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

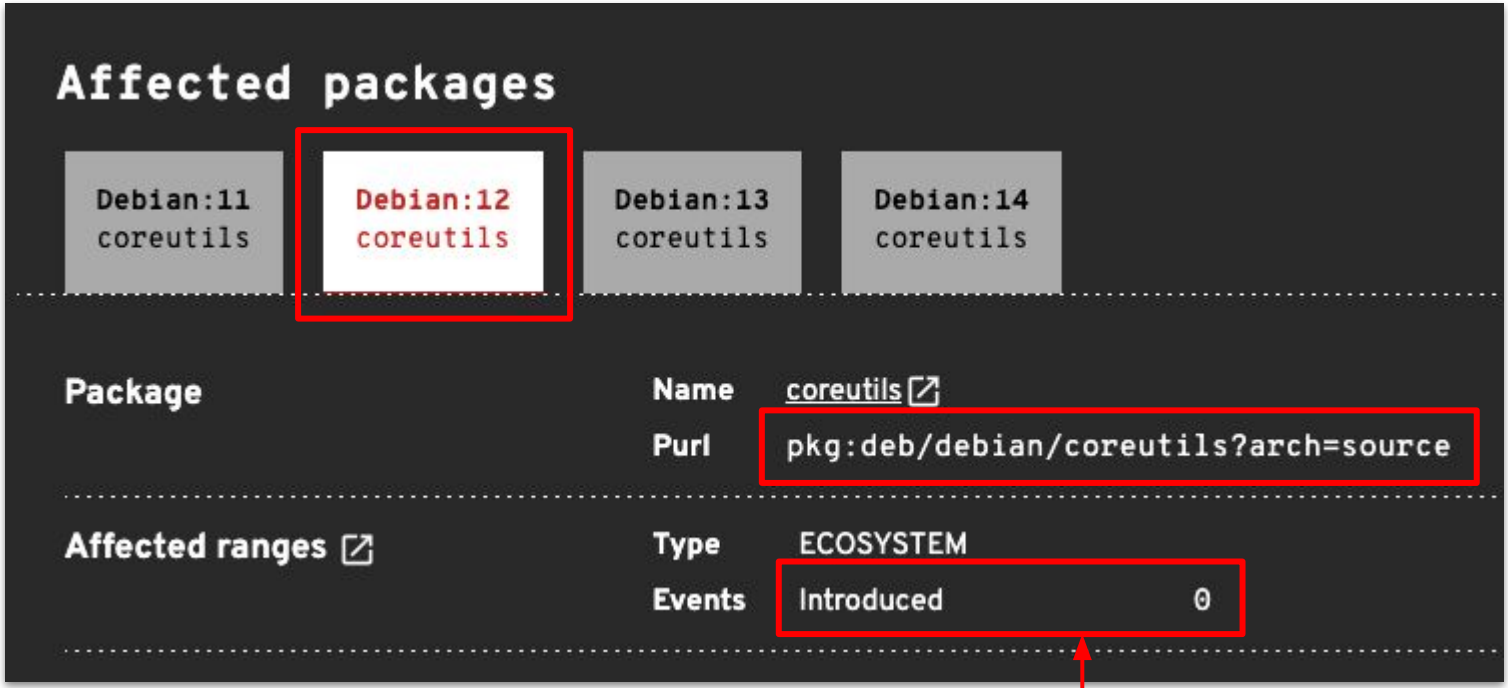
Upcoming Releases: v4.14.0

- 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 😜

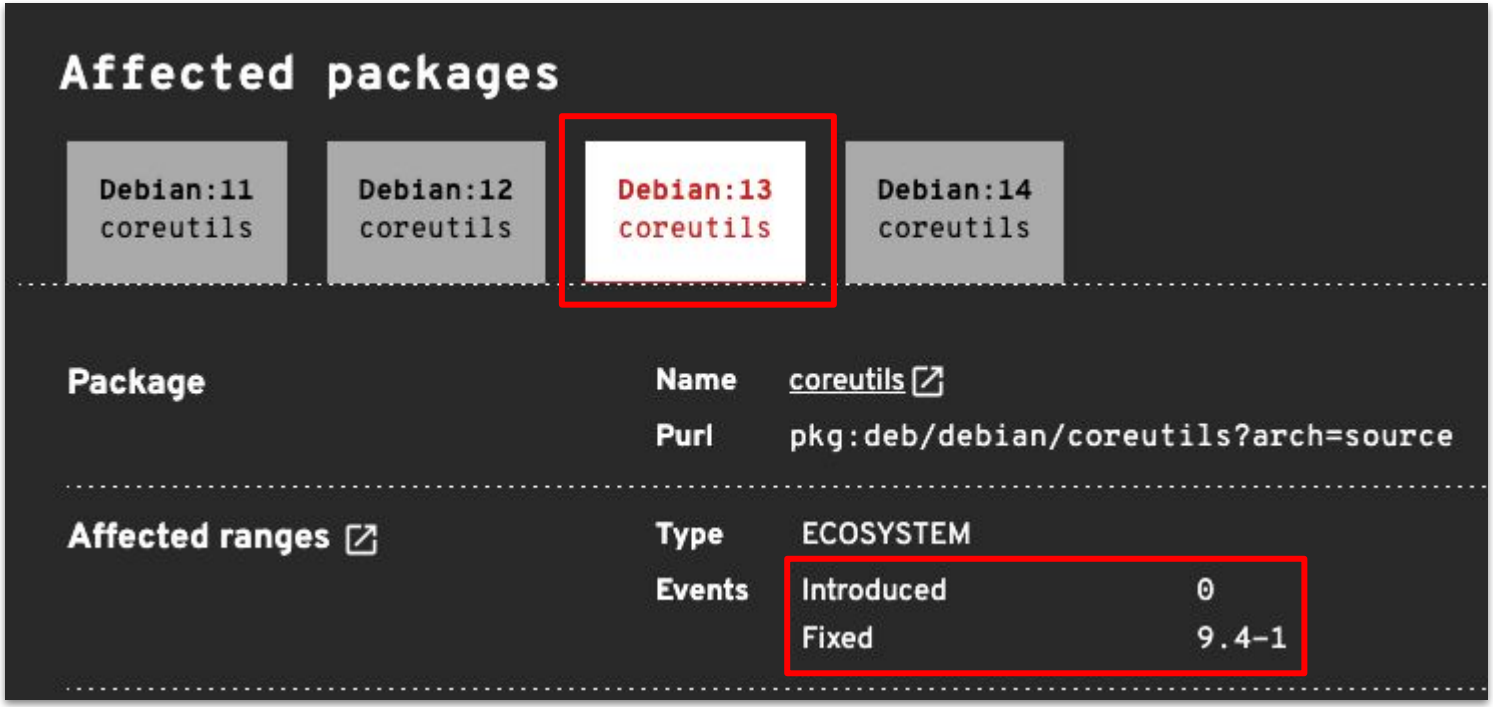
Linux Distro Version Matching



Affected packages as reported by OSV

“All versions”

