

OWASP DEPENDENCY-TRACK

Community Meeting
February 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

Agenda

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

Upcoming Releases

Upcoming Releases: v4.14.0

- Me last meeting: “*To be released within next 2 weeks*” 😊
- Realised that vulnerability matching logic needs more work

Linux Distro Version Matching

- Already done: ecosystem awareness
 - `114.0.5735.106-1~deb11u1 < 114.0.5735.133-1~deb12u1` (Debian)
 - `1.0a12 < 1.0b2.post345.dev456` (Python PEP-440)
 - `1.0~rc1^git1 > 1.0~rc1` (RPM)
 - etc.
- Missing: distro release awareness 😊

Linux Distro Version Matching

Affected packages

| | | | |
|------------------------|------------------------|------------------------|------------------------|
| Debian:11 coreutils | Debian:12 coreutils | Debian:13 coreutils | Debian:14 coreutils |
|------------------------|------------------------|------------------------|------------------------|

Package

| | |
|------|---|
| Name | coreutils |
| Purl | pkg:deb/debian/coreutils?arch=source |

Affected ranges

| | |
|--------|--------------|
| Type | ECOSYSTEM |
| Events | Introduced 0 |

Affected packages as reported by OSV

“All versions”

Linux Distro Version Matching

Affected packages

| | | | |
|------------------------|------------------------|------------------------|------------------------|
| Debian:11 coreutils | Debian:12 coreutils | Debian:13 coreutils | Debian:14 coreutils |
|------------------------|------------------------|------------------------|------------------------|

Package

| | |
|------|---|
| Name | coreutils  |
| Purl | pkg:deb/debian/coreutils?arch=source |

Affected ranges 

| Type | ECOSYSTEM | |
|--------|------------|-------|
| Events | Introduced | 0 |
| | Fixed | 9.4-1 |

Affected packages as reported by OSV

Linux Distro Version Matching

- Massive over-reporting if distro release is not taken into account
- Distro release is not always part of the PURL reported by OSV
 - must be inferred from elsewhere (i.e. OSV ecosystem name)
- Distro release can be version (e.g. 13) or code name (e.g. trixie)

Linux Distro Version Matching

```
{  
    "bom-ref": "pkg:deb/debian/coreutils@9.7-3?arch=amd64&distro=debian-13.3",  
    "type": "library",  
    "supplier": {...},  
    "name": "coreutils",  
    "version": "9.7-3",  
    "licenses": [...],  
    "purl": "pkg:deb/debian/coreutils@9.7-3?arch=amd64&distro=debian-13.3"  
    "properties": [...]  
},
```

Component PURL in your BOM

Linux Distro Version Matching

```
{  
    "bom-ref": "pkg:deb/debian/coreutils@9.7-3?arch=amd64&distro=trixie",  
    "type": "library",  
    "supplier": {...},  
    "name": "coreutils",  
    "version": "9.7-3",  
    "licenses": [...],  
    "purl": "pkg:deb/debian/coreutils@9.7-3?arch=amd64&distro=trixie",  
    "properties": [...]  
}
```

Component PURL in your BOM

Linux Distro Version Matching

```
{  
    "bom-ref": "pkg:deb/debian/coreutils@9.7-3?arch=amd64&distro=13",  
    "type": "library",  
    "supplier": {...},  
    "name": "coreutils",  
    "version": "9.7-3",  
    "licenses": [...],  
    "purl": "pkg:deb/debian/coreutils@9.7-3?arch=amd64&distro=13",  
    "properties": [...]  
}
```

Component PURL in your BOM

Linux Distro Version Matching

```
{  
  "bom-ref": "pkg:deb/debian/coreutils@9.7-3",  
  "type": "library",  
  "supplier": {...  
  },  
  "name": "coreutils",  
  "version": "9.7-3",  
  "licenses": [...  
  ],  
  "purl": "pkg:deb/debian/coreutils@9.7-3", ???  
  "properties": [...  
  ]  
},
```

