

The Shape of Things to come

Cyber Resilience Act and Open Source Development

11.334

Vulnerabilities in the
WP Ecosystem in 2025

10.359

Vulnerabilities

in Plugins in 2025

Hey 🖐️

Simon

simon.blog

WordPress since 2008

Product @ Patchstack



Oh myyy

The Cyber Resilience Act (CRA)

The Cyber Resilience Act (CRA)

GDPR but for Security

The Cyber Resilience Act (CRA)
Regulates **Products with digital Elements.**

The Cyber Resilience Act (CRA)
Will apply in full as of December 2027...

The Cyber Resilience Act (CRA)

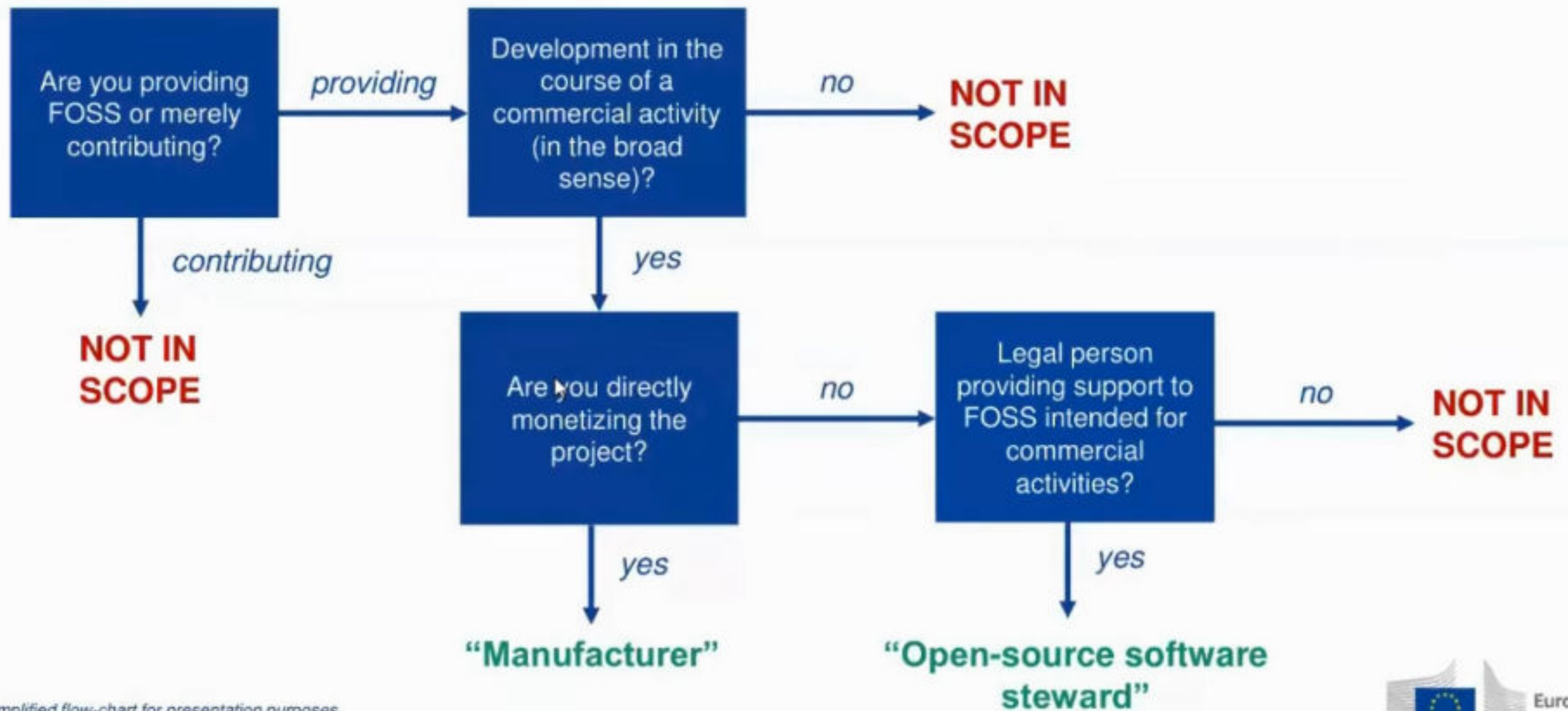
... but the obligation to report vulnerabilities and security incidents **already started this month** ✨

The Cyber Resilience Act (CRA)
open source software products are exempt*

Time for some CRA!

Details for Developers

Is your open-source project covered?*



* Simplified flow-chart for presentation purposes.

Developers

Does your product fall under CRA?

- Only Maintainers + Stewards
- in the course of **commercial activity** and direct monetisation
- when providing support for FOSS **intended for commercial activity**

Developers / Agencies

Requirements

- available on the market without known exploitable vulnerabilities
- secure by default configuration (and a reset)
- vulnerabilities to be addressed through security updates
- Design, develop, and produce to limit attack surfaces

Developers / Agencies

Oh, there's more - Vulnerability Management

"identify and document vulnerabilities and components [...] including by drawing up a software bill of materials in a commonly used [...] format covering at the very least the top-level dependencies of the products"

Oh S...

SBOM

Developers / Agencies

What 's SBOM?