Linux Distro Version Matching

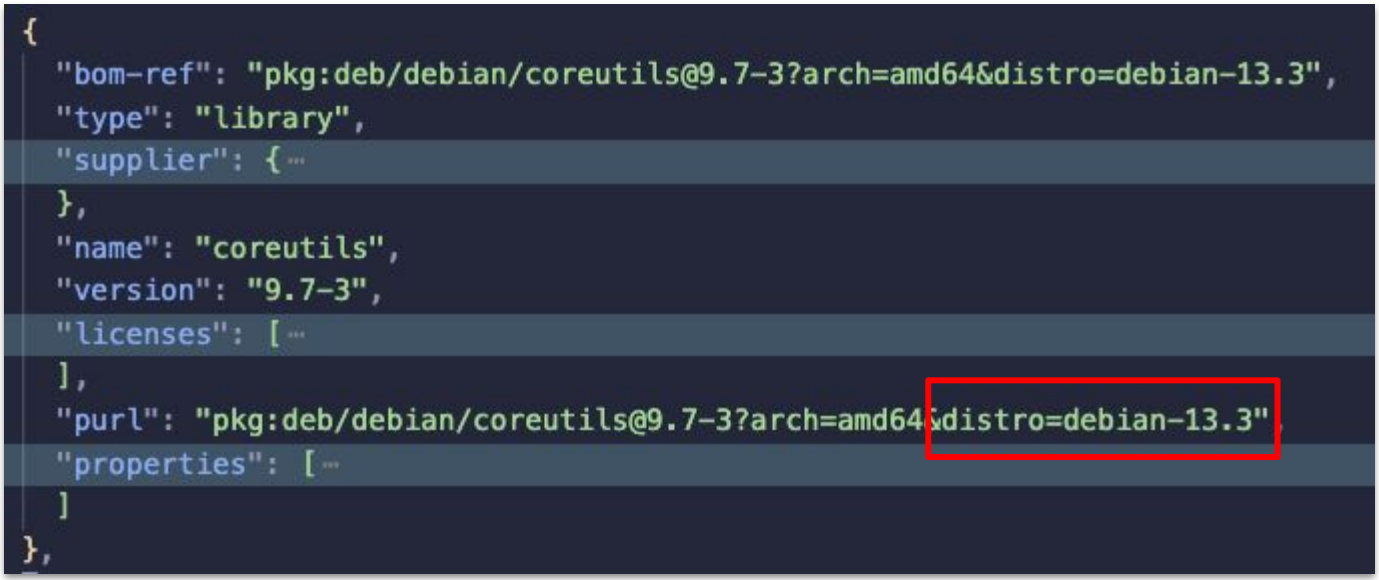


Affected packages as reported by OSV

Linux Distro Version Matching

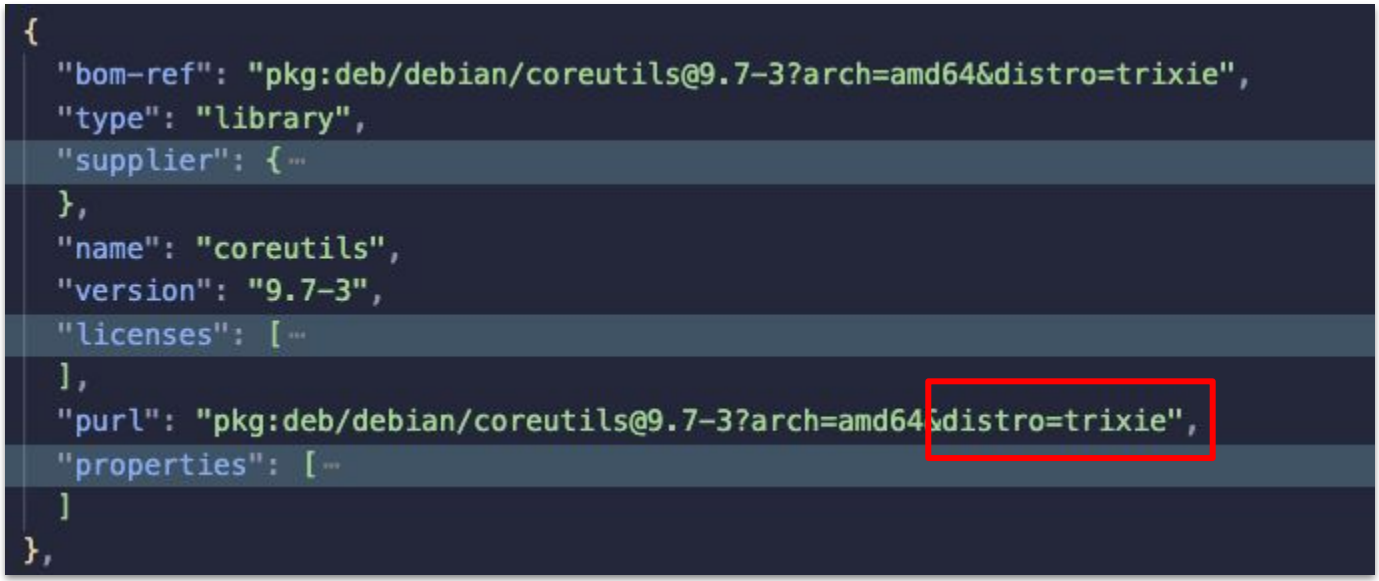
- *Massive* over-reporting if distro release is not taken into account
- Distro release is not always part of the PURL reported by OSV
  - must be inferred from elsewhere (i.e. OSV ecosystem name)
- Distro release can be version (e.g. 13) or code name (e.g. `trixie`)

