

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

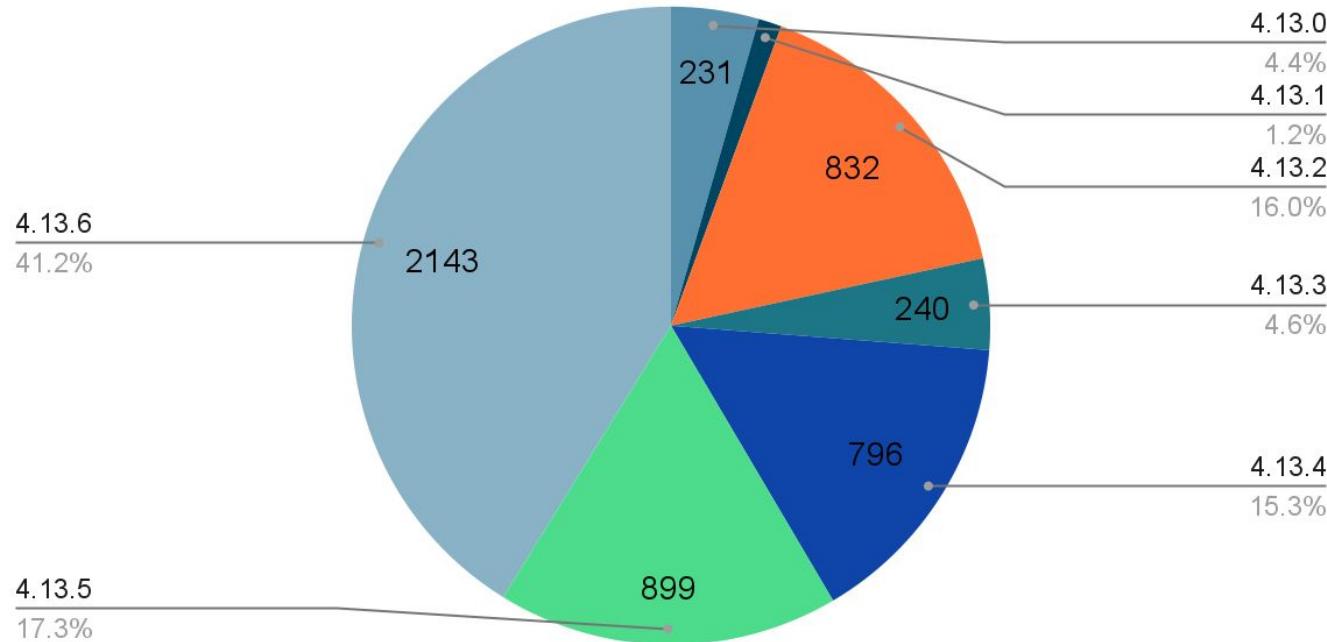
- Ecosystem-aware version comparisons
 - e.g. use *Alpine Linux*' algorithm for pkg :apk/libformw@6.6_p20251231-r0
 - Better accuracy for vulnerability analysis
 - More reliable version matching for policies
- Incremental OSV mirroring
- Bearer token authentication for repositories
- Support CycloneDX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

