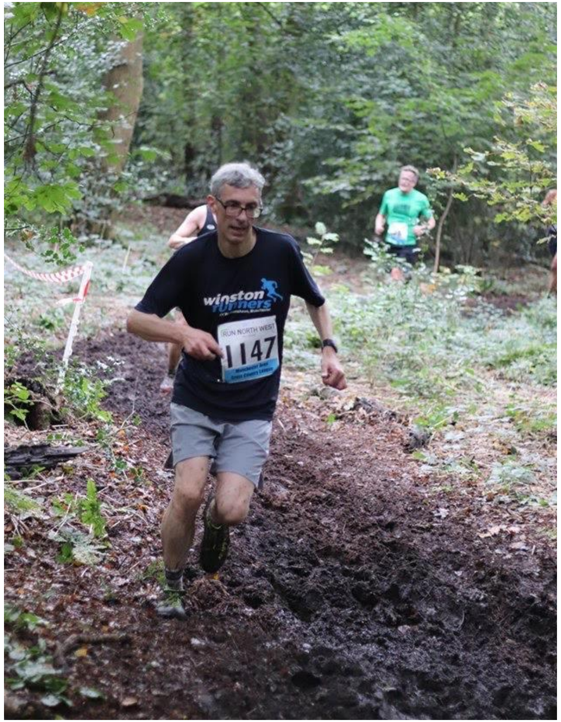
FOSDEM 2024

12 months of SBOMs

An Experience Report

FOSDEM 2024



CVE-Bin-Tool

- Binary vulnerability scanner
- Intel OSS since 2020 based on NVD
  - Now supports OSV and other sources
- GPL 3.0 or later Licence
- SBOM support since 2021 (SPDX and CycloneDX)
- CISA KEV support since 2022
- EPSS support since 2023
- GSOC project for past 3 years
- OpenSSF Best Practices
- 1000+ stars on GitHub

CVE-Bin-Tool - Release History

3.1	April 2022	
3.2	December 2022	- GSOC 2022 additions
3.2.1rc	May 2023	
3.2.1	May 2023	
3.3rc	December 2023	- GSOC 2023 additions
3.3rc2	January 2024	
3.3	February 2024	

SBOM4Python

- SBOM generator for Python modules
- Apache 2.0 Licence
- Generates SBOM in both SPDX and CycloneDX formats
    - SPDX Tag value, JSON, YAML
    - CycloneDX JSON
- Highest scoring SBOM generator according to SBOM Benchmark
- 21 stars on GitHub

SBOM4Python - Release History

0.4.0	November 2022	Package Supplier
0.5.0	January 2023	Enhanced supplier information
0.6.0	January 2023	Add CPE information for packages
0.7.0	January 2023	Package relationships
0.8.0	March 2023	More attributes and file support
0.9.0	March 2023	Updated licence handling
0.10.0	July 2023	Data enrichment and support for CycloneDX 1.5

Package details improvements from 0.4 to 0.10

```
PackageName: cve-bin-tool

SPDXID: SPDXRef-Package-1-cve-bin-tool

PackageVersion: 3.3

PrimaryPackagePurpose: APPLICATION

PackageSupplier: Person: Terri Oda (terri.oda@intel.com)

PackageDownloadLocation: https://pypi.org/project/cve-bin-tool/3.3

FilesAnalyzed: false

PackageChecksum: SHA1: 10ddd3a66ef44a6b7a7764603032c61ad4963151

PackageLicenseDeclared: GPL-3.0-or-later

PackageLicenseConcluded: GPL-3.0-or-later

PackageCopyrightText: NOASSERTION

PackageSummary: <text>CVE Binary Checker Tool</text>

ExternalRef: PACKAGE-MANAGER purl pkg:pypi/cve-bin-tool@3.3

ExternalRef: SECURITY cpe23Type cpe:2.3:a:terri_oda:cve-bin-tool:3.3:*:*:*:*:*:*:*
```

What have we done?

- Weekly GitHub Workflow (Monday 2am UTC)
- A clean virtual environment
- Install all dependencies (Ubuntu)
- Generate SBOM
    - In latest versions of SPDX (2.2/2.3) and CycloneDX (1.4/1.5)
    - For all versions of supported Python (3.7 to 3.11)