Linux Distro Version Matching



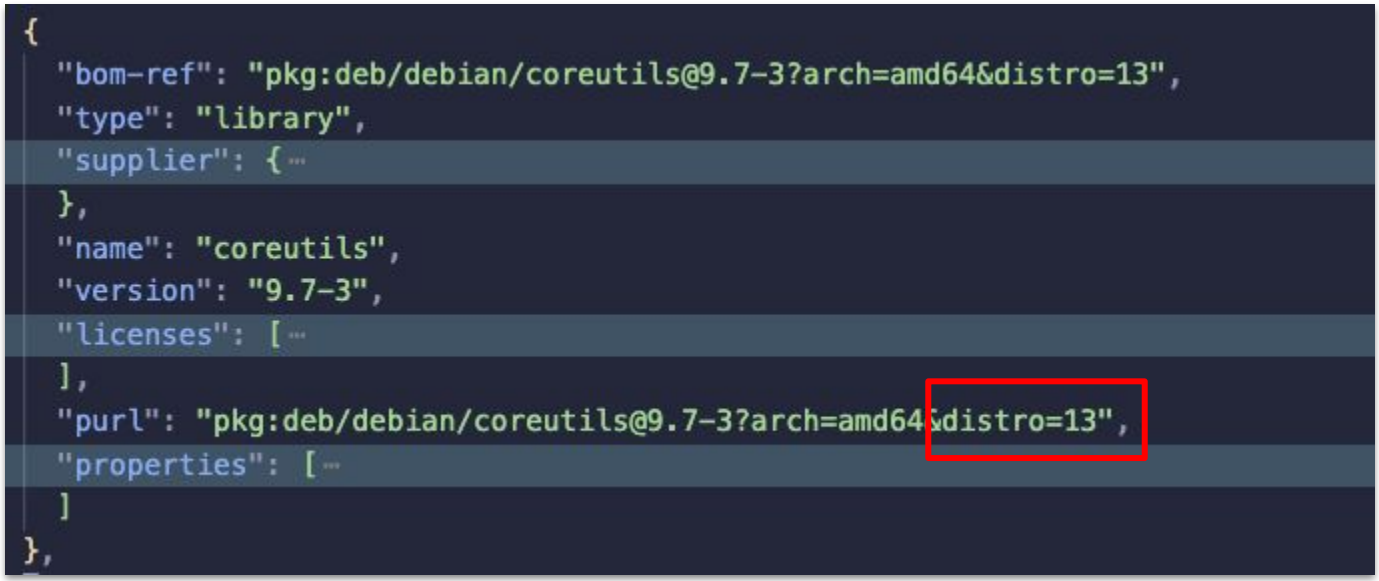
Component PURL in your BOM

Linux Distro Version Matching



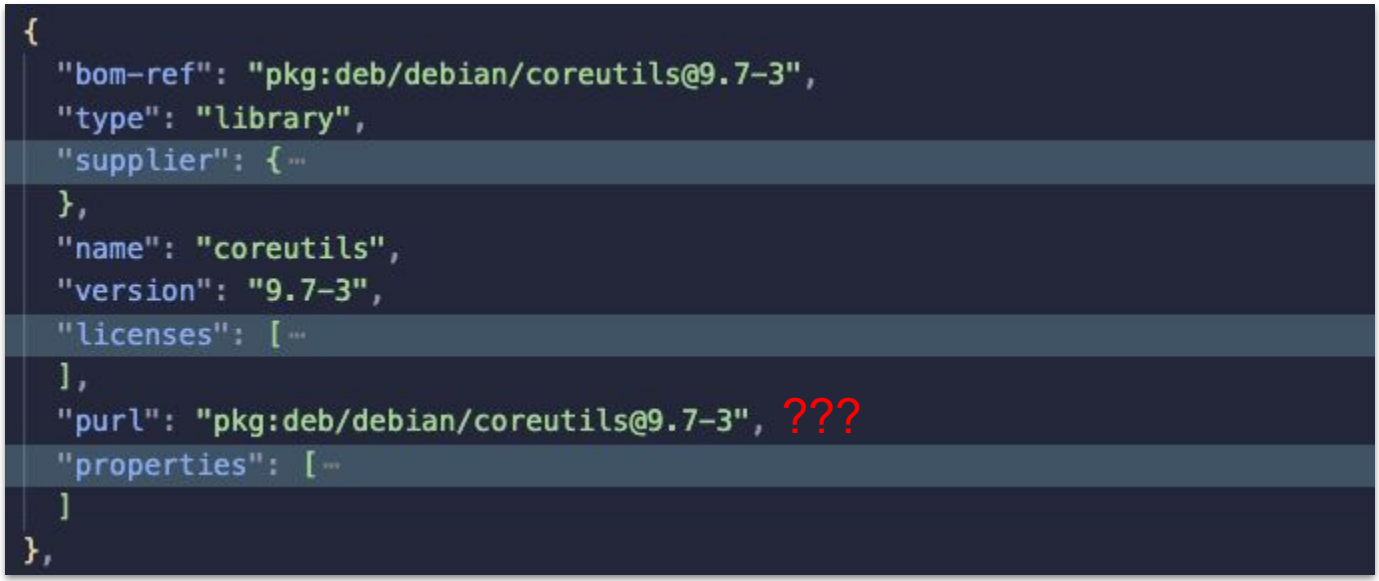
Component PURL in your BOM

Linux Distro Version Matching



