



# DEPENDENCY-TRACK COMMUNITY MEETING

DECEMBER  
2024

THE DEPENDENCY-TRACK TEAM

[www.owasp.org](https://www.owasp.org)

Dependency-Track Community Meeting - December 2024

# Organizational

- Community Meetings are recorded and [uploaded to YouTube](#)
- Slides will be published in the [DependencyTrack/community](#) repository
- Please use the Zoom chat to ask questions during the presentation
- There will be an open Q&A section towards the end

# AGENDA

---

Community outreach

01

v4.12.x bugfix releases

02

v4.13 update

03

Q&A

04



# Community Outreach



COMMUNITY OUTREACH

# KoalaCon



  
OWASP TRANSPARENCY EXCHANGE API

**OWASP Transparency  
Exchange API  
Overview**

oej wg 2024-11-15 v2.0  
Olle E Johansson - oej@edvina.net



<https://www.youtube.com/watch?v=NSzYW4WnEE>



## COMMUNITY OUTREACH

# Quarkus Insights

Quarkus Insights #188: CycloneDX SBOMs with Quarkus and OWASP DependencyTrack

```
[INFO] io.smallrye.config:smallrye-config-core:3.10.2 (compile)
[INFO]   org.eclipse.microprofile.config:microprofile-config-api:3.1 (compile)
[INFO]   io.smallrye.common:smallrye-common-classloader:2.8.0 (compile)
[INFO]   io.smallrye.config:smallrye-config-common:3.10.2 (compile)
[INFO] org.jboss.logmanager:jboss-logmanager:3.1.0.Final (compile)
[INFO] io.smallrye.common:smallrye-common-constraint:2.8.0 (compile)
[INFO] io.smallrye.common:smallrye-common-cpu:2.8.0 (compile)
[INFO] io.smallrye.common:smallrye-common-expression:2.8.0 (compile)
[INFO] io.smallrye.common:smallrye-common-net:2.8.0 (compile)
[INFO] io.smallrye.common:smallrye-common-ref:2.8.0 (compile)
[INFO] jakarta.json:jakarta.json-api:2.1.3 (compile)
[INFO] org.jboss.logging:jboss-logging-annotations:3.0.3.Final (compile)
[INFO] org.jboss.threads:jboss-threads:3.8.0.Final (compile)
[INFO]   io.smallrye.common:smallrye-common-annotation:2.8.0 (compile)
[INFO]   io.smallrye.common:smallrye-common-function:2.8.0 (compile)
[INFO] org.slf4j:slf4j-api:2.0.6 (compile)
[INFO] org.jboss.slf4j:slf4j-jboss-logmanager:2.8.0.Final (compile)
[INFO] io.quarkus:quarkus-bootstrap-runner:999-SNAPSHOT (compile)
[INFO] io.quarkus:quarkus-fs-util:0.0.10 (compile)
[INFO] org.antlr:antlr4-runtime:4.13.0 (compile)
[INFO] jakarta.persistence:jakarta.persistence-api:3.1.0 (compile)
[INFO] io.smallrye:jandex:3.2.3 (compile)
[INFO] org.hibernate.orm:hibernate-core:6.6.3.Final (compile)
[INFO]   jakarta.transaction:jakarta.transaction-api:2.0.1 (compile)
[INFO]   org.jboss.logging:jboss-logging:3.6.1.Final (compile)
[INFO]   org.hibernate.common:hibernate-commons-annotations:7.0.3.Final (compile)
[INFO] com.fasterxml:classmate:1.7.0 (runtime)
[INFO] net.bytebuddy:byte-buddy:1.14.18 (compile)
[INFO] jakarta.xml.bind:jakarta.xml.bind-api:4.0.2 (compile)
```

Alexey


@holly\_cummins @maxandersen Niklas Düster Steve Springett Alexey





<https://www.youtube.com/watch?v=NI3mE0SACPo>

## COMMUNITY OUTREACH

# Quarkus CycloneDX Extension

 QUARKUS

WHY ▾ LEARN ▾ EXTENSIONS ▾ COMMUNITY ▾ [START CODING](#)  ▾ 

[< Back to Guides](#) By Version 3.17.2 - Latest ▾

[Edit this Page](#)

## GENERATING CYCLONEDX BOMS

An SBOM (Software Bill of Material) is a manifest that describes what a given software distribution consists of in terms of components. In addition to that, it may include a lot more information such as relationships between those components, licenses, provenance, etc. SBOMs would typically be used by software security and software supply chain risk management tools to perform vulnerability and compliance related analysis.