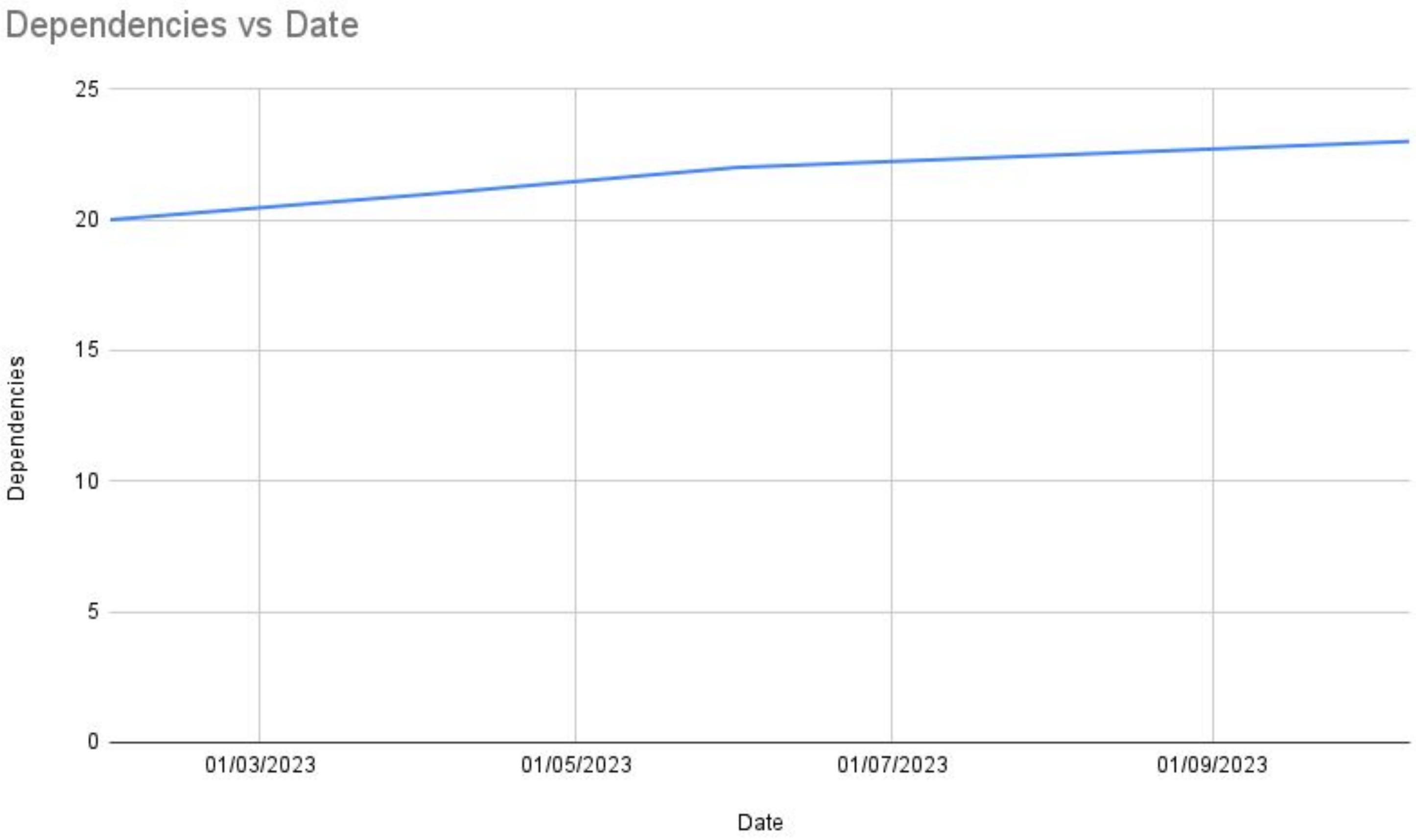
Python Dependencies

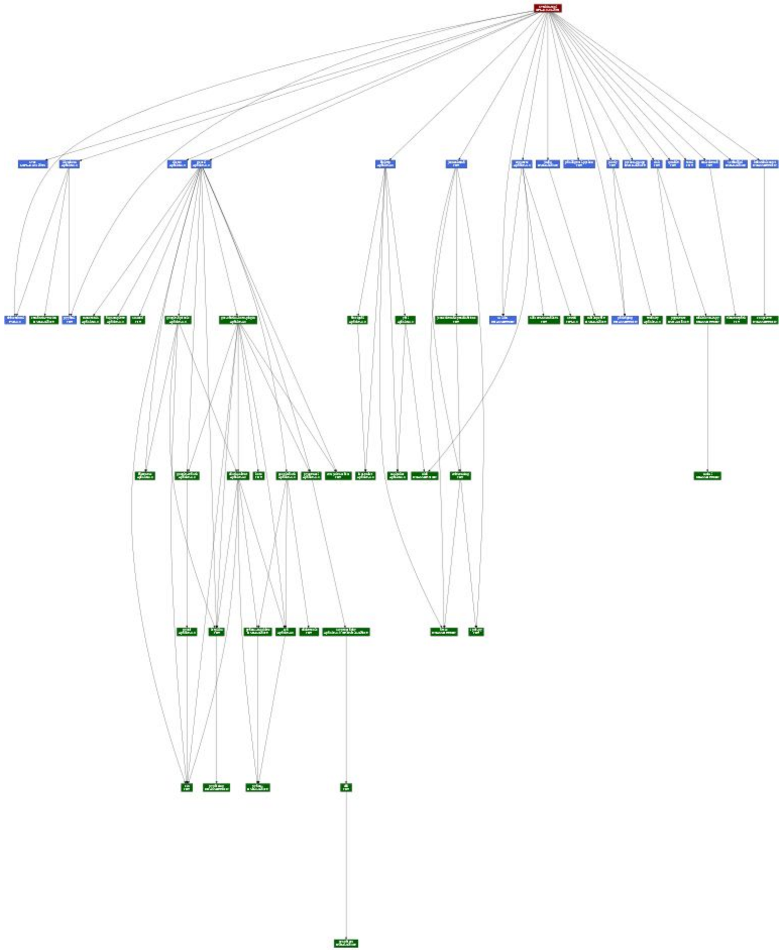
- Direct dependencies
- Environment
- **Nothing about transitive dependencies**

Requirements.txt - Direct dependencies

```
aiohttp[speedups]>=3.7.4

beautifulsoup4

cvss

defusedxml

distro

gsutil

importlib_metadata>=3.6; python_version < "3.10"

importlib_resources; python_version < "3.9"
```

FOSDEM 2024


Dependencies vs Date
25
20
15
10
5
0
Dependencies
01/03/2023
01/05/2023
01/07/2023
01/09/2023
Date



