

OWASP DEPENDENCY-TRACK

Community Meeting
September 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

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. Recent Releases
2. Important Notices
3. Q&A

Recent Releases

Recent Releases: v4.13.4

- Released August 26th.
- Support for NVD JSON 2.0 data feeds
- 5 bugfixes that landed since the v4.13.3 release.
- Base image and dependency updates.



<https://docs.dependencytrack.org/changelog/#v4-13-3>

Important Notices

NVD JSON 1.0 Data Feeds Discontinuation

◦ **Aug 20, 2025: NVD Technical Update**

We plan to deploy updates to NVD systems on August 20th 2025. This deployment includes the following relevant changes:

Decommissioning of Legacy Data Feed Files

As of **August 20th, 2025**, the following legacy Data Feed files have been removed from the NVD [Data Feeds Page](#) and are no longer available for access or download

- 1.1 Vulnerability Feeds
- 1.0 CPE Match Feed
- XML CPE Dictionary Files to include the Official CPE 2.2 and 2.3 Dictionary .zip and .gz

Any organizations making use of the legacy feed files will need to update their systems to use the 2.0 APIs or the 2.0 data feed files.

What It Means For You

- NVD mirroring via feed files (default) **no longer works** for versions <4.13.4.
- Upgrading to 4.13.4 is **strongly** recommended.
 - No manual action needed. *Just works*™ after upgrade.
- If upgrading not possible, enable API-based mirroring (available since 4.10.0).

Configuration

Analyzers

Vulnerability Sources

National Vulnerability Database

GitHub Advisories

Google OSV Advisories (Beta)

Repositories

Notifications

Integrations

Access Management

General

☒ Enable National Vulnerability Database mirroring

The National Vulnerability Database (NVD) is the largest publicly available source of vulnerability intelligence. It is maintained by a group within the National Institute of Standards and Technology (NIST) and builds upon the work of MITRE and others. Vulnerabilities in the NVD are called Common Vulnerabilities and Exposures (CVE). There are over 100,000 CVEs documented in the NVD spanning from the 1990's to the present.

This product uses data from the NVD API but is not endorsed or certified by the NVD.

NVD Feeds URL

 ✓☒ Enable mirroring via API

Why should I enable API mirroring?

☐ x Additionally download feeds

Feeds will not be parsed, but made available to other clients at `/mirror/nvd`

API endpoint

API key

How do I get an API key?

Last Modification (UTC)

After mirroring the NVD database once completely, all following mirror operations will only request data that was modified since its last successful execution.

⚠ Changing the last modification datetime manually is generally not recommended, but may be used to force re-ingestion of NVD data. Note that due to a limitation in the NVD's REST API, only data for 120 consecutive days can be requested when a last modification datetime is configured. Resetting the last modification datetime will cause the entire NVD database to be re-mirrored.

What We'll Be Doing

- Remove API-based mirroring.
 - Likely in v4.14.0, *most definitely* in v5.
 - NVD *no longer* plans to remove feeds entirely.
 - Feed-based mirroring is more reliable and airgap-friendly.
 - No authentication requirements, works out of the box.

OSS Index Authentication Requirement

Authentication Required

OSS Index now requires authentication. Learn why this improves stability, how to set up your token, and how upcoming paid tiers enable unlimited access.

[Create account](#)[What is an API token](#)

Sonatype OSS Index now requires all users — including automated tools — to authenticate using a personal [API token](#).

What's changing:

- All Sonatype OSS Index web and API access now requires authentication.
- Anonymous requests are no longer allowed.
- Most integrations will start failing if a token is not configured.

Why this is happening:

- High anonymous traffic (especially from automated tools) has made it harder to maintain stable, fair service.
- Authentication allows us to give developers more control and avoid one-size-fits-all limits.
- It also sets the foundation for usage-based tiers and future product improvements.

What you get when you authenticate:

- Higher rate limits, tied to your usage — not your shared IP.
- Better reliability, with traffic shaping based on real users.
- Tool-specific setup instructions, pre-filled with your token.
- Future usage visibility, support access, and optional upgrades.

How to get started:

1. [Create an account](#) — it's free
2. Get your [API token](#)
3. Configure your tools

<https://ossindex.sonatype.org/doc/auth-required>

OSS Index Authentication Requirement

Upcoming Paid Tier: Unlimited Access

In the near future, Sonatype OSS Index will offer a paid tier for teams and organizations that need unlimited component lookups and no rate limits.

This tier is designed for enterprise-scale use: continuous builds, integrated SCA tools, and environments that depend on high-volume access to the most accurate component and vulnerability data available.