Component PURL in your BOM

Linux Distro Version Matching



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

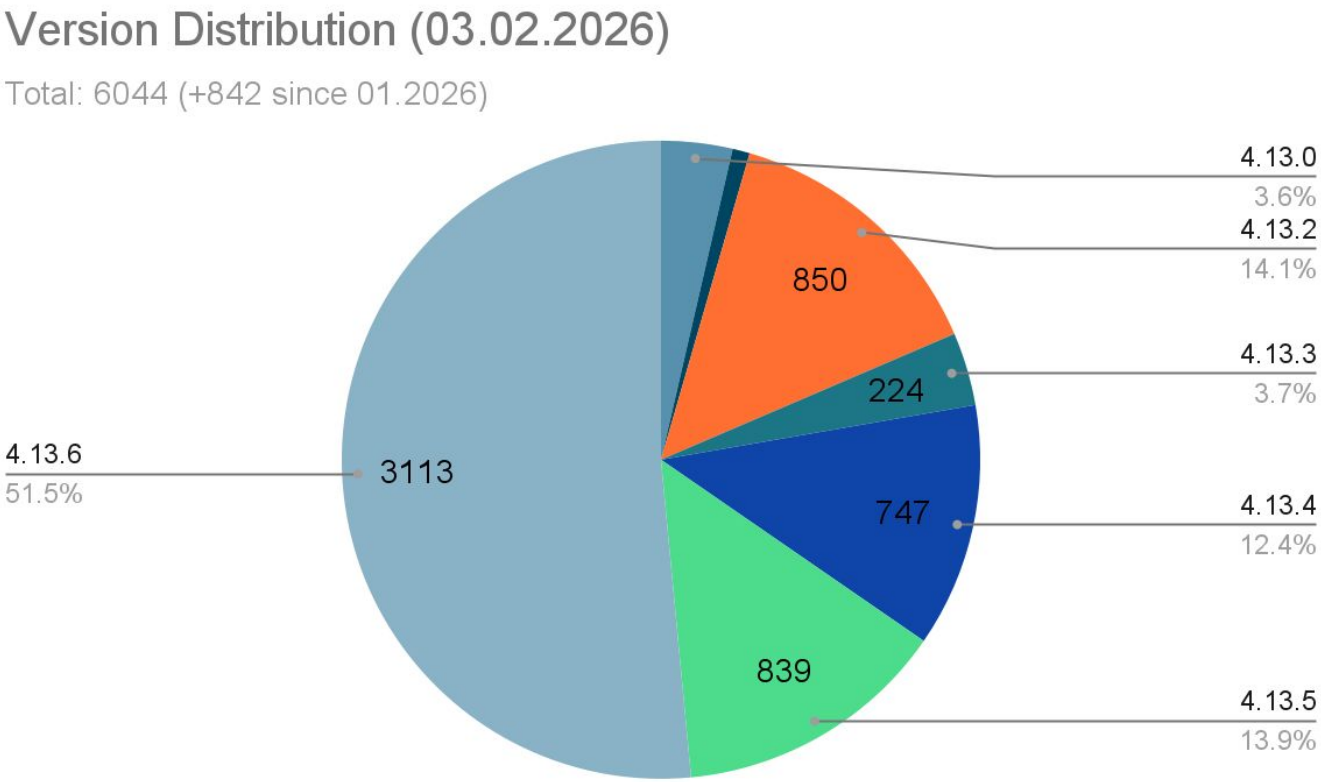
Linux Distro Version Matching: Planned Improvements

