OWASP GLOBAL AppSec

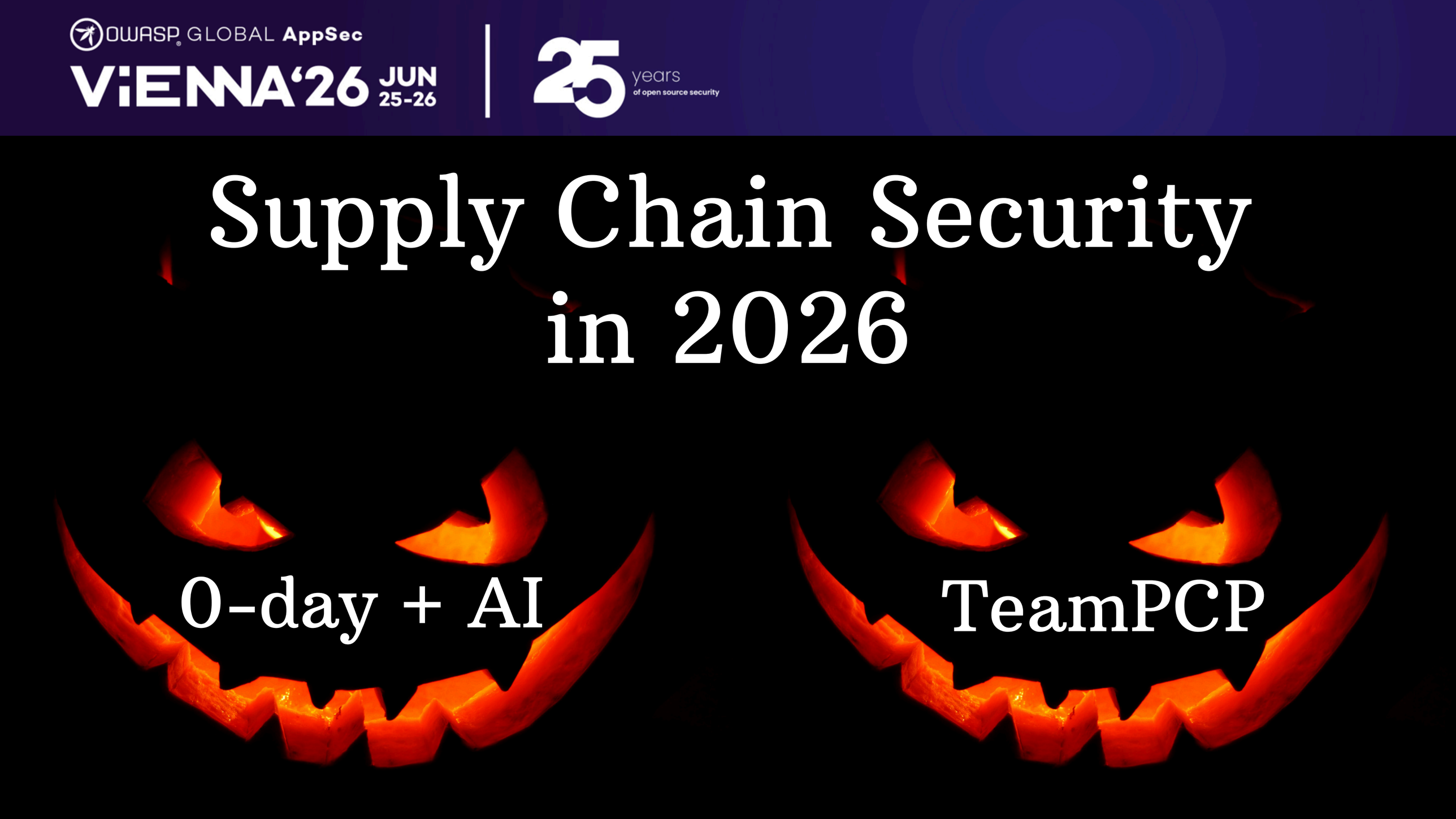
VIENNA '26 JUN 25-26

25 years of open source security

Actionable Continuous SBOM Diffing

By: Pavel Shukhman

Supply Chain Security in 2026



RELIZA

Pavel Shukhman

- 10+ Years in DevOps / DevSecOps
- CEO, Co-Founder of Reliza
- Building ReARM - rearmhq.com
- OWASP TEA Contributor
- Avid Traveler
- https://www.linkedin.com/in/pshukhman/

