



COMMUNITY
THE ASF CONFERENCE
CODE

Security United

Collaborative effort on securing Airflow ecosystem with
Alpha-Omega, PSF & ASF



Jarek Potiuk

Apache Airflow PMC member &
committer

Member of Apache Software
Foundation Security Committee



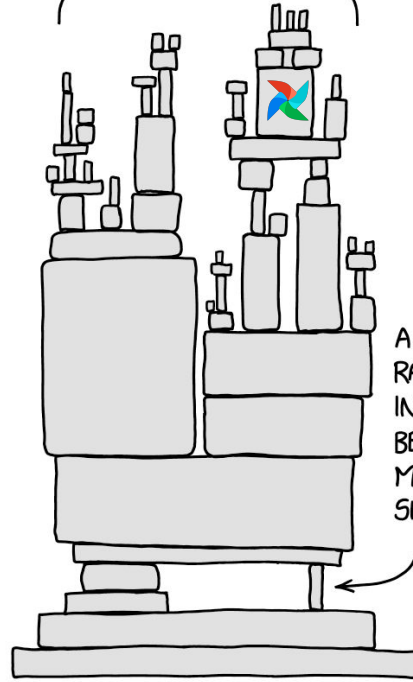
Michael Winser

Alpha-Omega co-founder

Eclipse Foundation Security
Strategy Ambassador

What is Supply Chain Risk

ALL MODERN DIGITAL
INFRASTRUCTURE



A PROJECT SOME
RANDOM PERSON
IN NEBRASKA HAS
BEEN THANKLESSLY
MAINTAINING
SINCE 2003

Supply Chain Risk Model

Vulnerabilities

Tampering

Availability

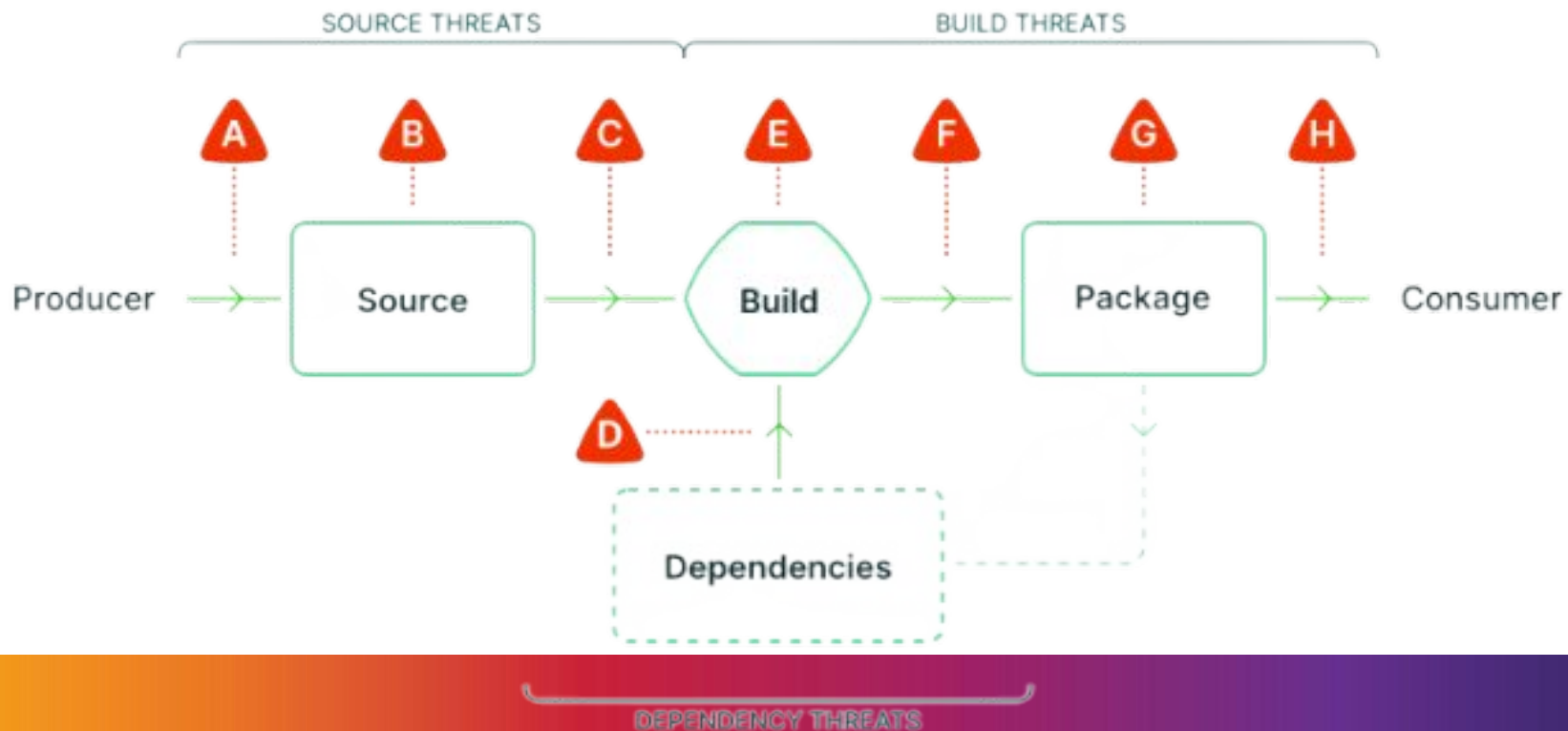
X

Culture

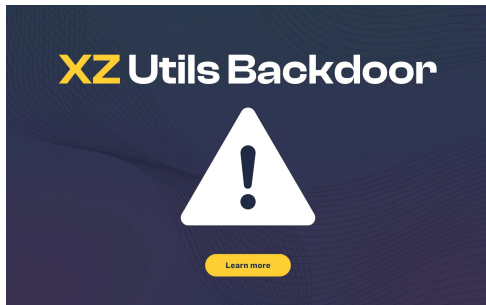
Process

Solutions

SLSA Threat Model



Why Now



[BLOG HOME](#) >

PyPI malware creators are starting to employ Anti-Debug techniques

By [Andrey Polkovnychenko](#) | December 13, 2022
8 min read

SHARE: [f](#) [in](#) [x](#)



SnykSec for Snyk

Posted on Jun 26 • Originally published at [snyk.io](#)



5

Polyfill supply chain attack embeds malware in JavaScript CDN assets

[#applicationsecurity](#) [#opensourcesecurity](#) [#javascript](#)



This Stuff is Hard

The 3 Fs of your supply chain

Fix

Fork

Forgo

One More F