Generated from SBOM using sbom2dot and dot

Observations

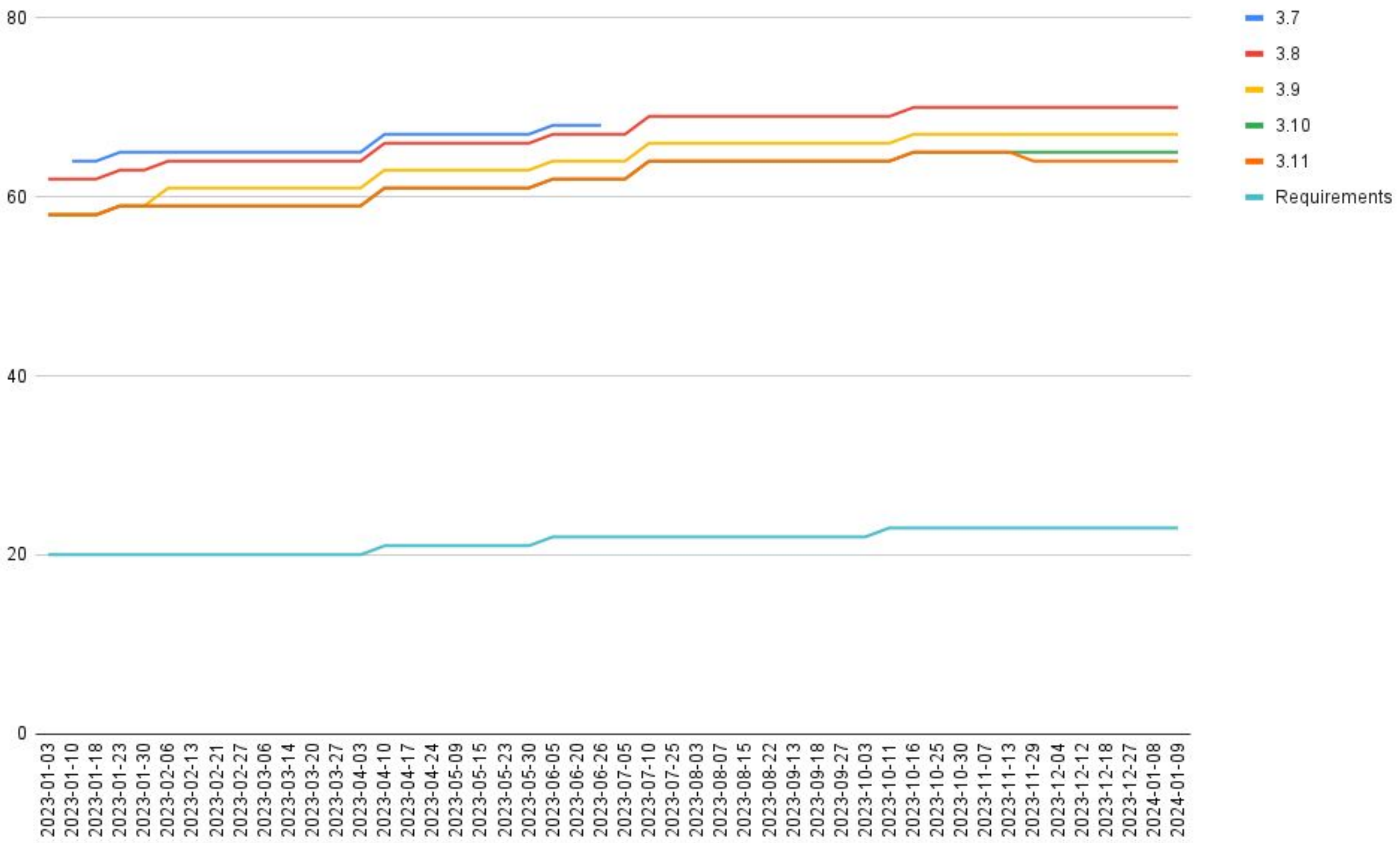
- Context
- SBOM Quality
- Velocity
- SBOM Data Analysis

Downloaded file history from git

sbomtrend used to summarise SBOM content

Context

- Nothing in SBOM says what environment is being used/targeted
    - What environment (Python)
    - What version (3.x)
    - What OS
- CycloneDX - add properties
- SPDX - can include comments


80
60
40
20
0
2023-01-03
2023-01-10
2023-01-18
2023-01-23
2023-01-30
2023-02-06
2023-02-13
2023-02-21
2023-02-27
2023-03-06
2023-03-14
2023-03-20
2023-03-27
2023-04-03
2023-04-10
2023-04-17
2023-04-24
2023-05-09
2023-05-15
2023-05-23
2023-05-30
2023-06-05
2023-06-20
2023-06-26
2023-07-05
2023-07-10
2023-07-25
2023-08-03
2023-08-07
2023-08-15
2023-08-22
2023-09-13
2023-09-18
2023-09-27
2023-10-03
2023-10-11
2023-10-16
2023-10-25
2023-10-30
2023-11-07
2023-11-13
2023-11-29
2023-12-04
2023-12-12
2023-12-18
2023-12-27
2024-01-08
2024-01-09
3.7
3.8
3.9
3.10
3.11
Requirements

Context

- Differences between versions of Python
  - More packages/different versions
- Transitive dependencies change independently of direct dependencies
- Later versions of the language need fewer dependencies

SBOM Quality

- Spdx-ntia-conformance tool
- Sbomscorecard
- Sbomqs
- Sbomaudit

SPDX NTIA Conformance (tool version 1.1.0)

```
Individual elements                            | Status
-------------------------------------------------------
All component names provided?                  | True
All component versions provided?               | True
All component identifiers provided?            | True
All component suppliers provided?              | False
SBOM author name provided?                     | True
SBOM creation timestamp provided?              | True
Dependency relationships provided?             | True
```

sbom-scorecard (tool version 0.0.7)

```
║ 1 │ Spec Compliance  │ 25/25 │                                        ║
║ 2 │ Package ID       │ 0/20  │ 0% have either purls (100%) or CPEs (0%) ║
║ 3 │ Package Versions │ 20/20 │                                        ║
║ 4 │ Package Licenses │ 14/20 │                                        ║
║ 5 │ Creation Info    │ 15/15 │
```