Smaller teams and hobbyists can continue using Sonatype OSS Index without charge. The component-based limits mean you can scan the same components as often as you like, which enables full DevOps best practices without penalty. Usage only scales as you add more applications and developers — in other words, at true enterprise scale.

<https://ossindex.sonatype.org/doc/auth-required>

What It Means For You

- OSS Index so far was the primary means of PURL-based analysis.
- Unless you configure authentication, you'll see a drop in vulns identified.
- If you run large Dependency-Track instances, consider looking into the upcoming paid tier.
- Even prior to this change, authentication granted higher rate limits, so it's recommended to setup anyway.

≡ Configuration

≡ Analyzers

Internal

Sonatype OSS Index

VulnDB

Snyk (Beta)

Trivy

≡ Vulnerability Sources

≡ Repositories

≡ Notifications

General



Enable OSS Index analyzer



Enable vulnerability alias synchronization

Registered email address

Registered email address

API token

.....



OSS Index is a service provided by Sonatype which identifies vulnerabilities in third-party components. Dependency-Track integrates natively with the OSS Index service to provide highly accurate results. Use of this analyzer requires a valid PackageURL for the components being analyzed.

Update

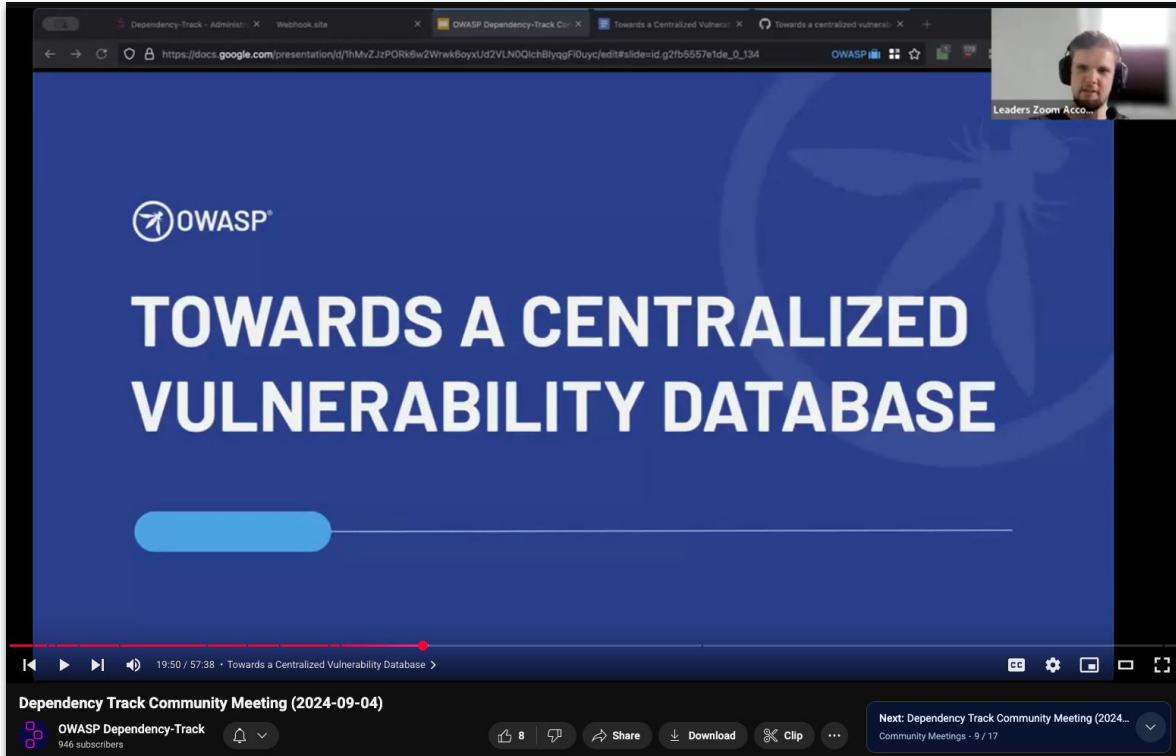
What We'll Be Doing: Short-Term

- Disable unauthenticated usage of OSS Index in v4.13.5.
- Log warnings when OSS Index is enabled but no AuthN configured.

What We'll Be Doing: Mid-Term

- Look into enabling the OSV integration by default.
 - Likely in v4.14.0, most definitely in v5.
 - Potentially only for a few selected ecosystems (e.g. Maven, NPM, ...).
 - Provides PURL-based matching data.
 - Does not require authentication.
 - Can use internal mirrors for air gapping.