One More **Funding**

Alpha-Omega Mission



**Protect society by
catalyzing sustainable
security improvements to
the most critical open
source software projects
and ecosystems**

Alpha-Omega Strategy

A

**Security
Staffing**

B

**Package
Repositories**

C

**Audits and
Remediation**

D

**Innovation &
Experiments**

13



Full Time Engineers
Hired



Security
Audits

\$8.3M

in Grants

Orgs
Funded

14

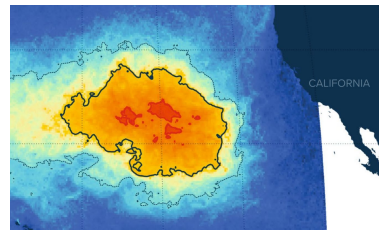
Origin Story: It's Always About People

Seth Larson and Michael Winser
present at PyCon

Jarek & Michael meet

From the Pacific Garbage Patch to
cleaning the Airflow beach

Alpha-Omega - Airflow PMC
collaboration



Beach Cleaning



So let's talk about Airflow Security

Airflow is secure

~~Airflow is secure~~

Airflow is active

in its security

Airflow is active

October 2, 2024 – October 9, 2024

Period: 1 week

Overview

154 Active pull requests

76 Active issues

105

Merged pull requests

49

Open pull requests

30

Closed issues

46

New issues

Excluding merges, **52 authors** have pushed **102 commits** to main and **124 commits** to all branches. On main, **4,799 files** have changed and there have been **20,429 additions** and **11,468 deletions**.



