Neue Perspektiven auf WordPress-Security

Für Entwickler*innen, Agenturen und Anwender*innen

Hej 👋

Simon Kraft

simon.blog/hi

WordPress seit 2008

Meetups seit 2012

Produkt @ Patchstack

11.334

Sicherheitslücken im
WP Ökosystem in 2025

~10.300

Sicherheitslücken
in Plugins in 2025

5 Stunden

Medianzeit bis zur Massenausnutzung
bei stark angegriffenen Sicherheitslücken

46 %

der Sicherheitslücken waren nicht gepatcht
vor der öffentlichen Bekanntmachung

Huiuiui

Der Cyber Resilience Act (CRA)

Der Cyber Resilience Act (CRA)

DSGVO aber für Security

Der Cyber Resilience Act (CRA)

Reguliert die Sicherheit von Produkten mit digitalen Elementen.

Der Cyber Resilience Act (CRA)

Tritt in großen Teilen erst 2027 inkraft...

Der Cyber Resilience Act (CRA)

... erste Teile gelten aber schon ab September 2026 ✨

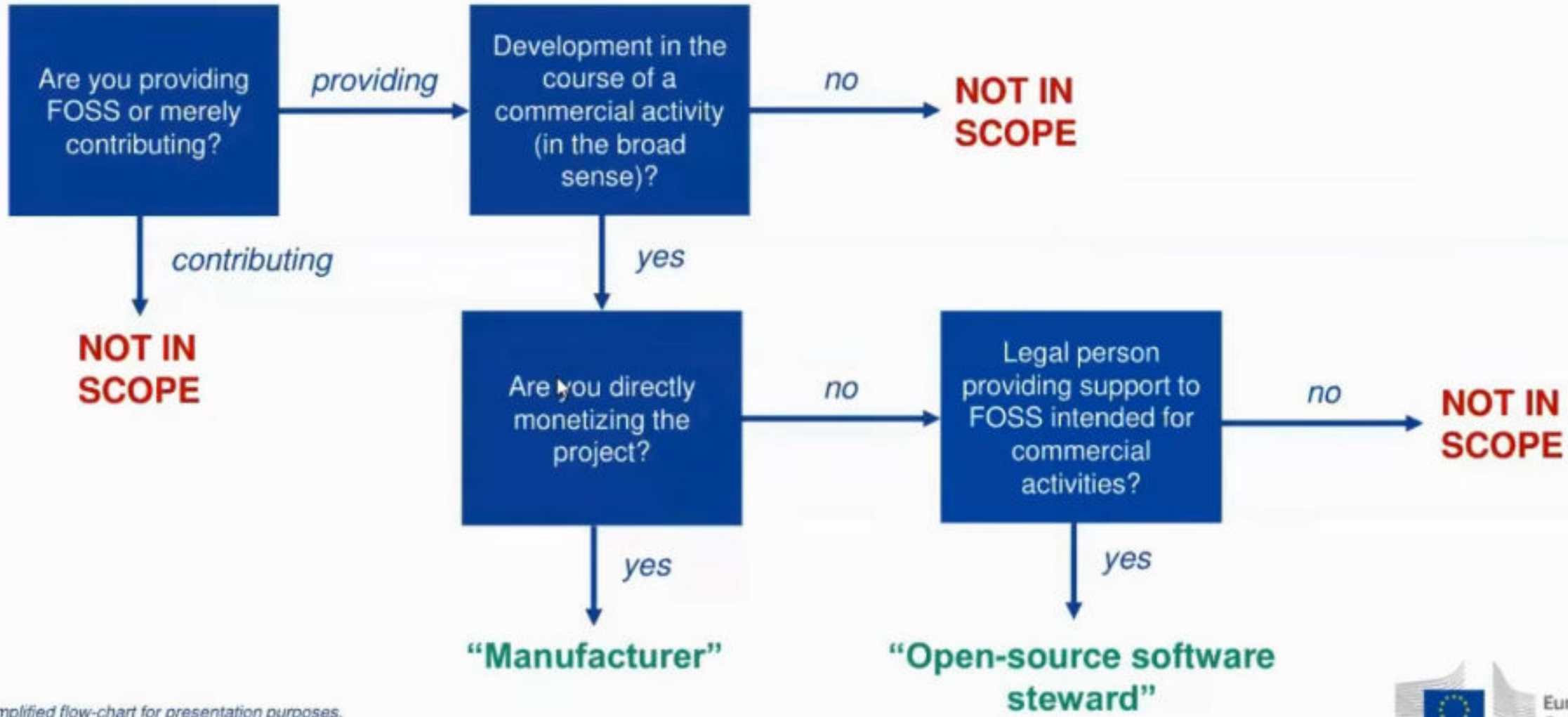
Der Cyber Resilience Act (CRA)

Open-Source-Software ist grundsätzlich ausgenommen*

Zeit für CRA!

Details für Entwickler*innen

Is your open-source project covered?*



* *Simplified flow-chart for presentation purposes.*

European Commission

Entwickler*innen

Wer ist betroffen?

- Maintainer + "Verwalter*innen"
- im Rahmen kommerzieller Aktivität / direkt monetarisiert
- wenn für kommerzielle Nutzung zur Verfügung gestellt

Entwickler*innen

Die Verwalter müssen für ihre Produkte eine Cybersicherheitsstrategie entwickeln. Die sollte die Dokumentation und die Beseitigung von Schwachstellen behandeln und den Austausch von Informationen über Schwachstellen fördern. […] Wenn sie erfahren, dass eine Sicherheitslücke in ihrer Software ausgenutzt wird, müssen sie das an Aufsichtsbehörden und Nutzer:innen melden.

