SBOM with OWASP Dependency Track

Tonimir Kišasondi

$ toc

What’s Software Composition Analysis (SCA)

Why should you care about your Software Bill of Materials (SBOM)

How to build a SBOM from your project

Analysing SBOMs with OWASP Dependency Track

- Hunting dependency vulnerabilities
- Enforcing software licences
- A few thoughts on CI/CD integration

$ Why should you care about your SBOM

You are building your application and you pull in about 5 well known, stable dependencies. Nothing major.

Your application now depends on a total of 135 packages.

Each package can have a security vulnerability.

Each package can have a licence not compatible with your project’s intention.

$ Why should you care about your SBOM

An upstream provider gets compromised. How can you see which packages are upstream, which packages are changed?

A common software library has a critical vulnerability. Can we easily find all deployed instances of this library?

$ What is Software Composition Analysis (SCA)

A Software Bill of Materials (SBOM) is a record of how a specific piece of software is built, what dependencies are used and the relationship of those dependencies, with associated metadata for both the build process and dependencies.

A Software Composition Analysis (SCA) tool can process and ingest SBOMs in order to detect vulnerabilities, enforce licence policies and enable the user to analyse his software’s dependency composition.

$ The good thing about standards is that…

You can choose from a number of standards: SWID, CycloneDX, SPDX

- Even more (proprietary) standards are upcoming
- We will focus on OWASP’s CycloneDX
- It’s compatible with EO14028 and NIST SSDF

$ How to build a SBOM from your project

1. Pick a SBOM standard (You probably want CycloneDX)
2. Pick a tool / package manager plugin
   a. https://cyclonedx.org/tool-center/
3. Build your project
4. Generate a SBOM from the built snapshot

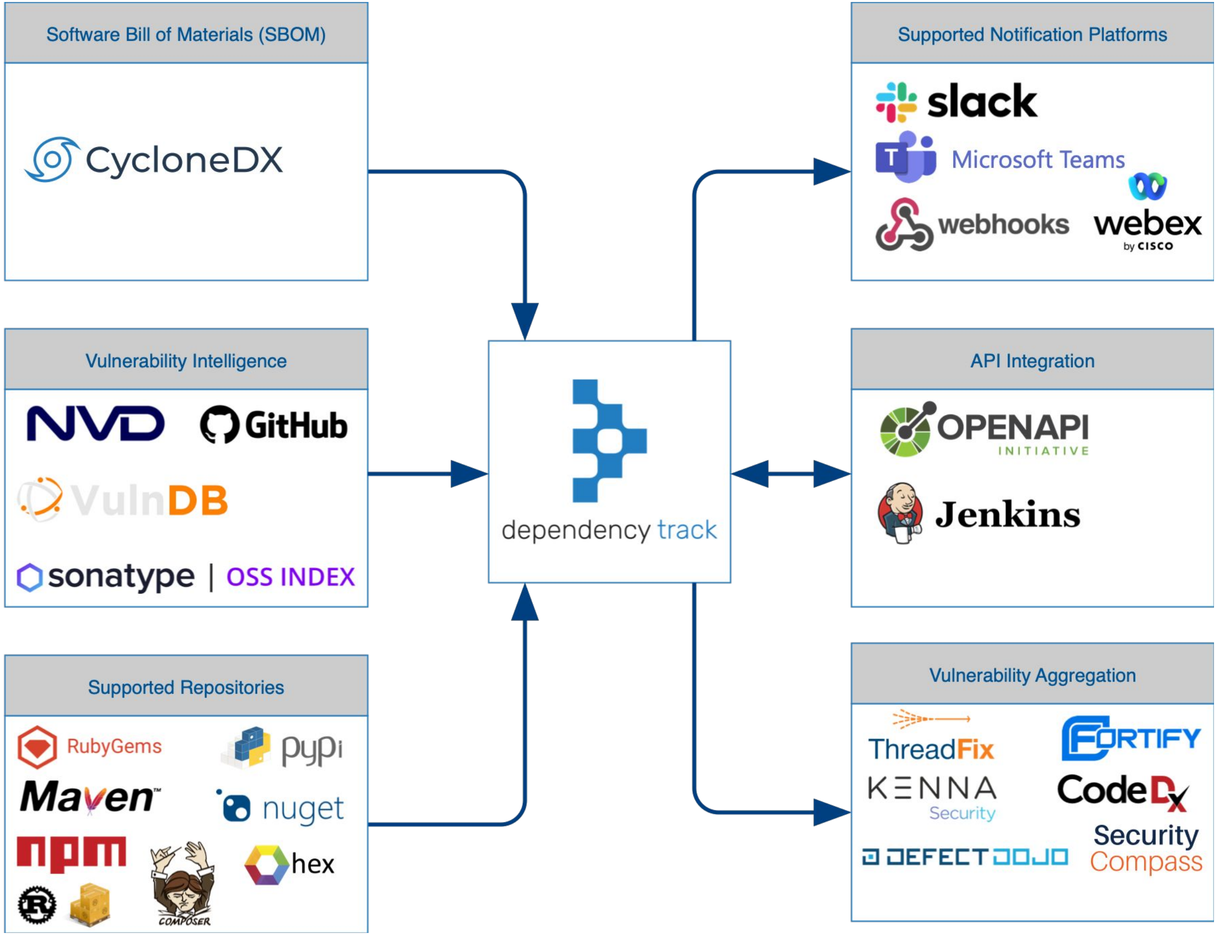
Let’s do this now and let’s see how the resulting SBOM looks like

$ Analysing SBOMs with OWASP Dependency Track

A SBOM is only one piece of the entire pipeline. We need a way to analyze the elements from the SBOM.

OWASP Dependency Track can help us with this:

https://dependencytrack.org/



Source: https://docs.dependencytrack.org/integrations/ecosystem/

$ Usual CI integration

There is an Jenkins plugin, and for everything else, there is an OpenAPI spec available.

Ideally you want to:

- Create a SBOM from each build of the project
- Have an SBOM available for each release / deployment
- Be able to track releases, deployments and SBOMs over time
- Require SBOMs from your vendors

Questions?

kisasondi@gmail.com

@kisasondi