Users and Contributors

Used by 12.3k

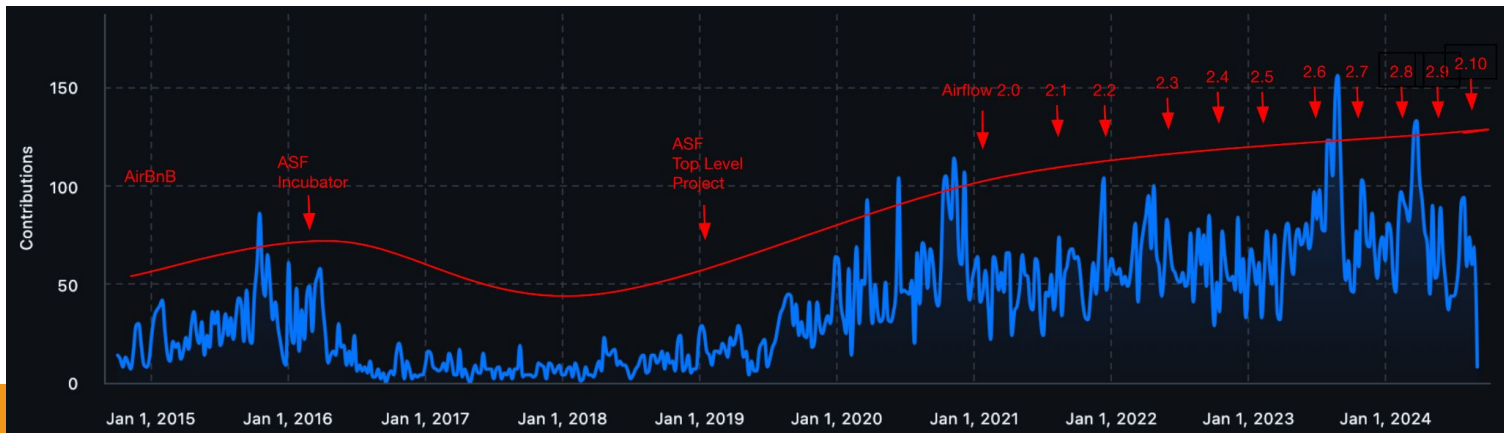
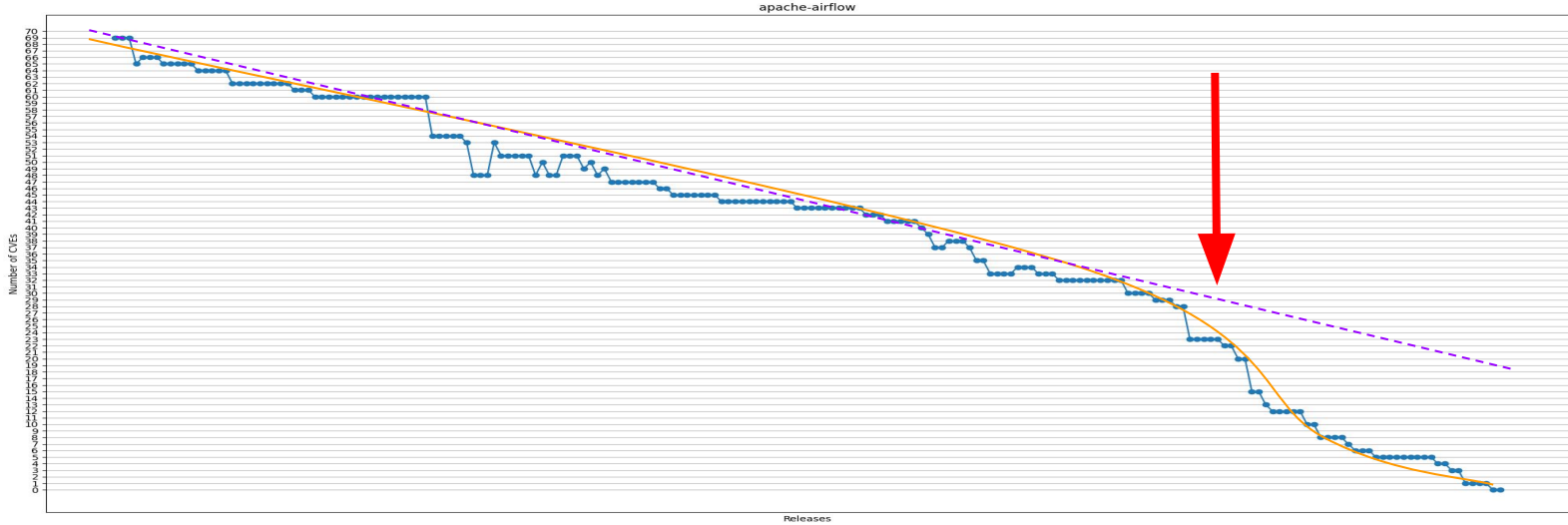


