



# DEPENDENCY-TRACK COMMUNITY MEETING

**FEBRUARY  
2025**

**THE DEPENDENCY-TRACK TEAM**

[www.owasp.org](https://www.owasp.org)

Dependency-Track Community Meeting - February 2025

# 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

---

Past & upcoming releases

01

Vulnerability DB update

02

Hyades update

03

Q & A

04



# PAST & UPCOMING RELEASES



# Past Releases

---

- v4.12.3
  - Released Jan. 27th
  - ⚠ Fixes GitHub Advisory mirroring ⚠
  - Fixes notification rule (“Alert”) test button failing for Jira
  - Fixes outdated database CHECK constraints for component and project classifiers
  - And more!



v4.12.3 Changelog  
<https://docs.dependencytrack.org/changelog/#v4-12-3>

# Upcoming Releases

- v4.12.4
  - 7 small fixes already backported
  - Release soon™
- v4.13.0
  - Refer to previous community meetings
  - *Definitely* will drop some planned issues from 4.13 milestone to not hold up the release forever
  - *Pending*: Summary notification support
  - *New*: Contribution to mirror vulnerability data from PHP Composer repositories
  - *New*: Contribution to make API keys and their handling more secure



v4.12.4 Milestone

<https://github.com/DependencyTrack/dependency-track/milestone/48>



v4.13.0 Milestone

<https://github.com/DependencyTrack/dependency-track/milestone/38>



# v4.13: API Key Changes

- v4.12 and earlier
  - Format: `<prefix>_<key>`
  - Example: `odt_PTtSk8tX8WQjccYhsMcmvQdvLs5UjHol`
  - Stored in clear text 🙅
  - Always viewable by admin users 🙅
- v4.13 going forward
  - Format: `<prefix>_<publicId>_<key>`
  - Example: `odt_aV8z5_PTtSk8tX8WQjccYhsMcmvQdvLs5UjHol`
  - Stored as SHA3-256 hash 👍
  - Full key only visible immediately after creation 👍
  - Public ID visible in logs, used to address keys via API (i.e. to update comment) 👍
- v4.12 to v4.13 migration
  - Hash existing keys
  - Mark keys as *legacy*, highlight as such in UI
  - Existing keys will continue to work
  - Assume first 5 characters of old API key to be public ID
  - Existing keys no longer viewable in full ⚠️
  - Users *encouraged* to re-generate keys
- Thanks to Thomas Schauer-Köckeis ([@Gepardgame](#)) for contributing this!



# VULNERABILITY DB UPDATE





# Vulnerability DB Update

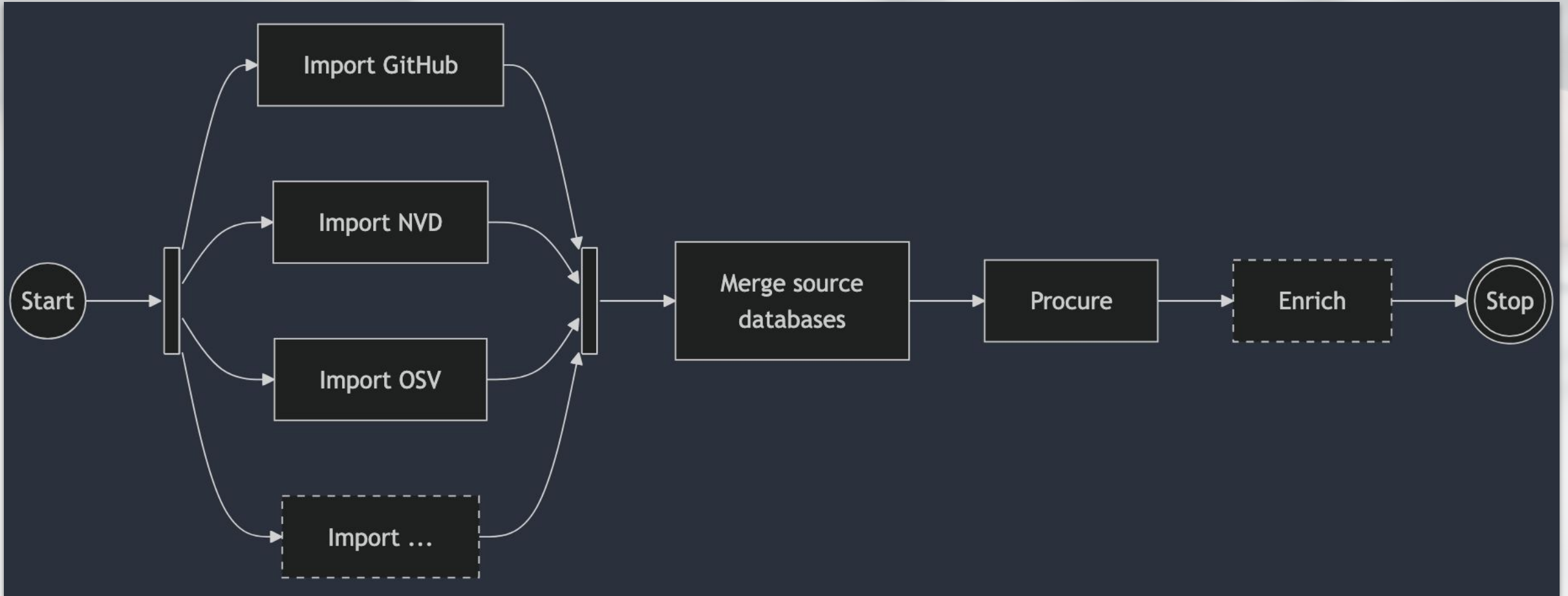
- Using existing DBs as-is won't work
  - Most are optimized for one-shot CLI tools
  - Need to compile multiple and normalize to our data model
- Data quality research necessary to know what sources to trust
- Proof-of-concept repo created to get things moving
  - *Note: Repo will be moved to the DependencyTrack org shortly!*



