OWASP DEPENDENCY-TRACK

Community Meeting
January 2026

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: v4.13.6
2. Upcoming Releases: v4.14.0
3. Telemetry Insights
4. v5 Update
5. Q&A

Past Releases

Past Releases: v4.13.6

- Released November 17th
- Fixes GHSA-7xvh-c266-cfr5 (MEDIUM, CVSSv3 4.8):
  Persistent Cross-Site-Scripting via welcome message
- Fixes GHSA-93r8-3g93-w2gq (MEDIUM, CVSSv3 5.4):
  Possible XML External Entity injection via validation of CycloneDX BOMs in XML format
- Adds new container image variant based on Alpine Linux
  55% smaller, fewer OS package vulnerabilities, etc.
- Fixes… much more!
  https://docs.dependencytrack.org/changelog/#v4-13-6

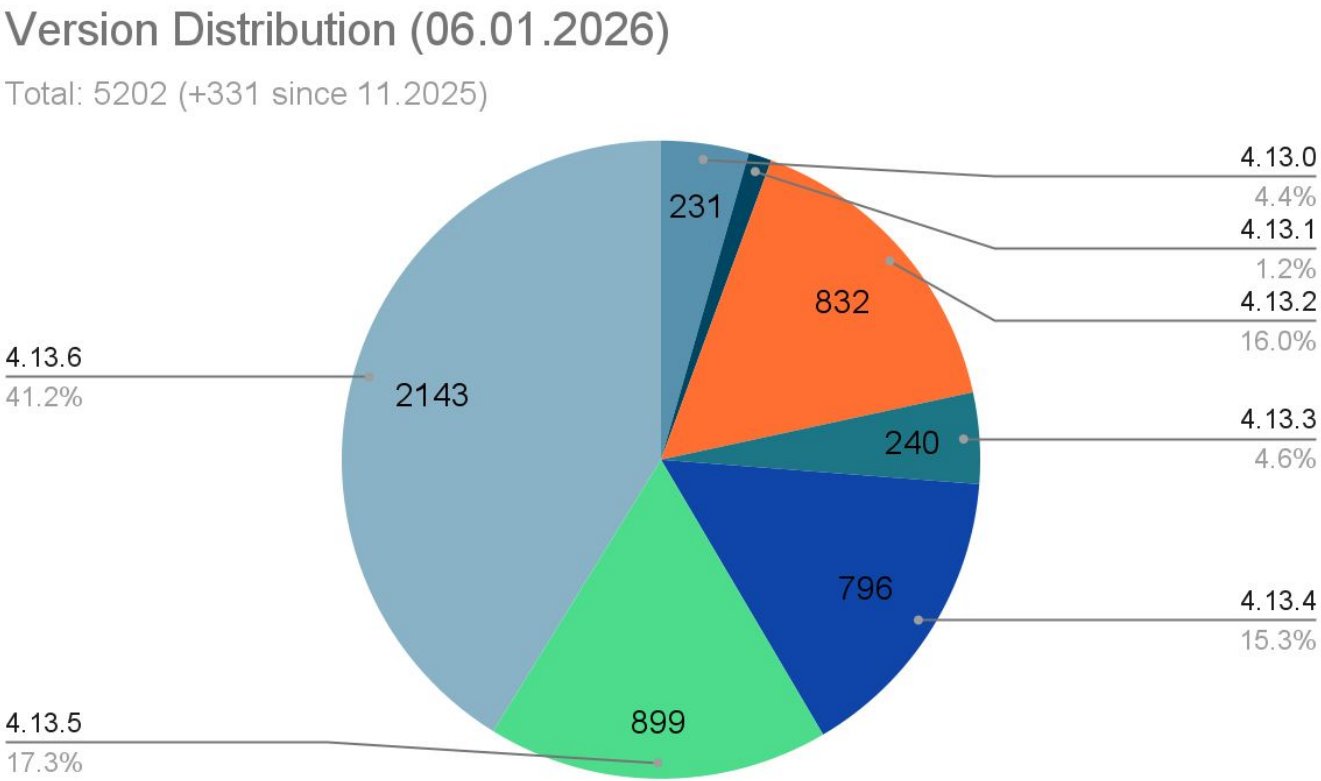
Upcoming Releases

Upcoming Releases: v4.14.0

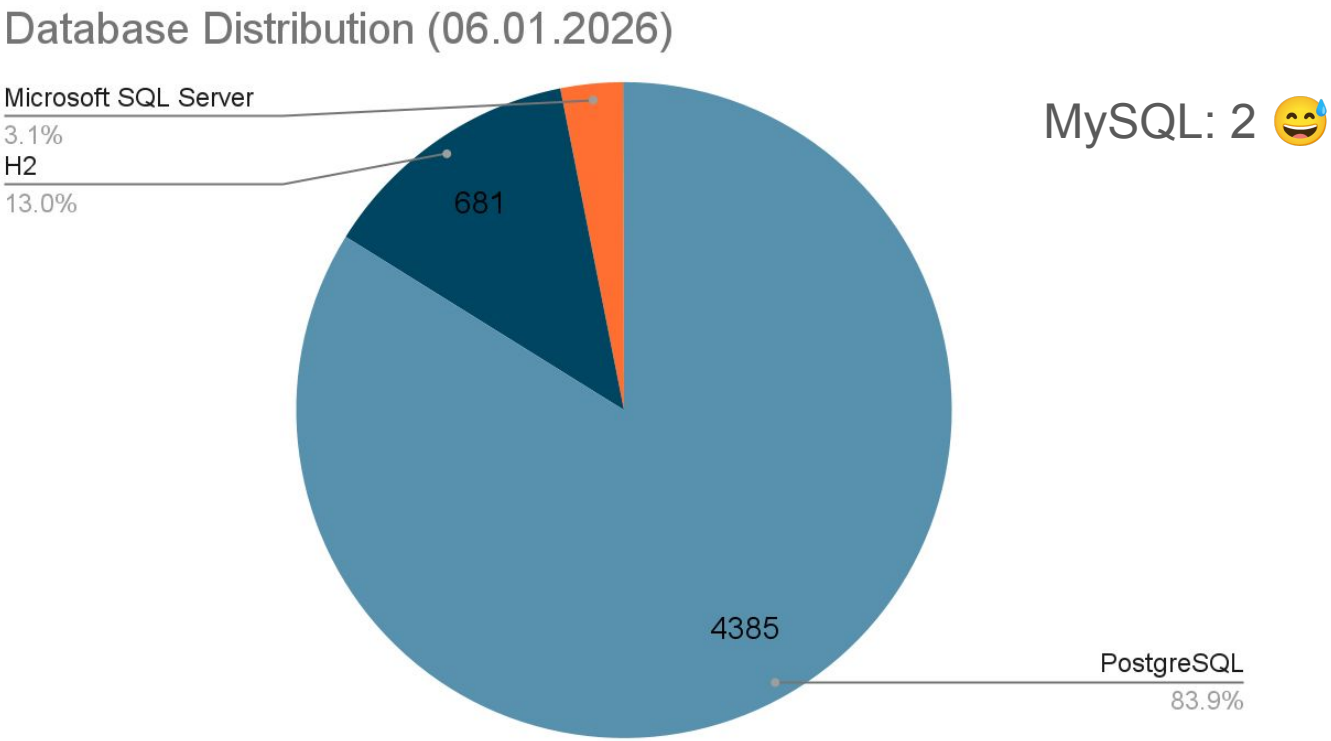
- Ecosystem-aware version comparisons
  - e.g. use *Alpine Linux'* algorithm for `pkg:apk/libformw@6.6_p20251231-r0`
  - Better accuracy for vulnerability analysis
  - More reliable version matching for policies
- Incremental OSV mirroring
- Bearer token authentication for repositories
- Support CycloneDX component scope
  - i.e., whether a component is required or optional etc.
- Support filtering by EPSS in global vulnerability audit
- … and many more minor enhancements
- To be released within next 2 weeks

