Last year at FOSDEM...

4. Forgotten dependencies

5 errors when building embedded systems
View the talk:
https://archive.fosdem.org/2023/schedule/event/5_errors_when_building/
Who’s Marta?

- Security Researcher by education
- Open Source user and developer since before 2000
  - Linux kernel, Yocto Project, KDE...
- Consultant in OSS security
- Trainer, public speaker, author
Who’s Marta?

- Security Researcher by education
- Open Source user and developer since before 2000
  - Linux kernel, Yocto Project, KDE...
- Consultant in OSS security
- Trainer, public speaker, author

Disclaimer 1: I have been involved in some things described
Disclaimer 2: This talk reflects my personal opinions only
Agenda

• Regulations
• Trends
• Events, vulnerabilities, incidents
• What to expect in 2024
Agenda

- Regulations – actually... one regulation
- Trends
- Events, vulnerabilities, incidents
- What to expect in 2024
Cyber Resilience Act – The basics simplified x100

- **Mandatory requirements** for all software products via the CE mark
  - Examples: no release with known vulnerabilities; secure configuration by default; updates provided during the support period of >=5 years (some exception possible), SBOMs
- In the final version applies to final products integrating OSS
- Will require **paperwork** (risk analysis, vulnerability management process)
  - Details of the actual standards/processes will be defined later
- Self-assessment by default
  - But some products with heavier requirements including an external audit
- Expected vote March 2024, then 3 years until implementation
Cyber Resilience Act – The integration question

- Current version excludes non-monetized OSS products
- But not their integration...
  - Risk analysis for all included components
  - *Will we do the paperwork* in an Open Source way?
Cyber Resilience Act – To know more

- LWN article about the first draft: https://lwn.net/Articles/944300/

Agenda

• Regulations
• Trends
• Events, vulnerabilities, incidents
• What to expect in 2024
Number of CVEs assigned

CVE = Common Vulnerability Enumeration
Data source : https://www.cve.org/About/Metrics
01 External funds
OpenSSF Alpha-Omega (eg. OpenSSL, Rust, Python, EF)
Sovereign Tech Fund (eg. Yocto Project)

02 Update of processes
Example: the Yocto Project has a security team now!

03 Tools
SBOM generation (CycloneDX or SPDX)
Dependency checking/CVE monitoring

04 How to do it long-term?
Agenda

- Regulations
- Long-term Trends
- Events, vulnerabilities, incidents
- What to expect in 2024
Exploited: August to October 2023
HTTP/2 clients doing massive creation and cancelling of streams
Result: much work on the server side and a DoS
Most HTTP servers affected
Less impact if using careful resource allocation:
  Example: Lighthttpd not affected
  https://redmine.lighttpd.net/boards/2/topics/11188

More information:
https://nvd.nist.gov/vuln/detail/CVE-2023-44487
« Bricked » trains

It happened in 2022, but published in 2023

- Some trains in Poland weren’t starting after maintenance
- Reverse engineering found (among other things):
  - Train locked after a long stop
  - Train locked after a GPS position match
  - Date lock
- Regulated market, certified software
- Nearly as many SW versions as trains
  - CI anyone?

Video: https://youtu.be/XrlrbfGZo2k?si=FrIs2AsBvscCzGki
Agenda

• Regulations
• Long-term Trends
• Events, vulnerabilities, incidents
• What to expect in 2024
The final version of the CRA voted, development of related standards. Similar regulation in other places.

**Regulations**

Can you use all possible dependencies? Finding replacements with an appropriate security policy.

**Triage of dependencies**

Currently we are generating SBOMs. Time to start using them.

**SBOM analysis**

Expect issues when an « internal » network gets exposed to the Internet.

**Unexpected network access**

More hardware/firmware issues expected. Watch out for network cards, phone chipsets, graphic cards.

**More hardware issues**

Watch out for security issues in projects that have no CVEs assigned.

**Unexpected issues**