



# DEPENDENCY-TRACK COMMUNITY MEETING

**MAY  
2024**

**THE DEPENDENCY-TRACK TEAM**

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

# AGENDA

---

Project Updates

01

Dependency-Track @ World Kinect

02

Q&A

03



# PROJECT UPDATES



## PROJECT UPDATES

# v4.11.0 Released 🎉

- 25 Contributors (Excluding Maintainers)
- Optimized BOM Ingestion
- BOM Validation<sup>1</sup>
- Global Vulnerability Audit View<sup>1</sup>
- Trivy Analyzer Integration<sup>1</sup>
- Extended UI Localization 🇩🇪 🇺🇸 🇪🇸 🇫🇷 🇮🇳 🇮🇹 🇯🇵 🇵🇱 🇵🇹 🇧🇷 🇷🇺 🇺🇦 🇨🇳
- API Key Management Improvements
- OpenAPI Spec Improvements

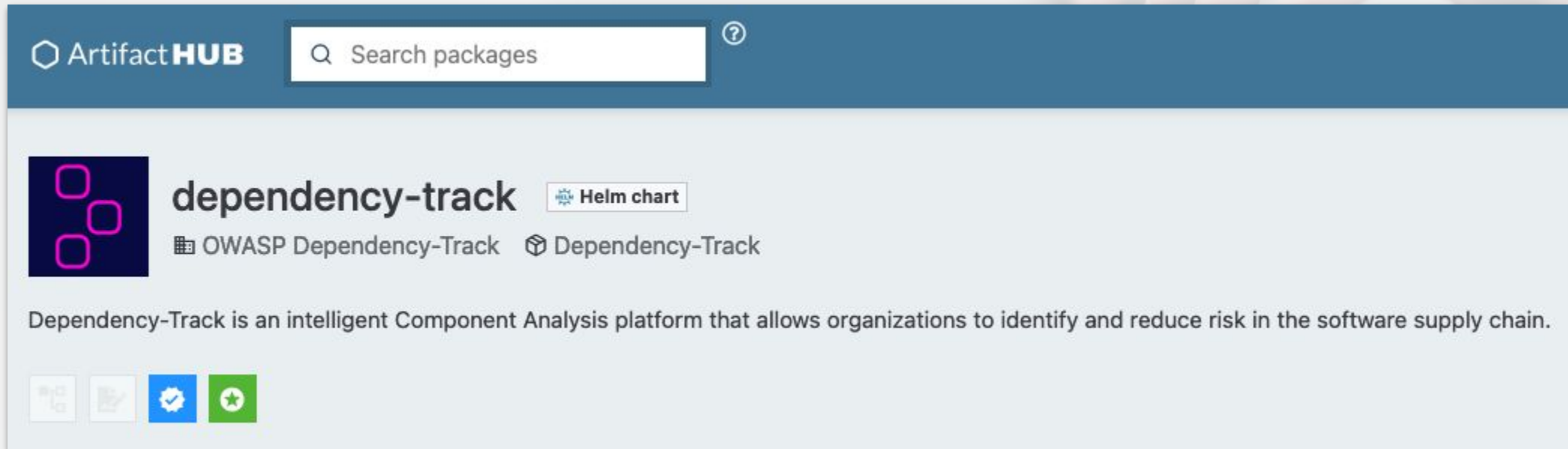


<https://docs.dependencytrack.org/changelog/>

<sup>1</sup> *Demoed in last community meeting*

PROJECT UPDATES

# Helm Chart



The screenshot shows the Artifact HUB interface. At the top is a dark blue header with the 'Artifact HUB' logo on the left and a search bar on the right containing the text 'Search packages'. Below the header, the main content area features the 'dependency-track' package. To the left of the package name is a logo consisting of three overlapping squares in shades of purple and blue. To the right of the package name is a 'Helm chart' badge. Below the package name, there are two smaller logos: 'OWASP Dependency-Track' and 'Dependency-Track'. A descriptive paragraph follows: 'Dependency-Track is an intelligent Component Analysis platform that allows organizations to identify and reduce risk in the software supply chain.' At the bottom of the package section, there are four small icons: a document, a list, a blue square with a white checkmark, and a green square with a white star.