Component PURL in your BOM

Linux Distro Version Matching

- 13 == debian-13 == debian-13.3 == trixie
- 20.04 == 20.04:LTS == ubuntu-20.04 == focal
- etc.
- version <-> code name conversion requires external knowledge

Linux Distro Version Matching: Planned Improvements

- During OSV mirroring, add distro PURL qualifier if missing
 - e.g. Debian:13 becomes distro=debian-13
- During vulnerability analysis:
 - If component PURL **and** affected PURL have a distro qualifier, only perform version comparison if the qualifier matches
 - Apply best-effort normalization so that ubuntu-24.04 matches focal etc.
- Testing with BOMs generated by cdxgen, Syft, and Trivy
- You can help testing:

<https://github.com/DependencyTrack/dependency-track/pull/5783>

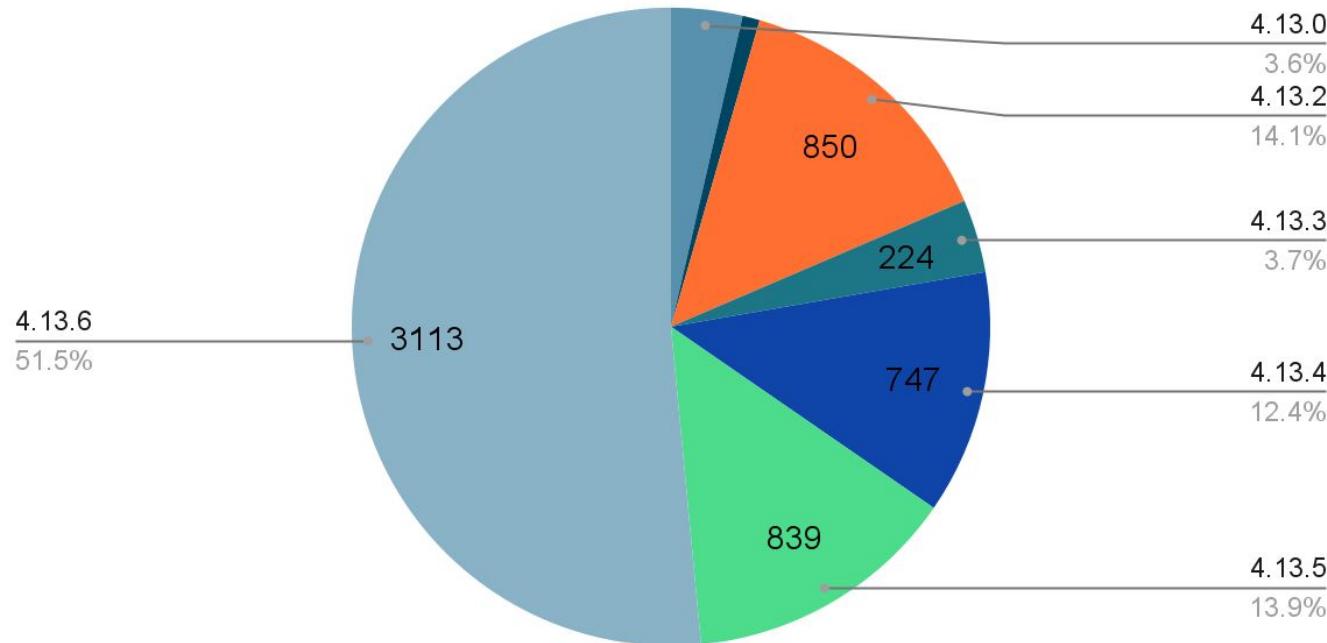


Telemetry Insights

Telemetry Insights

Version Distribution (03.02.2026)