- 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

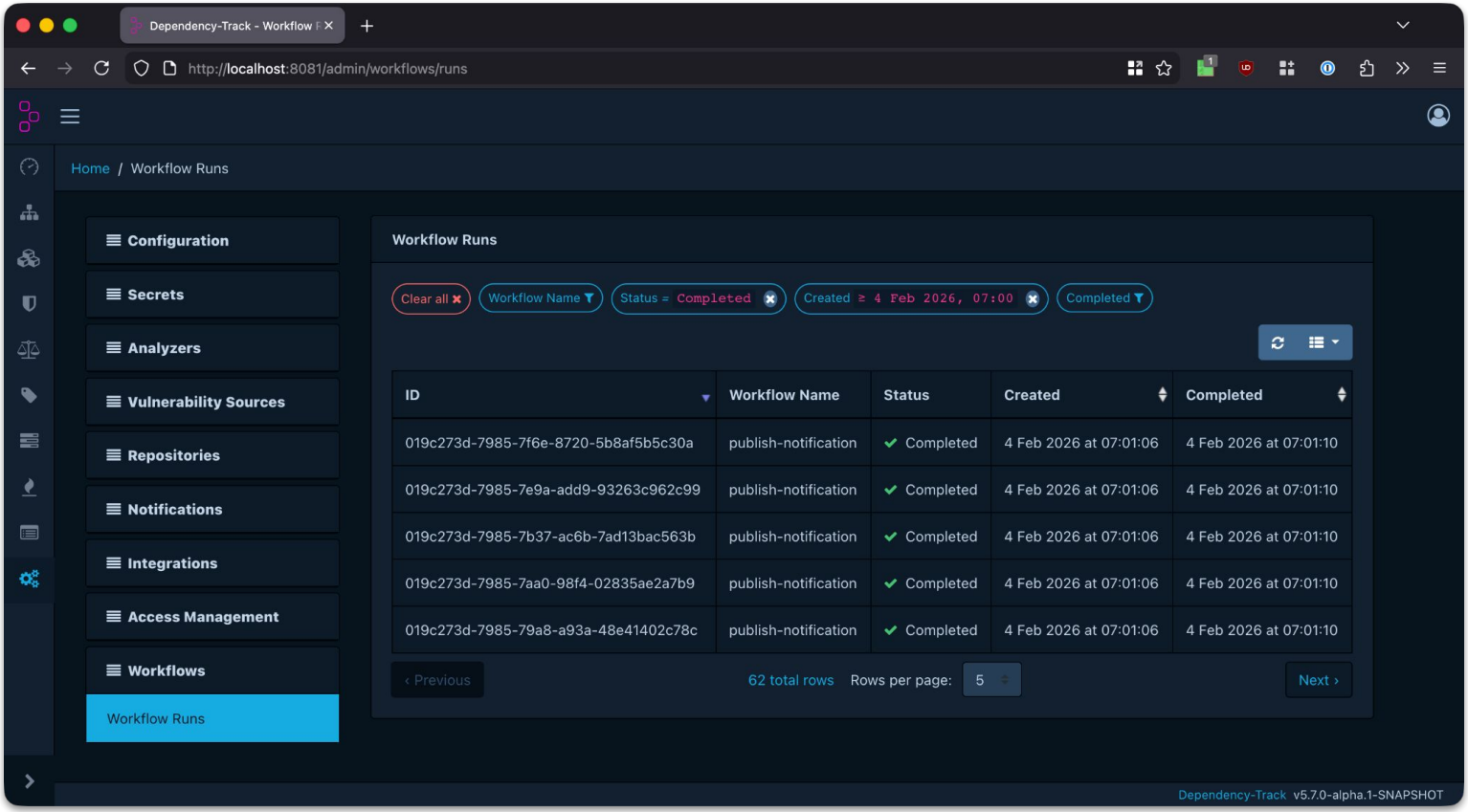


v5 Update

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

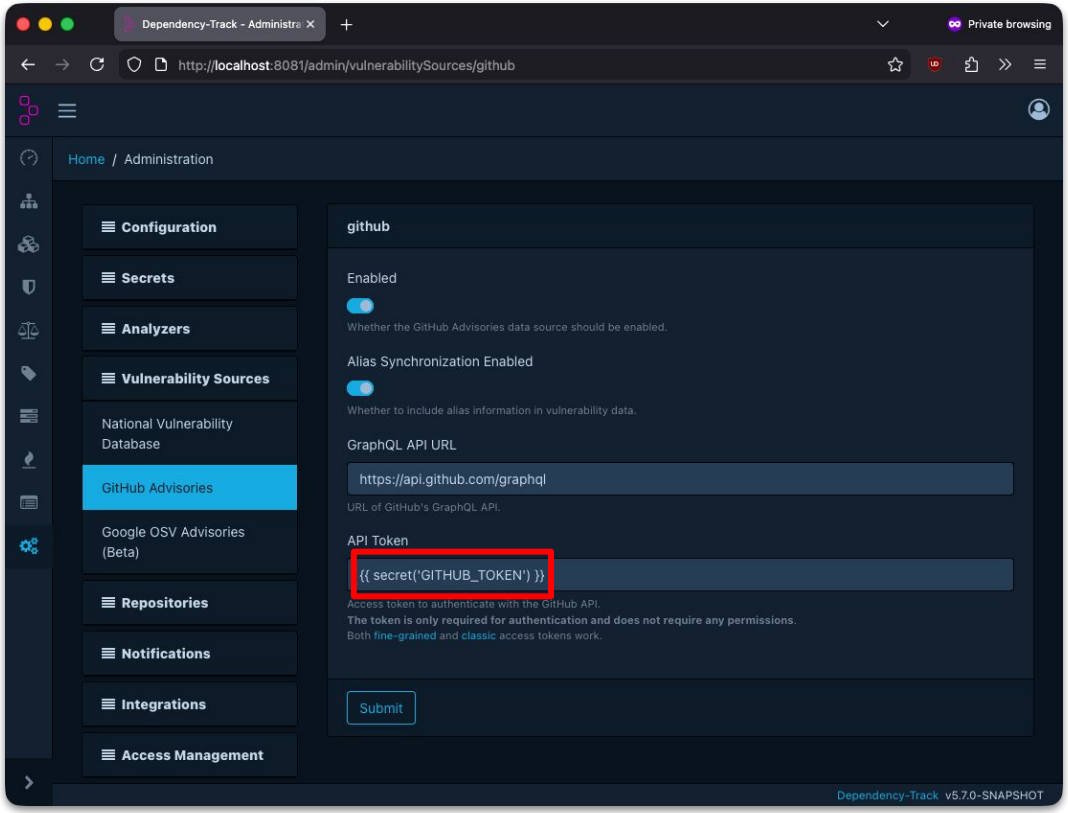
v5 Update: Viewing Workflow Runs