Telemetry Insights

Telemetry Insights



Telemetry Insights



Telemetry Insights: Reminder

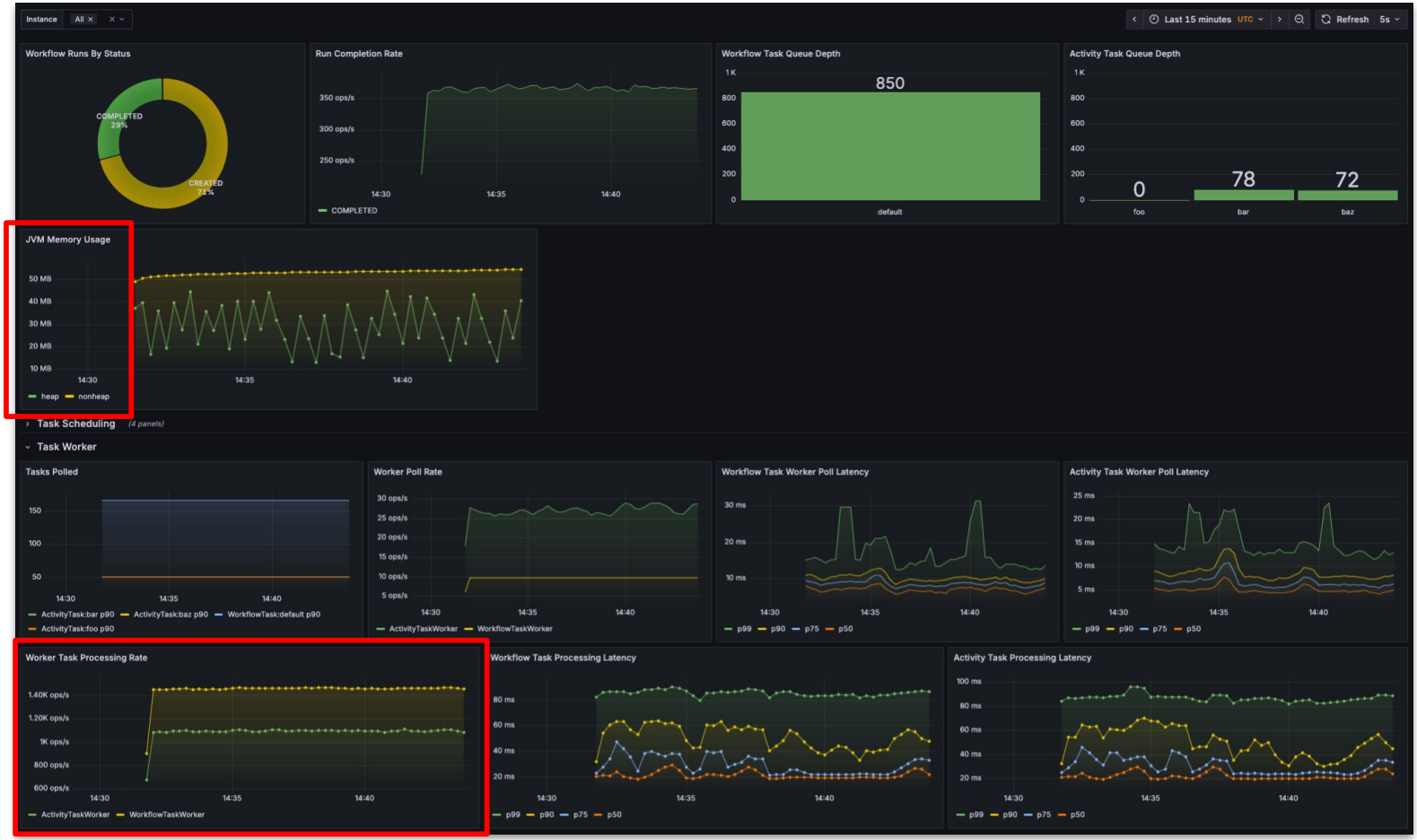
- *What* and *how frequently* data is collected is documented
- Last sent data is viewable in admin panel
- There are multiple ways to opt out
- Collection code is public