What We'll Be Doing: Long-Term



OWASP

TOWARDS A CENTRALIZED VULNERABILITY DATABASE

19:50 / 57:38 • Towards a Centralized Vulnerability Database

Dependency Track Community Meeting (2024-09-04)

OWASP Dependency-Track
946 subscribers

8 | Share | Download | Clip

Next: Dependency Track Community Meeting (2024...
Community Meetings - 9 / 17



<https://www.youtube.com/watch?v=hzelt7jv6dE&t=674s>

What We'll Be Doing: Long-Term



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

Towards a centralized vulnerability database for Dependency-Track #4122

Edit

New issue

Open

0 / 6



nscuro opened on Sep 4, 2024 · edited by nscuro

Edits

Member

...

Current Behavior

When Dependency-Track came into existence around 2013, the only public and widely accepted vulnerability database was the NVD. Since its inception, DT has supported mirroring of the NVD.

Over the past decade, multiple other public vulnerability databases came into existence:

- GitHub Security Advisories: github.com/advisories
- OSV: osv.dev

Assignees

No one - [Assign yourself](#)

Labels

enhancement

help wanted

p2

size/XL

Type

No type

What We'll Be Doing: Long-Term

README Apache-2.0 license

vuln-db

license **apache**

Proof of concept for OWASP Dependency-Track's own, centralized vulnerability database.

Refer to [DependencyTrack/dependency-track#4122](#) for details.

Concept

```
graph LR; Start((Start)) --> Import[Import]; Import --> ImportGitHub[Import GitHub]; Import --> ImportNVD[Import NVD]; Import --> ImportOSV[Import OSV]; Import --> ImportMore[Import ...]; ImportGitHub --> Merge[Merge source databases]; ImportNVD --> Merge; ImportOSV --> Merge; ImportMore --> Merge; Merge --> Procure[Procure]; Procure --> Enrich[Enrich]; Enrich --> Stop((Stop));
```

The flowchart illustrates the process of building a centralized vulnerability database. It starts with a 'Start' node, which leads to an 'Import' block. This block branches into four parallel import steps: 'Import GitHub', 'Import NVD', 'Import OSV', and 'Import ...'. All four import steps feed into a 'Merge source databases' block. This is followed by 'Procure' and 'Enrich' blocks, which finally lead to a 'Stop' node.

Usage

Importing

```
docker run -it --rm \
-e 'GITHUB_TOKEN=<your_github_token>' \
-v "${pwd}:/workspace" \
-w '/workspace' \
ghcr.io/dependencytrack/vuln-db:snapshot \
import github nvd osv
```

This will populate the following database files in parallel:

- github.sqlite
- nvd.sqlite
- osv.sqlite

Merging

```
docker run -it --rm \
-v "${pwd}:/workspace" \
-w '/workspace' \
ghcr.io/dependencytrack/vuln-db:snapshot \
merge --output=all.sqlite github.sqlite nvd.sqlite osv.sqlite
```

What We'll Be Doing: Long-Term

Scanning

⚠ Warning

Not fully implemented, don't expect useful results yet.

To get a rough idea of the data quality in a database, it can be leveraged to scan a CycloneDX. The implementation of this command is also intended to showcase how matching logic may work.

```
docker run -it --rm \
  -v "$(pwd):/workspace" \
  -w '/workspace' \
  ghcr.io/dependencytrack/vuln-db:snapshot \
  scan --ensure-indexes --database=all.sqlite bom.json
```

```
.../development/projects/dependency-track-vuln-db
+ matched: vers:maven/≥42.7.4/<42.7.7 (source: osv)
+ matched: vers:maven/≥42.7.4/<42.7.7 (source: github)

GHSA-j288-q9x7-2f5v
- org.apache.commons/commons-lang3@3.17.0
+ matched: vers:maven/≥3.0/<3.18.0 (source: github)
+ matched: vers:maven/≥3.0/<3.18.0 (source: osv)

GHSA-p75g-cxfj-7wrx
- io.pebbletemplates/pebble@3.2.3
+ matched: vers:maven/≤3.2.3 (source: osv)
+ matched: vers:maven/≤3.2.3 (source: github)

GHSA-xpw8-rcwv-8f8p
- io.netty/netty-codec-http2@4.1.86.Final
+ matched: vers:maven/<4.1.100.Final (source: osv)
+ matched: vers:maven/<4.1.100.Final (source: github)

GHSA-xq3w-v528-46rv
- io.netty/netty-common@4.1.86.Final
+ matched: vers:maven/≤4.1.114.Final (source: github)
+ matched: vers:maven/<4.1.115.Final (source: osv)

nscuro@devastation:~/development/projects/dependency-track-vuln-db <main>
$
```

Q&A