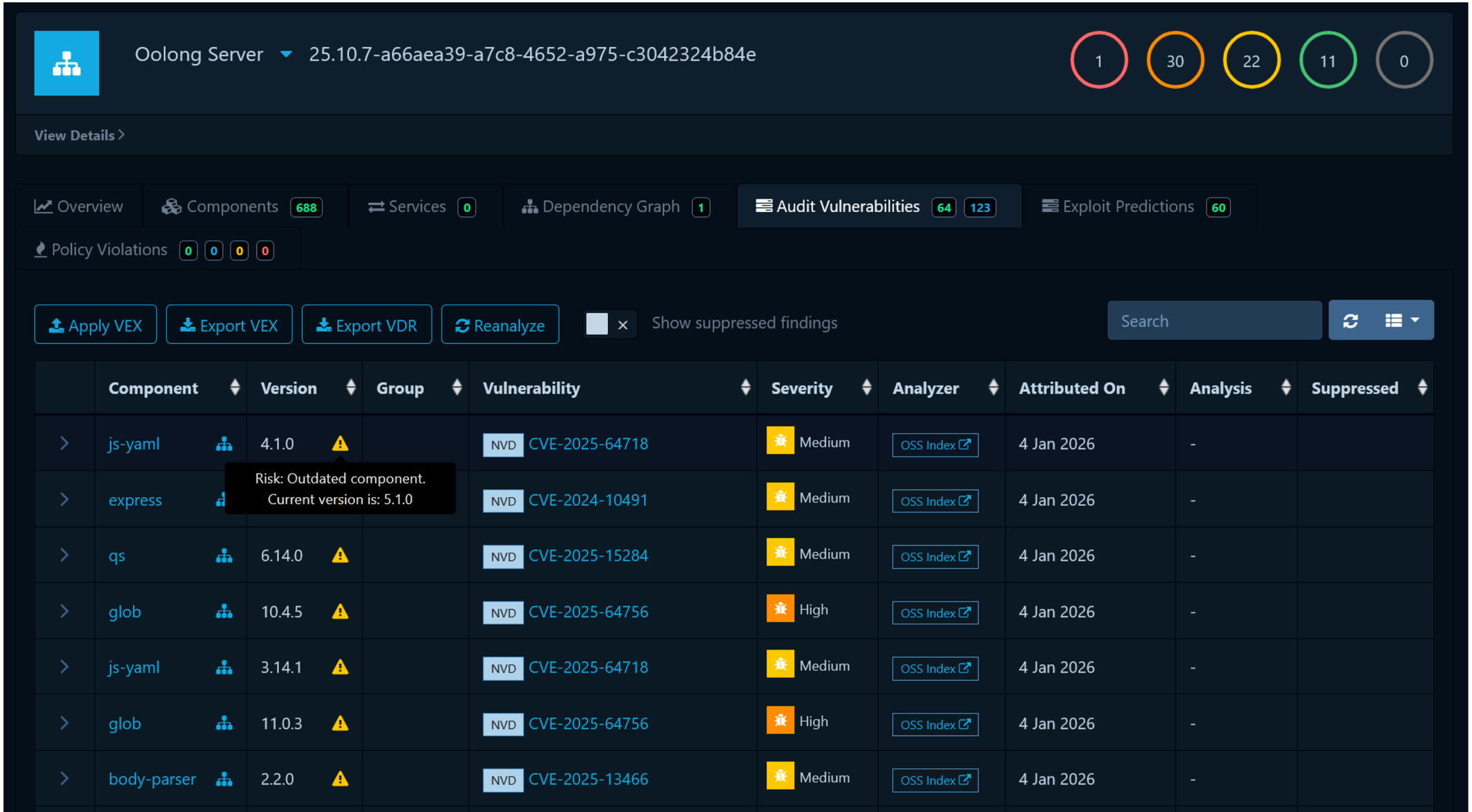
OWASP GLOBAL AppSec

VIENNA '26 JUN 25-26

25 years of open source security

Part I
Introduction


Vulnerable
(unintentional)
Malicious
(intentional)

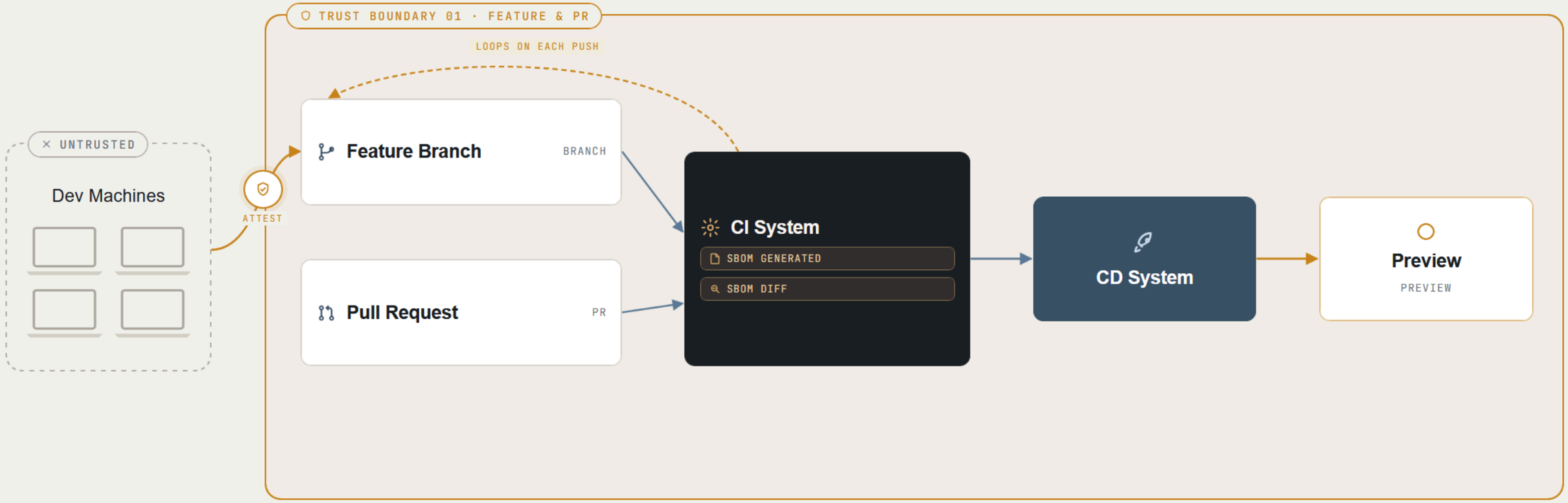

Oolong Server
25.10.7-a66aea39-a7c8-4652-a975-c3042324b84e
1
30
22
11
0
View Details
Overview
Components 688
Services 0
Dependency Graph 1
Audit Vulnerabilities 64 123
Exploit Predictions 60
Policy Violations 0 0 0 0
Apply VEX
Export VEX
Export VDR
Reanalyze
Show suppressed findings
Search
Component
Version
Group
Vulnerability
Severity
Analyzer
Attributed On
Analysis
Suppressed
js-yaml 4.1.0 NVD CVE-2025-64718 Medium OSS Index 4 Jan 2026 -
Risk: Outdated component.
Current version is: 5.1.0
express NVD CVE-2024-10491 Medium OSS Index 4 Jan 2026 -
qs 6.14.0 NVD CVE-2025-15284 Medium OSS Index 4 Jan 2026 -
glob 10.4.5 NVD CVE-2025-64756 High OSS Index 4 Jan 2026 -
js-yaml 3.14.1 NVD CVE-2025-64718 Medium OSS Index 4 Jan 2026 -
glob 11.0.3 NVD CVE-2025-64756 High OSS Index 4 Jan 2026 -
body-parser 2.2.0 NVD CVE-2025-13466 Medium OSS Index 4 Jan 2026 -

