

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

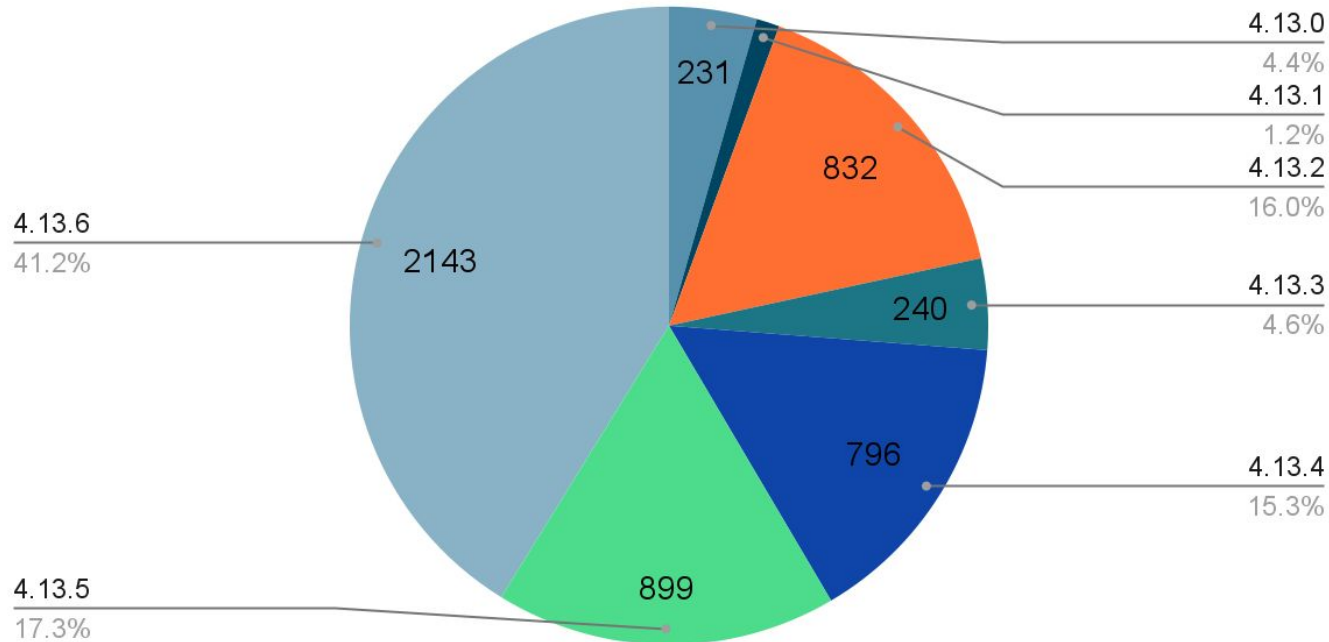
- Ecosystem-aware version comparisons
 - e.g. use *Alpine Linux*' algorithm for `pkg:apk/libformw@6.6_p20251231-r0`
 - Better accuracy for vulnerability analysis
 - More reliable version matching for policies
- Incremental OSV mirroring
- Bearer token authentication for repositories
- Support CycloneDX 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

Version Distribution (06.01.2026)

Total: 5202 (+331 since 11.2025)



Telemetry Insights

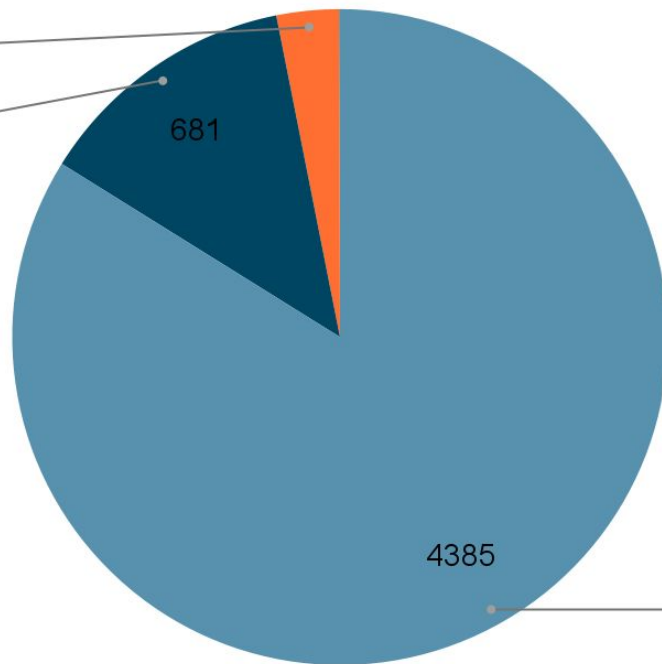
Database Distribution (06.01.2026)