This guide describes Quarkus SBOM generation capabilities following [CycloneDX](#) specification.

### Why Quarkus-specific tooling?

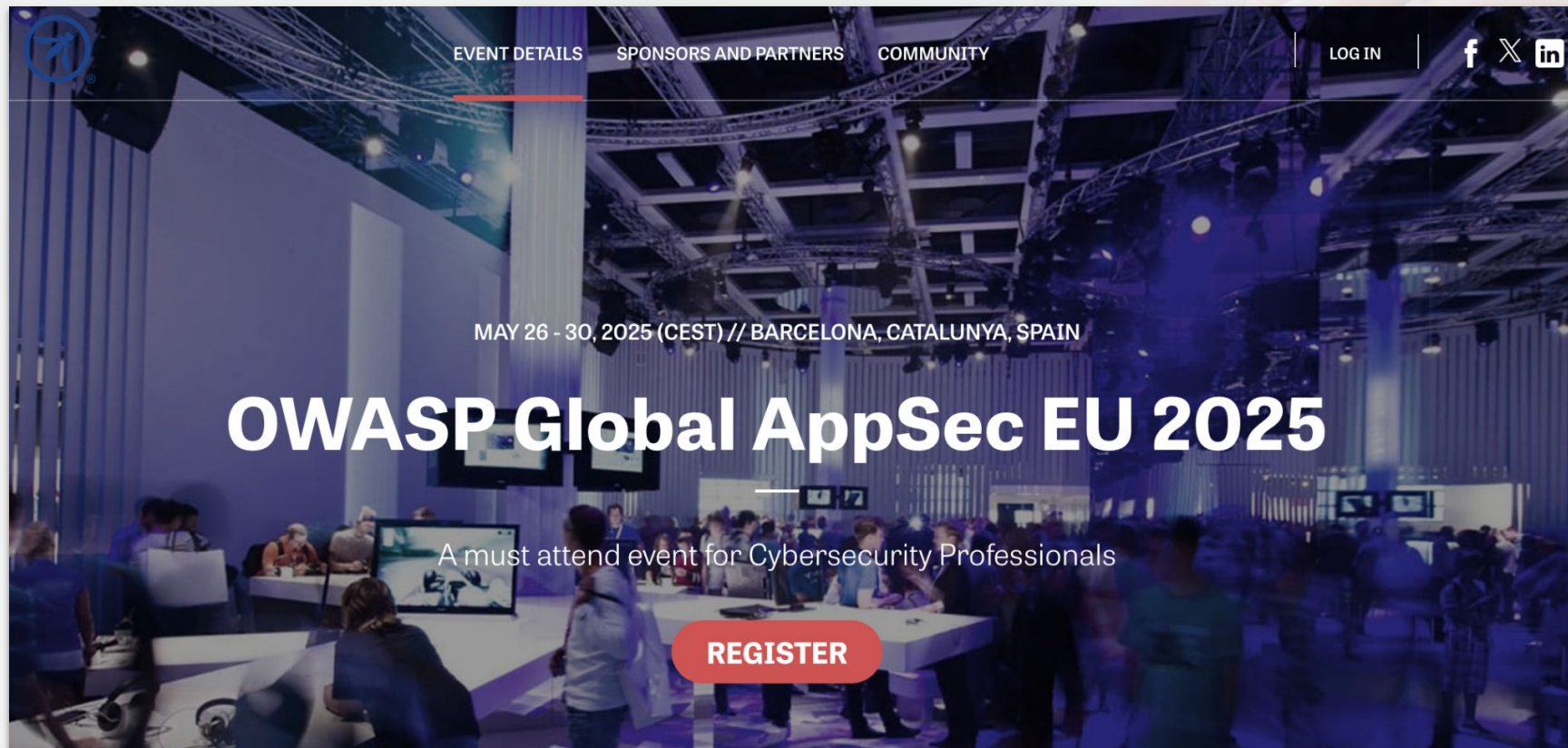
- Why Quarkus-specific tooling?
- Dependency SBOMs
  - Maven Dependency SBOMs
  - Gradle Dependency SBOMs
- Distribution SBOMs
  - Fast JAR
  - Uber JAR
  - Native image
  - Mutable JAR
- Quarkus Property Taxonomy