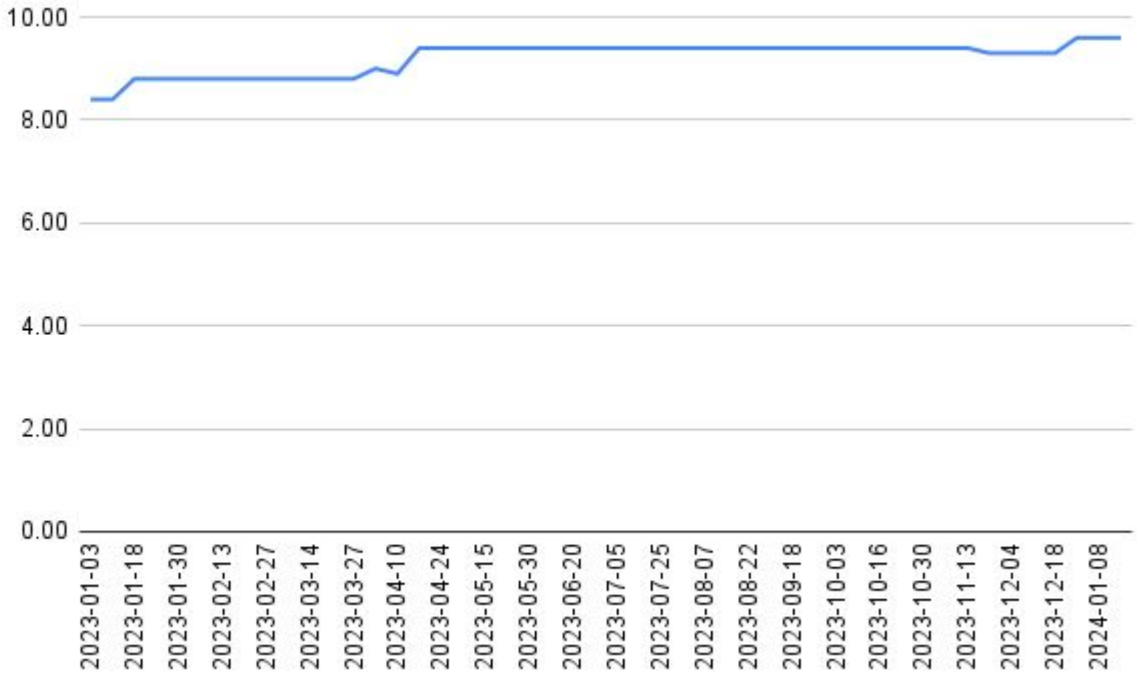
Start of 2023

sbom-scorecard (tool version 0.0.7)

```
║ 1 │ Spec Compliance   │ 25/25  │
║ 2 │ Package ID        │ 18/20  │ 94% have either purls (100%) or CPEs (94%)
║
║ 3 │ Package Versions │ 20/20  │
║ 4 │ Package Licenses │ 16/20  │
║ 5 │ Creation Info     │ 15/15  │
```

Start of 2024

Sbomqs (version 0.0.29)



sbomaudit (version 0.3.1)

```
"summary": [
     "text": "NTIA conformant: FAILED",
     "text": "Checks passed 370",
     "text": "Checks failed 19",
 ]
```

Start of 2023

sbomaudit (version 0.3.1)

```
"summary": [
     "text": "NTIA conformant: FAILED",
     "text": "Checks passed 564",
     "text": "Checks failed 23",
 ]
```

Start of 2024

Scan on 29th January 2024

```
[ ] Using latest version of package aiohttp: Version is 3.9.2; latest is 3.9.3
[ ] Using latest version of package multidict: Version is 6.0.4; latest is 6.0.5
[ ] Using latest version of package httplib2: Version is 0.20.4; latest is 0.22.0
[ ] Using latest version of package rsa: Version is 4.7.2; latest is 4.9
[ ] Using old version of package rsa: Age of release is 1072 days
[ ] Using latest version of package cryptography: Version is 42.0.1; latest is 42.0.2
[ ] Using latest version of package certifi: Version is 2023.11.17; latest is 2024.2.2
[ ] Using latest version of package urllib3: Version is 2.1.0; latest is 2.2.
```

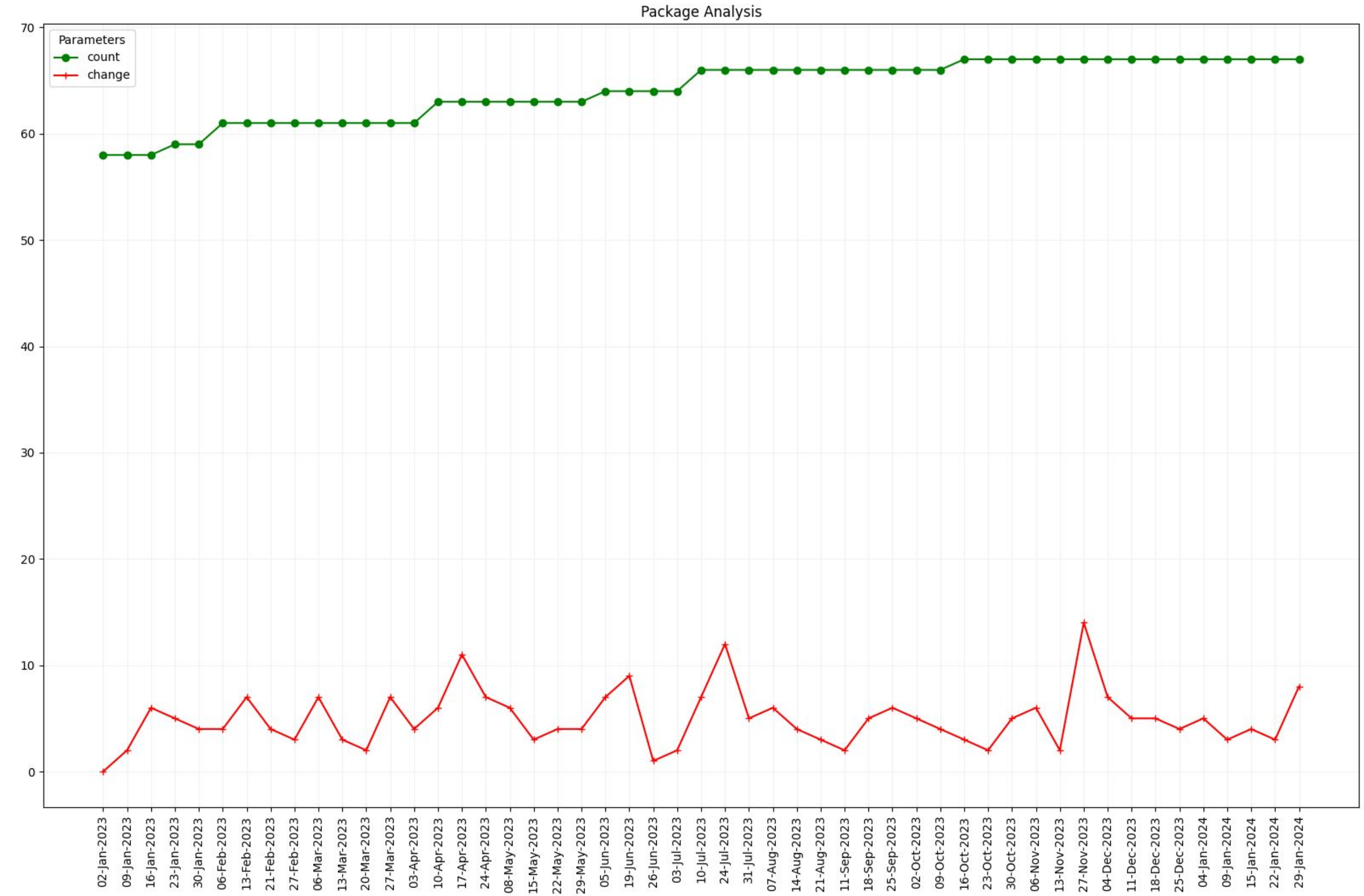
Not using latest version - Has version pinning been used?

