



# DEPENDENCY-TRACK COMMUNITY MEETING

**JANUARY  
2024**

**THE DEPENDENCY-TRACK TEAM**

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

# AGENDA

---

Project Updates

01

How IBM CISO uses Dependency-Track

02

Q&A

03



# PROJECT UPDATES



## Project Updates

# 4.10.0 & 4.10.1 Released

---

- **4.10.0** 2023-12-08
  - Support for NVD mirroring via REST API
  - Support for CycloneDX *supplier, manufacturer, and authors*
  - ...
- **4.10.1** 2023-12-15
  - Various bug fixes :)

## Project Updates

# NVD Data Feed Retirement Extension

Legacy Data Feed File Retirement Update 1,078 views

Subscribe ☐nvd-news  
to nvd-news

Dec 14, 2023, 9:03:02 PM ☆ ↶ ⋮

**Legacy Data Feed File Retirement Update:**

Due to feedback received from many different downstream data consumer groups after our previous reminder, we will again be extending the retirement date for the Legacy Data Feed files. However, we will still be retiring the 1.0 APIs.

Going forward, we will be improving capabilities to allow for bulk download of the NVD dataset. The legacy data feeds will remain available until this effort is completed.

The following data feed files will remain available until further notice:

- [https://nvd.nist.gov/vuln/data-feeds#JSON\\_FEED](https://nvd.nist.gov/vuln/data-feeds#JSON_FEED)
- <https://nvd.nist.gov/vuln/data-feeds#cpeMatch>
- <https://nvd.nist.gov/vuln/data-feeds#transxml>
- <https://nvd.nist.gov/vuln/data-feeds#comments>
- <https://nvd.nist.gov/products/cpe>

The following API endpoints will be retired on 12/18/2023 as previously communicated:

- <https://services.nvd.nist.gov/rest/json/cve/1.0/>
- <https://services.nvd.nist.gov/rest/json/cves/1.0/>
- <https://services.nvd.nist.gov/rest/json/cpes/1.0/>

V/r,  
National Vulnerability Database Team  
National Institute of Standards and Technology (NIST)  
[n...@nist.gov](mailto:n...@nist.gov)

<https://groups.google.com/a/list.nist.gov/g/nvd-news/c/aofnAd3HP2g>

## Project Updates

# v4.11

---

- Support for CISA Known Exploited Vulnerabilities (KEV)
- Export of CycloneDX BOMs in all supported specification versions, not just latest
- Reduction of false positives in CPE matching against NVD database
- Global audit view for vulnerabilities
- (Maybe) scaling of EPSS scores to component level



## Project Updates

# v4.11

---

- Support for CISA Known Exploited Vulnerabilities (KEV)
- Export of CycloneDX BOMs in all supported specification versions, not just latest
- ~~Reduction of false positives in CPE matching against NVD database (preponed to 4.10)~~
- Global audit view for vulnerabilities
- ~~(Maybe) scaling of EPSS scores to component level~~
- + Improvements to processing of uploaded BOMs
- + Trivy integration for vulnerability analysis
- + Tracking of *created* and *last used* timestamps for API keys
- + Ability to assign default teams to OIDC users
- Aiming for release in early to mid February

## Project Updates

# v5.x (Hyades)

- A bit behind on GA-readiness work
- Exciting new *vulnerability policy* feature

```
name: Example
description: Foo bar
author: Jane Doe
validUntil: 2024-01-01T00:00:00Z
conditions:
- vuln.id == "CVE-123" || vuln.aliases.exists(alias, alias.id == "CVE-123")
- |-
  component.name == "foo"
  && project.name == "bar"
  && "internal" in project.tags
  && !component.is_dependency_of(v1.Component{
    group: "org.springframework.boot",
    version: "vers:maven/>=2.7.1|<3|!=2.8.5"
  })
analysis:
  state: NOT_AFFECTED
  justification: CODE_NOT_REACHABLE
  details: Because foo bar baz
  suppress: true
ratings:
- method: CVSSv3
  vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L
  severity: medium
  score: 6.3
```

<https://github.com/DependencyTrack/hyades/issues/930>



Project Updates

# SANS Difference Makers Award



<https://www.youtube.com/watch?v=fDB3JyYmcpU>

## Project Updates

# Upcoming Presentations

- OpenUK – State of Open Conference – **Feb 7th**
  - *Hyades – Dependency Track for Enterprise Supply Chain Security with SBOM*
  - Sahiba Mittal, Meha Bhargava
- OWASP Netherlands – February 2024 Chapter Meetup – **Feb 15th**
  - *OWASP Dependency-Track* (Flagship Project Intro)
  - Niklas Düster