<https://github.com/DependencyTrack/dependency-track/issues/4122>



<https://github.com/nscurio/vuln-db>



```

1 package org.dependencytrack.vulndb.api;
2
3 public interface Importer {
4
5     Source source();
6
7     void init(final Database database);
8
9     void runImport() throws Exception;
10
11 }

```

```

1 package org.dependencytrack.vulndb.api;
2
3 import java.util.Collection;
4 import java.util.Map;
5
6 public interface Database {
7
8     Map<String, String> getSourceMetadata();
9
10    void putSourceMetadata(final String key, final String value);
11
12    void storeVulnerabilities(Collection<Vulnerability> vulns);
13
14 }

```

```

1 package org.dependencytrack.vulndb.api;
2
3 public interface Importer {
4
5     Source source();
6
7     void init(final Database database);
8
9     void runImport() throws Exception;
10
11 }

```

Choose Implementation of Importer (3 found)

- GitHubImporter (org.dependencytrack.vulndb.source.github) vuln-db
- NvdImporter (org.dependencytrack.vulndb.source.nvd) vuln-db
- OsvImporter (org.dependencytrack.vulndb.source.osv) vuln-db

← Update Database

✓

Update Database #11

Summary

Jobs

✓ Update source database (github)

✓ Update source database (nvd)

✓ Update source database (osv)

✓ Merge source databases

Run details

Usage


Workflow file

Manually triggered 5 minutes ago

Status

Total duration

Artifacts

 nscuro

↪ 65bb1f4

main

Success

5m 30s

—

update-database.yml

on: workflow\_dispatch

Matrix: Update source database

✓ Update source database (... 20s


✓ Update source databa... 1m 55s

✓ Update source databa... 2m 18s


→

✓ Merge source data


5 packages

 **source/osv**


Published yesterday by [Niklas](#) in [vuln-db/source/osv](#)

 **source/github**

Published yesterday by [Niklas](#) in [vuln-db/source/github](#)