+ 12,316

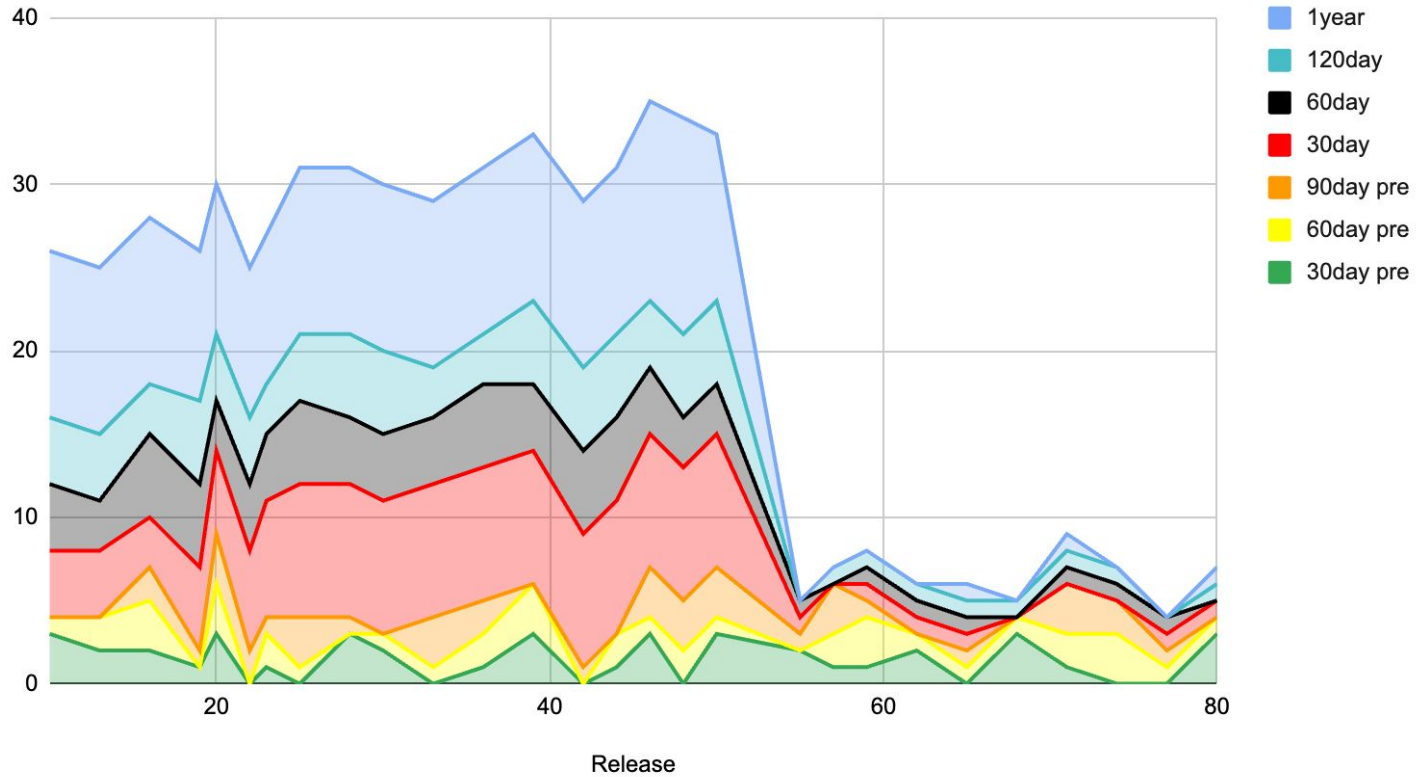
Contributors 3,086




+ 3,072 contributors



Closed, 30day, 60day, 120day and 1year



Security improvements in 2023-2024

- Dedicated security team
 - Created and documented detailed process
 - Introduced security model
 - Canned responses to issues
 - Disabled inherently insecure features
 - Hardened CI workflows
 - Introduced reproducible builds (provenance)
- 
- A decorative horizontal bar at the bottom of the slide, featuring a gradient from orange on the left to dark purple on the right.

