12 months of SBOMs

An Experience Report

Licenced under Creative Commons Attribution-ShareAlike 4.0 International Licence

© Anthony Harrison 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

© Anthony Harrison 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

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.4.0</td>
<td>November 2022</td>
<td>Package Supplier</td>
</tr>
<tr>
<td>0.5.0</td>
<td>January 2023</td>
<td>Enhanced supplier information</td>
</tr>
<tr>
<td>0.6.0</td>
<td>January 2023</td>
<td>Add CPE information for packages</td>
</tr>
<tr>
<td>0.7.0</td>
<td>January 2023</td>
<td>Package relationships</td>
</tr>
<tr>
<td>0.8.0</td>
<td>March 2023</td>
<td>More attributes and file support</td>
</tr>
<tr>
<td>0.9.0</td>
<td>March 2023</td>
<td>Updated licence handling</td>
</tr>
<tr>
<td>0.10.0</td>
<td>July 2023</td>
<td>Data enrichment and support for CycloneDX 1.5</td>
</tr>
</tbody>
</table>

© Anthony Harrison 2024
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: 10ddd3a66e44a6b7a7764603032c61ad4963151

PackageLicenseDeclared: GPL-3.0-or-later

PackageLicenseConcluded: GPL-3.0-or-later

PackageCopyrightText: NOASSERTION

PackageSummary: CVE Binary Checker Tool

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"
Generated from SBOM using sbom2dot and dot

© Anthony Harrison 2024
Observations

- Context
- SBOM Quality
- Velocity
- SBOM Data Analysis

Downloaded file history from git

`sbtomtrend` 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
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
<table>
<thead>
<tr>
<th>Individual elements</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>All component names provided?</td>
<td>True</td>
</tr>
<tr>
<td>All component versions provided?</td>
<td>True</td>
</tr>
<tr>
<td>All component identifiers provided?</td>
<td>True</td>
</tr>
<tr>
<td>All component suppliers provided?</td>
<td>False</td>
</tr>
<tr>
<td>SBOM author name provided?</td>
<td>True</td>
</tr>
<tr>
<td>SBOM creation timestamp provided?</td>
<td>True</td>
</tr>
<tr>
<td>Dependency relationships provided?</td>
<td>True</td>
</tr>
</tbody>
</table>

© Anthony Harrison 2024
# sbom-scorecard (tool version 0.0.7)

<table>
<thead>
<tr>
<th></th>
<th>Spec Compliance</th>
<th>25/25</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Package ID</td>
<td>0/20</td>
<td>0% have either purls (100%) or CPEs (0%)</td>
</tr>
<tr>
<td>3</td>
<td>Package Versions</td>
<td>20/20</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Package Licenses</td>
<td>14/20</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Creation Info</td>
<td>15/15</td>
<td></td>
</tr>
</tbody>
</table>

Start of 2023

© Anthony Harrison 2024
sbom-scorecard (tool version 0.0.7)

<table>
<thead>
<tr>
<th></th>
<th>Spec Compliance</th>
<th>25/25</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Package ID</td>
<td>18/20</td>
</tr>
<tr>
<td>3</td>
<td>Package Versions</td>
<td>20/20</td>
</tr>
<tr>
<td>4</td>
<td>Package Licenses</td>
<td>16/20</td>
</tr>
<tr>
<td>5</td>
<td>Creation Info</td>
<td>15/15</td>
</tr>
</tbody>
</table>

Start of 2024
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 httpplib2: 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?
Packages with 5+ version changes
## Packages - frequent updates

<table>
<thead>
<tr>
<th>Package</th>
<th>No of Updates</th>
<th>Security Fixes</th>
</tr>
</thead>
<tbody>
<tr>
<td>gsutil</td>
<td>10 (5.17 - &gt; 5.27)</td>
<td>None</td>
</tr>
<tr>
<td>argcomplete</td>
<td>12 (2.0.0 -&gt; 3.2.2)</td>
<td>None</td>
</tr>
<tr>
<td>cryptography</td>
<td>12 (39.0.0 -&gt; 42.0.1)</td>
<td>Yes</td>
</tr>
<tr>
<td>google-auth</td>
<td>24 (2.15.0 -&gt; 2.27.0)</td>
<td>None</td>
</tr>
<tr>
<td>plotly</td>
<td>11 (5.11.0 -&gt; 5.18.0)</td>
<td>None</td>
</tr>
<tr>
<td>urllib3</td>
<td>10 (1.26.13 -&gt; 2.1.0)</td>
<td>Yes</td>
</tr>
<tr>
<td>rich</td>
<td>16 (13.0.0 -&gt; 13.7.0)</td>
<td>None (remove use of unmaintained package)</td>
</tr>
<tr>
<td>xmlschema</td>
<td>11 (2.11 -&gt; 3.0.1)</td>
<td>None</td>
</tr>
<tr>
<td>lib4sbom</td>
<td>10 (0.3.0 -&gt; 0.6.1)</td>
<td>None</td>
</tr>
<tr>
<td>rpds-py</td>
<td>12 (0.8.10 -&gt; 0.17.1)</td>
<td>None</td>
</tr>
</tbody>
</table>