Total: 6044 (+842 since 01.2026)



v5 Update

v5 Update

- Modified release process to support pre-releases
 - 0.7.0-alpha.1, 0.7.0-rc.2, etc.
- Released 5.7.0-alpha.0 / 0.7.0-alpha.0
- Will publish new pre-releases every 1-2 weeks
- Removed Kafka requirement from notification publishing
 - notification-publisher service decommissioned
 - New architecture documented:
<https://dependencytrack.github.io/hyades/snapshot/architecture/design/notifications/>
 - Publishing to Kafka still possible:
<https://dependencytrack.github.io/hyades/snapshot/usage/notifications/publishers/#kafka>
- Improved UX of using managed secrets
- Added ability to test integration configuration in UI

v5 Update: Viewing Workflow Runs

The screenshot shows the Dependency-Track application interface in a web browser. The title bar reads "Dependency-Track - Workflow Runs". The URL is "http://localhost:8081/admin/workflows/runs". The left sidebar has a dark theme with various icons and a list of modules: Configuration, Secrets, Analyzers, Vulnerability Sources, Repositories, Notifications, Integrations, Access Management, and Workflows. The "Workflow Runs" item under Workflows is highlighted with a blue background. The main content area is titled "Workflow Runs" and displays a table of workflow runs. The table has columns: ID, Workflow Name, Status, Created, and Completed. There are dropdown arrows next to the first four columns. The table contains five rows, each with a unique ID, the workflow name "publish-notification", a status of "Completed" indicated by a green checkmark, and a creation and completion time of "4 Feb 2026 at 07:01:06" and "4 Feb 2026 at 07:01:10". At the bottom of the table, there are navigation links for "Previous" and "Next", and a "Rows per page:" dropdown set to "5". The footer of the page says "Dependency-Track v5.7.0-alpha.1-SNAPSHOT".

| ID | Workflow Name | Status | Created | Completed |
|--------------------------------------|----------------------|-------------|------------------------|------------------------|
| 019c273d-7985-7f6e-8720-5b8af5b5c30a | publish-notification | ✓ Completed | 4 Feb 2026 at 07:01:06 | 4 Feb 2026 at 07:01:10 |
| 019c273d-7985-7e9a-add9-93263c962c99 | publish-notification | ✓ Completed | 4 Feb 2026 at 07:01:06 | 4 Feb 2026 at 07:01:10 |
| 019c273d-7985-7b37-ac6b-7ad13bac563b | publish-notification | ✓ Completed | 4 Feb 2026 at 07:01:06 | 4 Feb 2026 at 07:01:10 |
| 019c273d-7985-7aa0-98f4-02835ae2a7b9 | publish-notification | ✓ Completed | 4 Feb 2026 at 07:01:06 | 4 Feb 2026 at 07:01:10 |
| 019c273d-7985-79a8-a93a-48e41402c78c | publish-notification | ✓ Completed | 4 Feb 2026 at 07:01:06 | 4 Feb 2026 at 07:01:10 |

v5 Update: Viewing Workflow Runs

- To be added soon (although low priority):
 - Detail view to inspect history, see errors and results
 - Controls to pause, resume, cancel, delete workflow runs
 - Potentially basic graphs for status distribution, task queue depths, etc.
 - Controls to pause and resume task queues
 - Controls to update task queue sizes

v5 Update: Using Managed Secrets (Before)

The screenshot shows the Dependency-Track administration interface for managing GitHub Advisory Sources. The left sidebar lists various configuration sections: 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 the GitHub configuration settings:

- Enabled:** A toggle switch is turned on.
- Alias Synchronization Enabled:** A toggle switch is turned on.
- GraphQL API URL:** The value is `https://api.github.com/graphql`.
- API Token:** The value is `{{ secret('GITHUB_TOKEN') }}`, which is highlighted with a red rectangular box.

Below the API Token input field, there is explanatory text: "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." At the bottom of the panel is a "Submit" button.

At the bottom right of the screen, the text "Dependency-Track v5.7.0-SNAPSHOT" is visible.

v5 Update: Using Managed Secrets (After)

The screenshot shows the Dependency-Track v5 Administration interface. The left sidebar has a dark theme with various icons and sections: Configuration, Secrets, Analyzers, Vulnerability Sources, GitHub Advisories (highlighted in blue), Google OSV Advisories (Beta), Repositories, Notifications, Integrations, Access Management, and Workflows.