– netzpolitik.org

Entwickler*innen

Anforderungen

- Software ohne bekannte Sicherheitslücken
  - sichere Standardkonfiguration + Reset
- Angriffsflächen reduzieren + Sicherheits-Updates
- Dokumentation von Komponenten (SBOM)
- Koordinierte Offenlegung von Schwachstellen (VDP)

Ach du S...

SBOM

Entwickler*innen / Agenturen

Was ist SBOM?

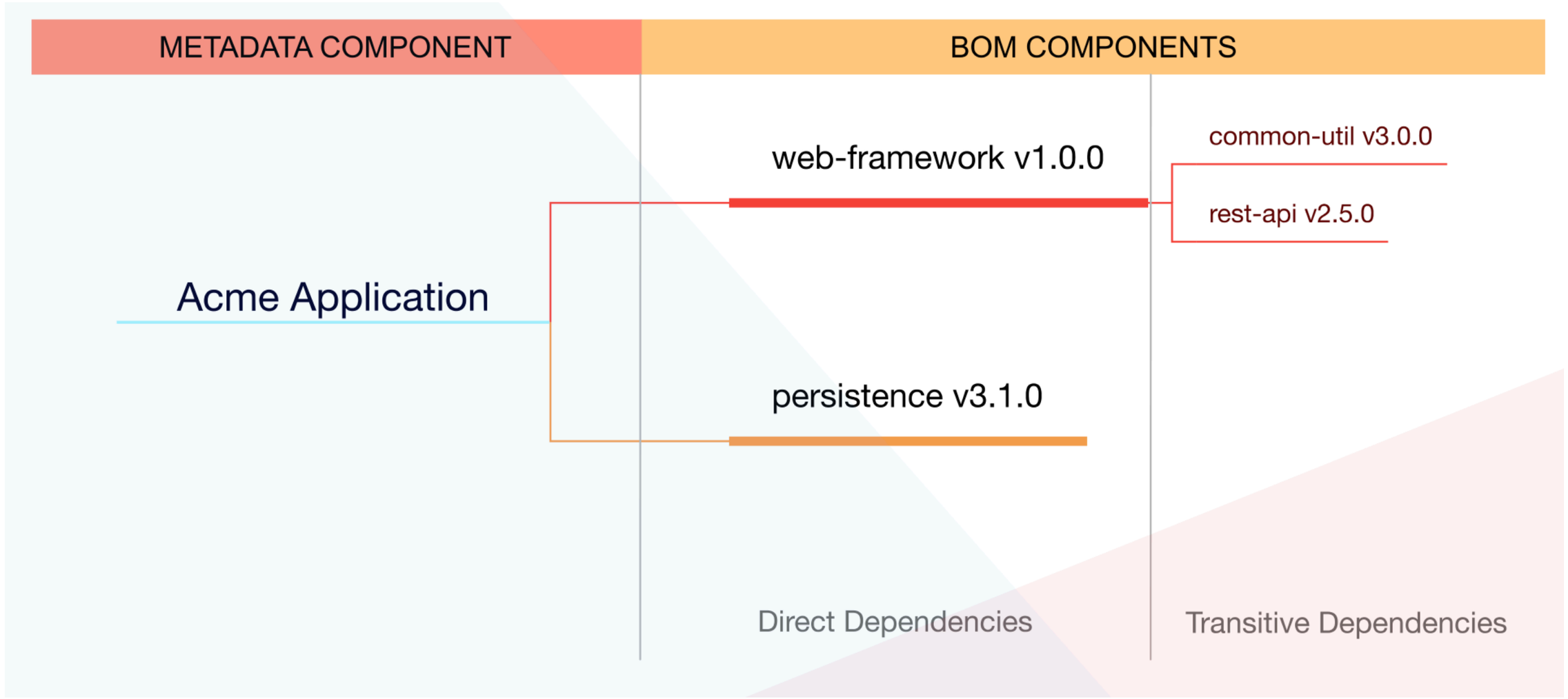
- Software Bill of Materials -> Software-Stücklisten
- Eine Zutaten-Liste für Software
- Supply-Chain-Sicherheit
- Generierung heute z.B. via GitLab

Entwickler*innen / Agenturen

SBOM Standard(s)

- OWASP CycloneDX
- SPDX

CycloneDX Dependency Graph



...

Wie viele Dependencies hat WordPress Core?

2.571

Wie viele Dependencies hat WordPress Core? (Laut GitHub)

Argh, da ist noch mehr - Vulnerability Management

- Eine Policy für koordinierte Offenlegung von Schwachstellen einführen und durchsetzen
- Maßnahmen ergreifen um das Teilen von Informationen über potentielle Schwachstellen […] zu ermöglichen […]

Entwickler*innen / Agenturen

VDP's

- Vulnerability Disclosure Program
- legt Parameter fest, wie mit Meldungen umgegangen wird

Entwickler*innen / Agenturen

mVDP's

- gemanaged
- kümmert sich um Benachrichtigung, Triage und Reports
- Einfacher Einbau für Entwickler*innen und Agenturen

Wie wäre es mit

Hausaufgaben?

- [ ] Security by Design
- [ ] An einem mVDP teilnehmen
- [ ] SBOMs kennenlernen (und verstehen)

bis Sep 2026

Danke 🤟

Simon Kraft
simon.blog/hi
simon.k@patchstack.com

Vulnerability Database

mVDP

Anhang

Patchstacks

State of WordPress Security 2026

Anhang

- 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://de.wordpress.org/plugins/protect-login
- https://de.wordpress.org/plugins/two-factor