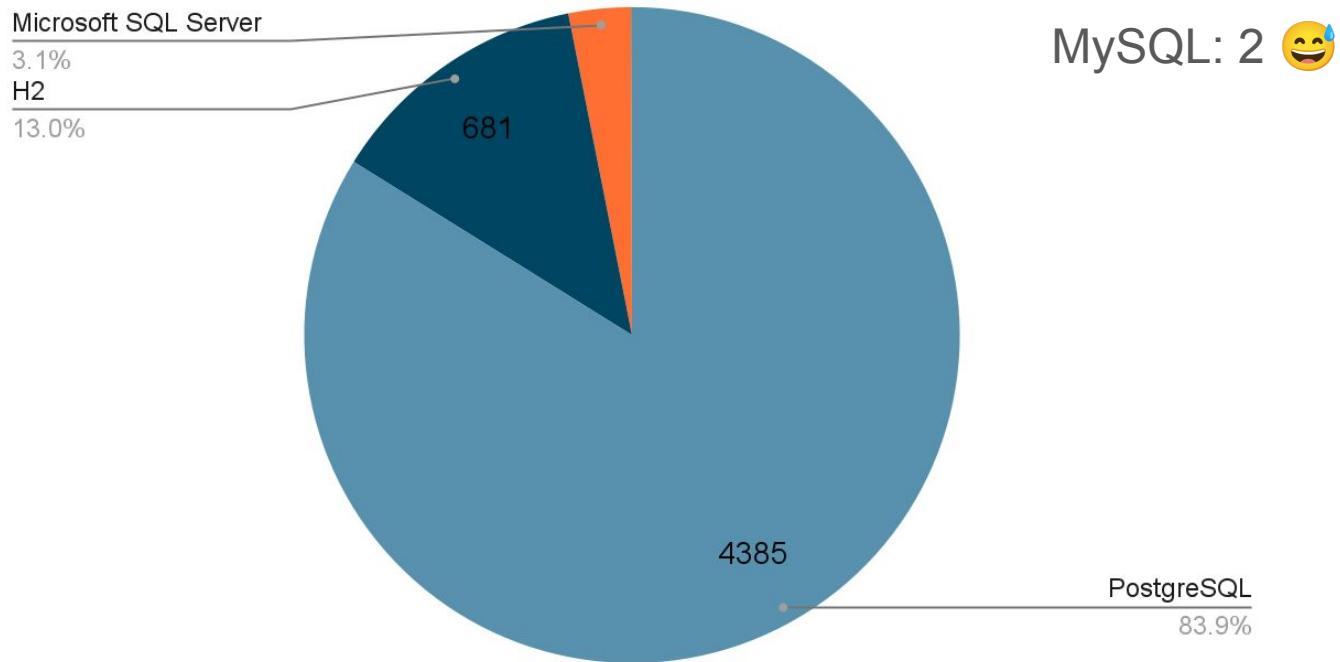
Version Distribution (06.01.2026)

Total: 5202 (+331 since 11.2025)



Telemetry Insights

Database Distribution (06.01.2026)



Telemetry Insights: Reminder

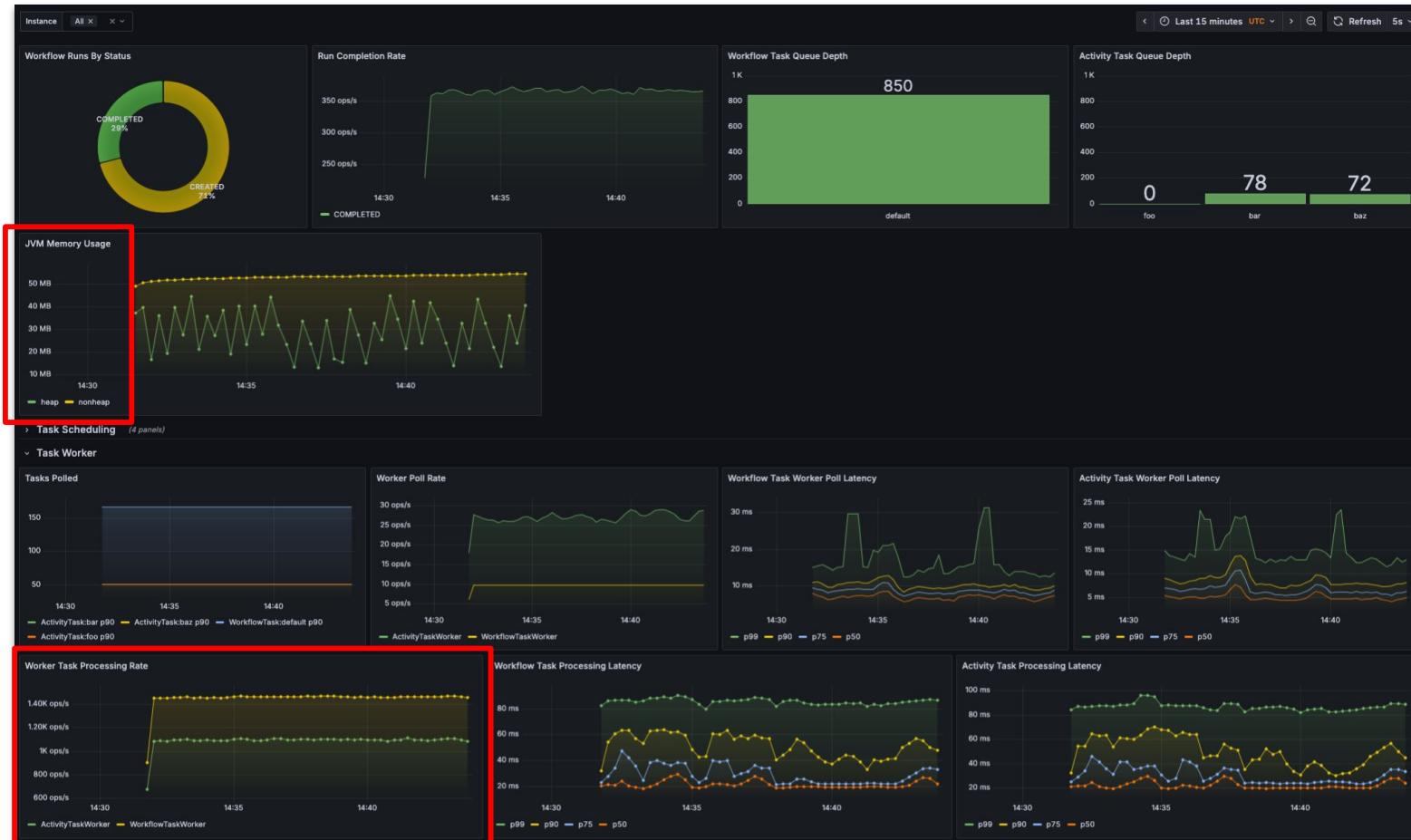
- *What and how frequently* data is collected is documented
- Last sent data is viewable in admin panel
- There are multiple ways to opt out
- Collection code is public