Airflow

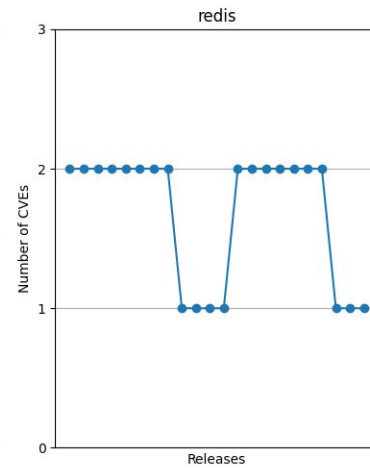
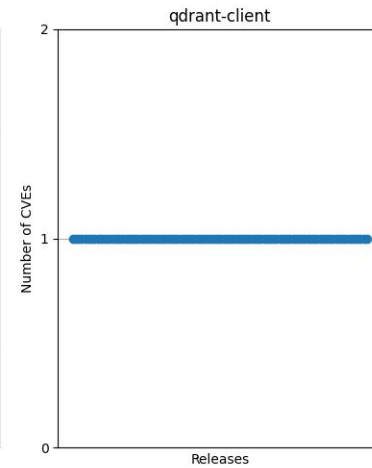
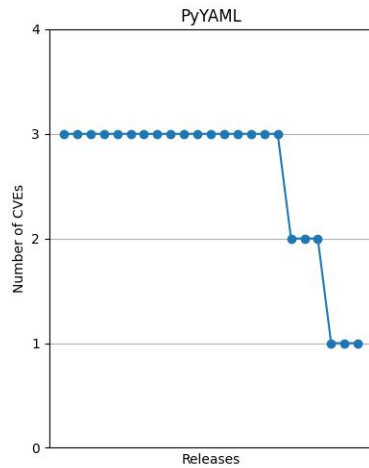
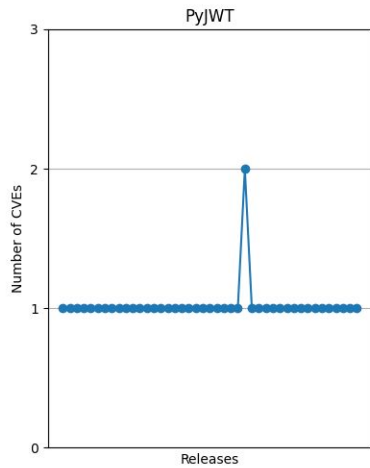
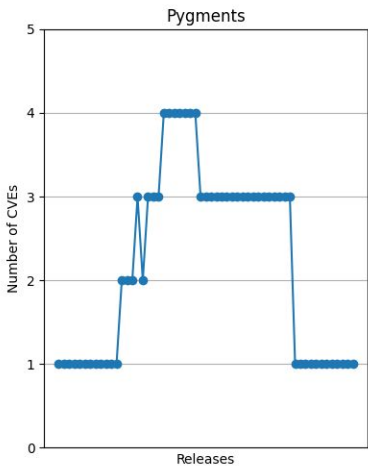
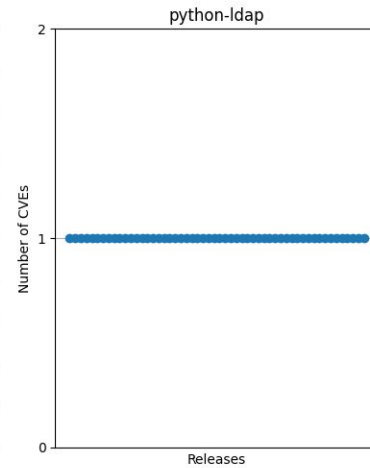
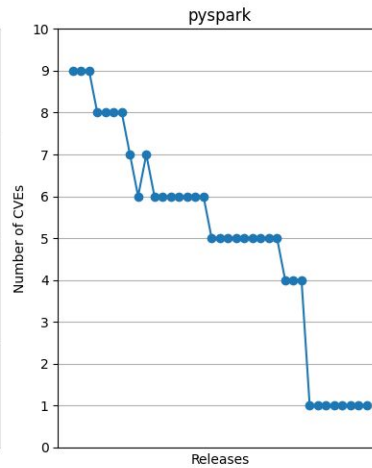
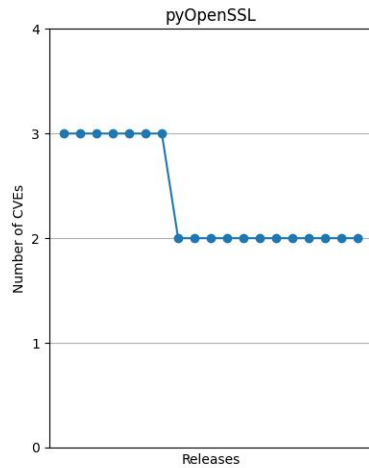
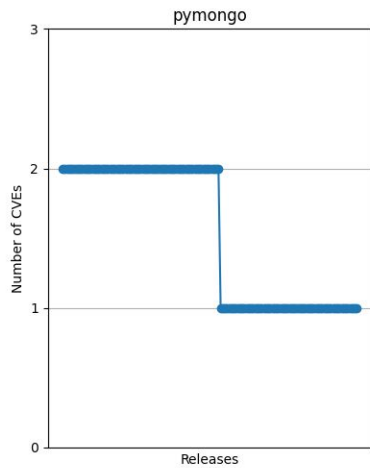
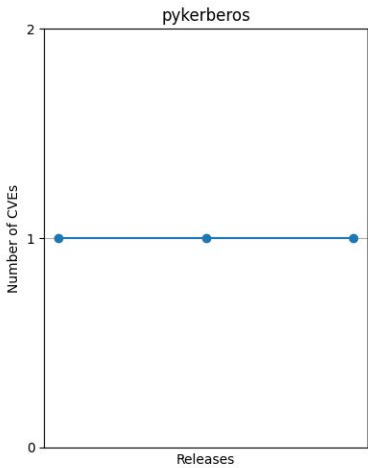
- Active security team (15 people, ~ 5 more active)
- Airflow: 62 committers, 33 PMC members
- 3000+ (!!!) contributors
- Airflow is big “enough” to attract funding
 - Stakeholders
 - Sovereign Tech Fund : 2023
 - Alpha-Omega Fund: 2024