SBOM Quality

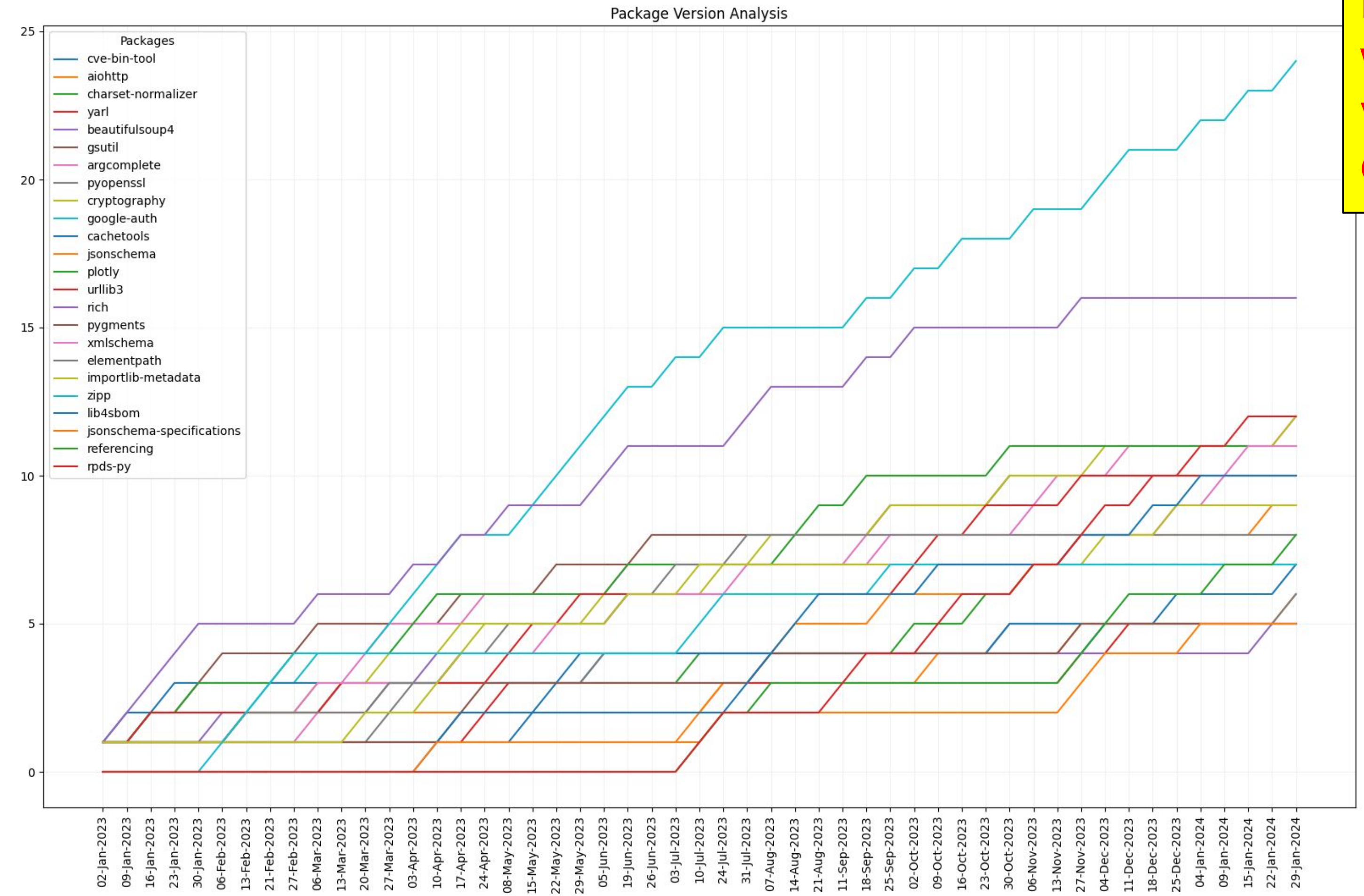
- NTIA conformance is difficult
    - Metadata missing from packages
    - Particular issue is accurate supplier information
- Data enrichment enhances quality of SBOM

Velocity

- How much change?
- What is changing?
- What is not changing?