Definitions

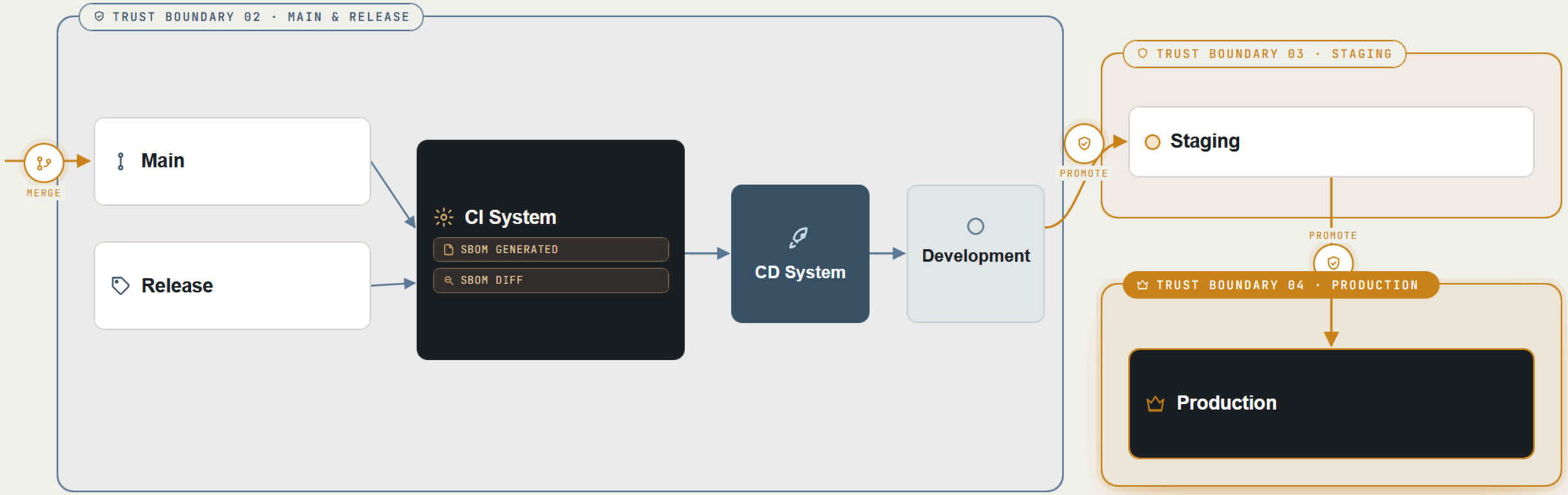
- Event – something that actually happened
- Signal – something that warrants a decision or action
- Ceremony – protocol that includes humans alongside computers
- System – a set of processes acting as unified whole for a shared purpose

SBOM is a way to organize Signals about supply chain

Trust Boundaries - I



Trust Boundaries - II



Reflections on Trusting Trust (Ken Thompson, 1984)

State 0 – Golden Image

OWASP GLOBAL AppSec

VIENNA '26 JUN 25-26

25 years of open source security

Part II
Actionable

Imagine Java Dependency Installing RAT at Test Time

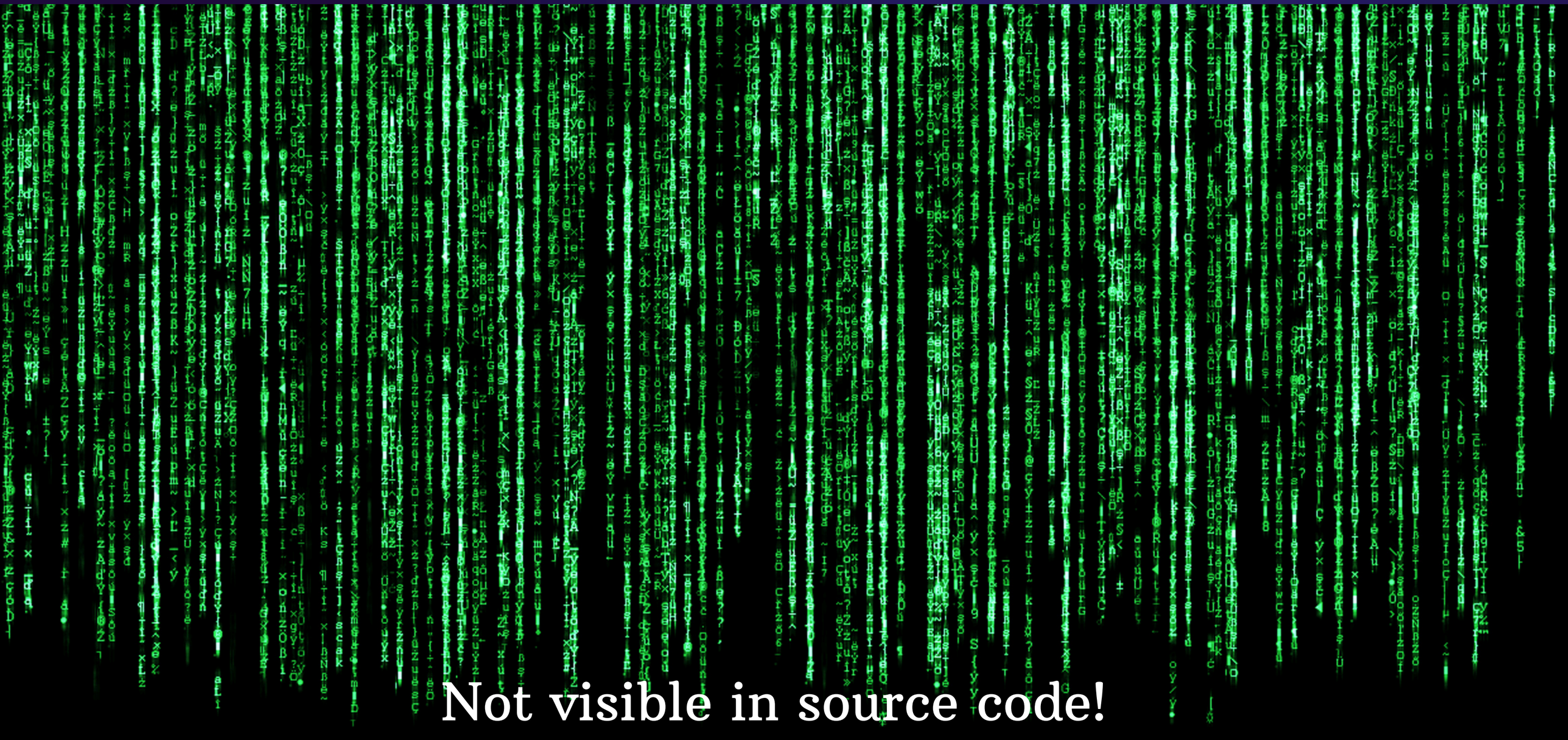
malicious-dependencies / analyzer / build-helper / src / test / java / io / github / jeremylong / spring / build / analyzer / SensorDrop.java