Dependency tree

```
1  apache-airflow v3.0.0.dev0
2  ├── aiohttp v3.10.5
3  │   ├── aiohappyeyeballs v2.4.0
4  │   ├── aiosignal v1.3.1
5  │   │   └── frozenlist v1.4.1
6  │   ├── async-timeout v4.0.3
7  │   ├── attrs v24.2.0
8  │   ├── frozenlist v1.4.1
9  │   ├── multidict v6.0.5
10 │   └── yarl v1.9.6
11 │       ├── idna v3.8
12 │       └── multidict v6.0.5
13 ├── alembic v1.13.2
14 │   ├── importlib-metadata v8.4.0
15 │   │   └── zipp v3.20.1
16 │   ├── importlib-resources v6.4.4
17 │   │   └── zipp v3.20.1
18 │   ├── mako v1.3.5
19 │   │   └── MarkupSafe v2.1.5
20 │   ├── sqlalchemy v1.4.53
21 │   │   └── greenlet v3.0.3
22 │   └── typing-extensions v4.12.2
23 ├── argcomplete v3.5.0
24 ├── asgiref v3.8.1
25 │   └── typing-extensions v4.12.2
26 └── attrs v24.2.0
```

579

```
551 │   └── urllib3 v2.2.2
552 ├── rfc3339-validator v0.1.4
553 │   └── six v1.16.0
554 ├── rich v13.8.0
555 │   ├── markdown-it-py v3.0.0
556 │   │   └── mdurl v0.1.2
557 │   ├── pygments v2.18.0
558 │   └── typing-extensions v4.12.2
559 ├── rich-argparse v1.5.2
560 │   └── rich v13.8.0
561 │       ├── markdown-it-py v3.0.0
562 │       │   └── mdurl v0.1.2
563 │       ├── pygments v2.18.0
564 │       └── typing-extensions v4.12.2
565 ├── setproctitle v1.3.3
566 ├── sqlalchemy v1.4.53
567 │   └── greenlet v3.0.3
568 ├── sqlalchemy-jsonfield v1.0.2
569 │   └── sqlalchemy v1.4.53
570 │       └── greenlet v3.0.3
571 ├── sqlparse v0.5.1
572 ├── tabulate v0.9.0
573 ├── tenacity v9.0.0
574 ├── termcolor v2.4.0
575 ├── unicodedcsv v0.14.1
576 ├── universal-pathlib v0.2.2
577 │   └── fsspec v2024.6.1
578 └── werkzeug v2.2.3
579 │   └── MarkupSafe v2.1.5
```



Airflow Security Ecosystem

- Users
- Committers and PMC members
- Airflow Dependencies

Security regulations

- Regulations are coming (CRA, PLD ...)
- We have less than 2 years
- Everyone is impacted
- Everyone needs to be involved

Experiment starts ...

United effort

- Apache Software Foundation
- Airflow PMC
- Python Software Foundation
- Alpha-Omega Fund
- Some users (indirectly)

Involved parties

- OpenRefactory (analysing source code for bugs)
- CDXGen (generating SBOMs and other inventories)
- OSTIF (security audits)
- External researchers/security specialists