Package Analysis
Parameters
count
change
70
60
50
40
30
20
10
0
02-Jan-2023
09-Jan-2023
16-Jan-2023
23-Jan-2023
30-Jan-2023
06-Feb-2023
13-Feb-2023
21-Feb-2023
27-Feb-2023
06-Mar-2023
13-Mar-2023
20-Mar-2023
27-Mar-2023
03-Apr-2023
10-Apr-2023
17-Apr-2023
24-Apr-2023
08-May-2023
15-May-2023
22-May-2023
29-May-2023
05-Jun-2023
19-Jun-2023
26-Jun-2023
03-Jul-2023
10-Jul-2023
24-Jul-2023
31-Jul-2023
07-Aug-2023
14-Aug-2023
21-Aug-2023
11-Sep-2023
18-Sep-2023
25-Sep-2023
02-Oct-2023
09-Oct-2023
16-Oct-2023
23-Oct-2023
30-Oct-2023
06-Nov-2023
13-Nov-2023
27-Nov-2023
04-Dec-2023
11-Dec-2023
18-Dec-2023
25-Dec-2023
04-Jan-2024
09-Jan-2024
15-Jan-2024
22-Jan-2024
29-Jan-2024

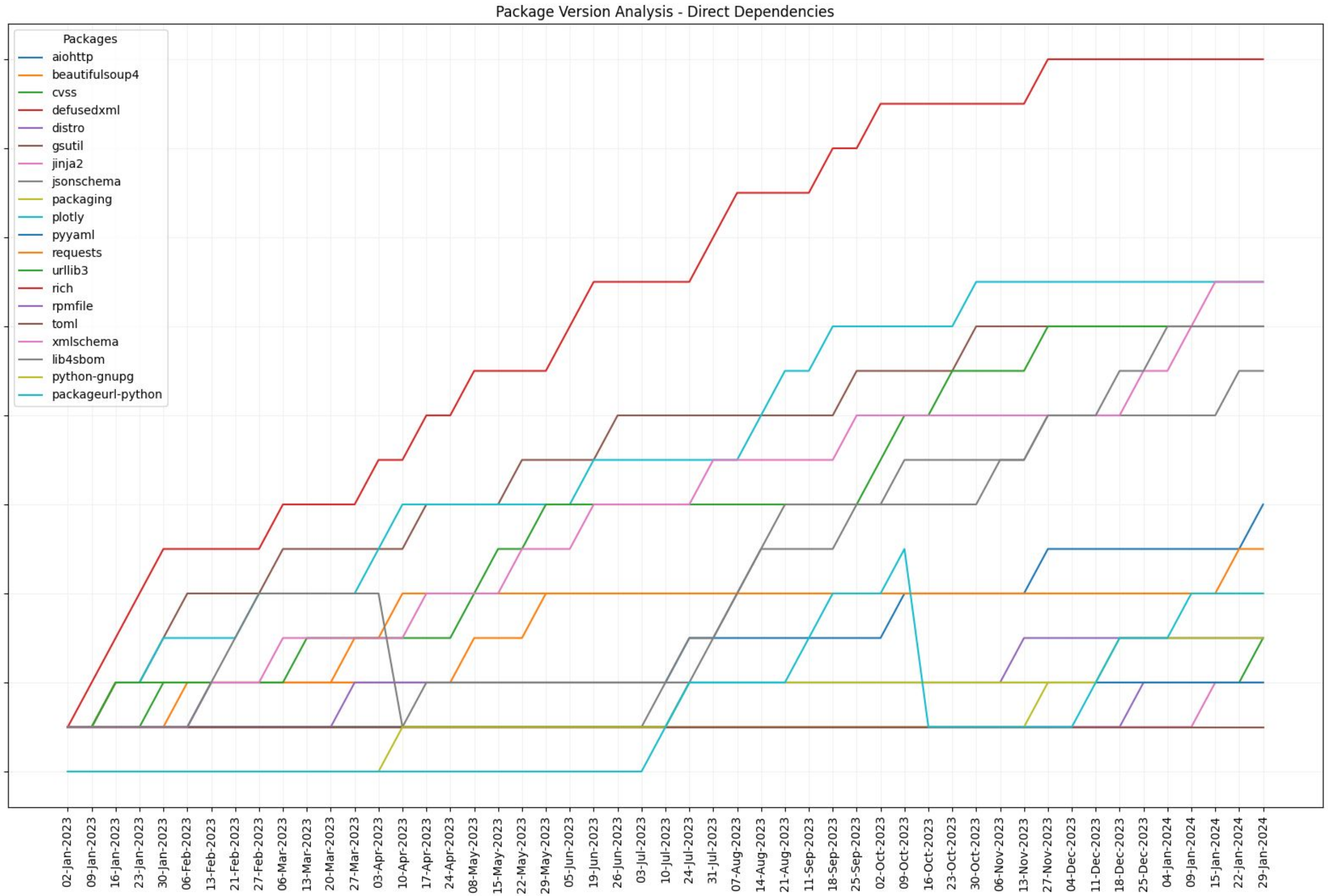


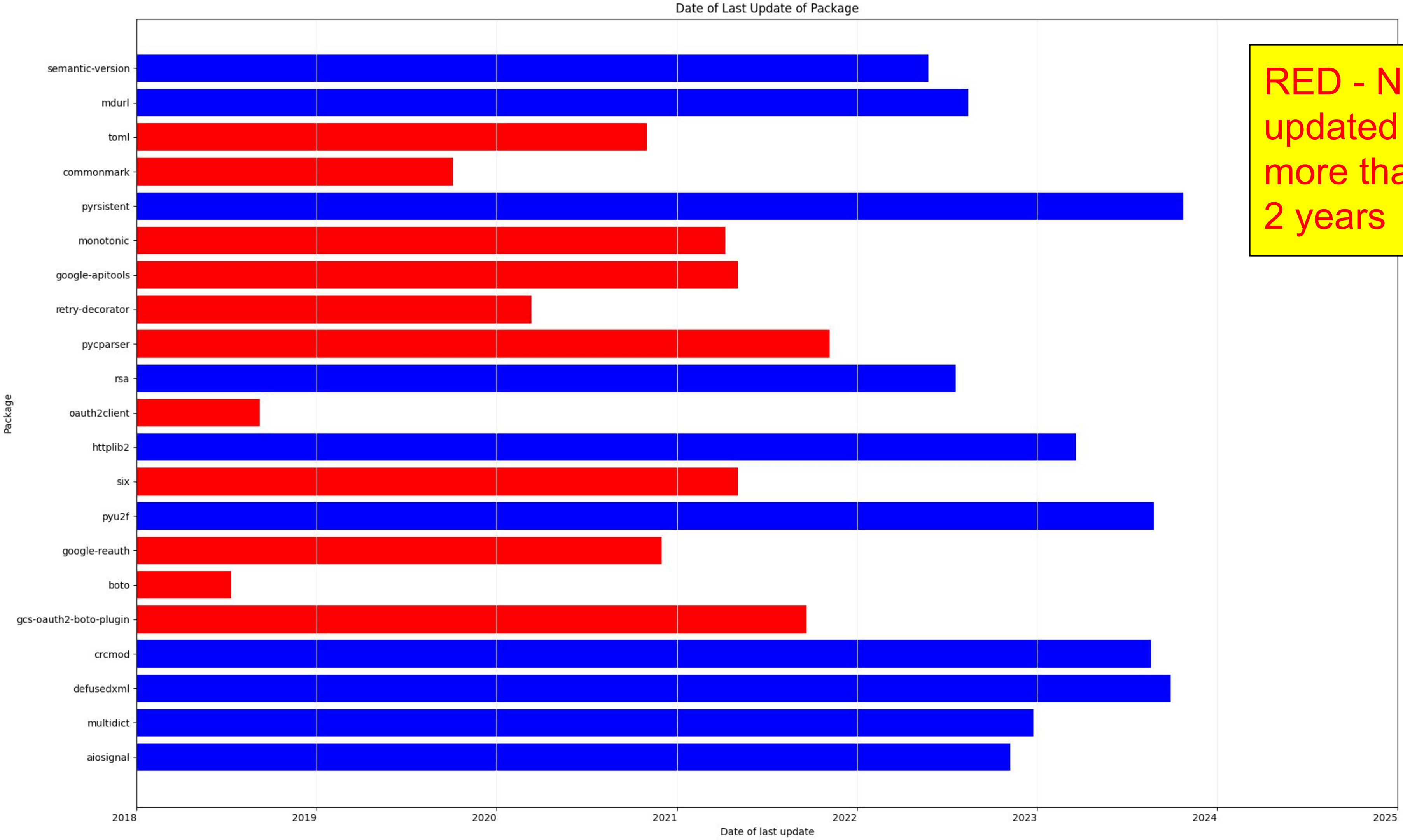
Packages with 5+ version changes

Packages - frequent updates

🟩 Green - direct dependencies

Package	No of Updates	Security Fixes
🟩 gsutil	10 (5.17 - > 5.27)	None
argcomplete	12 (2.0.0 -> 3.2.2)	None
cryptography	12 (39.0.0 -> 42.0.1)	Yes
google-auth	24 (2.15.0->2.27.0)	None
🟩 plotly	11 (5.11.0 -> 5.18.0)	None
🟩 urlib3	10 (1.26.13 -> 2.1.0)	Yes
🟩 rich	16 (13.0.0 -> 13.7.0)	None (remove use of unmaintained package)
🟩 xmlschema	11 (2.11 -> 3.0.1)	None
🟩 lib4sbom	10 (0.3.0 -> 0.6.1)	None