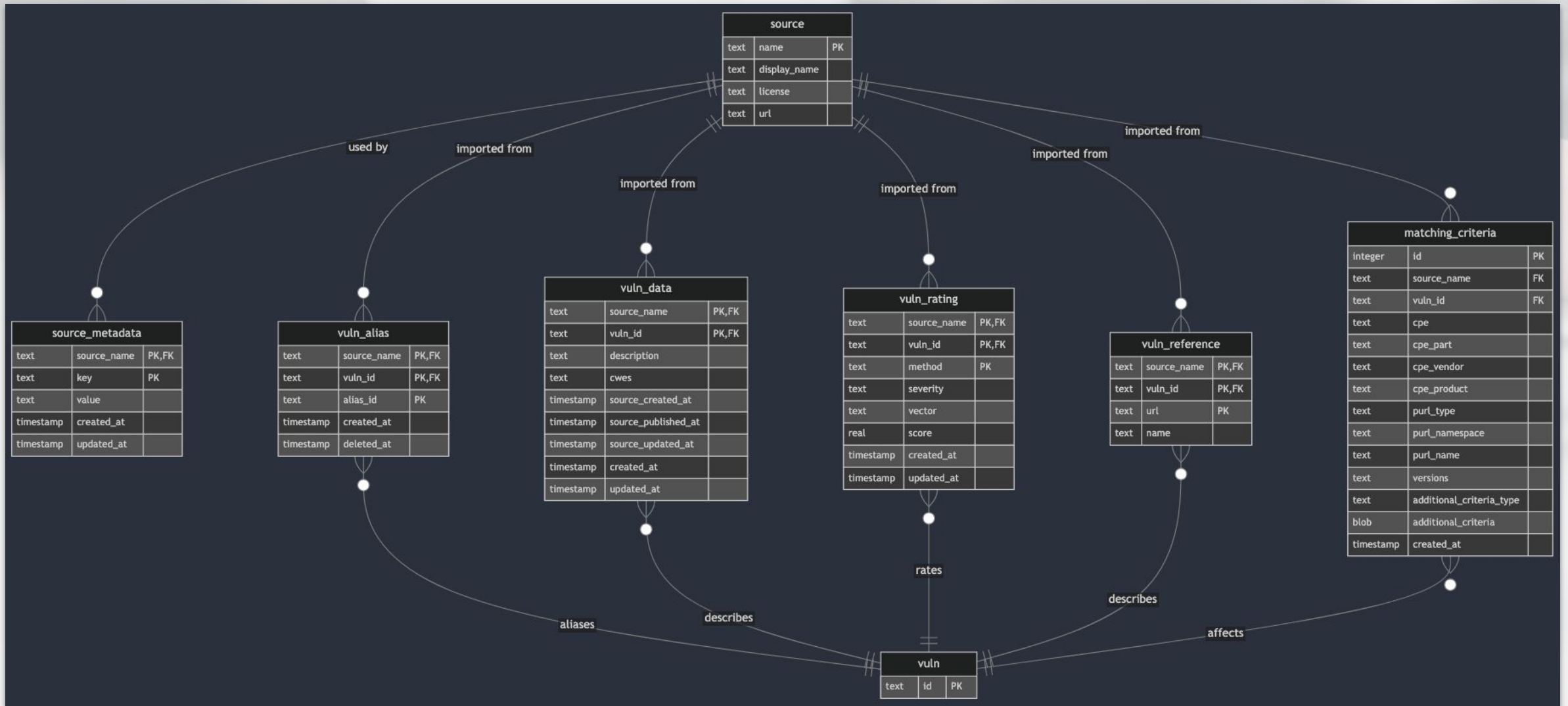
 **source/nvd**

Published yesterday by [Niklas](#) in [vuln-db/source/nvd](#)

 **source/all**

Published yesterday by [Niklas](#) in [vuln-db/source/all](#)





duckdb all.sqlite

source_name varchar	vuln_id varchar	purl_type varchar	purl_namespace varchar	purl_name varchar	versions varchar
github	GHSA-h6jh-7gv5-28vg	pypi		tensorflow-cpu	vers:pypi/ ≥ 2.4.0 <2.4.3
osv	CVE-2022-42719	deb	debian	linux	vers:deb/ ≥ 0 <6.0.2-1
github	GHSA-27rc-728f-x5w2	pypi		tensorflow	vers:pypi/<2.8.4
github	GHSA-824j-wqm8-89mj	nuget		Microsoft.NetCore.App.Ru...	vers:nuget/ ≥ 7.0.0  ≤ 7.0.2
osv	CVE-2019-17010	deb	debian	thunderbird	vers:deb/ ≥ 0 <1%3A68.3.0-1
osv	CVE-2006-1059	deb	debian	samba	vers:deb/ ≥ 0 <3.0.22-1
osv	CVE-2024-46724	deb	debian	linux-6.1	vers:deb/ ≥ 0 <6.1.119-1%7Edeb11u1
osv	GHSA-grpp-gx5h-pvh8	maven	com.xebialabs.depl...	deployit-plugin	vers:maven/ ≥ 0 <7.5.5
osv	CVE-2020-22028	deb	debian	ffmpeg	vers:deb/ ≥ 0 <7%3A4.3-2
osv	GHSA-7mqj-xgf8-p59v	maven	org.apache.nifi	nifi-web-ui	vers:maven/ ≥ 1.10.0 <1.28.0
osv	GHSA-mxf2-4r22-5hq9	maven	org.xwiki.platform	xwiki-platform-web	vers:maven/ ≥ 1.0 <13.10.6
github	GHSA-6528-wvf6-f6qg	pypi		pycrypto	vers:pypi/ ≤ 2.6.1
osv	CVE-2024-21145	deb	debian	openjdk-17	vers:deb/ ≥ 0 <17.0.12%2B7-2%7Edeb12u1
osv	CVE-2014-3695	deb	debian	pidgin	vers:deb/ ≥ 0 <2.10.10-1
osv	CVE-2021-3731	deb	debian	ledgersmb	vers:deb/ ≥ 0 <1.6.9%2Bds-2%2Bdeb11u2
15 rows					6 columns