Goals and Principles

- We want to review ALL our dependencies (700+ !)
- We are leading and learning and adapting
- Automation to scale
- Your project's "perspective" is important
- Always remember the people

Inventory - automated in about 50%


	A	B	C	D	E	F	G	H	I	J	K
	Name	Author	Version	Description	Core	Devel	Depth	Licenses	Purl	Pypi	Vcs
39	python-nvd3	Belaid Arezqui <areski@g	0.16.0	Python NVD3 - C	TRUE	FALSE	1	MIT	pkg:pypi/py	https://pyhon-nvd3	
50	unicodectsv	Jeremy Dunck <jdunck@c	0.14.1	Python2's stdlib	TRUE	FALSE	1	0BSD	pkg:pypi/ur	https://pyicodectsv	
68	cron-descriptor	Adam Schubert <adam.sc	1.4.3	A Python library	TRUE	FALSE	1	MIT	pkg:pypi/cr	https://pyjdescriptor	
69	croniter	Matsumoto Taichi, kiorky <	3.0.3	croniter provides	TRUE	FALSE	1	MIT	pkg:pypi/cr	https://py/croniter	
72	deprecated	Laurent LAPORTE <tantal	1.2.14	Python @deprec	TRUE	FALSE	1	MIT	pkg:pypi/de	https://py/precated	
73	dill	Mike McKerns <mmckerns	0.3.3	serialize all of Py	TRUE	FALSE	1	0BSD, BSD-3-C	pkg:pypi/dil	https://pydation/dill	
100	jmespath	James Saryerwinnie <js@	1.0.1	JSON Matching	TRUE	FALSE	1	MIT	pkg:pypi/jm	https://py	https://git
107	lazy-object-proxy	Ionel Cristian Mărieș <con	1.10.0	A fast and thorou	TRUE	FALSE	1	0BSD, BSD-2-C	pkg:pypi/la	https://py	https://git
14	setproctitle	Daniele Varrazzo <daniele	1.3.3	A Python module	TRUE	FALSE	1	0BSD, BSD-3-C	pkg:pypi/se	https://pytproctitle	
165	argcomplete	Andrey Kislyuk <kislyuk@	3.5.0	Bash tab comple	TRUE	FALSE	1	Apache-2.0	pkg:pypi/ar	https://pycomplete	
165	asgiref	Django Software Foundati	3.8.1	ASGI specs, help	TRUE	FALSE	1	0BSD, BSD-3-C	pkg:pypi/as	https://pyo/asgiref/	
194	colorlog	Sam Clements <sam@bo	6.8.2	Add colours to th	TRUE	FALSE	1	MIT	pkg:pypi/cc	https://py-colorlog	
197	flask-caching	Peter Justin <peter.justin@	2.3.0	Adds caching su	TRUE	FALSE	1	0BSD	pkg:pypi/flu	https://pyc-caching	
223	psutil	Giampaolo Rodola <g.rod	6.0.0	Cross-platform li	TRUE	FALSE	1	0BSD, BSD-3-C	pkg:pypi/ps	https://pyolo/psutil	
231	tenacity	Julien Danjou <julien@da	9.0.0	Retry code until	TRUE	FALSE	1	Apache-2.0	pkg:pypi/te	https://py3/tenacity	
263	universal-pathlib		0.2.2	pathlib api exten	TRUE	FALSE	1	MIT	pkg:pypi/ur	https://pyal_pathlib	

