Struggles with making SBOMs for C apps

FOSDEM - Feb 2025

Modern languages (like Dart here) are easy

```yaml
- name: Checkout pubspec.lock
  uses: actions/checkout@44c2b7a8a4ea60a981eaca3cf939b5f4305c123b # v4.1.5
  with:
    sparse-checkout: packages/dart/sshnoports/pubspec.lock
    sparse-checkout-cone-mode: false
- name: Install Syft
  uses: anchore/sbom-action/download-syft@7ccf588e3cf3cc2611714c2eeae48550fbc17552
- name: Generate SBOMs
  run: |
    syft scan file:./packages/dart/sshnoports/pubspec.lock \
      -o 'spdx-json=tarballs/dart_sshnoports_sbom.spdx.json' \
      -o 'cyclonedx-json=tarballs/dart_sshnoports_sbom.cyclonedx.json'
```

Syft and Trivy will happily convert a lock file to an SBOM

syft

https://github.com/anchore/syft

aqua trivy

https://trivy.dev/

But C doesn’t give me a lock file - Doh!

It’s a HUGE problem

Lines of open source code

C	6,478,818,405
C++	2,274,903,905
…	
Rust	57,723,210

Source: openhub.net/languages (Feb 2025)

https://media.ccc.de/v/emf2024-87-cheri-and-arm-morello

Hi, I’m Chris

@cpswan

https://chris.swanz.net

Agenda

- ➔ Stuff that I've tried and found wanting
  - ◆ cmake-sbom, Conan, cve-bin-tool, it-depends
- ➔ Stuff that shows promise
  - ◆ Yocto, Zephyr
- ➔ Mainstream Linux distros might solve the 80%
- ➔ CMake is likely the #1 focus for the residue
  - ◆ LOTS of long tail to worry about :(

How not to make an SBOM for a C project

cmake-sbom

+ Helpful for NTIA boilerplate

- Doesn’t address dependencies
- SPDX only

https://github.com/DEMCON/cmake-sbom

I chat with Ryan Ware (at Intel at the time)

Conan

+ Many popular dependencies already packaged

- Syft claims to generate SBOMs from conan.lock, but… incomplete CFEs
- Docs hadn’t caught up with 2.0
  - Which makes adoption hard

https://conan.io/

cve-bin-tool

+ Binary scanning saves tool chain integration

- Limited dependency recognition
- False positives for patched old versions

https://github.com/intel/cve-bin-tool

it-depends

+ Claims support for CMake projects
+ CycloneDX support in Dec ‘24 release (after ~3y of lying fallow)

- Empty return for CMake projects (issue #66 open since Feb 2022)
- Appeared to be abandoned (until Dec)

https://github.com/trailofbits/it-depends

Rays of hope

Yocto

https://www.yoctoproject.org/

Zephyr

https://github.com/swinslow/cmake-spdx

https://www.zephyrproject.org/

Next?

Mainstream Linux distros get SBOMs
(like Yocto they already the dependency metadata)

debian

alpine
Linux

fedora

archlinux

CMake gets a way to express dependencies into SBOMs

Review

- Existing tools aren’t useful yet
  - cmake-sbom, Conan, cve-bin-tool, it-depends
- It’s easy if you’re already a package manager
  - Yocto, Zephyr
- Mainstream Linux distros might solve the 80%
- CMake is likely the #1 focus for the residue
  - LOTS of long tail to worry about :(

Resources

Blog posts
https://sbomify.com/2024/11/18/c-conundrum/

Yocto
https://docs.yoctoproject.org/5.0.6/dev-manual/sbom.html

Thanks for your time

chris@atsign.com

@cpswan

Questions?