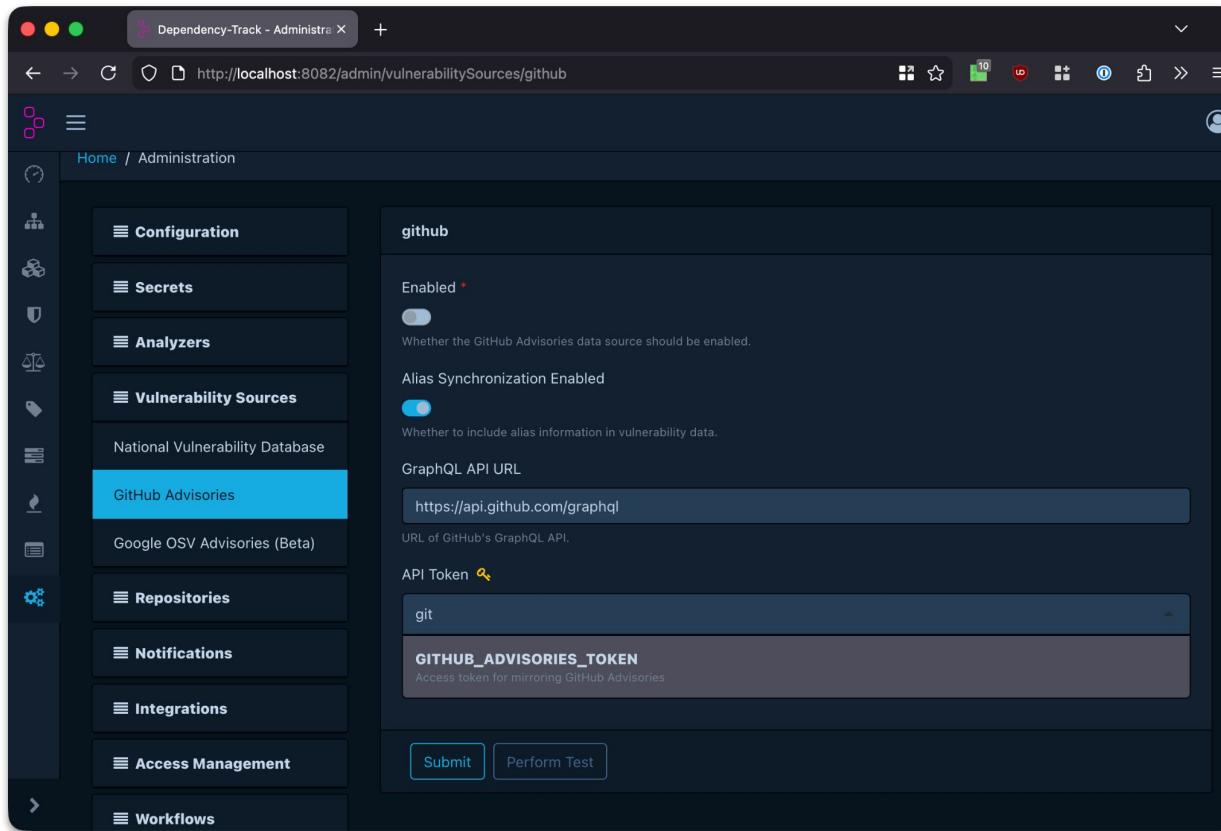
The main right panel is titled "github". It contains the following configuration fields:

- Enabled ***: A toggle switch that is turned on.
- Alias Synchronization Enabled**: A toggle switch that is turned off.
- GraphQL API URL**: A text input field containing the value `https://api.github.com/graphql`.
- API Token 🔑**: A dropdown menu labeled "Select a secret". This field is highlighted with a red rectangular border.

Below the dropdown, there is a note: "The token is only required for authentication and does not require any permissions. Both **fine-grained** and **classic** access tokens work."