Assessment

Relevant OPSF Scores and details							Actions					Num Action: 17				
Score	Code	Maint	Dang	Secur	Pack	Vulne	Governance	Lifecycle sta	Unpatched \	Industry imp	Add Secur	Follow up w	Propose Tru	Follow up w	Propose ma	Num Action
3.7	1	0	10	0					Yes	Medium	Yes	Yes	Yes		Yes	4
3	0	0	-1	0						Medium	Yes		Yes	Yes	Yes	4
4.7	3	10	10	0						Medium	Yes		Yes	Yes	Yes	3
5.1	1	10	10	0						Medium	Yes		Yes	Yes	Yes	3
4.4	1	0	10	0						Medium	Yes		Yes	Yes	Yes	3
5.5	1	10	-1	10						High			Yes	Yes	Yes	3
4.7	5	0	10	0						High	Yes		Yes	Yes	Yes	3
3.6	0	0	10	10				Yes		Medium		Yes	Yes	Yes	Yes	3
3.4	0	0	10	0						Medium	Yes		Yes	Yes	Yes	3
5.4	3	10	10	10						High			Yes	Yes	Yes	2
4.6	8	4	10	0						High	Yes		Yes			2
4.3	1	0	10	0						Medium	Yes			Yes	Yes	2
4.4	5	0	10	9						Medium			Yes	Yes	Yes	2
5.8	2	10	10	10						High			Yes	Yes	Yes	2
5.8	9	10	10	0						High	Yes		Yes		Yes	2
4.9	2	10	10	0						Medium	Yes			Yes	Yes	2

packaging workflow not detectedWarn: no GitHub/GitLab publishing workflow detected.

Open Refactory: Bugs analysis

- 2 months
 - 719 Packages
 - 14 Bugs Reported
 - 3 High, 6 Medium, 5 Low severity
- 
- A decorative horizontal bar at the bottom of the slide with a color gradient from orange on the left to purple on the right.

Experiment in progress ...

Actions

- 16 projects to start with
- Add security policies
- Follow up on unsecure workflows
- Propose Trusted Publishing
- Follow up on unpatched vulnerabilities
- Propose mandatory code reviews

Long term targets

- Full automation and coverage
- Run targeted audits and projects
- Target ALL projects
- Regular, incremental process
- Spread the methodology / findings
- Contribute to other efforts (PSF)

What YOU can do?

Think security


- Start similar efforts
- Know your dependencies
- Support security efforts of similar initiatives
- Contribute security reports

Learnings?

One thing to realise

**Your project's security depends on Your
engagement with Your supply chain**

Takeaways

- Supply chain relationships are a **human problem**
 - The transitive problem: every (new) dependency creates **exponential risk over time**
 - Current vulnerabilities are less important than **sustained security** handling and project health
 - Make **security a first-class priority** in every project plan
- 



Thank You!

Bird of a Feather where we can continue conversation



Resources

[SLSA](#)

[SSDF](#)

[Alpha-Omega Project](#)

[Case Study Eclipse Temurin: Pioneering
Software Supply Chain Security](#)

[Open Source Software Foundation](#)

[Airflow Security](#)

[Python Security](#)