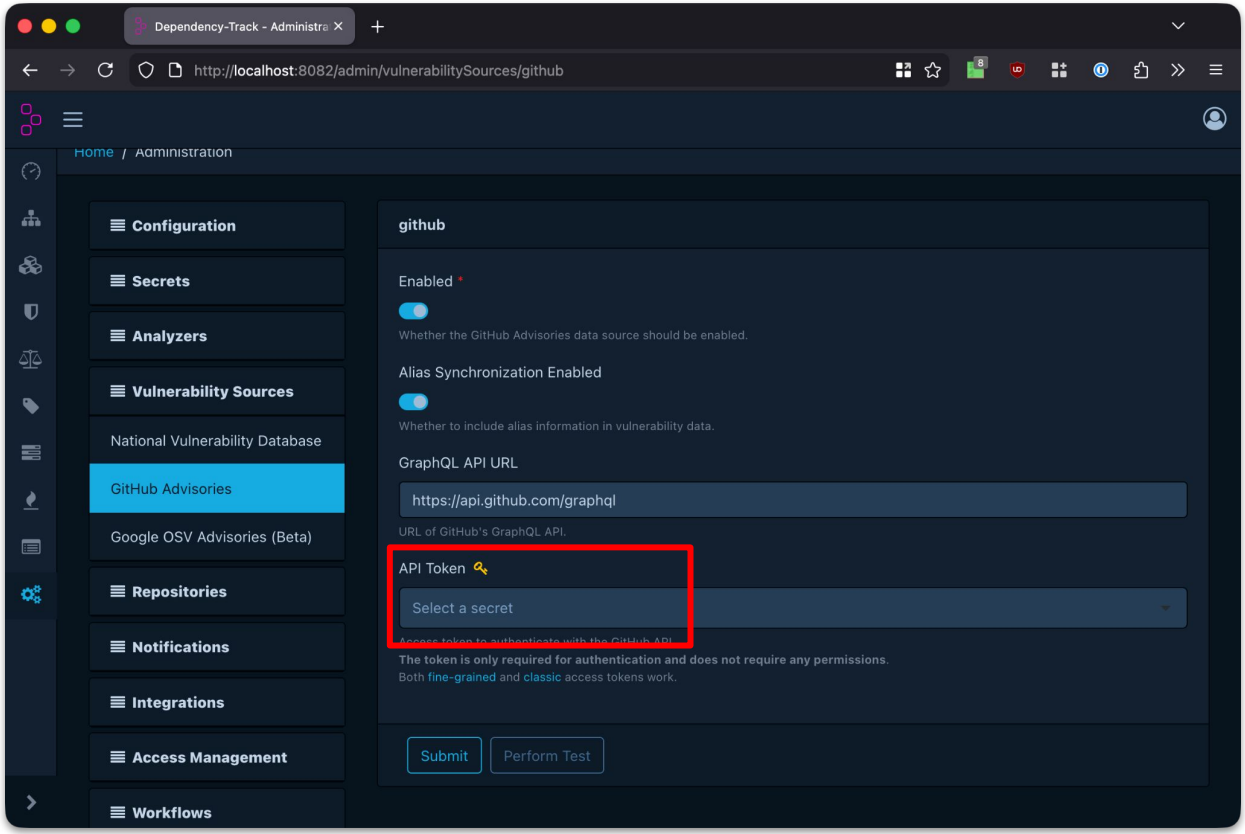
v5 Update: Viewing Workflow Runs

- 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

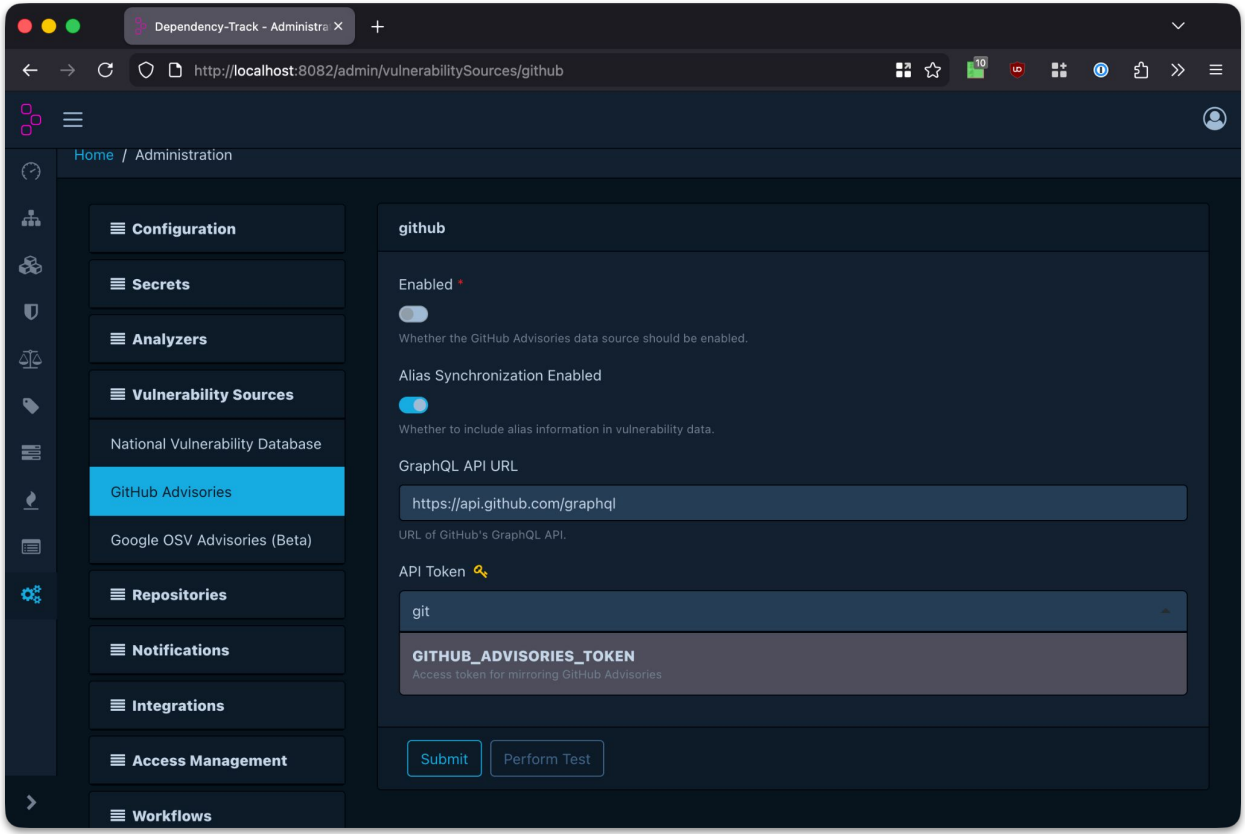
v5 Update: Using Managed Secrets (Before)