<https://sched.co/1Xl5A>



<https://www.meetup.com/owasp-chapter-netherlands-meetup/events/298627782/>



# How IBM CISO uses Dependency-Track



How IBM CISO uses Dependency-Track

# Background

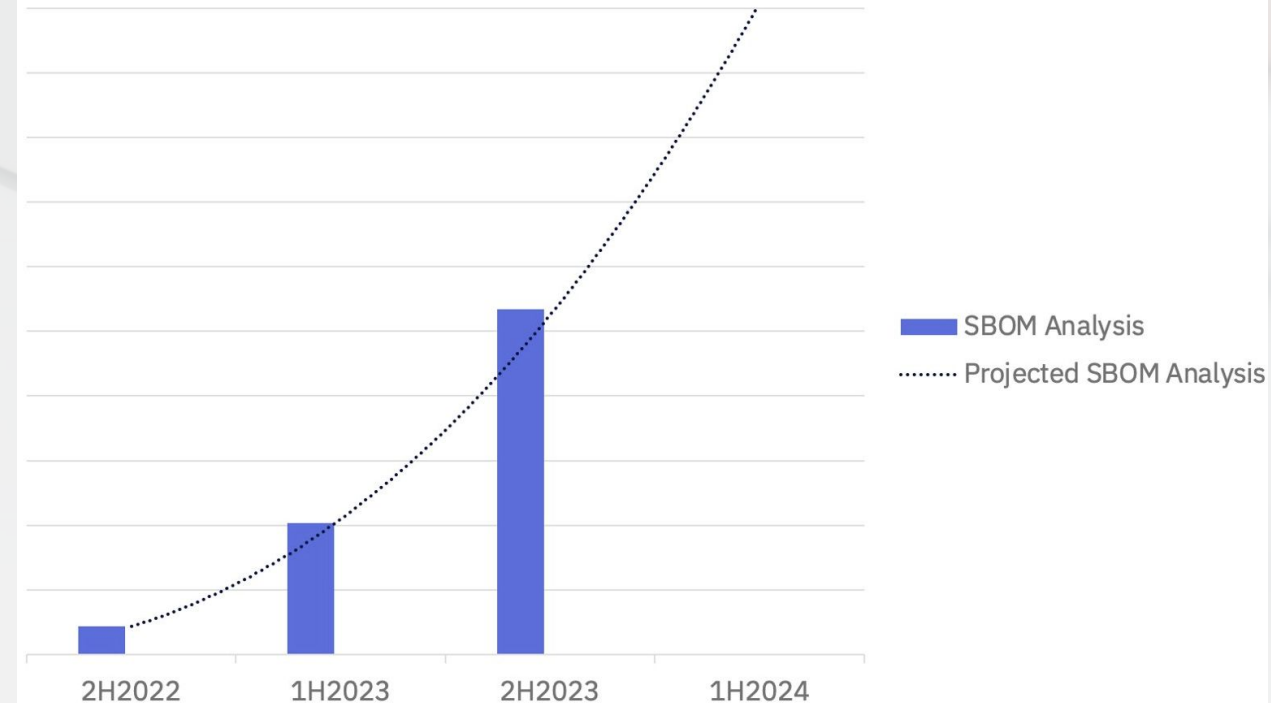
## What we are assessing:

- Third Party Security Risk Management (Suppliers, Vendors, OEMs)
- Mergers & Acquisitions
- IBM Product Security
- Open Source Security

## Business Value:

- 2327% increase YoY in SBOM assessments
- 95% reduction of assessment time per SBOM
- Increased awareness of 3<sup>rd</sup> party cyber hygiene