D

duckdb all.sqlite

```

D select source_name
      , vuln_id
      , additional_criteria_type
      , additional_criteria::json
  from matching_criteria
 where additional_criteria is not null
 order by vuln_id
 limit 5;
  
```

source_name varchar	vuln_id varchar	additional_criteri... varchar	CAST(additional_criteria AS "json") json
osv	G0-2020-0001	go-imports	"[{\"path\": \"github.com/gin-gonic/gin\", \"symbols\": [\"Default\", ...
osv	G0-2020-0002	go-imports	"[{\"path\": \"github.com/proglottis/gpgme\"}]"
osv	G0-2020-0003	go-imports	"[{\"path\": \"github.com/revel/revel\"}]"
osv	G0-2020-0004	go-imports	"[{\"path\": \"github.com/nanobox-io/golang-nanoauth\", \"symbols\": ...
osv	G0-2020-0005	go-imports	"[{\"path\": \"go.etcd.io/etcd/wal\", \"symbols\": [\"Create\", \"Repa...

D

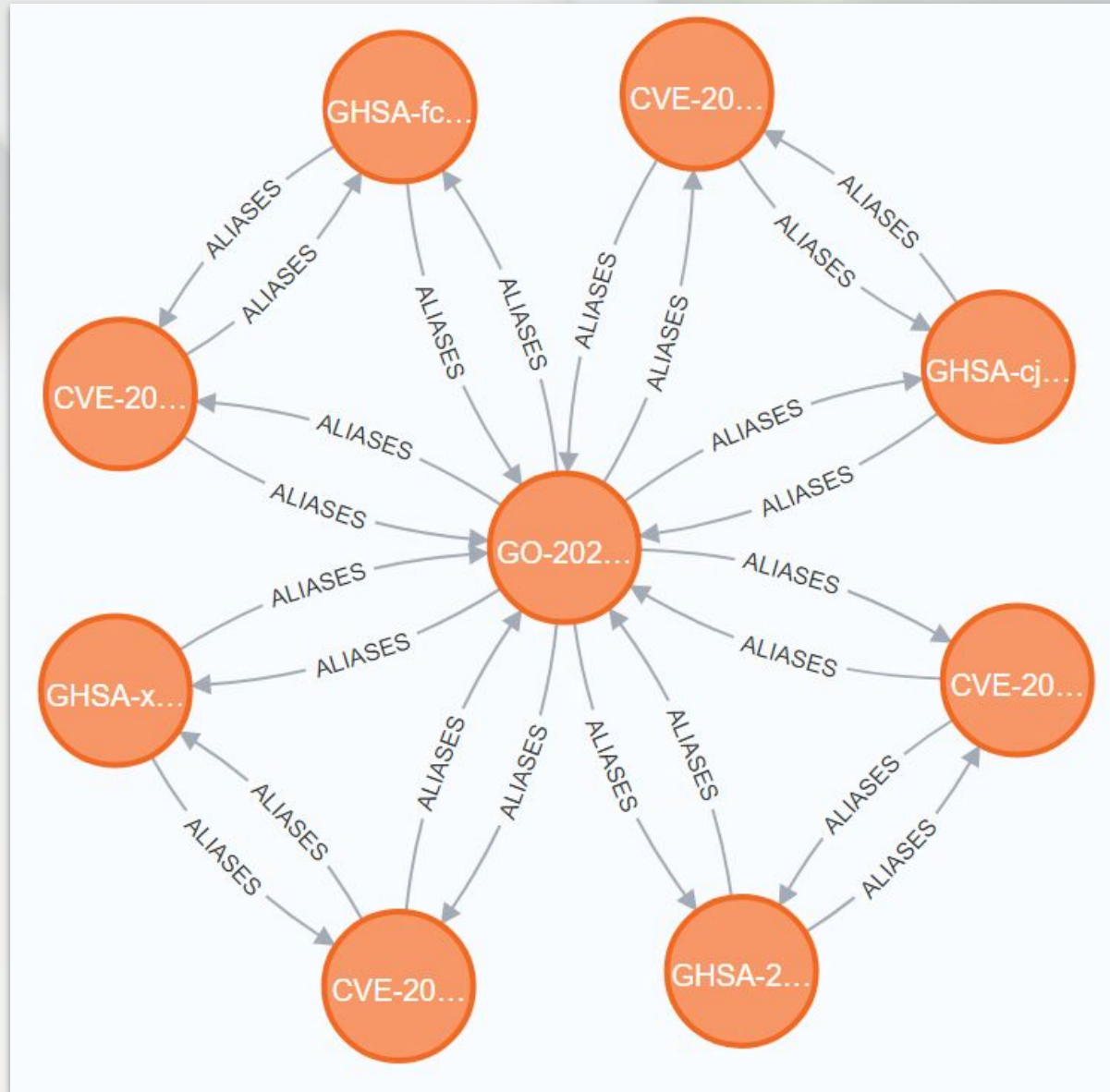


duckdb all.sqlite

```
, json_group_array(json_object(source_name, alias_id)) as aliases
from cve_aliases
group by vuln_id
order by vuln_id desc
limit 10;
```

vuln_id varchar	aliases json
CVE-2025-24898	[{"github": "GHSA-rpmj-rpgj-qmpm"}]
CVE-2025-24884	[{"osv": "GHSA-hcr5-wv4p-h2g2"}, {"github": "GHSA-hcr5-wv4p-h2g2"}]
CVE-2025-24883	[{"osv": "GHSA-q26p-9cq4-7fc2"}, {"github": "GHSA-q26p-9cq4-7fc2"}]
CVE-2025-24882	[{"osv": "GHSA-qv35-3gw6-8q4j"}, {"osv": "G0-2024-3038"}, {"github": "GHSA-qv35-3gw6-8q4j"}]
CVE-2025-24856	[{"github": "GHSA-hj78-p4h7-m5fv"}]
CVE-2025-24814	[{"github": "GHSA-68r2-fwcg-qpm8"}, {"osv": "BIT-solr-2025-24814"}, {"osv": "GHSA-68r2-fwcg-qpm8"}]
