OWASP DEPENDENCY-TRACK

Community Meeting
November 2025

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

Call for Guest Presentations

- Want to brag about the cool DT setup you've built?
- Want to vent about what needs improvement?
- Want to get input on DT-related designs?
- Want to propose changes?

We'd love to host you here!

Agenda

1. Past Releases: v4.13.5
2. Upcoming Releases: v4.13.6
3. Telemetry Insights
4. v5 Update
5. Guest Presentation: sbomify
6. Q&A

Past Releases

Past Releases: v4.13.5

- Released October 7th
- Fixes BOM validation issues related to SPDX license IDs
- Fixes GHSA-83g2-vgqh-mgxc (MEDIUM, CVSSv3 4.7):
  Possible disclosure of private NuGet repository credentials to api.nuget.org
- Fixes… much more!
  https://docs.dependencytrack.org/changelog/#v4-13-5

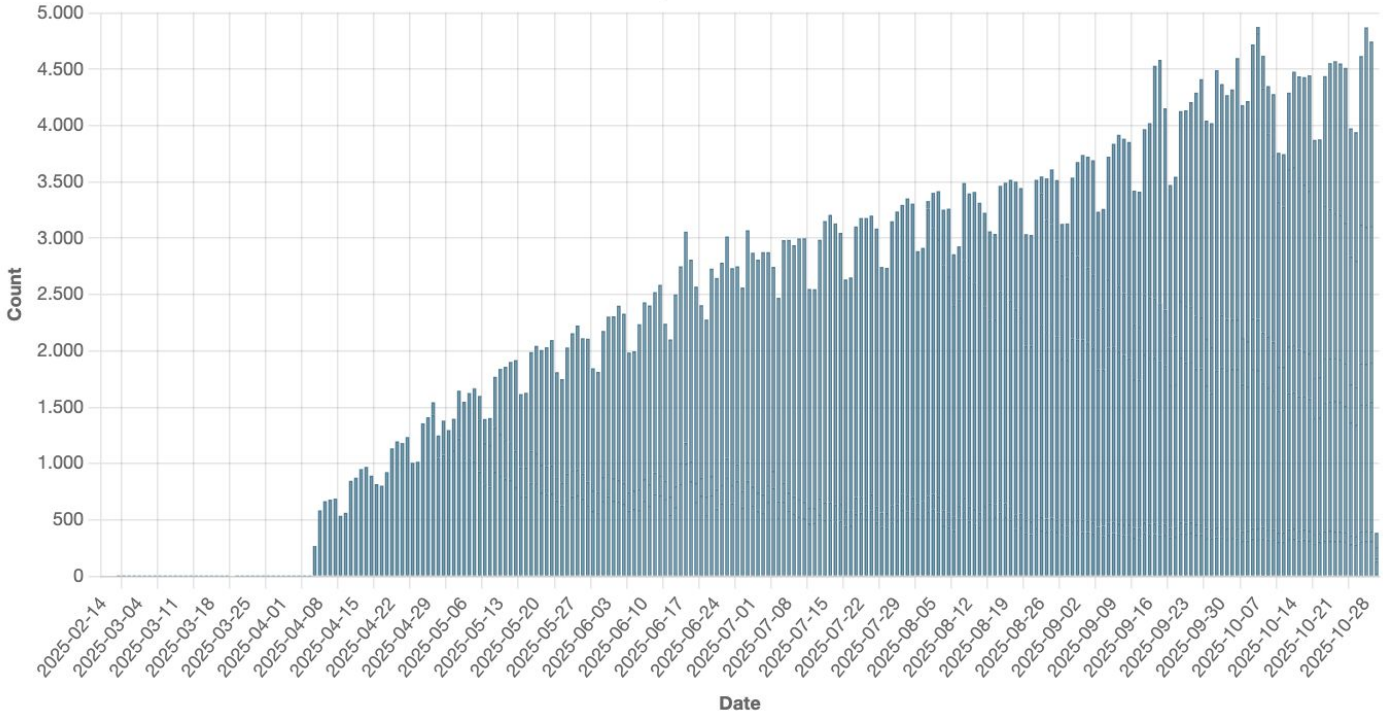
Upcoming Releases

Upcoming Releases: v4.13.6

- Fixes multiple FK constraint issues during API delete operations
- Fixes internal analyzer failing due to stale Lucene search index
  - Only applicable when fuzzy analysis is enabled (it's disabled by default)
- Fixes inefficient DB migration in v4.13.5
- Fixes a responsibly disclosed vulnerability
  - Details to be published upon release
- Aiming for release within one week