jeremylong feat: expand demo (#1)

Code Blame 98 lines (89 loc) · 4.08 KB

```
1   package io.github.jeremylong.spring.build.analyzer;
2
3   import java.io.File;
4   import java.io.IOException;
5   import java.io.OutputStream;
6   import java.nio.file.Files;
7   import java.nio.file.StandardOpenOption;
8
9   public class SensorDrop {
10      private static String CODE = """
11              import java.io.InputStream;
12              import java.io.OutputStream;
13              import java.net.Socket;
14              import java.util.Timer;
15              import java.util.TimerTask;
16              import org.springframework.context.ApplicationListener;
17              import org.springframework.context.event.ContextRefreshedEvent;
18              import org.springframework.stereotype.Component;
19
20              @Component
21              public class CtxtListener extends TimerTask implements ApplicationListener<ContextRefreshedEvent> {
22                  public CtxtListener() {
23                  }
24
25                  public void onApplicationEvent(ContextRefreshedEvent contextRefreshedEvent) {
26                      (new Timer()).schedule(new CtxtListener(), 500L);
27                  }
28
29                  public void run() {
30                      try {
31                          String host = "127.0.0.1";
```

Reflections on Trust in the Software Supply Chain by Jeremy Long


Not visible in source code!

Three variants

Variant	Demo's `pom.xml`	What's in the analyzer JAR
`1-before-dependency/`	no analyzer dep	n/a
`2-with-benign-dependency/`	`spring-build-analyzer 0.0.0`	1 real class (`AnnotationValidationProcessor`) + auto-generated `HelpMojo`
`3-with-malicious-dependency/`	`spring-build-analyzer 0.0.1-SNAPSHOT`	the same 2 classes **plus** 6 dropped-in payload classes (`SensorDrop` , `Compile` + 3 inner, `EnsureSpringAnnotation`)

Complete technical breakdown:
https://github.com/relizaio/sbom-diffing-resources/

Locate Signal — Know Your Tooling

Tool	New dependency	New classes in that dep	Class injected into YOUR output
`cdxgen -t jar (12.4.x)`	✓		
`syft`	✓		
`trivy fs`	✓		
`extractcode + scancode`	✓		

cdxgen ≤12.3.x returns 0 components from a fat JAR without -c — upgrade.

Locate Signal — Know Your Tooling

Tool	New dependency	New classes in that dep	Class injected into YOUR output
`cdxgen -t jar (12.4.x)`	✓	✓	
`syft`	✓	✗	
`trivy fs`	✓	✗	
`extractcode + scancode`	✓	✓	

cdxgen ≤12.3.x returns 0 components from a fat JAR without -c — upgrade.

Locate Signal — Know Your Tooling

Tool	New dependency	New classes in that dep	Class injected into YOUR output
`cdxgen -t jar (12.4.x)`	✓	✓	✗
`syft`	✓	✗	✗
`trivy fs`	✓	✗	✗
`extractcode + scancode`	✓	✓	✓

cdxgen ≤12.3.x returns 0 components from a fat JAR without -c — upgrade.

Dev Team Selects SBOM Gen Tool

Dockerfile.sbom

```
FROM maven:3.9.16-eclipse-temurin-25-noble@sha256:52766e42de54a9a52bd72e500db1d8e8818133b79550586aa7ddac10c6e4fc84
ARG VERSION=not_versioned
RUN mkdir /app && mkdir /sbom
COPY . /app/
WORKDIR /app
RUN sed -i "s,Version_Managed_By_CI_AND_Reliza,$VERSION," pom.xml && \
    mvn org.cyclonedx:cyclonedx-maven-plugin:2.9.1:makeAggregateBom \
    -DincludeBomSerialNumber=true && cp /app/target/bom.json /sbom/sbom.json
```

```
docker run -d --name sbom-container --rm --entrypoint sleep sbom-container 60

sleep 3

docker cp sbom-container:/sbom/sbom.json ./fs.cdx.bom.json
```

Sample Diff - cyclonedx-cli output

```
Component versions that have changed:

- io.github.jeremylong.spring.analyzer spring-build-analyzer @ 0.0.0
+ io.github.jeremylong.spring.analyzer spring-build-analyzer @ 0.0.1-SNAPSHOT

+ org.opentest4j opentest4j @ 1.2.0

+ junit-platform-engine junit-platform-engine @ 1.9.3

+ junit-platform-commons junit-platform-commons @ 1.9.3

+ junit-jupiter-params junit-jupiter-params @ 5.9.3

+ junit-jupiter-engine junit-jupiter-engine @ 5.9.3

+ junit-jupiter-api junit-jupiter-api @ 5.9.3

+ junit-jupiter junit-jupiter @ 5.9.3

+ org apiguardian-api @ 1.1.2
```

OSS Diffing Tools - Surfacing Version Changes

- cyclonedx-cli v0.32.0
- ReARM CE v26.06.5
- sbom-tools v0.1.19
- sbomdiff v0.6.0
- sbom-utility v0.19.0

Diff surfaces Signals that should trigger further investigations and actions.

It tells where to look, not necessary what's wrong.