At the bottom of the panel are two buttons: "Submit" and "Perform Test".

v5 Update: Using Managed Secrets (After)



v5 Update: Using Managed Secrets (After)

The screenshot shows the Dependency-Track Administration interface at <http://localhost:8082/admin/vulnerabilitySources/github>. The left sidebar has a dark theme with various icons and navigation items. The main panel is titled "github" and contains configuration settings for the GitHub Advisory data source.

Enabled *: A toggle switch is turned off, indicating the GitHub Advisory data source is disabled.

Alias Synchronization Enabled: A toggle switch is turned on, indicating alias information will be included in vulnerability data.

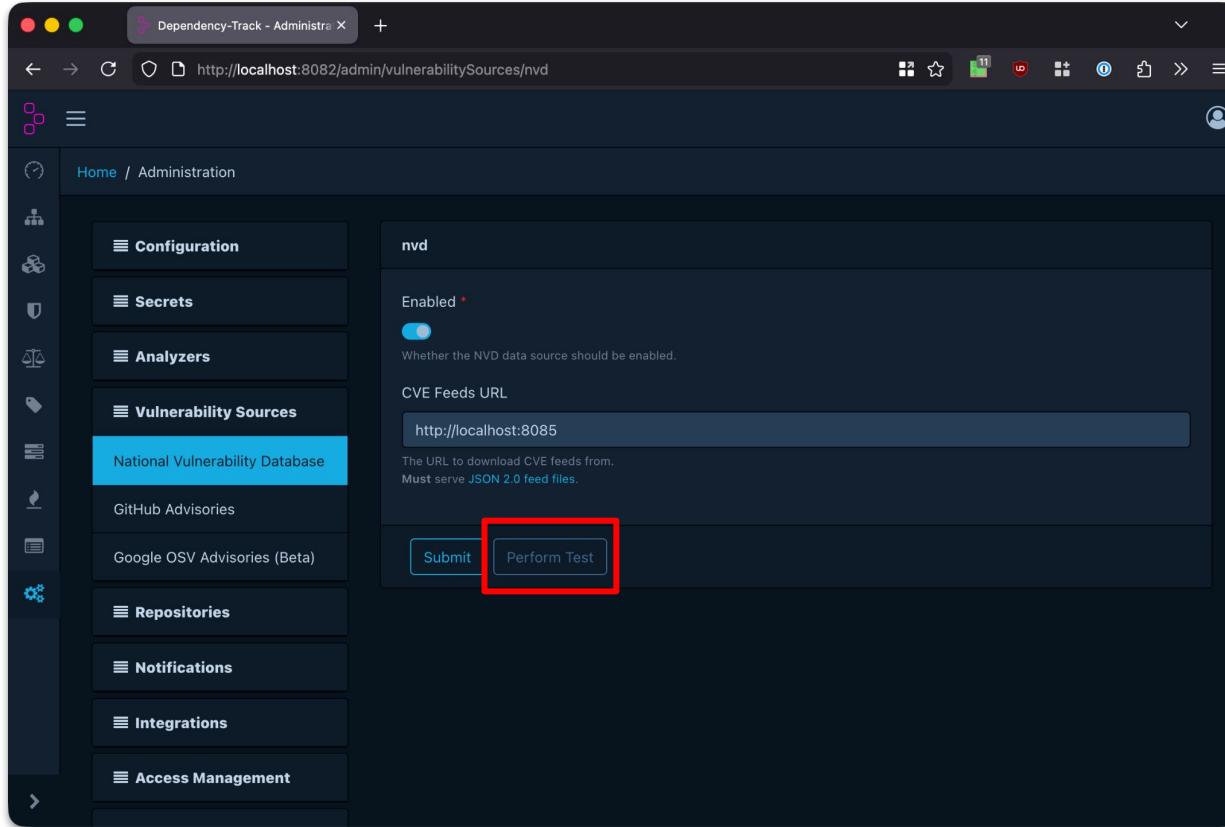
GraphQL API URL: The URL is set to <https://api.github.com/graphql>.