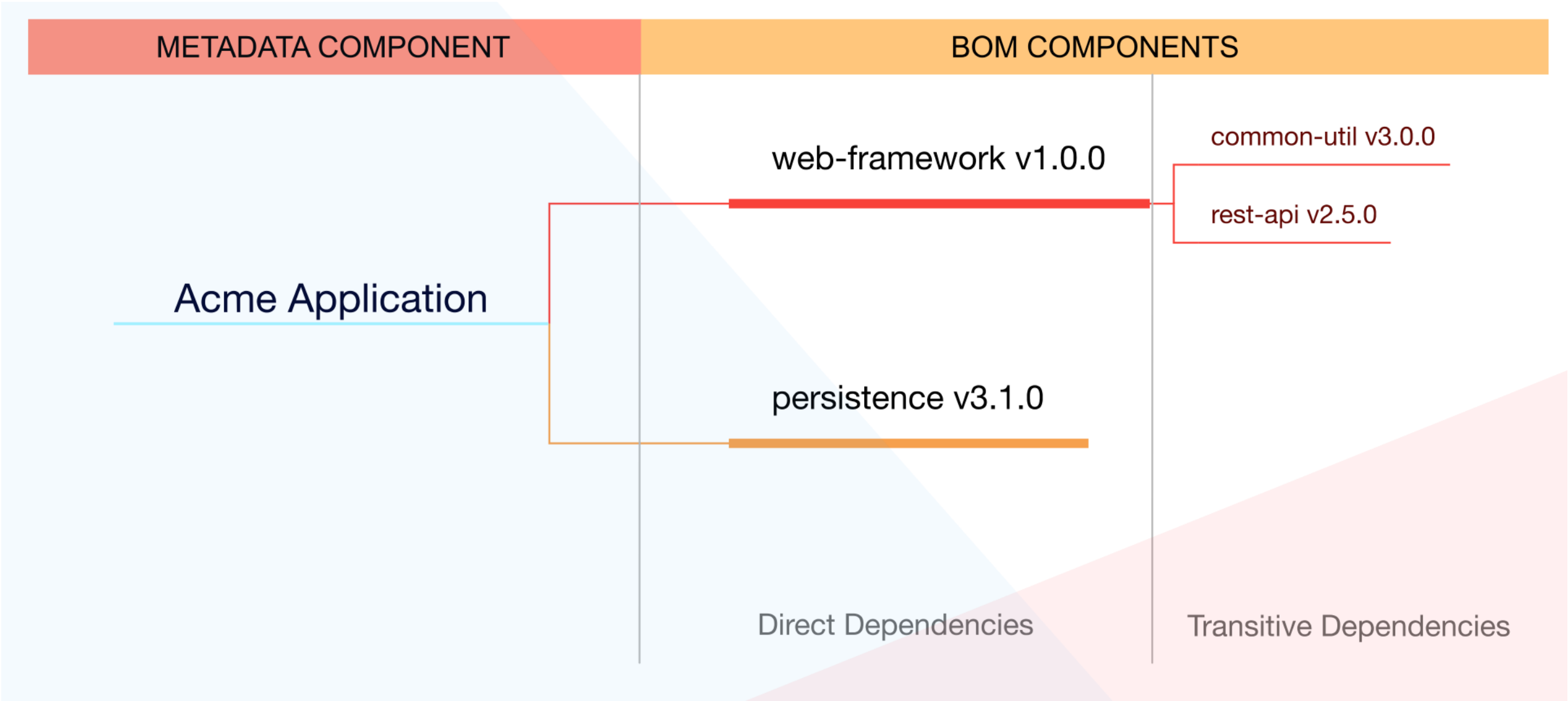
- Software Bill of Materials
- An ingredients list for software
- Supply chain security
- Automatically generated

Developers / Agencies

SBOM Standard(s)

- OWASP CycloneDX
- SPDX

CycloneDX Dependency Graph



...

No. of dependencies in WordPress Core?

2.571

No. of dependencies in WordPress Core!

Eh, there's still more – Vulnerability Management

- put in place and enforce a policy on **coordinated vulnerability disclosure**
- take measures to facilitate the **sharing of information about potential vulnerabilities** [...], including by providing a contact address for the reporting of vulnerabilities discovered [...]

Developers / Agencies

VDP 's

- Vulnerability Disclosure Program
- sets parameters on how to handle disclosure

Developers / Agencies

mVDP 's

- managed
- handle notifications and reporting
- ease of implementation for developers/agencies

How about some
Homework?

- ☐ Security by Design
- ☐ Join a mVDP
- ☐ Familiarise yourself with SBOMs

ASAP

Tchau! 🤘

Simon Kraft

simon.blog/hi

simon.k@patchstack.com

Vulnerability Database

mVDP



Bonus Content

Patchstack's

State of WordPress Security 2026



Apendix

- <https://patchstack.com/whitepaper/2025-mid-year-vulnerability-report/>
- <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32024R2847>
- <https://netzpolitik.org/2024/cyber-resilience-act-aufatmen-fuer-die-open-source-community/>
- <https://about.gitlab.com/de-de/blog/the-ultimate-guide-to-sboms/>
- <https://wordpress.org/plugins/protect-login>
- <https://wordpress.org/plugins/two-factor>
- <https://github.com/orcwg/cra-hub/blob/main/inventory.md>