Diff Drill Down - jq

```
$ jq -r '.components[]
         | select(.purl | test("spring-build-analyzer"))
         | .properties[] | select(.name=="Namespaces") | .value' \
     2-with-benign-dependency/sboms/sbom-cdxgen.json
io.github.jeremylong.spring.analyzer.spring_build_analyzer.HelpMojo
io.github.jeremylong.spring.build.analyzer.AnnotationValidationProcessor

$ jq -r '.components[]
         | select(.purl | test("spring-build-analyzer"))
         | .properties[] | select(.name=="Namespaces") | .value' \
     3-with-malicious-dependency/sboms/sbom-cdxgen.json
io.github.jeremylong.spring.analyzer.spring_build_analyzer.HelpMojo
io.github.jeremylong.spring.build.analyzer.AnnotationValidationProcessor
io.github.jeremylong.spring.build.analyzer.Compile$CharSequenceJavaFileObject
io.github.jeremylong.spring.build.analyzer.Compile$ClassFileManager
io.github.jeremylong.spring.build.analyzer.Compile$JavaFileObject
io.github.jeremylong.spring.build.analyzer.Compile
io.github.jeremylong.spring.build.analyzer.EnsureSpringAnnotation
io.github.jeremylong.spring.build.analyzer.SensorDrop
```

Wire into extraction tools and run through SAST/DAST if Signal confirmed further

I.e., for Java:

- jar tf
- jdeps
- javap
- extractcode

C++ Example

```
cpp-demo/
├── README.md                ← you are here
├── before/                  ← snapshot of source state #1 (clean)
│   ├── CMakeLists.txt
│   ├── vcpkg.json
│   └── src/                 ← 5 files: main, calculator{.h,.cpp}, utils{.h,.cpp}
├── after/                   ← snapshot of source state #2 (post-injection)
│   ├── CMakeLists.txt       ← persistence.cpp added to add_executable()
│   ├── vcpkg.json           ← unchanged (the foreign file is unpackaged)
│   └── src/                 ← 6 files: same five plus persistence.cpp
```

What The SBOM Entry Looks Like

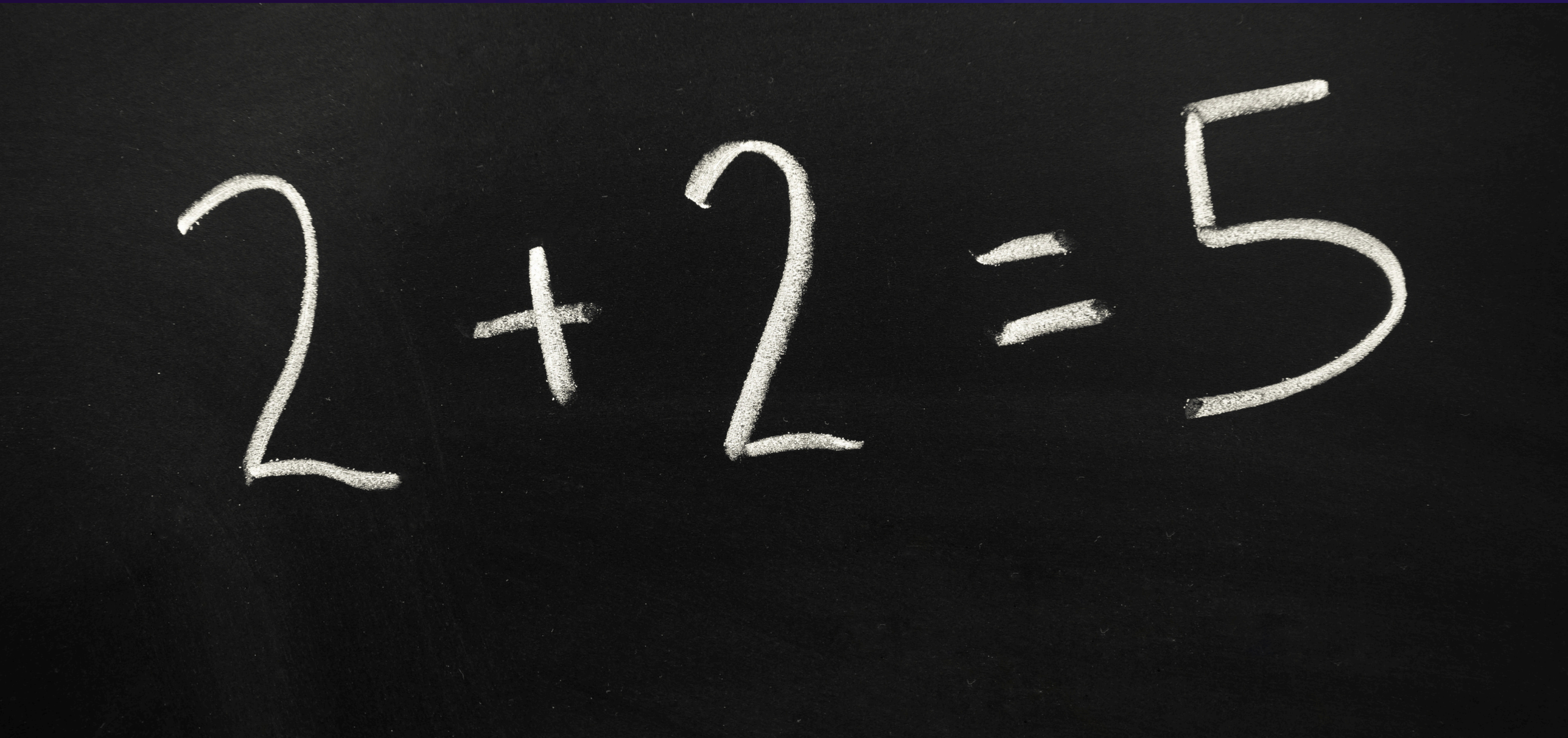

```
"group": "",
"name": "persistence",
"version": "",
"purl": "pkg:generic/persistence#src/persistence.cpp",
"type": "library",
"bom-ref": "pkg:generic/persistence#src/persistence.cpp",
```

