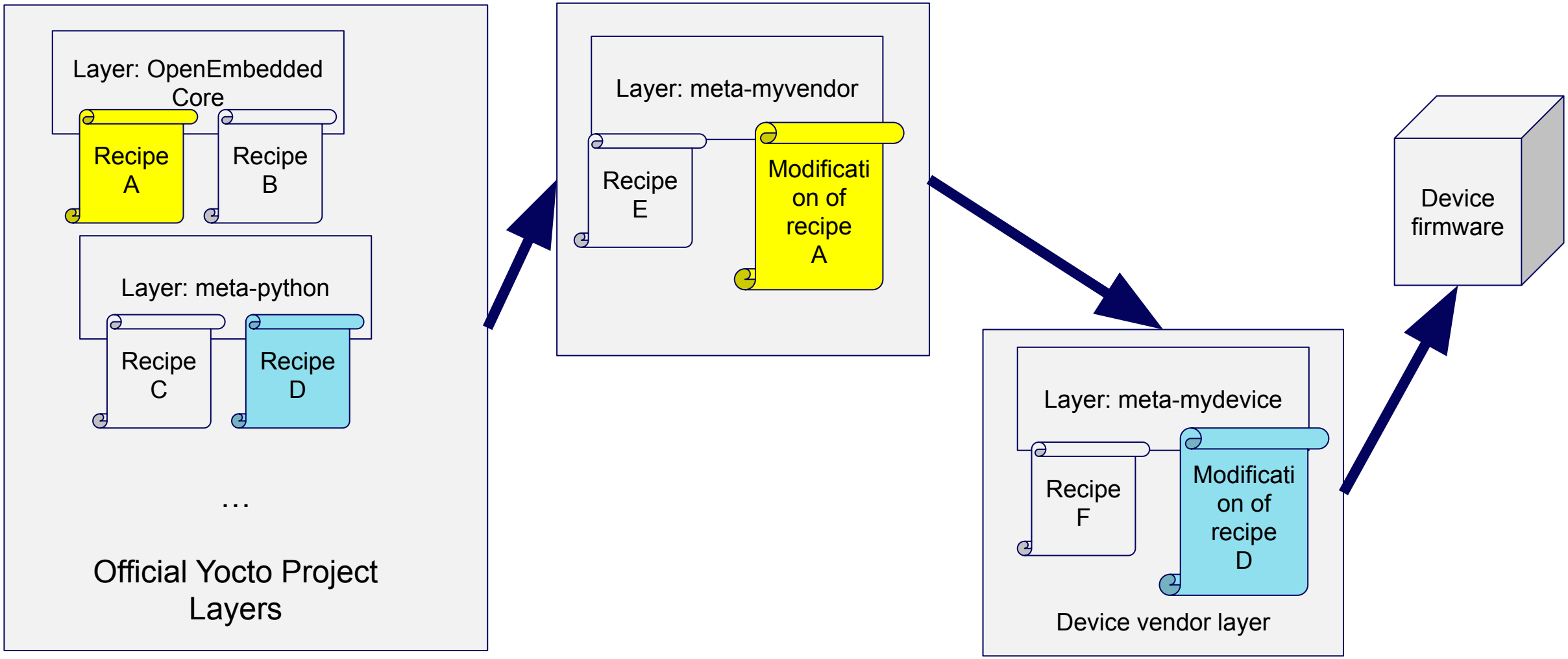
Yocto Project ecosystem example



Yocto Project ecosystem example



Yocto Project ecosystem example



Where are vulnerabilities in all that?

- We do a final image scan for known CVEs!

What is cve-check?

- Yocto Project tool for checking for known vulnerabilities
- Features
  - Fast (2-3 min overhead of a complete build)
  - Uses metadata from recipes (versions, machine-readable package name...)
  - Has an option of overrides (CVE_STATUS/CVE_IGNOREs)
  - Supports patches fixing CVEs (if tagged)
- Limitations
  - Uses package versions only, no tests if vulnerability is present
  - No support of embedded code (either copied, or using package managers)
  - Uses only the NVD database (as of early 2025)
- To learn more
  - OE Workshop 2023 talk “cve-check: all you wanted to know” https://www.youtube.com/watch?v=32UYr0K2PR0

