dtec.bw
JAHRESTAGUNG 2024

Accuracy Evaluation of SBOM Tools for Web Applications and System-Level Software

Andreas Halbritter, Dominik Merli
Institut für innovative Sicherheit, Technische Hochschule Augsburg

Motivation

Recent vulnerabilities in software like Log4j [1] raise the question whether the software supply chain is secured sufficiently.
Governmental initiatives in the United States (US) [3] and the European Union (EU) [3] demand a Software Bill of Materials (SBOM) for solving this issue. An SBOM has to be produced by using creation tools and it has to be accurate and complete. In the past, there had been investigations in this field of research.
However, no detailed investigation of several tools producing SBOMs has been conducted regarding accuracy and reliability. For this reason, we present a selection of four popular programming languages: Python, C, Rust and Typescript.
For web application software we consider Python and Typescript while for system-level software C and Rust are investigated.

Results

There is no recommendation for a specific tool as no tool fulfills every requirement, only two tools can be recommended in a limited way. Many tools do not provide a complete SBOM, as they do not depict every test package and
dependency. Governmental initiatives should define further specifications on SBOM for example regarding their accuracy and depth. Further research in this field, for example for proprietary tools or other programming languages is desirable.

Table 1: Tools and their NTIA fullfillment

Programming language	Tool	C	SN	CN	VOC	OUI	DR	AOSD	TS	HOC	LP	OCR	LI
Python	Syft	+	-	+	+	+	-	+	+	-	-	-	-
	Cdxgen	+	-	+	+	+	+	+	+	-	-	-	o
	CycloneDX-Python	+	o	+	+	+	o	+	+	-	-	-	o
	SBOM4Python	-	-	+	+	-	-	+	+	-	-	-	-
C	Syft	-	-	+	+	+	-	+	+	o	-	-	-
	Cdxgen	-	-	+	+	+	o	+	+	-	-	-	o
	CycloneDX-Conan-Extension	+	o	+	+	+	+	+	+	-	-	-	+
Rust	Syft	+	-	+	+	+	-	+	+	-	-	-	-
	Cdxgen	-	-	+	+	+	o	+	+	+	-	-	o
	SBOM4Rust	+	-	+	+	-	+	+	+	-	-	-	-
Typescript-npm	Syft	+	-	+	+	+	-	+	+	-	-	-	+
	Cdxgen	+	-	+	+	+	+	+	+	+	-	-	o
	CycloneDX-Npm	+	o	+	+	+	+	+	+	+	-	-	+
	Covenant	+	-	+	+	+	o	+	+	+	-	-	+

Present data field (+), Partially present data field (o) and not present data field (-)
Completeness (C), Supplier Name (SN), Component Name (CN), Version of the Component (VOC), Other Unique Identifiers (OUI)
Dependency Relationship (DR), Author of the SBOM Data (AOSD), Timestamp (TS), Hash of the component (HOC), Lifecycle phase (LP)
Other component relationship (OCR), License information (LI)

Measurement Method

The tools build the base for four sample software projects and their package manager. For manual checking, the software projects are kept small with a small amount of packages and a single dependency. The open-source analysis tools are categorized as programming language dependent and general tools, and run in the standard execution mode on the software projects.
The results were checked against completeness and the National Telecommunications and Information Administration (NTIA) [4] minimum and recommended elements.

References

[1] 2021. Alert Apache Log4j vulnerabilities. Retrieved 2024-05-10 from https://www.ncsc.gov.uk/news/apache-log4j-vulnerability
[2] Joseph R. Biden Jr. 2021. Executive Order on Improving the Nation's Cybersecurity. Retrieved 2024-05-10 from https://www.whitehouse.gov/briefing room/presidential-actions/2021/05/12/executive-order-on-improving-thenations-cybersecurity/
[3] 2022. Cyber Resilience Act. Retrieved 2023-08-30 from https://eur-lex.europa.eu/resource.html?uri=cellar:864f472b-34e9-11ed-9c68-01aa75ed71a1.0020.02/DOC_1&format=PDF
[4] 2021. sbom minimum elements report. Retrieved 2024-05-01 from https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf

THA Technische Hochschule Augsburg | THA_innos Institut für innovative Sicherheit

unibw.de
hsu-hh.de
dtecbw.de

DS2CCP
Digital Sensor-2-Cloud Campus-Platform

gefördert durch
dtec.bw
Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr

Finanziert von der Europäischen Union
NextGenerationEU