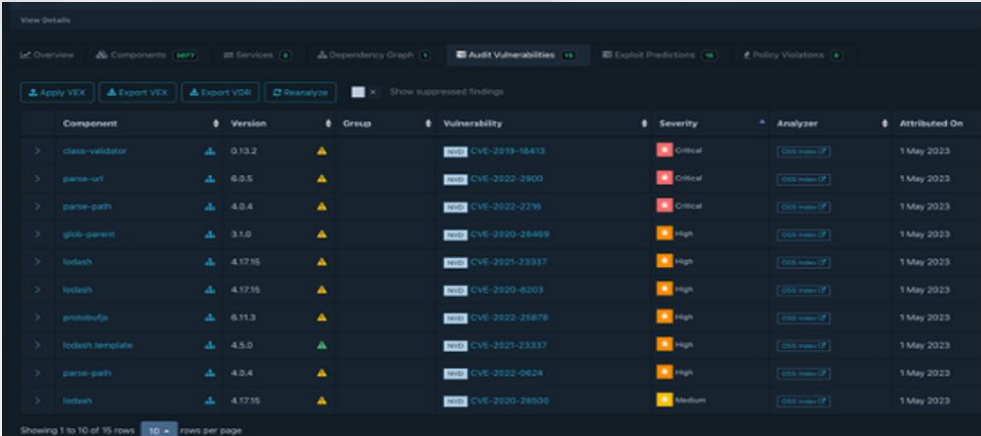
SBOM Analysis Trends





How IBM CISO uses Dependency-Track

# Automation Efficiencies



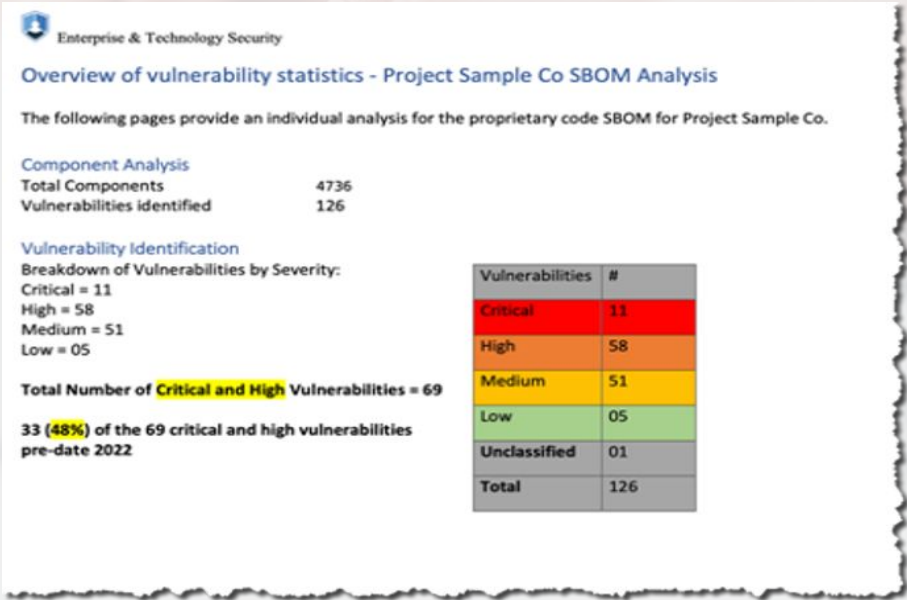
Component	Version	Group	Vulnerability	Severity	Analyzer	Attributed On
class-validator	0.13.2		CVE-2019-18413	Critical	OWASP	1 May 2023
parse-url	6.0.5		CVE-2022-2900	Critical	OWASP	1 May 2023
parse-path	4.0.4		CVE-2022-2216	Critical	OWASP	1 May 2023
glob-parent	3.1.0		CVE-2020-28489	High	OWASP	1 May 2023
lodash	4.17.15		CVE-2021-23337	High	OWASP	1 May 2023
lodash	4.17.15		CVE-2020-8203	High	OWASP	1 May 2023
protobufjs	6.11.3		CVE-2022-25878	High	OWASP	1 May 2023
lodash.template	4.5.0		CVE-2021-23337	High	OWASP	1 May 2023
parse-path	4.0.4		CVE-2022-0624	High	OWASP	1 May 2023
lodash	4.17.15		CVE-2020-28505	Medium	OWASP	1 May 2023

summary	components	out-of-date-components	vulns	crit-high-vulns
---------	------------	------------------------	-------	-----------------

Summary of all projects:

- Number of components up to date: 2353 out of 10815, or 21.8%
- Number of components not up to date: 4860 out of 10815, or 44.9%
- Number of components unknown if up to date: 3602 out of 10815, or 33.3%
- Vulnerabilities by Severity for all projects:
  - Number of CRITICAL Vulnerabilities: 48, or 10.3%
  - Number of HIGH Vulnerabilities: 225, or 48.5%
  - Number of MEDIUM Vulnerabilities: 176, or 37.9%
  - Number of LOW Vulnerabilities: 13, or 2.8%
  - Number of Vulnerabilities with an Unknown Severity: 2, or 0.4%
- Total Number of Vulnerabilities: 464

name	version	vulnerability	severity	source
snakeyaml	1.26	CVE-2022-1471	CRITICAL	NVD
mercurial	3.1.2	CVE-2017-1000116	CRITICAL	NVD
commons-text	1.9	CVE-2022-42889	CRITICAL	NVD
esapi	2.2.0.0	CVE-2022-23457	CRITICAL	NVD
quartz	2.3.0	CVE-2019-13990	CRITICAL	NVD
snakeyaml	1.33	CVE-2022-1471	CRITICAL	NVD
class-validator	0.12.2	CVE-2019-18413	CRITICAL	NVD
minimist	1.2.5	CVE-2021-44906	CRITICAL	NVD
quartz	2.3.0	CVE-2019-13990	CRITICAL	NVD
snakeyaml	1.29	CVE-2022-1471	CRITICAL	NVD
json-schema	0.2.3	CVE-2021-3918	CRITICAL	NVD



Enterprise & Technology Security

## Overview of vulnerability statistics - Project Sample Co SBOM Analysis

The following pages provide an individual analysis for the proprietary code SBOM for Project Sample Co.

**Component Analysis**

Total Components	4736
Vulnerabilities identified	126

**Vulnerability Identification**

Breakdown of Vulnerabilities by Severity:

- Critical = 11
- High = 58
- Medium = 51
- Low = 05

**Total Number of Critical and High Vulnerabilities = 69**

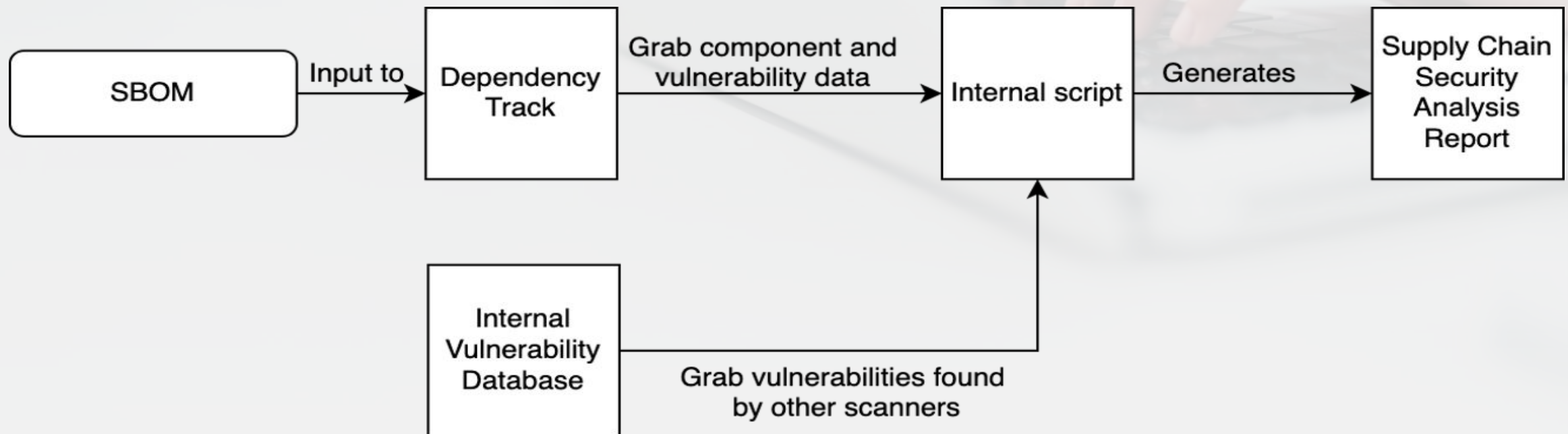
**33 (48%) of the 69 critical and high vulnerabilities pre-date 2022**

Vulnerabilities	#
Critical	11
High	58
Medium	51
Low	05
Unclassified	01
<b>Total</b>	<b>126</b>



How IBM CISO uses Dependency-Track

# Automation Architecture



How IBM CISO uses Dependency-Track

# Contributing Back



\*<https://twitter.com/JJLendl/status/1502127201893953545>



# Q&A