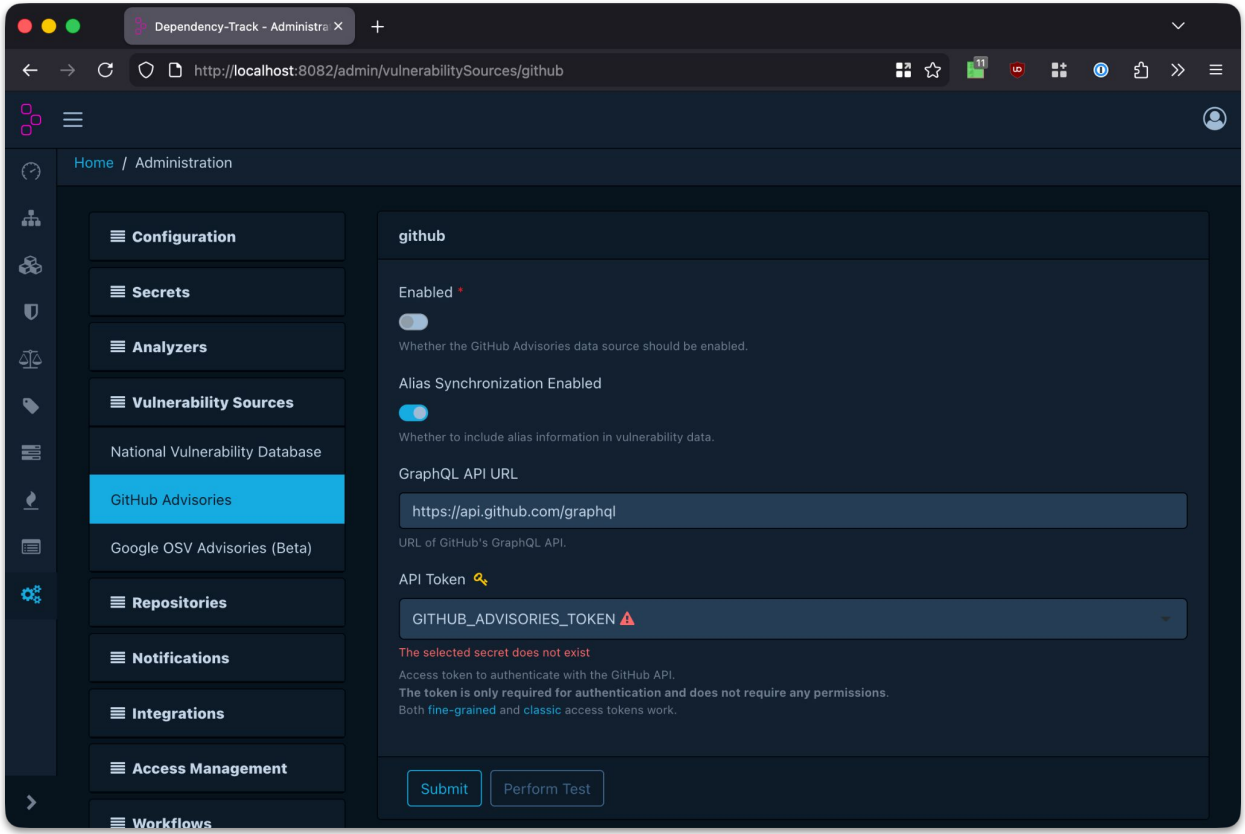
v5 Update: Using Managed Secrets (After)



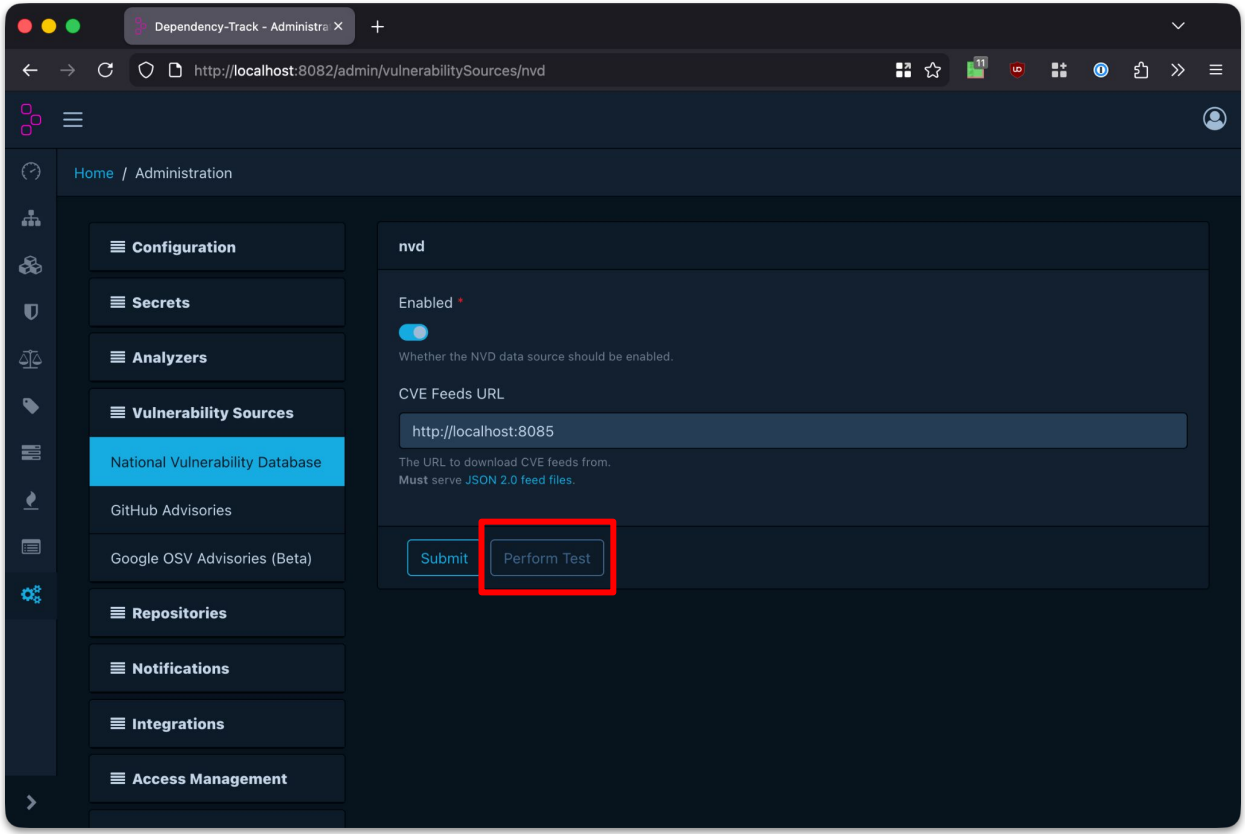
v5 Update: Using Managed Secrets (After)