Microsoft SQL Server

3.1%

H2

13.0%



MySQL: 2 🤗

Telemetry Insights: Reminder

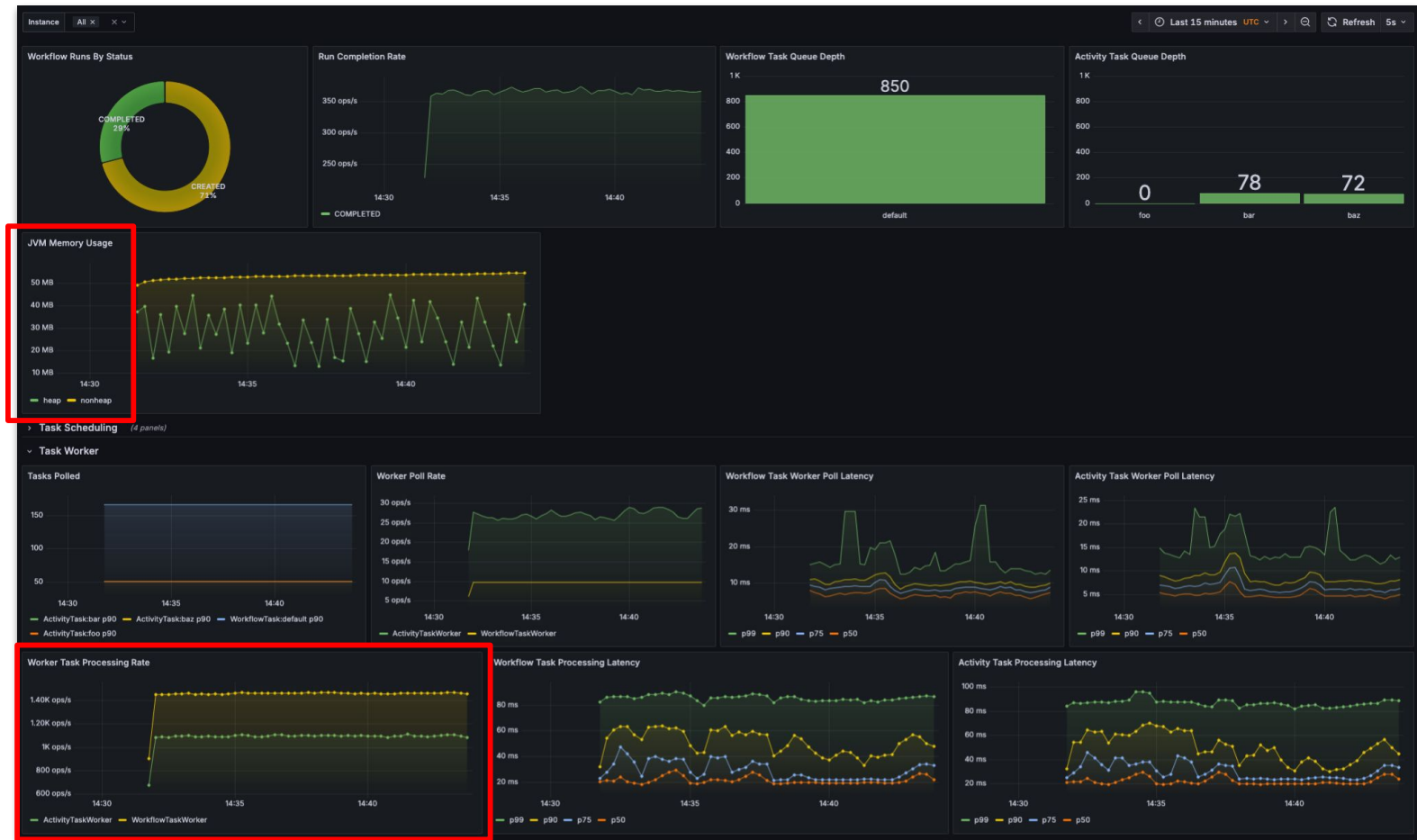
- *What and how frequently* data is collected is documented
- Last sent data is viewable in admin panel
- There are multiple ways to opt out
- Collection code is public