<https://artifacthub.io/packages/helm/dependencytrack/dependency-track>

## PROJECT UPDATES

# v4.12.0 Plans

---

- Add support for Known Exploited Vulnerabilities (KEV) - [#2267](#)
  - Originally planned for v4.11, but more research and planning necessary
  - Want to support multiple data sources (CISA, VulnCheck, inTheWild.io?)
  - Interplay with EPSS?
- Update check - [#3638](#)
  - Notify users when new version(s) of Dependency-Track are available
- Support for Collection projects - [#3258](#)
  - Make use of project parent-child relationships for metrics aggregation



## PROJECT UPDATES

# v4.12.0 Plans

---

- Full upgrade to Java 21 – [#3682](#) ✓
  - Container images already ship with Java 21 runtime since v4.10
- Planning not 100% complete
- Plenty of pending PRs to review and merge

## PROJECT UPDATES

# Project Hyades

- Main objective is still to reach GA – See GA Roadmap [#860](#)
- Current focuses:
  - Configuration management across multiple services / instances
  - Docs, docs, docs. Configuration, Operations, Development, ...
  - Improving Developer Experience to make contributing easier
  - Porting of changes from v4.11.0 🤖



## PROJECT UPDATES

# For Contributors

---

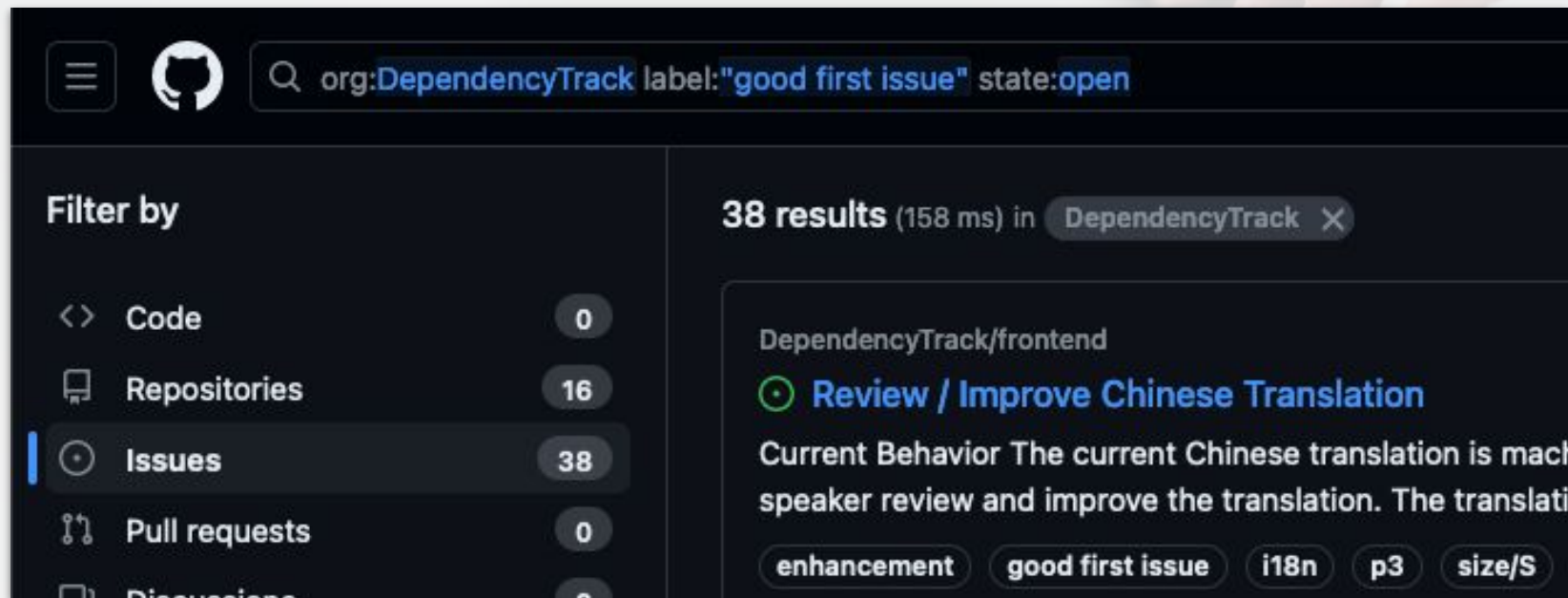
- Can now request *feature branches* from maintainers
- Naming pattern: feature-<something>
- Container images pushed to Docker Hub (docker.io)
- Easier to get early community feedback



<https://github.com/DependencyTrack/dependency-track/blob/master/DEVELOPING.md#feature-branches>

PROJECT UPDATES

# For New Contributors



<https://github.com/search?q=org%3ADependencyTrack%20label%3A%22good%20first%20issue%22%20is%3Aopen&type=issues>

PROJECT UPDATES

# Contributor Spotlight



**Marlon Pina Tojal**

fnxpt



**Adam Setch**

setchy



# DEPENDENCY-TRACK @ WORLD KINECT





# QUESTIONS & ANSWERS