rpds-py	12 (0.8.10 -> 0.17.1)	None


Package Version Analysis - Direct Dependencies
Packages
aiohttp
beautifulsoup4
cvss
defusedxml
distro
gsutil
jinja2
jsonschema
packaging
plotly
pyyaml
requests
urllib3
rich
rpmfile
toml
xmlschema
lib4sbom
python-gnupg
packageurl-python
0
2
4
6
8
10
12
14
16
02-Jan-2023
09-Jan-2023
16-Jan-2023
23-Jan-2023
30-Jan-2023
06-Feb-2023
13-Feb-2023
21-Feb-2023
27-Feb-2023
06-Mar-2023
13-Mar-2023
20-Mar-2023
27-Mar-2023
03-Apr-2023
10-Apr-2023
17-Apr-2023
24-Apr-2023
08-May-2023
15-May-2023
22-May-2023
29-May-2023
05-Jun-2023
19-Jun-2023
26-Jun-2023
03-Jul-2023
10-Jul-2023
24-Jul-2023
31-Jul-2023
07-Aug-2023
14-Aug-2023
21-Aug-2023
11-Sep-2023
18-Sep-2023
25-Sep-2023
02-Oct-2023
09-Oct-2023
16-Oct-2023
23-Oct-2023
30-Oct-2023
06-Nov-2023
13-Nov-2023
27-Nov-2023
04-Dec-2023
11-Dec-2023
18-Dec-2023
25-Dec-2023
04-Jan-2024
09-Jan-2024
15-Jan-2024
22-Jan-2024
29-Jan-2024



RED - Not updated for more than 2 years

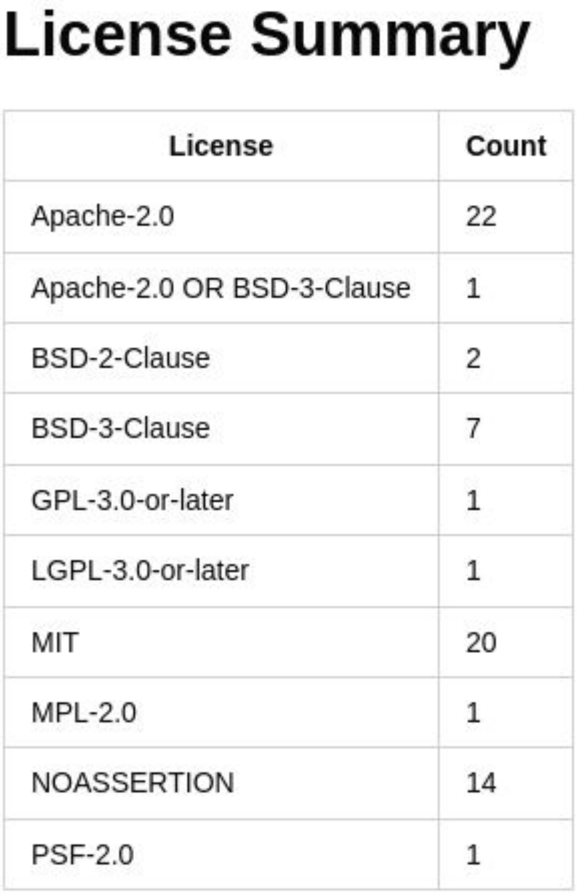
Velocity

- There is at least one change **every** week
- 10 packages have 10 updates or more per year
  - Functionality changes or security fixes?
- 21 packages have not been updated in past 12 months
  - Unmaintained?
- If using dependency pinning
  - Direct dependencies change frequently

