OWASP®

DEPENDENCY-TRACK COMMUNITY MEETING

THE DEPENDENCY-TRACK TEAM

JUNE
2024

www.owasp.org

AGENDA

Project Updates	01
Dependency-Track @ Backbase	02
Q&A	03

PROJECT UPDATES

PROJECT UPDATES

v4.11.1, v4.11.2, v4.11.3 Released 🎉

- v4.11.0:   May 7th

- v4.11.1:   May 19th

- v4.11.2:   June 1st

- v4.11.3:   June 3rd

- Various bugfixes backported from the in-progress v4.12.0

- Translation improvements for Japanese 🇯🇵 and French 🇫🇷

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

v4.12.0 - Notable Changes So Far

- Java 21 baseline
  - Affects users deploying the *executable WAR*, or building custom container images
- Swagger 2 → OpenAPI v3
  - `/api/swagger.json` → `/api/openapi.yaml`, `/api/openapi.json`
- Java EE → Jakarta EE 10
  - Only relevant when deploying DT as WAR into application servers (e.g. Tomcat)
- Default to BOM Processing V2
  - BOM Processing V1 is <u>removed</u>
  - Reminder: V2 can be enabled in DT v4.11 via *Administration → Experimental*
- Support for import of CycloneDX v1.6 BOMs

Project Hyades

- Helm chart being migrated to DependencyTrack/helm-charts

- Still porting changes from DT v4.x
  - Thanks Caroline (leec94) for helping! 🙏

ADOPTERS.md

Adopters

This is a list of organizations that have spoken publicly about their adoption or production users that have added themselves (in alphabetical order):

- [Coming Soon]

This is a list of adopters in early stages of production or pre-production (in alphabetical order):
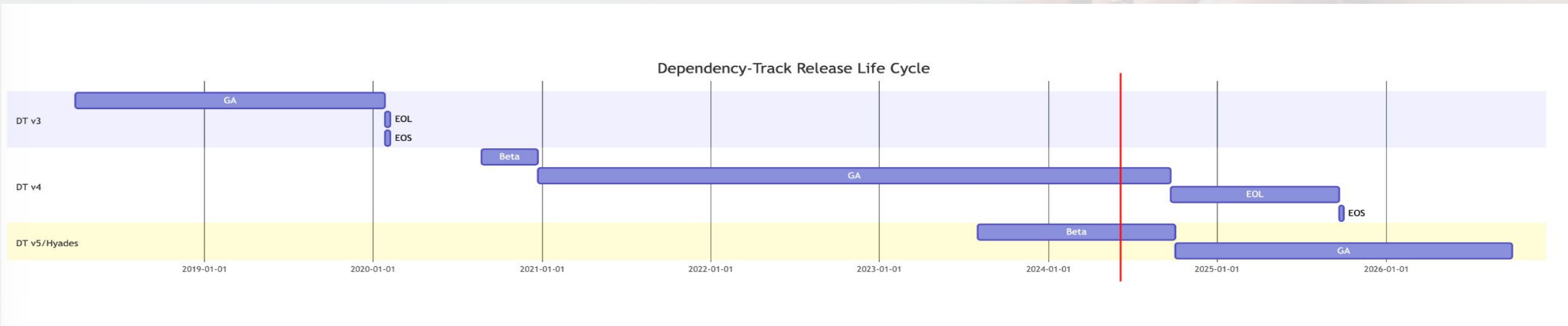
- Apex Fintech Solutions has integrated OWASP Dependency-Track into their CI/CD pipeline as part of the DevSecOps program. This integration allows for the upload of SBOMs (Software Bill of Materials) to the platform for comprehensive component analysis and a detailed understanding of the software inventory used in software applications. By analyzing the components in our monorepo, we enhance our vulnerability management program and gain valuable insights into transitive dependencies, which traditional SCA (Software Composition Analysis) tools often overlook.

If you have adopted OWASP Depenency Track and would like to be included in this list, feel free to submit a PR updating this file or open an issue.

https://github.com/DependencyTrack/dependency-track/blob/master/ADOPTERS.md

Future of Dependency-Track

Dependency-Track Release Life Cycle

*The dates are not finalised yet.

EOL (End Of Life)
- Community bug fixes and security patches may still be accepted during the end-of-life (EOL) phase.
- Critical bugs (Priority 1) and vulnerabilities with demonstrable impact may be addressed by the DT Team during EOL.
- Patch versions may be released periodically

| 8

QUESTIONS
& ANSWERS