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

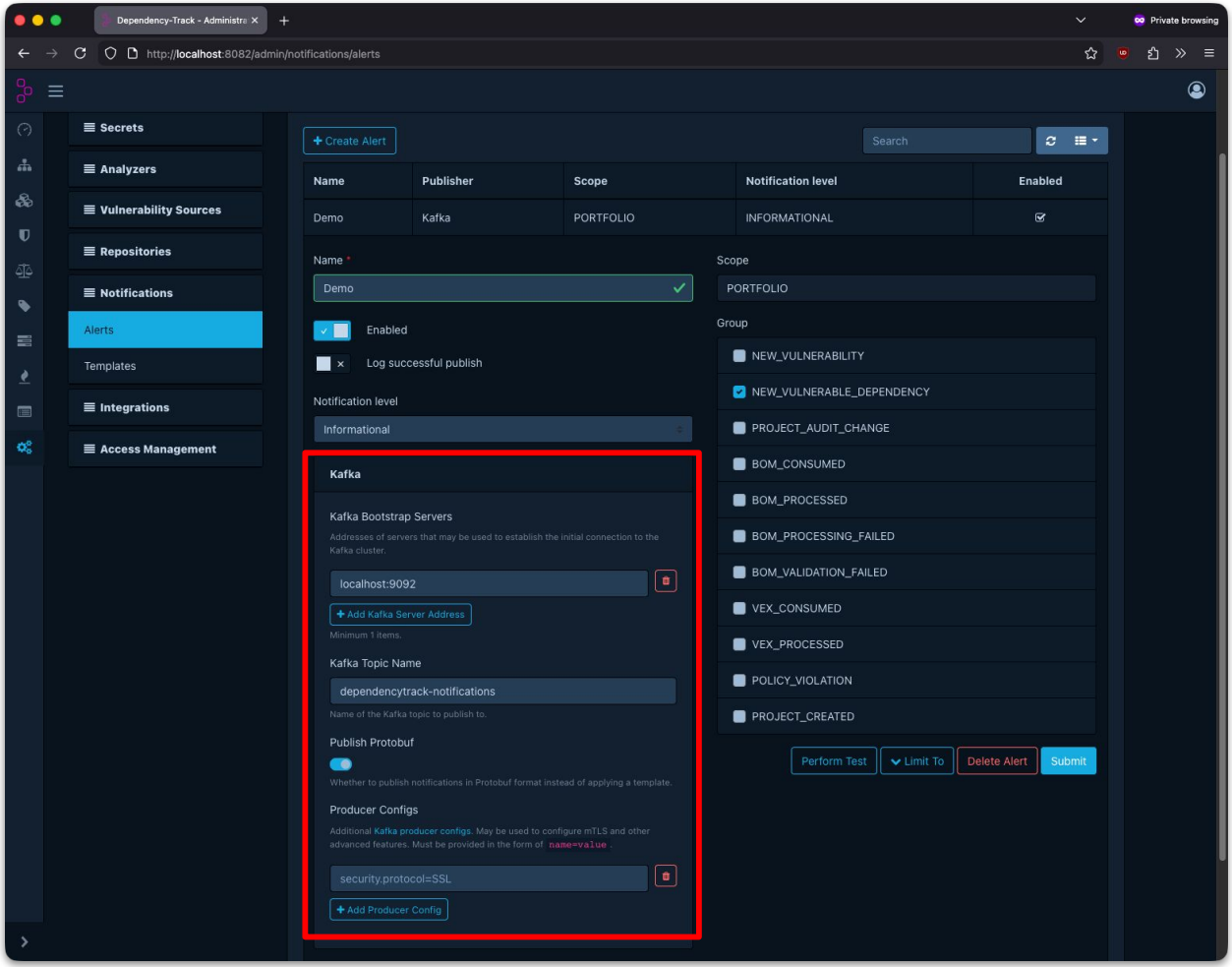
v5 Update

v5 Update

- Progressing with Kafka dependency removal
  - Durable execution engine merged
    - https://github.com/DependencyTrack/hyades-apiserver/pull/1138
    - https://github.com/DependencyTrack/hyades-apiserver/pull/1607
    - https://github.com/DependencyTrack/hyades-apiserver/tree/main/dex
  - Notification publishing being migrated to durable execution
    - https://github.com/DependencyTrack/hyades-apiserver/pull/1489
    - https://github.com/DependencyTrack/hyades-apiserver/pull/1624
    - Separate notification-publisher service being decommissioned
    - ~90% completed
  - Next: vulnerability-analyzer migration