FOSDEM 2024

SBOM Data Analysis

- Invalid license identifiers reported in SPDX as License Comment
- 26 packages out 70 have incorrect license identifiers
  - How many of these packages have been updated in the past 12 months?
- Apache 2 and BSD most common error



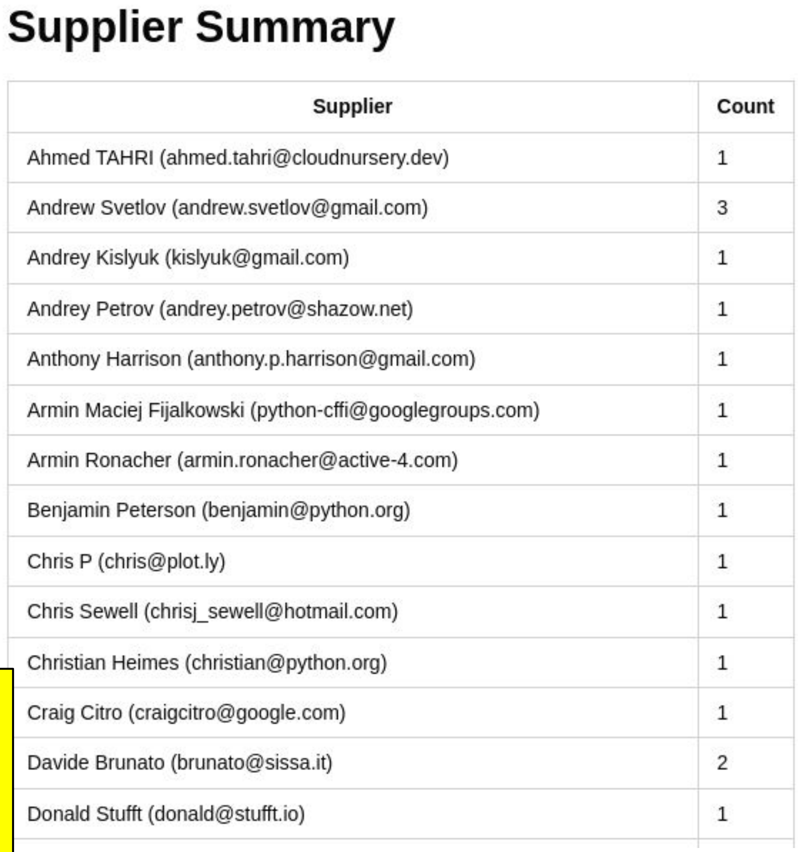
License Summary

License	Count
Apache-2.0	22
Apache-2.0 OR BSD-3-Clause	1
BSD-2-Clause	2
BSD-3-Clause	7
GPL-3.0-or-later	1
LGPL-3.0-or-later	1
MIT	20
MPL-2.0	1
NOASSERTION	14
PSF-2.0	1

Generated from SBOM using sbom2doc

SBOM Data Analysis

- Lots of different suppliers!
- Could be used to identify the suppliers you are most dependent on
  - Maybe you should be supporting them!
- 4 packages with unknown suppliers
  - 3 updated in last 12 months



Supplier Summary

Supplier	Count
Ahmed TAHRI (ahmed.tahri@cloudnursery.dev)	1
Andrew Svetlov (andrew.svetlov@gmail.com)	3
Andrey Kislyuk (kislyuk@gmail.com)	1
Andrey Petrov (andrey.petrov@shazow.net)	1
Anthony Harrison (anthony.p.harrison@gmail.com)	1
Armin Maciej Fijalkowski (python-cffi@googlegroups.com)	1
Armin Ronacher (armin.ronacher@active-4.com)	1
Benjamin Peterson (benjamin@python.org)	1
Chris P (chris@plot.ly)	1
Chris Sewell (chrisj_sewell@hotmail.com)	1
Christian Heimes (christian@python.org)	1
Craig Citro (craigcitro@google.com)	1
Davide Brunato (brunato@sissa.it)	2
Donald Stufft (donald@stufft.io)	1

Generated from SBOM using sbom2doc

Change Analysis

```
Summary
-------
Version changes:  39
License changes:  12
Removed packages: 2
New packages:     11
```

Generated from SBOM using sbomdiff

Change from start of 2023 to start of 2024

Vulnerability Management

- SBOM from start of 2023
  - 6 vulnerable products (7 HIGH, 6 MEDIUM)
- SBOM from start of 2024
  - 1 vulnerable product (1 MEDIUM)

Key Takeaways

- Generate SBOM for **all** supported environments
- Generate SBOM in CycloneDX and SPDX
- Help to improve quality of package metadata
- Use tools to analyse SBOM
- Install latest versions of ALL packages at installation time

  -
    ```
    pip install <module> --upgrade --upgrade-strategy=eager
    ```
- Keep packages up to date
- Use latest version of Python that you can to minimise number of dependencies

Next Steps

- Do same for file changes (use SBOM4Files)
- Generate Vulnerability documents with each SBOM

Links to Tools

Cve-bin-tool - https://github.com/intel/cve-bin-tool and https://pypi.org/project/cve-bin-tool/

Sbom4python - https://pypi.org/project/sbom4python/

Sbomdiff - https://pypi.org/project/sbomdiff/

Sbom2doc - https://pypi.org/project/sbom2doc/

Sbom2dot - https://pypi.org/project/sbom2dot/

Sbomtrend - https://pypi.org/project/sbomtrend/

Sbomaudit - https://pypi.org/project/sbomaudit/

Sbomqs - https://github.com/interlynk-io/sbomqs

Sbomscorecard - https://github.com/eBay/sbom-scorecard

Ntia-conformance-checker - https://pypi.org/project/ntia-conformance-checker/

Contact Details

LinkedIn

GitHub

anthony@aph10.com