Software Bill of Materials for web front-ends

Read first:

https://www.w3.org/2023/03/secure-the-web-forward/papers.html#sbom-web

This is a dirty presentation on the topic

lol ;-)

Software Bill of Materials for web front-ends

Who am I**?**

- Name: Jan Kowalleck
- My Background:
  - Software engineer, Architect, Tech Lead,
    Web-Dev since early 2000
  - Author & maintainer of SBOM related tools & libraries
  - OWASP CycloneDX Project Co-Lead

Software Bill of Materials for web front-ends

What is a “Software Bill of Materials”**?**

- list of ingredients of a software product
- short: SBOM, SBoM
- *is not: “how” the product was manufactured* nor what was used during manufacturing processes

Software Bill of Materials for web front-ends

What is a “web front-end”**?**

- part of a product that is fetched by and run in a web-browser - call it “web deliverable”
- may consist of internal/external packages and components
- may be generated by tools like “webpack”

Software Bill of Materials for web front-ends

Why SBOM for web deliverables?

- know what you are shipping to web-browsers
  - know what you depend on
  - know licensing situations
- identify security issues
- identify your supply chain risks

Software Bill of Materials for web front-ends

How to generate SBOM for web deliverables**?**

- use existing document standard {CycloneDX/SPDX/…}
- write and maintain by hand
- use evidence-based generators
  like “CycloneDX webpack plugin”

Software Bill of Materials for web front-ends

How to fetch SBOM for web deliverables**?**

- See the other presentation:
  ”Establish Standards to Support Web Access to SBOM Data”

Software Bill of Materials for web front-ends

Questions?