<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>

The screenshot shows the Dependency-Track Admin interface with the URL <http://localhost:8082/admin/notifications/alerts>. The left sidebar has a dark theme with various navigation items: Secrets, Analyzers, Vulnerability Sources, Repositories, Notifications (selected), Alerts (highlighted in blue), Templates, Integrations, and Access Management.

The main content area displays a table of alerts:

Name	Publisher	Scope	Notification level	Enabled
Demo	Kafka	PORTFOLIO	INFORMATIONAL	<input checked="" type="checkbox"/>

Below the table, there is a form for creating a new alert:

Name *: Demo (highlighted with a green checkmark)

Scope: PORTFOLIO

Group (checkboxes): NEW_VULNERABILITY (unchecked), NEW_VULNERABLE_DEPENDENCY (checked), PROJECT_AUDIT_CHANGE (unchecked), BOM_CONSUMED (unchecked), BOM_PROCESSED (unchecked), BOM_PROCESSING_FAILED (unchecked), BOM_VALIDATION_FAILED (unchecked), VEX_CONSUMED (unchecked), VEX_PROCESSED (unchecked), POLICY_VIOLATION (unchecked), PROJECT_CREATED (unchecked)

Notification level: Informational

Kafka (section highlighted with a red box):

- Kafka Bootstrap Servers**: localhost:9092
- Add Kafka Server Address** button
- Kafka Topic Name**: dependencytrack-notifications
- Publish Protobuf** checkbox (unchecked)
- Producer Configs**: security.protocol=SSL
- Add Producer Config** button

At the bottom right are buttons: Perform Test, Limit To, Delete Alert, and Submit (highlighted in blue).

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

v5 Update: Secret Management

The screenshot shows the Dependency-Track administration interface version v5.7.0-SNAPSHOT. The URL is <http://localhost:8081/admin/secrets/management>. The left sidebar has a 'Secrets' section with 'Secret Management' selected. The main panel is titled 'Secret Management' and contains a table with columns: Name, Description, Created, Updated, and Actions. A message at the bottom of the table says 'No matching records found'. The interface includes a top navigation bar with tabs and a search bar.

Dependency-Track - Administration

http://localhost:8081/admin/secrets/management

Home / Administration

Configuration

Secrets

Secret Management

Analyzers

Vulnerability Sources

Repositories

Notifications

Integrations

Access Management

Secret Management

+ Create

Search

Name Description Created Updated Actions

No matching records found

Dependency-Track v5.7.0-SNAPSHOT

v5 Update: Secret Management

The screenshot shows a web browser window for 'Dependency-Track - Administration' at the URL <http://localhost:8081/admin/secrets/management>. The browser is in 'Private browsing' mode. The left sidebar has a dark theme with various icons and navigation links, including 'Home / Administration', 'Configuration', 'Secrets' (which is currently selected), 'Analyzer', 'Vulnerability Source', 'Repositories', 'Notifications', 'Integrations', and 'Access Management'. A modal dialog titled 'Create secret' is open in the center. It contains three input fields: 'Name *' with the value 'GITHUB_TOKEN', 'Value *' with the value 'github_pat_...', and 'Description' with the value 'GitHub Access Token'. At the bottom right of the dialog are 'Cancel' and 'OK' buttons. The status bar at the bottom of the browser window displays 'Dependency-Track v5.7.0-SNAPSHOT'.