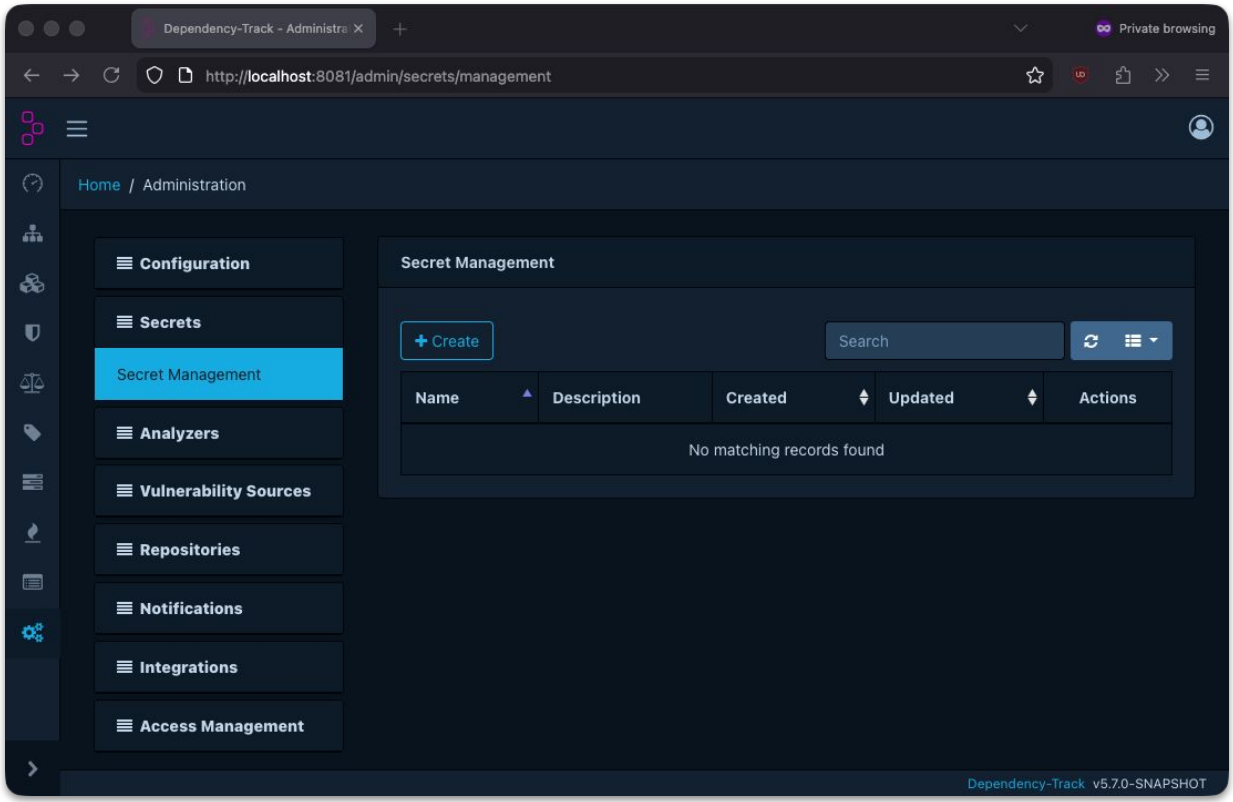


Metrics of a demo application processing 1 million workflows, each consisting of 3 steps ("activities").
https://github.com/DependencyTrack/hyades-apiserver/tree/main/dex/benchmark