CVE-2025-24802	[{"github": "GHSA-hj49-h7fq-px5h"}]
CVE-2025-24800	[{"github": "GHSA-wwx5-gpgr-vxr7"}]
CVE-2025-24795	[{"github": "GHSA-r2x6-cjg7-8r43"}]
CVE-2025-24794	[{"github": "GHSA-m4f6-vcj4-w5mx"}]
10 rows	
2 columns	

D



<https://github.com/google/osv.dev/issues/888>

# Vulnerability DB Update

- Wanna help?
  - Implement importers for data sources you care about
    - <https://github.com/nscuro/vuln-db?tab=readme-ov-file#extending>
    - Amazon Linux advisories?
    - Red Hat OVAL feed?
    - Chinese National Vulnerability Database?
    - More, more, more!
  - Use the generated database(s) to conduct research
    - <https://github.com/nscuro/vuln-db?tab=readme-ov-file#research>
  - Contribute to the data model
  - Contribute to scanning algorithms based on the data
    - <https://github.com/nscuro/vuln-db?tab=readme-ov-file#scanning>



<https://github.com/DependencyTrack/dependency-track/issues/4122>



<https://github.com/nscuro/vuln-db>



# HYADES UPDATE



# Hyades Update

- 4 ADRs for Kafka removal done
- Working on design docs for workflow orchestration and notification publishing solutions
- When docs ready: Start merging into main branch
- Almost all PRs from DT v4.12.x ported
- Release of v0.6.0 once everything is ported



ADRs related to Kafka removal  
<https://github.com/DependencyTrack/hyades/pull/1619>



# SNEAK PEEK: WORKFLOWS





# QUESTIONS & ANSWERS