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

v5 Update

v5 Update

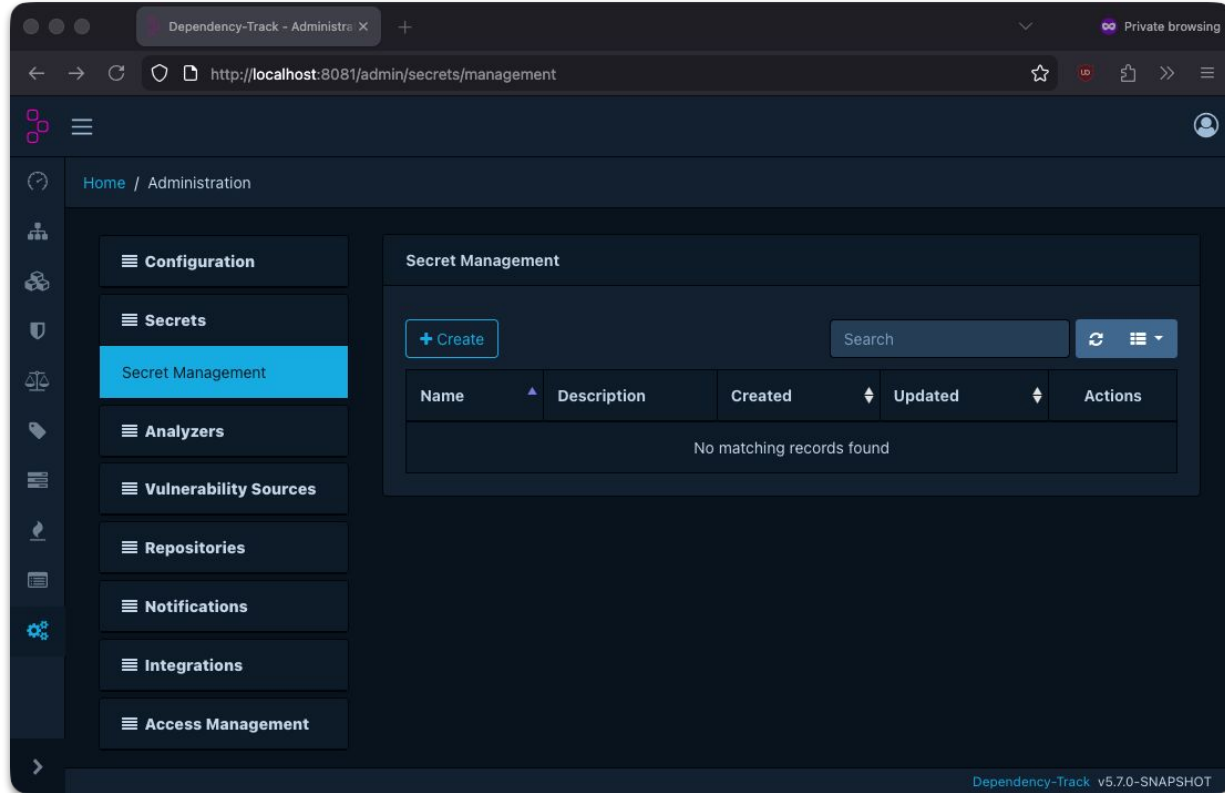
- Progressing with Kafka dependency removal
 - Durable execution engine merged
 - <https://github.com/DependencyTrack/hyades-apiserver/pull/1138>
 - <https://github.com/DependencyTrack/hyades-apiserver/pull/1607>
 - <https://github.com/DependencyTrack/hyades-apiserver/tree/main/dex>
 - Notification publishing 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