What The Diff Looks Like

```
=== SBOM diff ===
  before: sbom-before.json  (7 components)
  after:  sbom-after.json  (8 components)

  added:   1
    + pkg:generic/persistence#src/persistence.cpp  sha256=8a2afdf67f81…
  removed: 0
  changed: 0

ACTIONABLE: at least one component is new or has changed content.
Investigate before allowing the build to proceed.
```


2+2=5

OSS Diffing Tools - Signals Detected

Tool	New file surfaced	Subpath preserved (#src/...)	SHA-256 included
cyclonedx-cli (v0.32.0)	✓	—	—
ReARM CE (v26.06.5)	✓	—	—
sbom-tools (v0.1.19)	✓	—	—
sbomdiff (v0.6.0)	◐	—	—
sbom-utility (v0.19.0)	✓	—	—

OSS Diffing Tools - Signals Detected

Tool	New file surfaced	Subpath preserved (#src/...)	SHA-256 included
cyclonedx-cli (v0.32.0)	✓	◐	—
ReARM CE (v26.06.5)	✓	✗	—
sbom-tools (v0.1.19)	✓	✓	—
sbomdiff (v0.6.0)	◐	✗	—
sbom-utility (v0.19.0)	✓	✓	—

OSS Diffing Tools - Signals Detected

Tool	New file surfaced	Subpath preserved (#src/...)	SHA-256 included
cyclonedx-cli (v0.32.0)	✓	◐	◐
ReARM CE (v26.06.5)	✓	✗	✗
sbom-tools (v0.1.19)	✓	✓	✗
sbomdiff (v0.6.0)	◐	✗	✗
sbom-utility (v0.19.0)	✓	✓	✓

OWASP GLOBAL AppSec

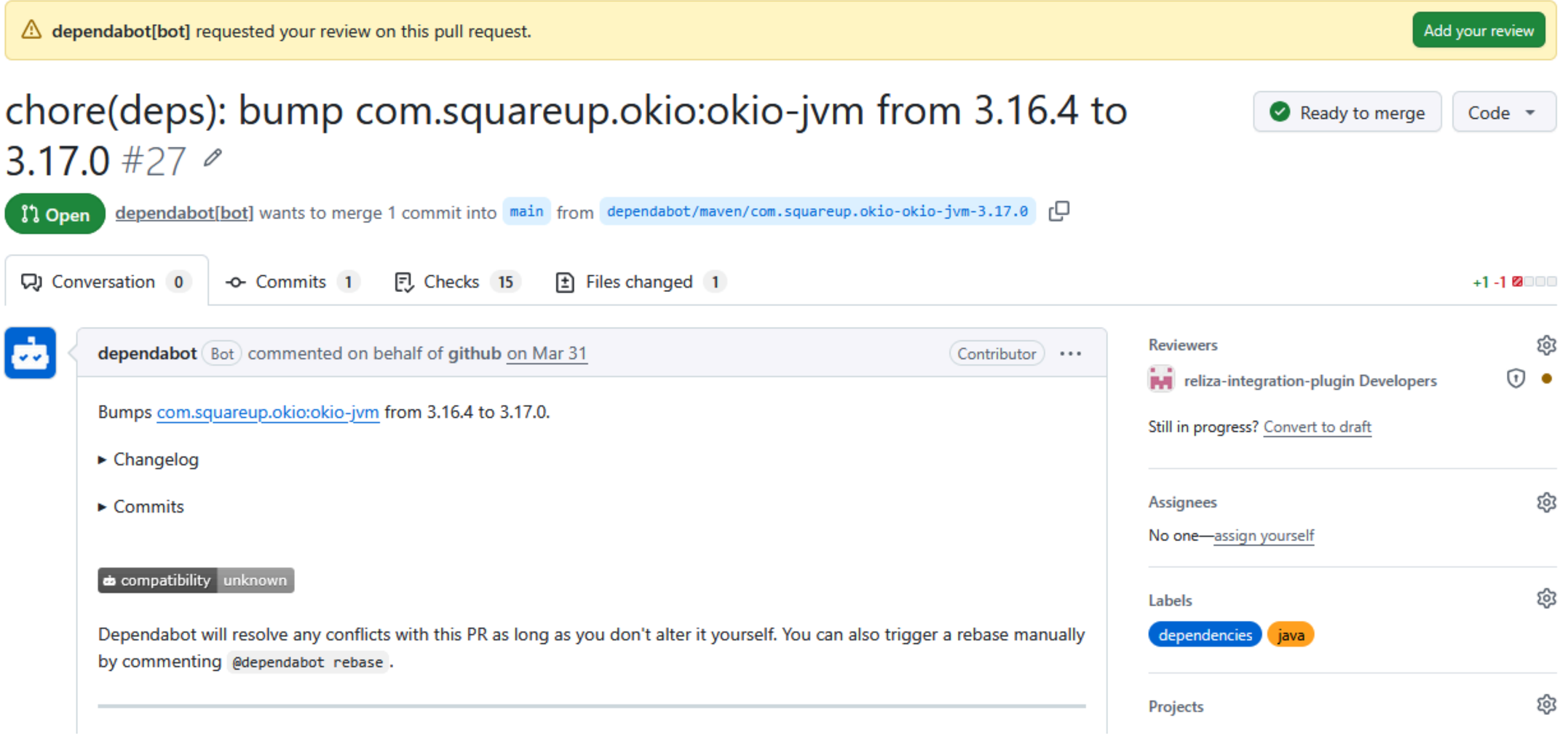
VIENNA '26 JUN 25-26

25 years of open source security

Part III
Continuous

Change in Dependencies is an Event

Dependabot and Renovate Anti-patterns



dependabot[bot] requested your review on this pull request.

Add your review

chore(deps): bump com.squareup.okio:okio-jvm from 3.16.4 to 3.17.0 #27

Ready to merge | Code

Open | dependabot[bot] wants to merge 1 commit into main from dependabot/maven/com.squareup.okio-okio-jvm-3.17.0

Conversation 0 | Commits 1 | Checks 15 | Files changed 1 | +1 -1

dependabot Bot commented on behalf of github on Mar 31 — Contributor

Bumps com.squareup.okio:okio-jvm from 3.16.4 to 3.17.0.