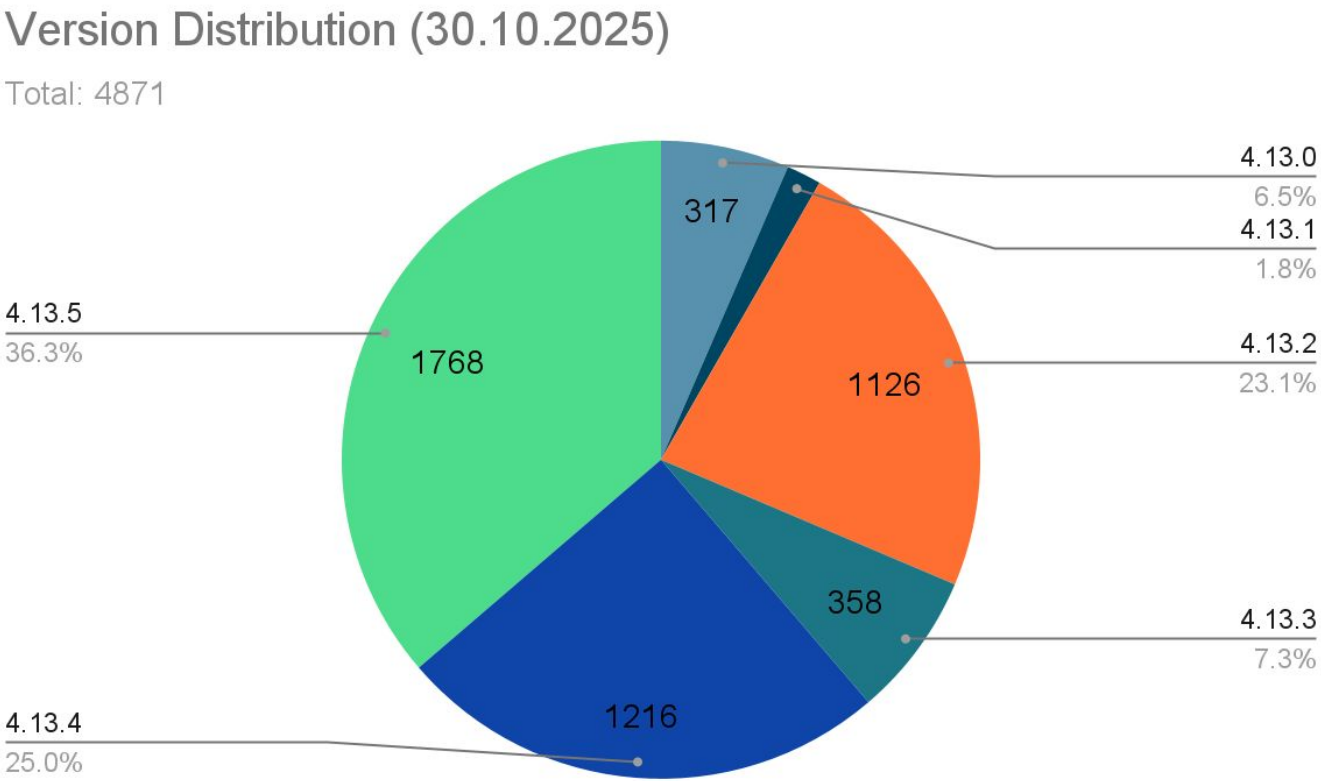
Telemetry Insights

Telemetry Insights: Unique Check-Ins



Unique daily system check-ins across stable versions (4.13.0 - 4.13.5)

Telemetry Insights: Version Distribution



Telemetry Insights: Reminder

- *What* and *how frequently* data is collected is documented
- Last sent data is viewable in admin panel
- There are multiple ways to opt out
- Collection code is public

https://docs.dependencytrack.org/getting-started/telemetry/

v5 Update

v5 Update

- Mirroring of vulnerability data sources migrated to plugin system, separate mirror-service decommissioned (ADR-010)
- More reliable notifications using the outbox pattern (ADR-011)
- Key-value store with support for optimistic concurrency control for plugins (ADR-012)
- Currently migrating notification publishers to plugin system
- Reviewing contribution to add support for CSAF advisories
- Portfolio access control being rolled out in a large deployment
  - >200k projects
  - ~3k teams

Guest Presentation:

Scaling SBOM Management with Real-World and CISA Insights

Q&A