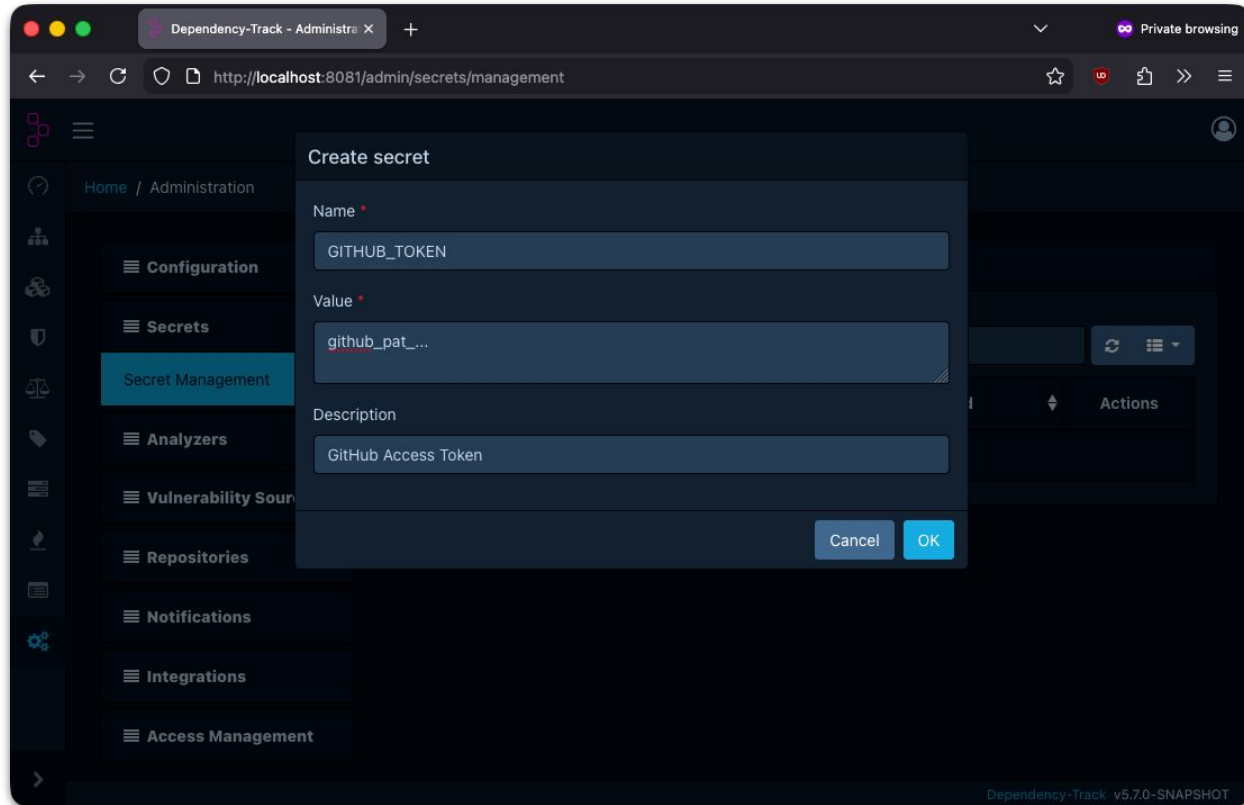
Metrics of a demo application processing 1 million workflows, each consisting of 3 steps (“activities”).

<https://github.com/DependencyTrack/hyades-apiserver/tree/main/dex/benchmark>

v5 Update: Secret Management



v5 Update: Secret Management



v5 Update: Secret Management

The screenshot displays the 'Secret Management' page in the Dependency-Track v5.7.0-SNAPSHOT web application. The browser's address bar shows the URL `http://localhost:8081/admin/secrets/management`. The left sidebar contains a navigation menu with the following items: Home, Configuration, Secrets, Secret Management (highlighted), Analyzers, Vulnerability Sources, Repositories, Notifications, Integrations, and Access Management. The main content area is titled 'Secret Management' and includes a '+ Create' button, a search bar, and a table of secrets. The table has columns for Name, Description, Created, Updated, and Actions. One secret is listed: 'GITHUB_TOKEN' with the description 'GitHub Access Token' and a creation date of '7 Jan 2026 at 15:18:48'. The Actions column for this secret contains icons for edit, update, and delete. Below the table, it states 'Showing 1 to 1 of 1 rows'. The bottom right corner of the page indicates the version 'Dependency-Track v5.7.0-SNAPSHOT'.