A recipe with vulnerability fixes

```
SUMMARY = "GRUB2 is the next-generation GRand Unified Bootloader"

DESCRIPTION = "GRUB2 is the next generaion of a GPLed bootloader \
intended to unify bootloading across x86 operating systems. In \
addition to loading the Linux kernel, it implements the Multiboot \
standard, which allows for flexible loading of multiple boot images."

HOMEPAGE = "http://www.gnu.org/software/grub/"
SECTION = "bootloaders"

LICENSE = "GPL-3.0-only"
LIC_FILES_CHKSUM = "file://COPYING;md5=d32239bcb673463ab874e80d47fae504"

CVE_PRODUCT = "grub2"

SRC_URI = "${GNU_MIRROR}/grub/grub-${PV}.tar.gz \
           file://autogen.sh-exclude-pc.patch \
           file://grub-module-explicitly-keeps-symbole-.module_license.patch \
           file://0001-grub.d-10_linux.in-add-oe-s-kernel-name.patch \
           file://0001-RISC-V-Restore-the-typcast-to-long.patch \
           file://0001-misc-Implement-grub_strlcpy.patch \
           file://CVE-2024-45781.patch \
           file://CVE-2024-45782_CVE-2024-56737.patch \
           file://CVE-2024-45780.patch \
           file://CVE-2024-45783.patch \
           file://CVE-2025-0624.patch \
           file://CVE-2024-45774.patch \
           file://CVE-2024-45775.patch \
           file://CVE-2025-0622-01.patch \
           file://CVE-2025-0622-02.patch \
           file://CVE-2025-0622-03.patch \
           file://CVE-2024-45776.patch \
           file://CVE-2024-45777.patch \
           file://CVE-2025-0690.patch \
           file://CVE-2025-1118.patch \
           file://CVE-2024-45778_CVE-2024-45779.patch \
           file://CVE-2025-0677_CVE-2025-0684_CVE-2025-0685_CVE-2025-0686_CVE-2025-0689.patch \
           file://CVE-2025-0678_CVE-2025-1125.patch \
"
```

YGREKY

The official YP grub2 recipe https://git.openembedded.org/openembedded-core/tree/meta/recipes-bsp/grub/grub2.inc

hash 1fe39a59d2d9dc6909ba88bfceaf6fd4222c13d2

For grub2 version 2.12

Status “overrides” examples

YGREKY

- CVE_STATUS[CVE-2019-14586] = "fixed-version: The CPE in the NVD database doesn't reflect correctly the vulnerable versions."
- CVE_STATUS[CVE-2022-26488] = “not-applicable-platform: Issue only applies on Windows”
- CVE_STATUS[CVE-2021-25317] = "not-applicable-config: This concerns /var/log/cups having lp ownership, our /var/log/cups is root:root, so this doesn't apply."

This looks like VEX, doesn’t it?

YGREKY

- We need it automated: a typical embedded device build is 200+ packages
- Manual touch possible, but for a (very) small number of entries

When we tried to output VEX… (1)

YGREKY

- Many entries can be generated
- But some do not fit neither SPDX nor VEX
  - Would need specific, non-standard extensions, at least
  - No VEX expression (various formats) for:
    - “The entry is wrong, waiting for the NVD update”
    - “Disputed”
    - “Abandoned project, there will be no fix”

When we tried to output VEX... (2)

YGREKY

- Need at least two levels of assessments
  - Generic, always true
    - Could move to CVE enrichment?
  - Depending on product, build etc
    - “Typical” VEX

When we tried to output VEX... (3)

YGREKY

- Interesting open problems - VEX statements changed by further layers
  - Layers may add patches
  - Layers may change configuration options

Current status and open questions

- We generate VEX today
  - Not in the mainline YP yet
  - Based on OpenVEX, but with additional statuses
  - Part of software doing cve-check outside of the build
  - The code is here: https://gitlab.com/ygreky/public/yocto-vex-check
- Looking for more standard solutions
  - Embedded vendors often use multiple tools (operating systems) in one project
  - Will likely need to merge VEX records from various tools

Questions?

Contact: Marta Rybczynska
marta.rybczynska@ygreky.com
LinkedIn:
https://www.linkedin.com/in/mrybczynska/