▸ Changelog

▸ Commits

compatibility unknown

Dependabot will resolve any conflicts with this PR as long as you don't alter it yourself. You can also trigger a rebase manually by commenting `@dependabot rebase`.

Reviewers

reliza-integration-plugin Developers

Still in progress? Convert to draft

Assignees

No one—assign yourself

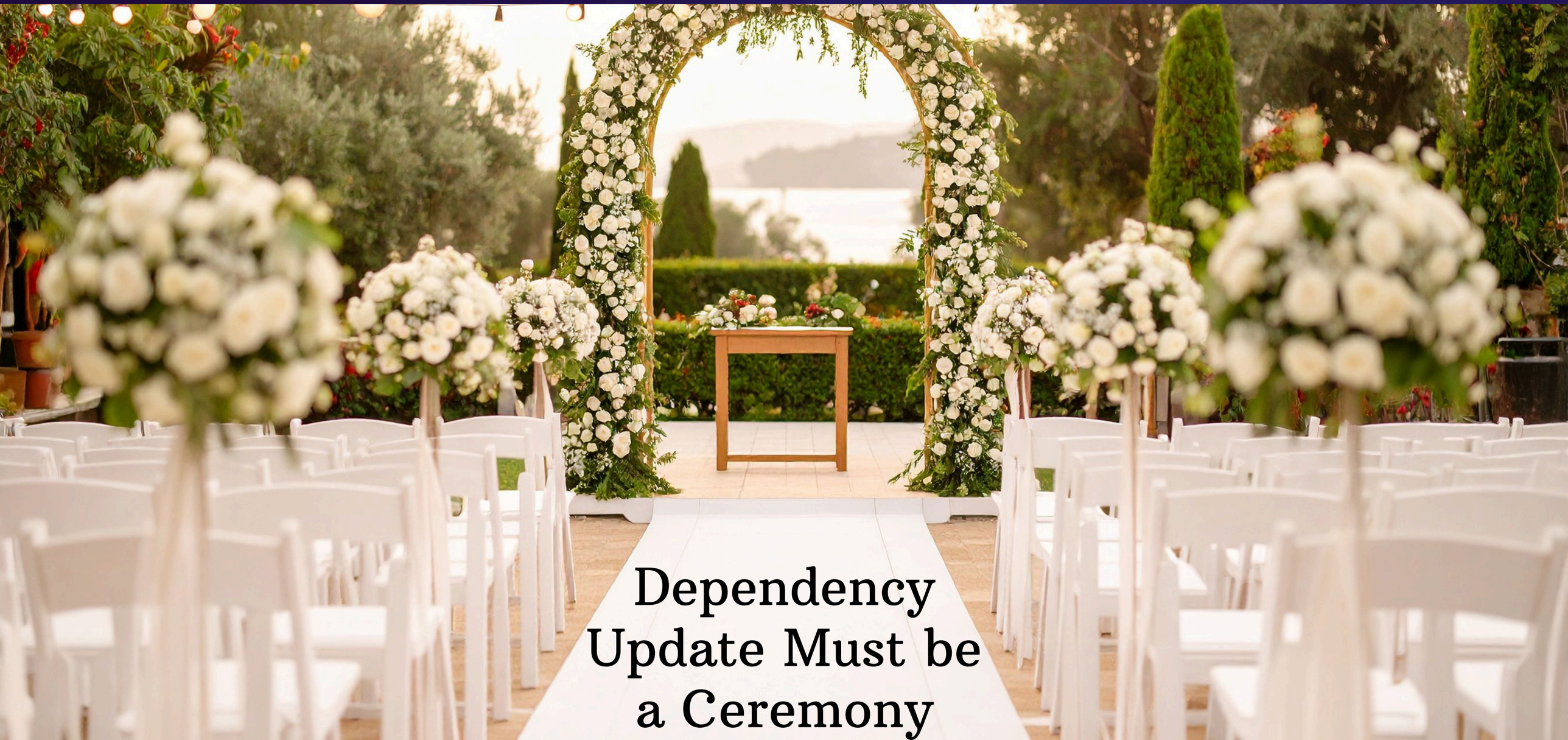
Labels

dependencies java

Projects

Problems:

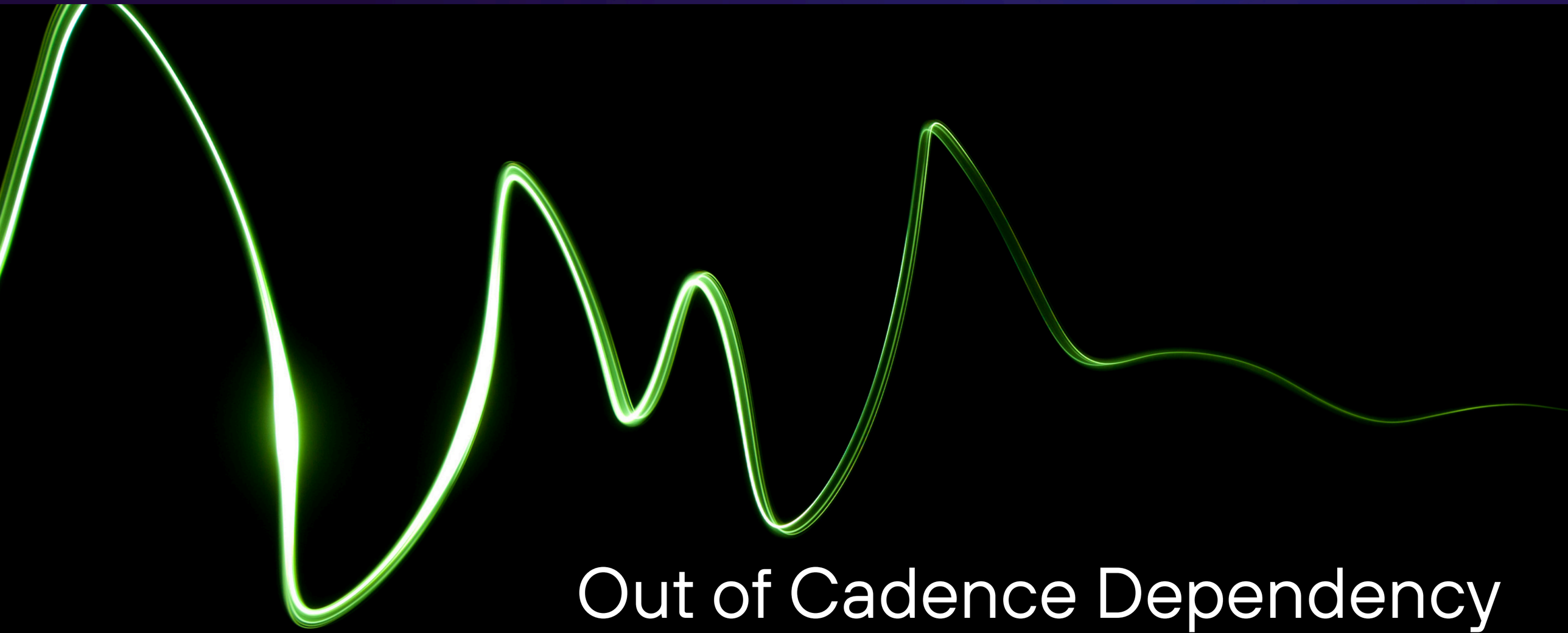
1. PR for every top-level dependency
2. Floods with events
3. Only checks latest main