© Anthony Harrison 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
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

<table>
<thead>
<tr>
<th>License</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apache-2.0</td>
<td>22</td>
</tr>
<tr>
<td>Apache-2.0 OR BSD-3-Clause</td>
<td>1</td>
</tr>
<tr>
<td>BSD-2-Clause</td>
<td>2</td>
</tr>
<tr>
<td>BSD-3-Clause</td>
<td>7</td>
</tr>
<tr>
<td>GPL-3.0-or-later</td>
<td>1</td>
</tr>
<tr>
<td>LGPL-3.0-or-later</td>
<td>1</td>
</tr>
<tr>
<td>MIT</td>
<td>20</td>
</tr>
<tr>
<td>MPL-2.0</td>
<td>1</td>
</tr>
<tr>
<td>NOASSERTION</td>
<td>14</td>
</tr>
<tr>
<td>PSF-2.0</td>
<td>1</td>
</tr>
</tbody>
</table>

Generated from SBOM using sbom2doc

© Anthony Harrison 2024
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

<table>
<thead>
<tr>
<th>Supplier</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ahmed TAHRI (<a href="mailto:ahmed.tahri@cloudnursery.dev">ahmed.tahri@cloudnursery.dev</a>)</td>
<td>1</td>
</tr>
<tr>
<td>Andrew Svetlov (<a href="mailto:andrew.svetlov@gmail.com">andrew.svetlov@gmail.com</a>)</td>
<td>3</td>
</tr>
<tr>
<td>Andrey Kislyuk (<a href="mailto:kislyuk@gmail.com">kislyuk@gmail.com</a>)</td>
<td>1</td>
</tr>
<tr>
<td>Andrey Petrov (<a href="mailto:andrey.petrov@shazow.net">andrey.petrov@shazow.net</a>)</td>
<td>1</td>
</tr>
<tr>
<td>Anthony Harrison (<a href="mailto:anthony.p.harrison@gmail.com">anthony.p.harrison@gmail.com</a>)</td>
<td>1</td>
</tr>
<tr>
<td>Armin Maciej Fijalkowski (<a href="mailto:python-cffi@googlegroups.com">python-cffi@googlegroups.com</a>)</td>
<td>1</td>
</tr>
<tr>
<td>Armin Ronacher (<a href="mailto:armin.ronacher@active-4.com">armin.ronacher@active-4.com</a>)</td>
<td>1</td>
</tr>
<tr>
<td>Benjamin Peterson (<a href="mailto:benjamin@python.org">benjamin@python.org</a>)</td>
<td>1</td>
</tr>
<tr>
<td>Chris P (<a href="mailto:chris@plot.ly">chris@plot.ly</a>)</td>
<td>1</td>
</tr>
<tr>
<td>Chris Sewell (<a href="mailto:chrisj_sewell@hotmail.com">chrisj_sewell@hotmail.com</a>)</td>
<td>1</td>
</tr>
<tr>
<td>Christian Heimes (<a href="mailto:christian@python.org">christian@python.org</a>)</td>
<td>1</td>
</tr>
<tr>
<td>Craig Citro (<a href="mailto:craigcitro@google.com">craigcitro@google.com</a>)</td>
<td>1</td>
</tr>
<tr>
<td>Davide Brunato (<a href="mailto:brunato@sissa.it">brunato@sissa.it</a>)</td>
<td>2</td>
</tr>
<tr>
<td>Donald Stift (<a href="mailto:donald@stuff.io">donald@stuff.io</a>)</td>
<td>1</td>
</tr>
</tbody>
</table>
Change Analysis

Summary

--------

Version changes: 39
License changes: 12
Removed packages: 2
New packages: 11

Change from start of 2023 to start of 2024

© Anthony Harrison 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


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/

© Anthony Harrison 2024
Contact Details

LinkedIn

GitHub

anthony@aph10.com