v5 Update: Secret Management

The screenshot shows the Dependency-Track administration interface with a dark theme. The left sidebar contains a navigation menu with the following items:

- Configuration
- Secrets** (selected)
- Analyzers
- Vulnerability Sources
- Repositories
- Notifications
- Integrations
- Access Management

The main content area is titled "Secret Management". It features a table with the following data:

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

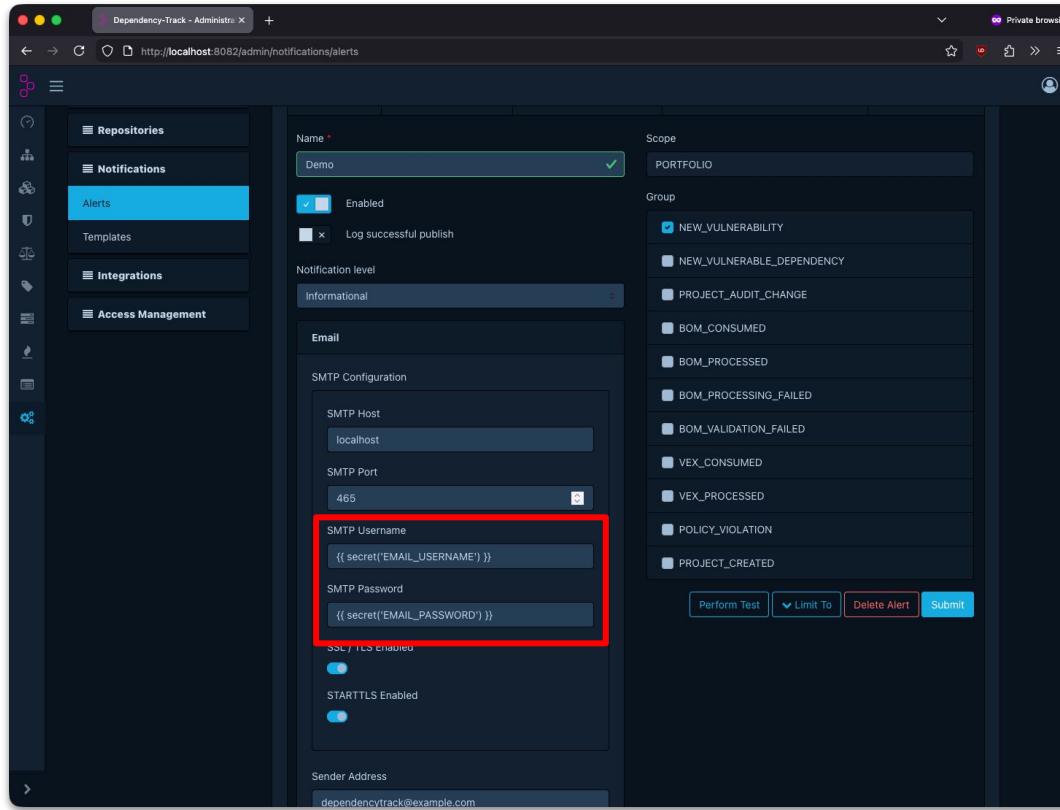
Below the table, a message states "Showing 1 to 1 of 1 rows". The browser address bar shows the URL `http://localhost:8081/admin/secrets/management`. The bottom right corner of the interface displays the version "Dependency-Track v5.7.0-SNAPSHOT".

v5 Update: Secret Management

The screenshot shows the Dependency-Track administration interface for managing GitHub Advisory secrets. The left sidebar menu includes Configuration, Secrets (selected), Analyzers, Vulnerability Sources, National Vulnerability Database, GitHub Advisories (highlighted in blue), Google OSV Advisories (Beta), Repositories, Notifications, Integrations, and Access Management. The main panel displays configuration for the GitHub source, with the "Enabled" toggle switch turned on. The "Alias Synchronization Enabled" toggle switch is also turned on. The "GraphQL API URL" field contains the value "https://api.github.com/graphql". The "API Token" field contains the placeholder code "{{ secret('GITHUB_TOKEN') }}", which is highlighted with a red box. A note below the token field states: "Access token to authenticate with the GitHub API. The token is only required for authentication and does not require any permissions. Both fine-grained and classic access tokens work." A "Submit" button is at the bottom of the form.

Dependency-Track v5.7.0-SNAPSHOT

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