Dependency Update Must be a Ceremony

OWASP GLOBAL AppSec
VIENNA'26 JUN 25-26

25 years of open source security

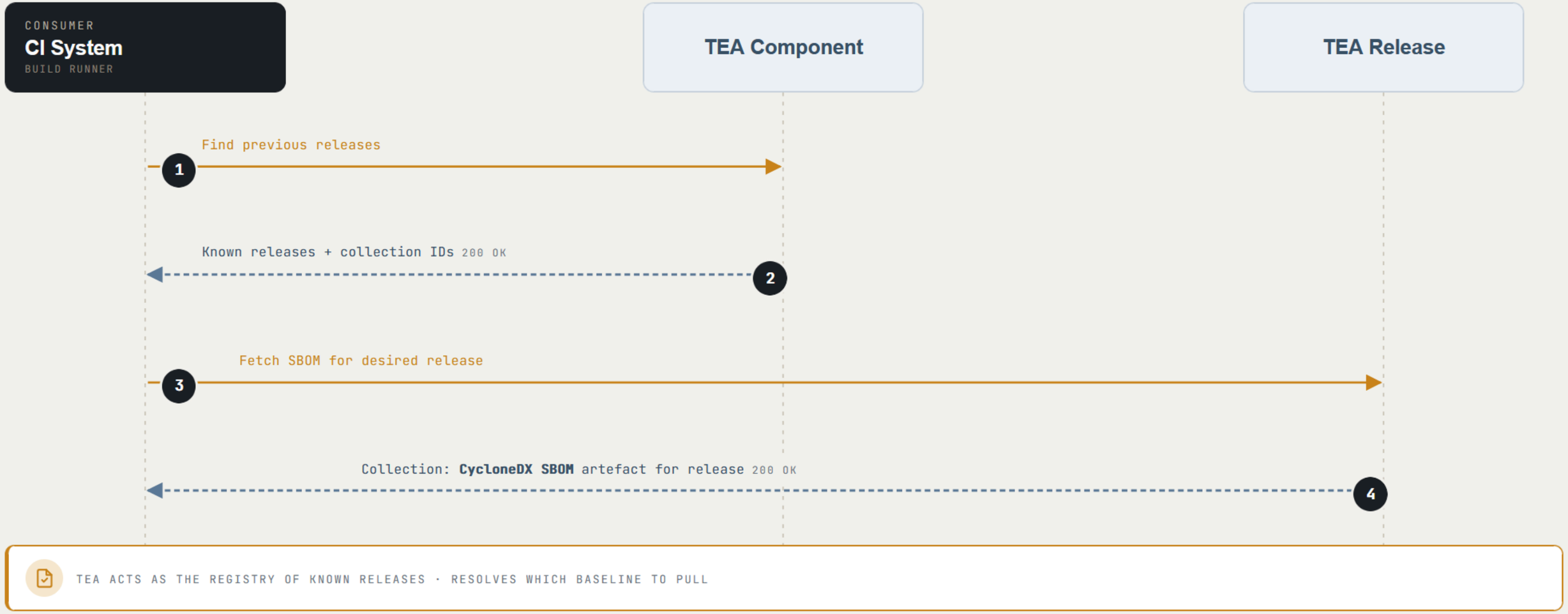


Out of Cadence Dependency Change becomes a Signal

What to Diff Against?

https://github.com/CycloneDX/transparency-exchange-api/

TEA as SBOM Registry for Diffing



OWASP GLOBAL AppSec
VIENNA'26 JUN 25-26

25 years of open source security

TEA Future: Becoming Distributed Source of Knowledge about Supply Chain

TL;DR

Generate SBOMs continuously. This handles the *vulnerable*. Diff consecutive SBOMs, and treat component changes as a Signal to investigate the *malicious*.

References

- https://www.cs.cmu.edu/~rdriley/487/papers/Thompson_1984_ReflectionsonTrustingTrust.pdf
- https://www.youtube.com/watch?v=GXdHoxDgAYI
- https://github.com/jeremylong/malicious-dependencies
- https://github.com/relizaio/sbom-diffing-resources
- https://github.com/CycloneDX/transparency-exchange-api
- https://github.com/cdxgen/cdxgen
- https://github.com/anchore/syft
- https://github.com/aquasecurity/trivy
- https://github.com/sbom-tool/sbom-tools
- https://github.com/anthonyharrison/sbomdiff
- https://github.com/CycloneDX/cyclonedx-cli
- https://github.com/CycloneDX/sbom-utility
- https://github.com/relizaio/rearm
- https://github.com/jqlang/jq
- https://github.com/DependencyTrack/dependency-track/

OWASP GLOBAL AppSec

VIENNA'26 JUN 25-26

25 years of open source security

THANK YOU!