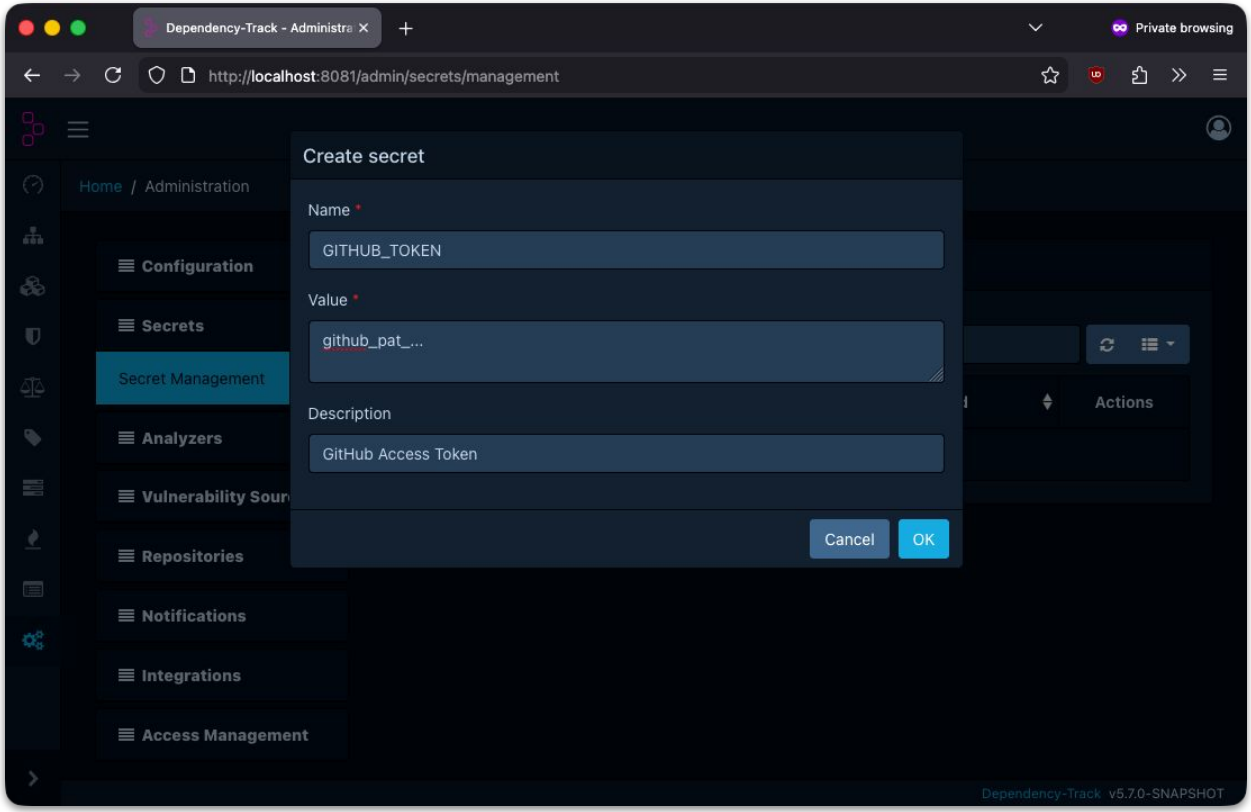


Publishing notifications to Kafka is still possible, it just needs to be configured on a per-alert basis.