API Token: The token field contains the placeholder `GITHUB_ADVISORIES_TOKEN`, which is highlighted with a red warning icon. Below the field, a message states: "The selected secret does not exist".

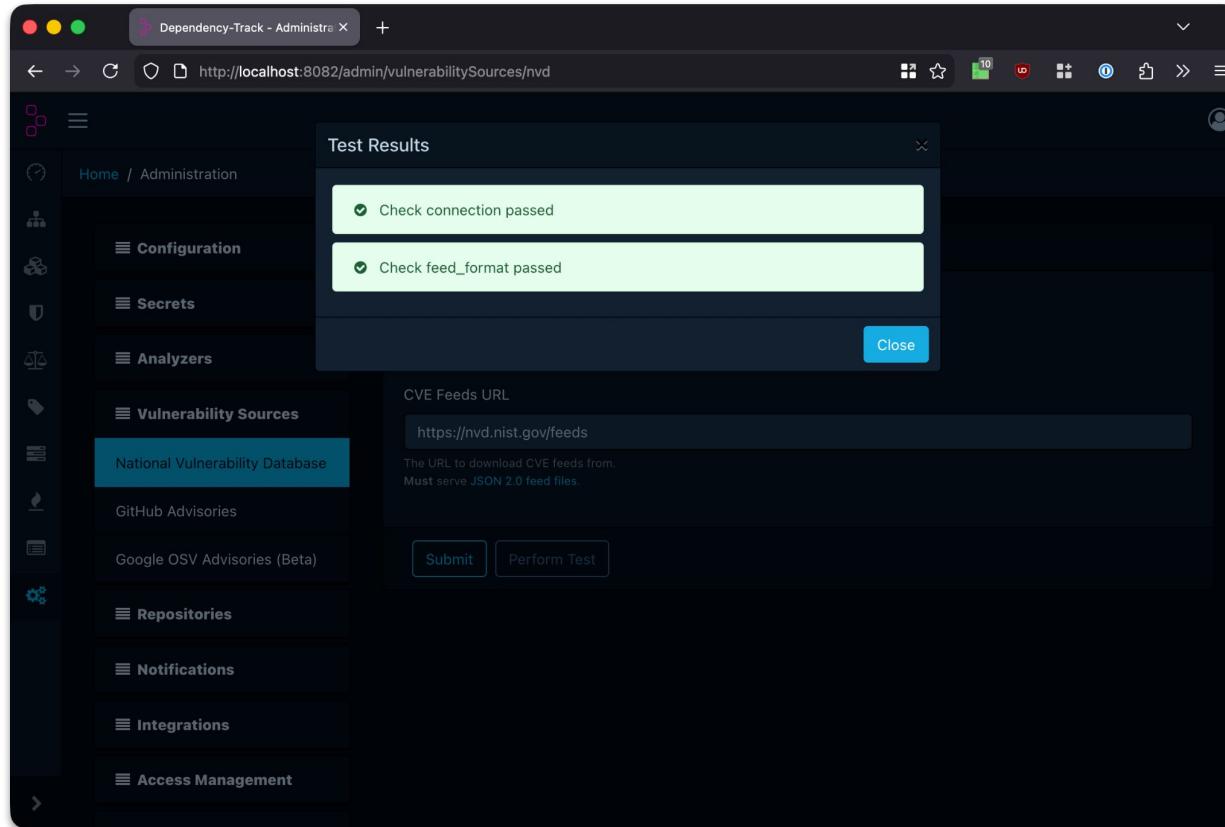
Access Token Notes: A note explains that the token is only required for authentication and does not require any permissions, mentioning both fine-grained and classic access tokens work.

Action Buttons: At the bottom are two buttons: "Submit" and "Perform Test".