<https://quarkus.io/guides/cyclonedx>



COMMUNITY OUTREACH

# Hackathon @ Global AppSec Barcelona?







# v4.12.x

# Bugfix Releases



## V4.12.X BUGFIX RELEASES

# v4.12.1 & v4.12.2

---



<https://docs.dependencytrack.org/changelog/#v4-12-2>

- Resolve excessive memory usage in some recurring tasks
  - Portfolio repository metadata analysis (*aka "latest version check"*)
  - Portfolio metrics update
- Fix various inaccuracies in the Trivy integration
  - Epoch part of OS package versions not correctly submitted to Trivy server
  - Wrong name of Go packages submitted to Trivy server
- Fix missing URL encoding of tag names and vulnerability IDs in frontend
  - Tag names containing special characters broke the Tags view
  - Custom vulnerabilities with slashes couldn't be viewed
- Prevent duplicate policy violations caused by race conditions
- Fix cache issues after frontend upgrades
  - i.e. (parts of) old frontend still cached, causing various UI issues
  - Let us know if you still run into this please!
- A lot more!

V4.12.X BUGFIX RELEASES

# CVE-2024-54002

## Enumeration of managed users via /api/v1/user/login endpoint

 **Published**  **Moderate** nscurso published GHSA-9w3m-hm36-w32w 32 minutes ago · 1 comment

| Package   | Affected versions | Patched versions |
|---|-------------------|------------------|
|  <b>org.dependencytrack:dependency-track</b> (Maven) | < 4.12.2          | 4.12.2           |

nscurso opened last week · edited ▾

Description

Description

Performing a login request against the `/api/v1/user/login` endpoint with a username that exist in the system takes significantly longer than performing the same action with a username that is not known by the system.

Impact

The observable difference in request duration can be leveraged by actors to enumerate valid names of *managed* users. LDAP and OpenID Connect users are not affected.

Severity

 **Moderate** 5.3 / 10

CVSS v3 base metrics

|                     |           |
|---------------------|-----------|
| Attack vector       | Network   |
| Attack complexity   | Low       |
| Privileges required | None      |
| User interaction    | None      |
| Scope               | Unchanged |
| Confidentiality     | Low       |
| Integrity           | None      |
| Availability        | None      |

[Learn more about base metrics](#)

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVE ID

CVE-2024-54002



# v4.13 Update





# v4.13 Update

---

- Already merged
  - ORM's L2 cache disabled globally -> lower memory footprint - [apiserver/#4310](#)
  - Reduction of database operations when updating vulnerability data - [apiserver/#4359](#)
- Still planned (see last community meeting):
  - Collection projects - [apiserver/#3258](#)
  - Scheduled summary notifications - [apiserver/#3925](#)
  - Better configuration documentation - [apiserver/#3768](#)
  - First vulnerability DB improvements - [apiserver/#4122](#)
- Promising new contributions
  - Assigning of permissions to individual API keys - [Alpine/#674](#)
  - Storage of API keys in hashed format - [Alpine/#687](#)
  - New API endpoint to delete projects in bulk - [apiserver/#4383](#)



# QUESTIONS & ANSWERS

