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

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

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)

Entwickler*innen

Hausaufgaben bis 09.2026

- [x] Sicherheit mitdenken
- [x] Sicherheitslücken managen (VDPs)
  - [x] und an EU melden (ENISA)
- [ ] SBOMs vorbereiten

Ach du S...

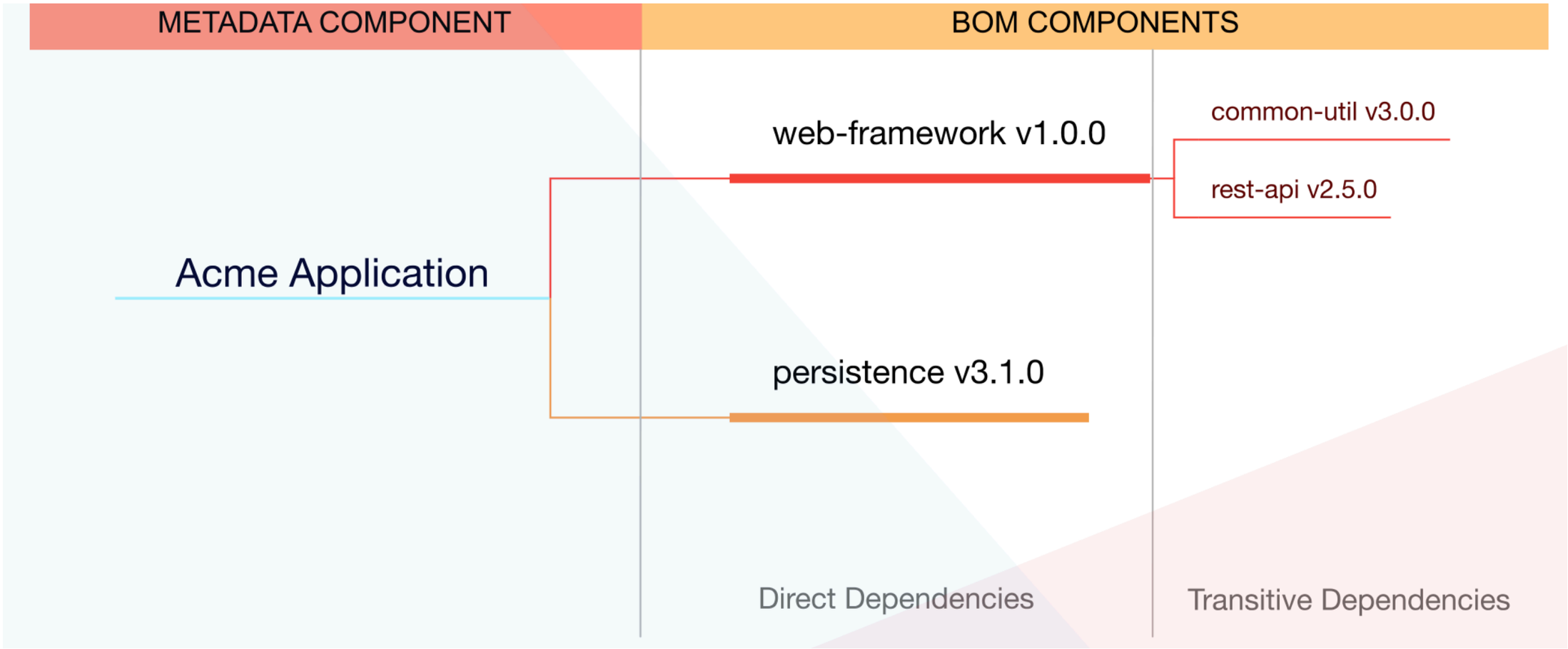
SBOM

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

CycloneDX Dependency Graph



2.334

Wie viele Dependencies hat WordPress Core?

Zurück zur WordPress-Security

7.966

Sicherheitslücken im WP Ökosystem in 2024

7.633

Sicherheitslücken
in Plugins in 2024

Agenturen / Anwender*innen

Praktische WP-Security

- Login-Sicherheit
- Minimierte Angriffsoberfläche
- Hygiene

Agenturen / Anwender*innen

Login-Sicherheit

- Passwort-Komplexität
- Multi-Faktor-Authentifizierung

Agenturen / Anwender*innen

Angriffsoberflächen minimieren

- XML-RPC-API deaktivieren
- Minimale User-Rechte
- WordPress-spezifische WAF

Agenturen / Anwender*innen

Hygiene I

- Regelmäßige automatische Backups
- Regelmäßige Updates

Agenturen / Anwender*innen

Hygiene II

- Vorsichtige Plugin-Auswahl
- Spezialisierte kleine Plugins statt All-In-One-Lösungen

Danke 🤘

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

Vulnerability Database

mVDP

Anhang

Patchstacks Mid-Year Vulnerability Report 2025

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