Home / Administration

Secret Management

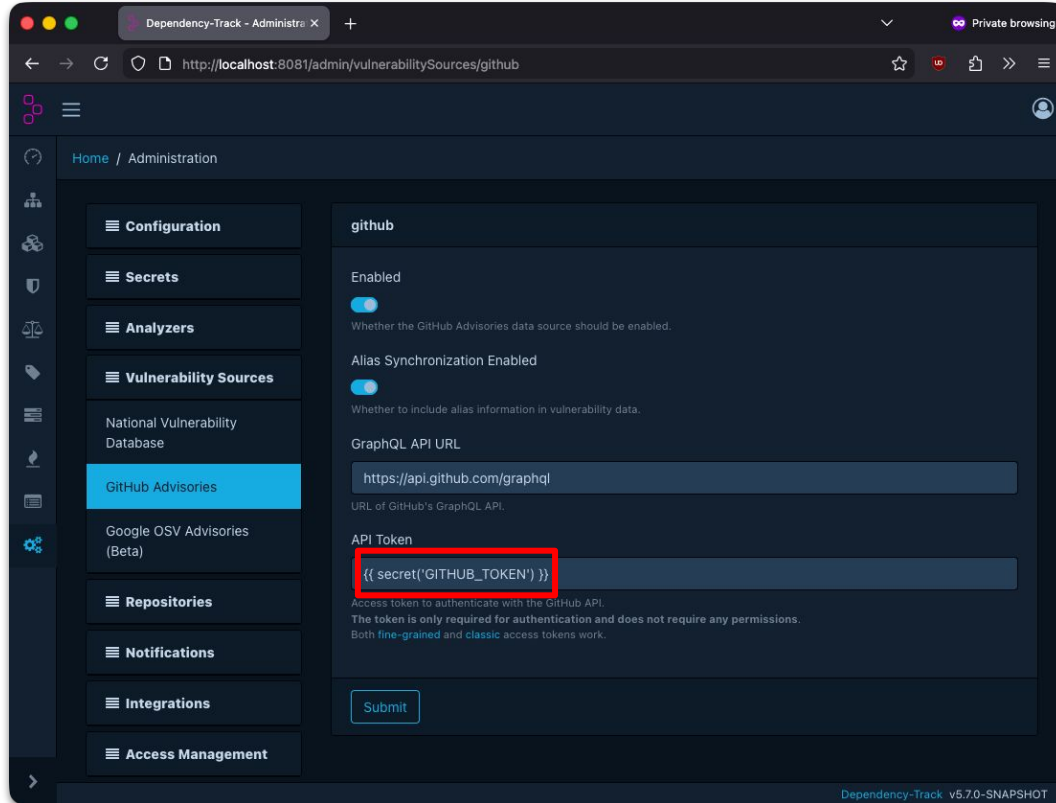
[+ Create](#)

Name	Description	Created	Updated	Actions
GITHUB_TOKEN	GitHub Access Token	7 Jan 2026 at 15:18:48	-	Edit Update Delete

Showing 1 to 1 of 1 rows

Dependency-Track v5.7.0-SNAPSHOT

v5 Update: Secret Management



v5 Update: Secret Management

The screenshot displays the Dependency-Track v5 Admin UI in a private browser window. The URL is `http://localhost:8082/admin/notifications/alerts`. The left sidebar contains navigation links: Repositories, Notifications (selected), Alerts, Templates, Integrations, and Access Management. The main content area is titled "Alerts" and shows configuration for a "Demo" alert. The "Name" field is "Demo" with a green checkmark. The "Scope" is "PORTFOLIO". The "Group" section lists various alert types, with "NEW_VULNERABILITY" selected. The "Notification level" is "Informational". The "Email" section is expanded, showing "SMTP Configuration". The "SMTP Host" is "localhost" and the "SMTP Port" is "465". The "SMTP Username" and "SMTP Password" fields are highlighted with a red box and contain the secret placeholders `{{ secret('EMAIL_USERNAME') }}` and `{{ secret('EMAIL_PASSWORD') }}` respectively. Below these fields are checkboxes for "SSL/TLS Enabled" and "STARTTLS Enabled", both of which are checked. The "Sender Address" is "dependencytrack@example.com". At the bottom right, there are buttons for "Perform Test", "Limit To", "Delete Alert", and "Submit".

Dependency-Track - Adminstr...

http://localhost:8082/admin/notifications/alerts

Repositories

Notifications

Alerts

Templates

Integrations

Access Management

Name *

Demo

Enabled

Log successful publish

Notification level

Informational

Email

SMTP Configuration

SMTP Host

localhost

SMTP Port

465

SMTP Username

{{ secret('EMAIL_USERNAME') }}

SMTP Password

{{ secret('EMAIL_PASSWORD') }}

SSL/TLS Enabled

STARTTLS Enabled

Sender Address

dependencytrack@example.com

Scope

PORTFOLIO

Group

NEW_VULNERABILITY

NEW_VULNERABLE_DEPENDENCY

PROJECT_AUDIT_CHANGE

BOM_CONSUMED

BOM_PROCESSED

BOM_PROCESSING_FAILED

BOM_VALIDATION_FAILED

VEX_CONSUMED

VEX_PROCESSED

POLICY_VIOLATION

PROJECT_CREATED

Perform Test

Limit To

Delete Alert

Submit

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