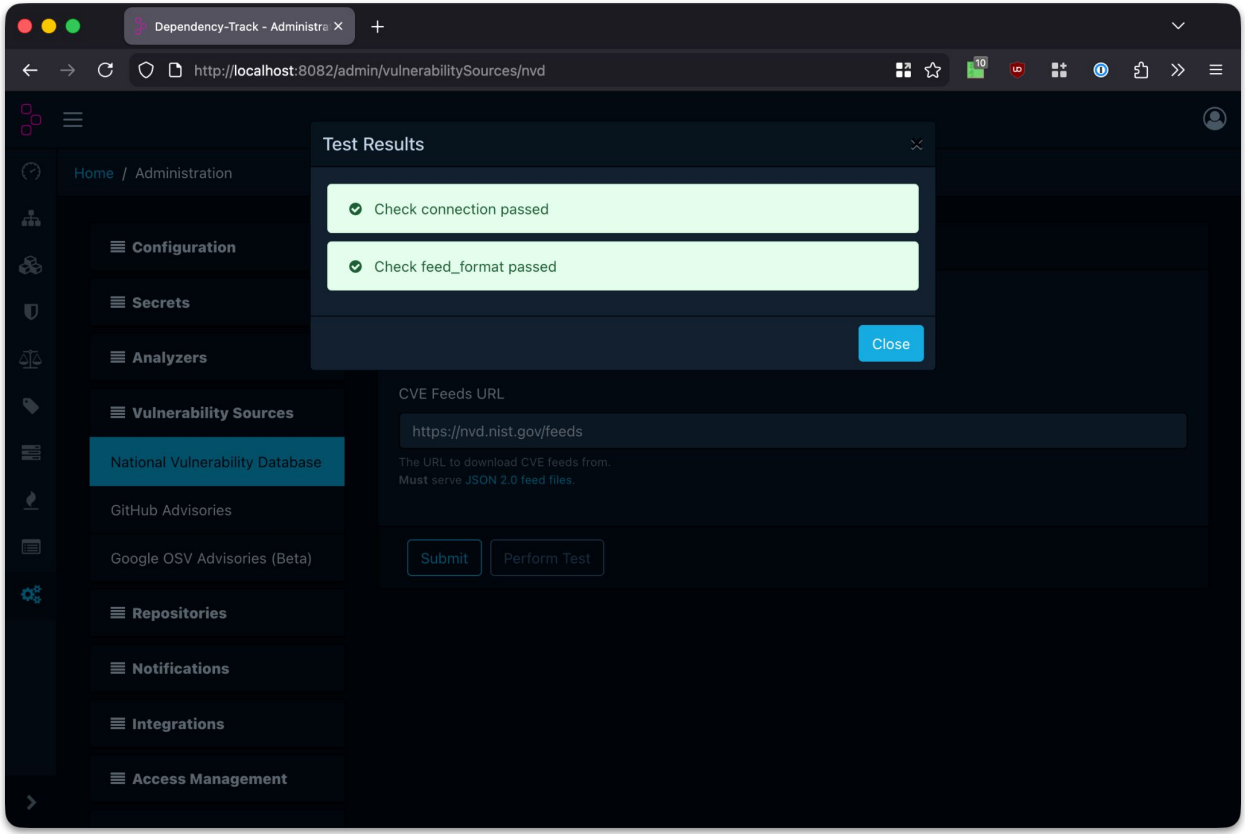
v5 Update: Using Managed Secrets (After)



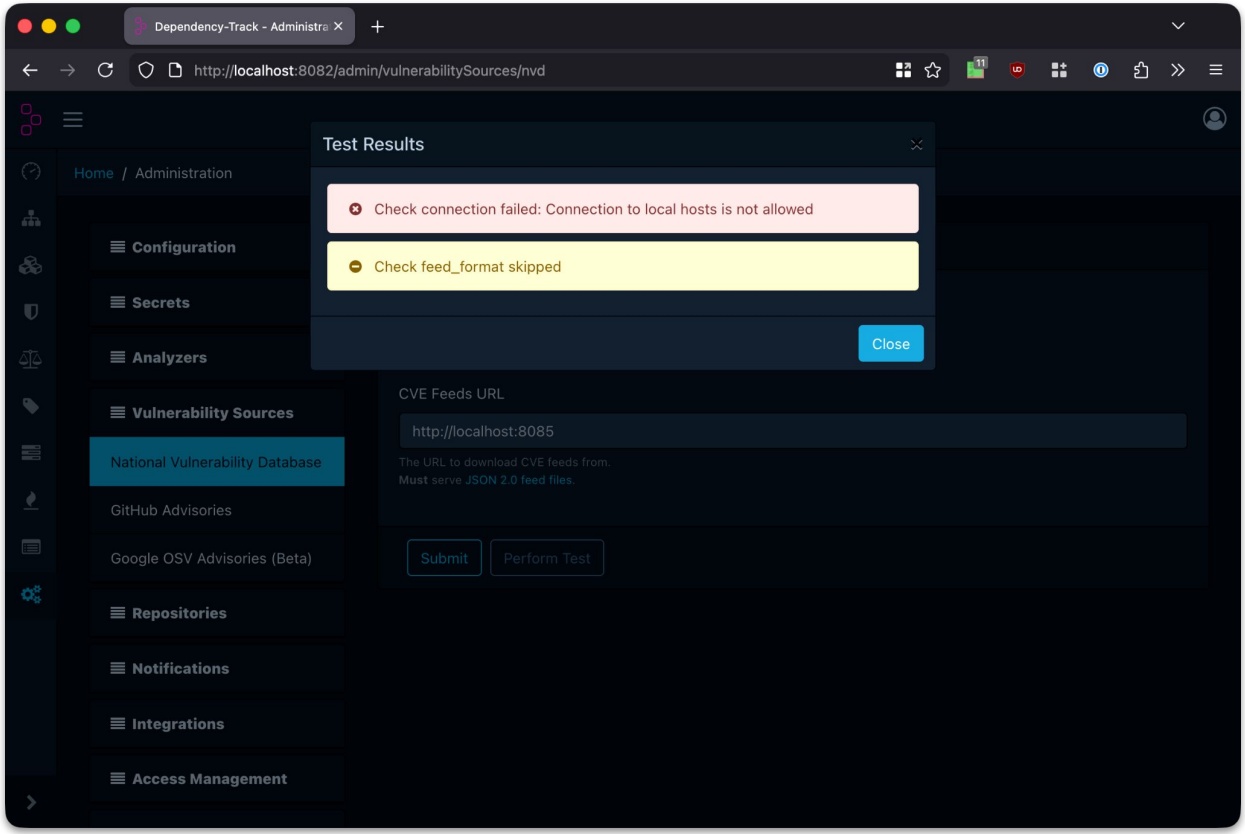
v5 Update: Testing Integrations



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