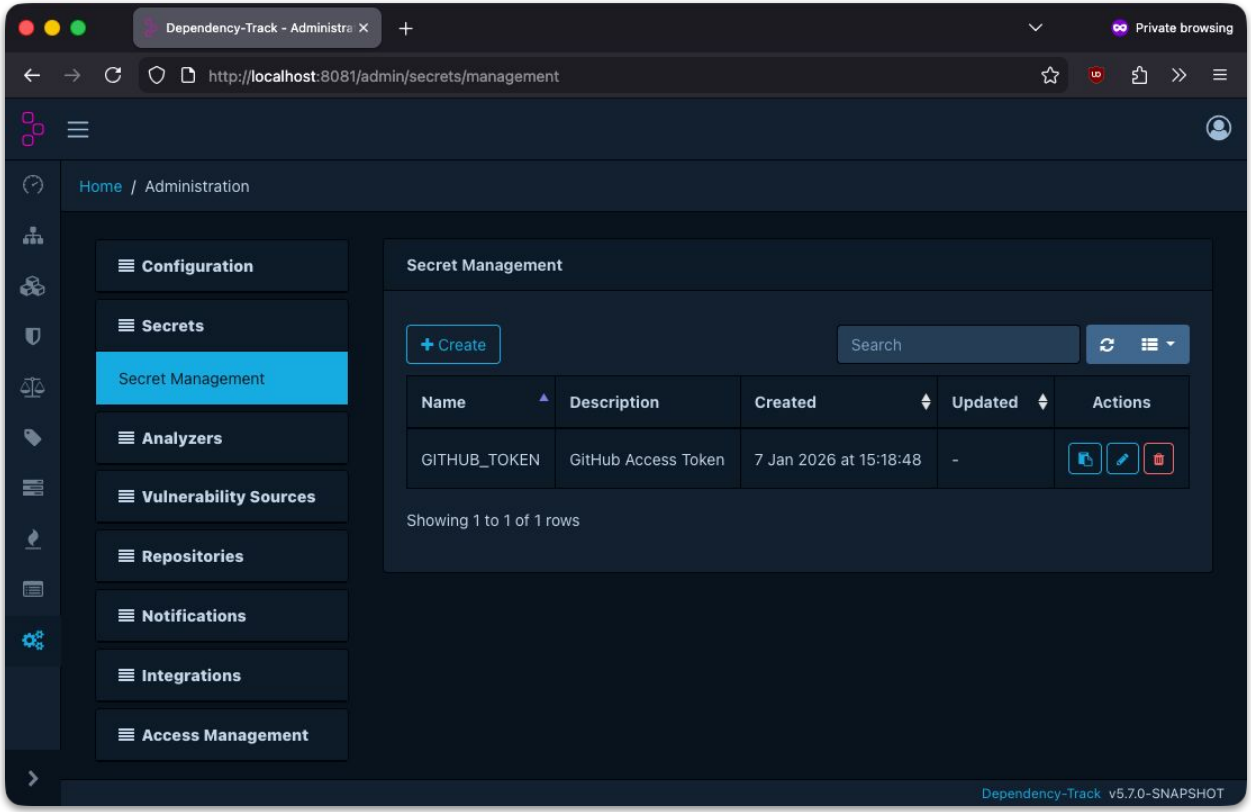
v5 Update: Secret Management



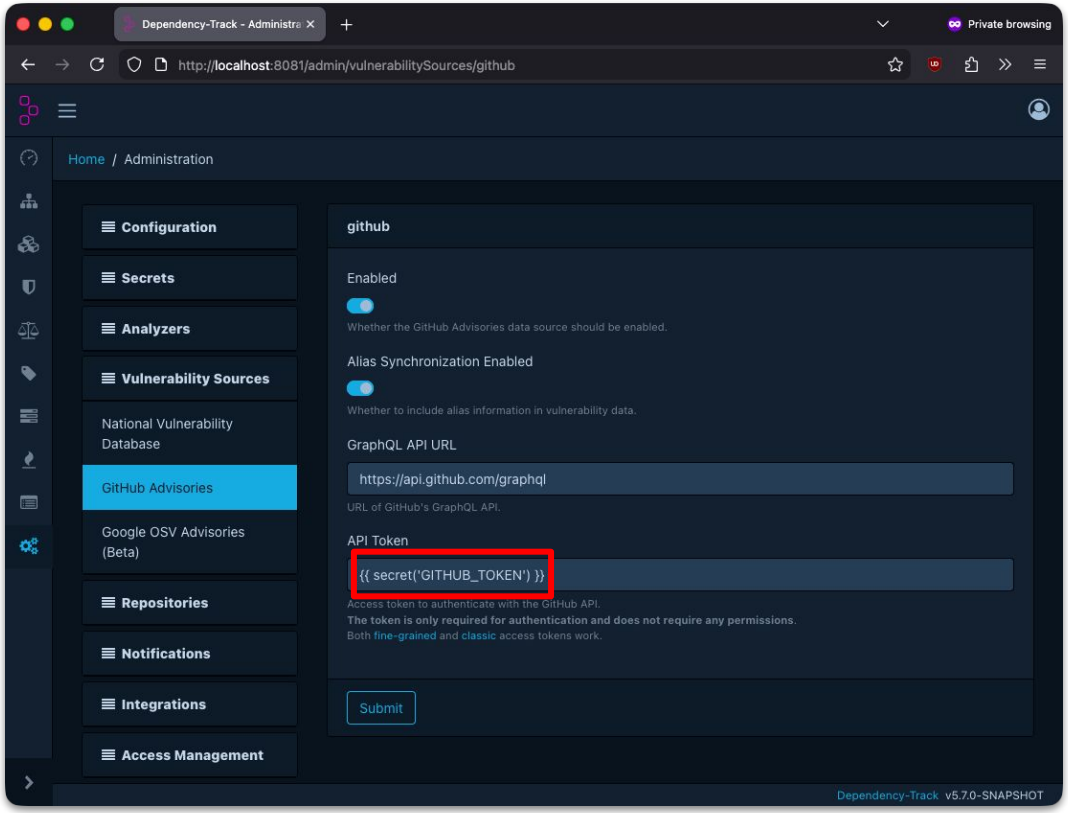
v5 Update: Secret Management



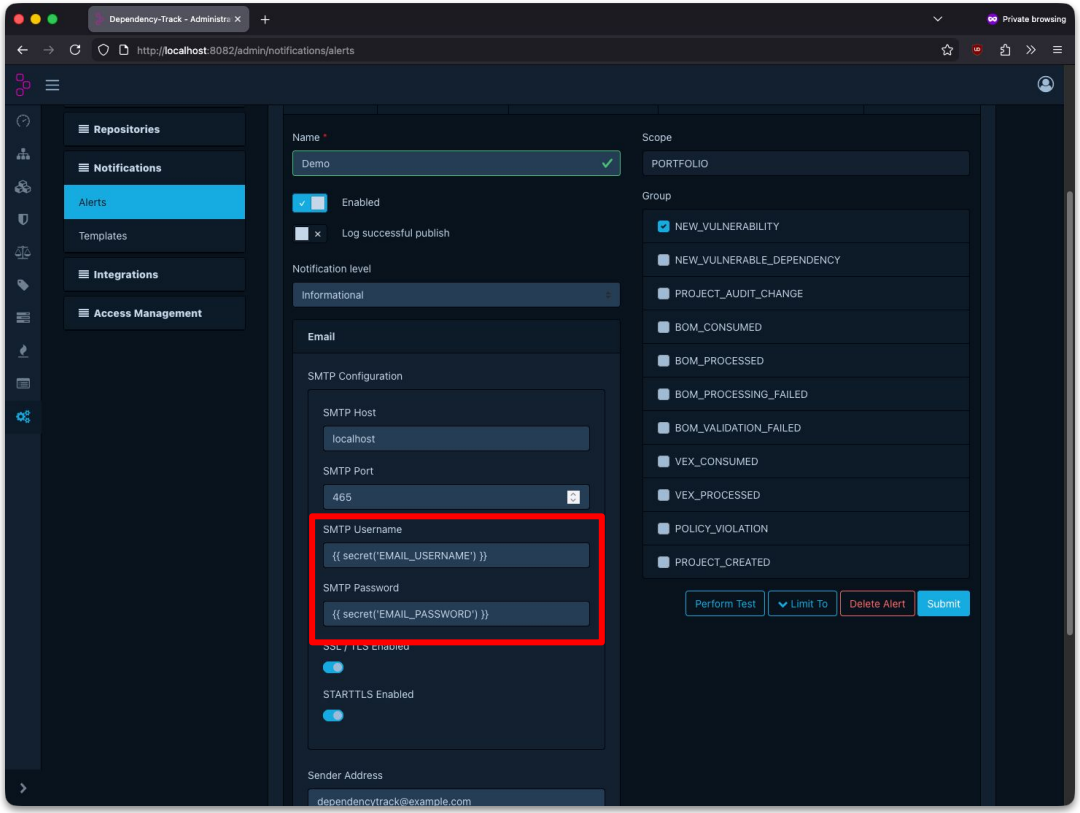
v5 Update: Secret Management



v5 Update: Secret Management



v5 Update: Secret Management



v5 Update: Secret Management

- Supports multiple “providers”
  - Currently: database and environment variables
  - Future: AWS Secret Manager, HashiCorp Vault, …
- Database provider uses *envelope encryption* and supports *key rotation*

https://dependencytrack.github.io/hyades/0.7.0-SNAPSHOT/usage/secret-management/overview/
https://dependencytrack.github.io/hyades/0.7.0-SNAPSHOT/usage/secret-management/providers/

Q&A