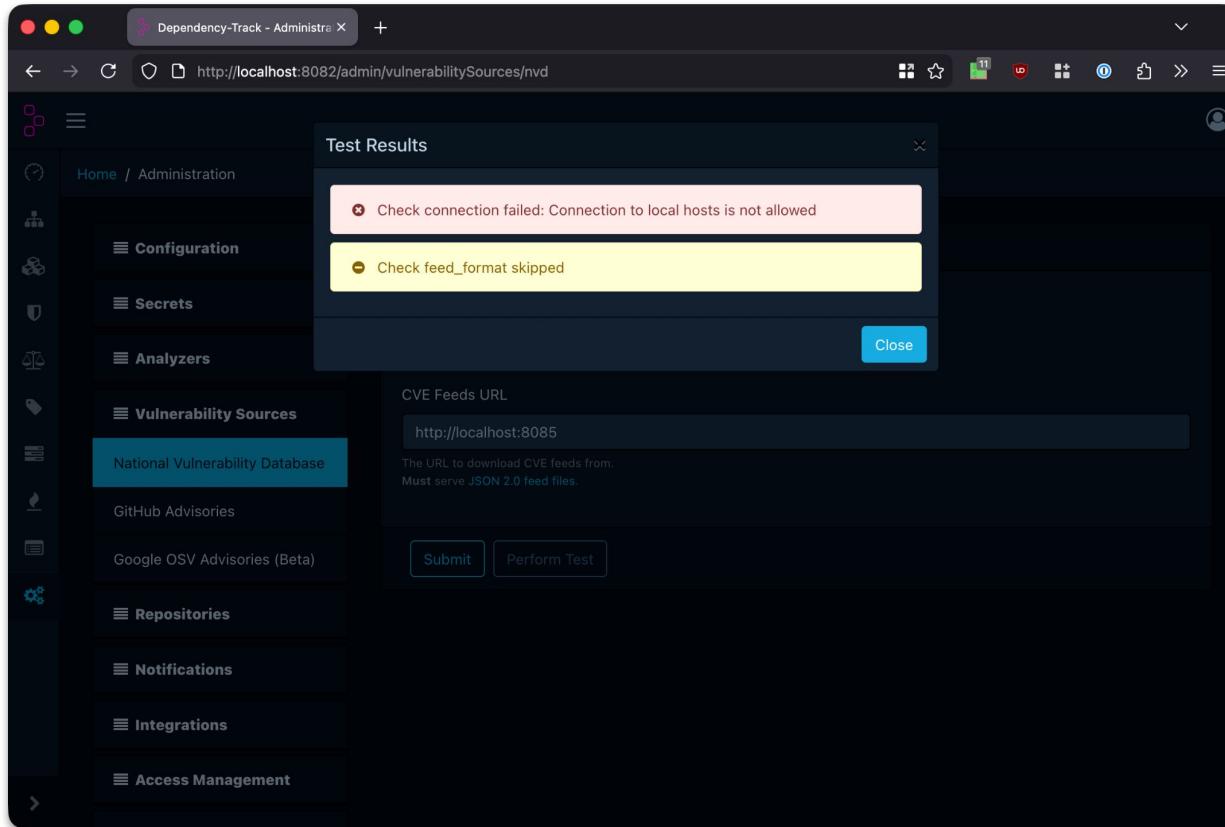
v5 Update: Testing Integrations



v5 Update: Testing Integrations



v5 Update: Testing Integrations



v5 Update: Testing Integrations

- Testing a configuration does **not** require saving it first
- Due to potential of abuse for SSRF, does **not** allow connections to localhost or local network by default
 - Must be allowed explicitly by a system admin via config file / env variable
- Test results are vague on purpose
 - Detailed information must still be acquired from logs
- Not all integrations support this yet, but will do for GA release

v5 Update: Currently in Progress

- Dropping Kafka requirement for vulnerability analysis (~45% done)
- Decommissioning vulnerability-analyzer service
- Setting up internal instance for dogfooding
- Still aiming for GA by end of Q1 🤞

Q&A