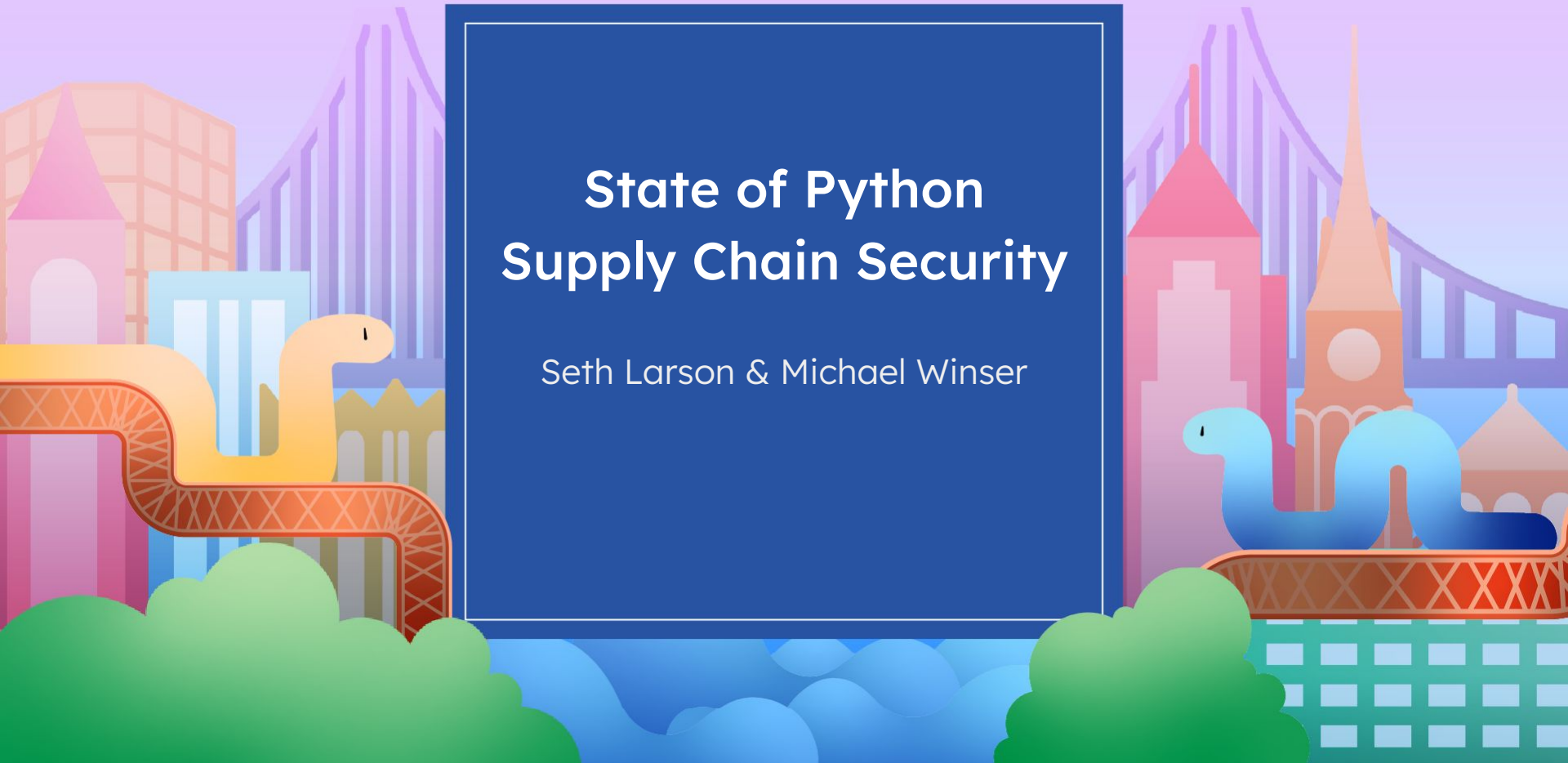


# State of Python Supply Chain Security

Seth Larson & Michael Winser



**Seth Larson**



Security Developer-in-Residence  
Python Software Foundation

**Michael Winsor**

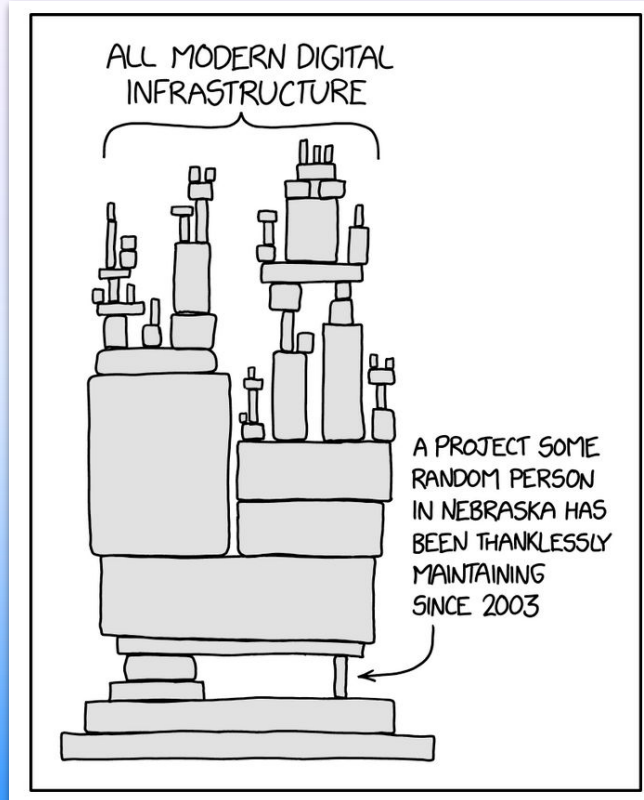


Co-Founder  
Alpha-Omega

# What is Supply Chain Security?



# Obligatory XKCD



# Supply Chain Risks

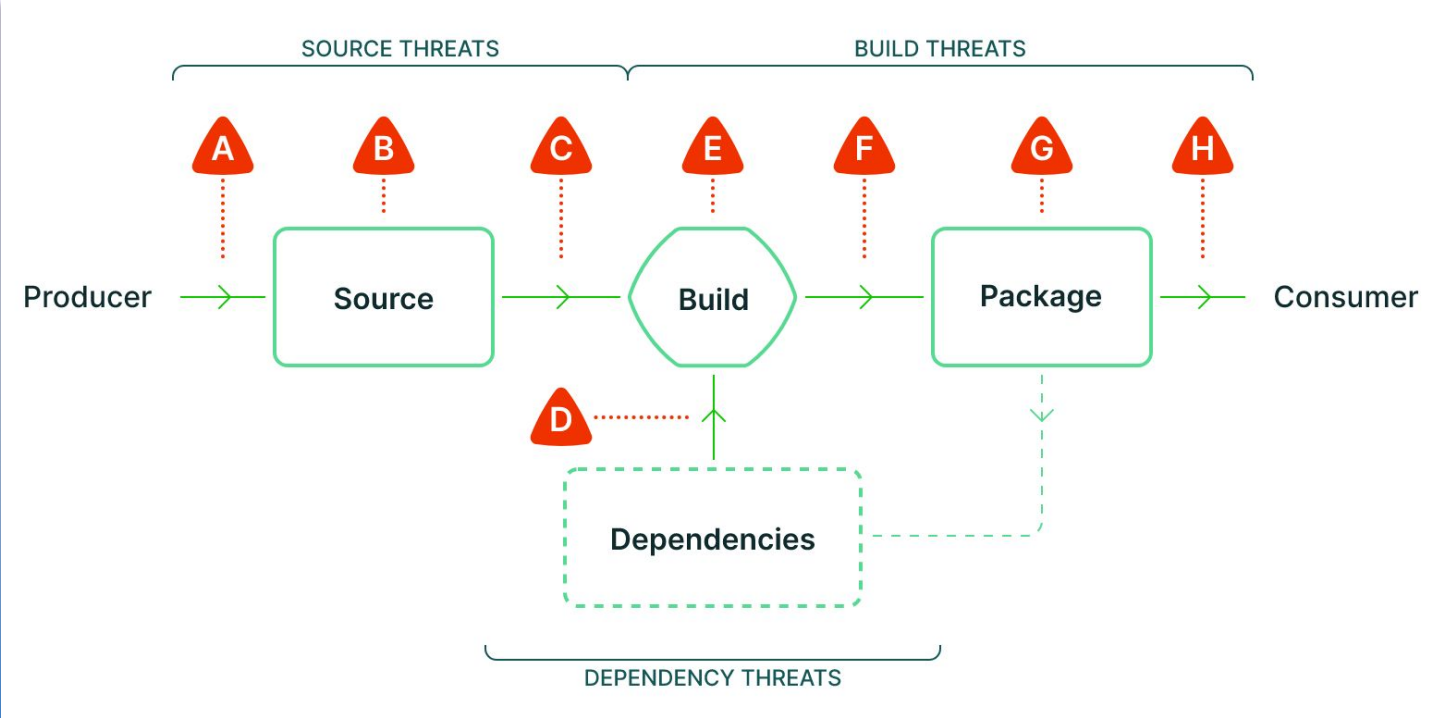
Vulnerabilities

Tampering

Availability



# SLSA



# About Alpha-Omega

**Improve global software supply chain security by partnering with Open Source**

**Alpha:** Improve the security posture of the most critical projects through staffing.

**Omega:** Automated security analysis, metrics, and remediation for wider range of projects.



# Alpha: Catalyzing Sustainable Security



*write less, do more*

2018 US 24



# Omega: Scaled approaches to open source security



3500+ Packages

200+ Bugs Reported

90 Security Bugs

32 High Severity

51% Fixed

Open | Refactory

# PSF Security Developer-in-Residence role

“We are grateful for the funding from the Alpha-Omega Project that enabled us to hire Seth Larson, who is both a security expert and a well-loved member of the Python community.”

- Deb Nicholson, Executive Director of the PSF



What got done  
in the past year?



# Vulnerability Management



## Release Managers & Experts

- Hugo van Kemenade
- Thomas Wouters
- Pablo Galindo Salgado
- Łukasz Langa
- Steve Dower (Windows)
- Ned Deily (macOS)

## Python Security Response Team

[security@python.org](mailto:security@python.org)

[security-announce@python.org](mailto:security-announce@python.org)

“Highly trusted cabal of  
Python developers”

Triage and remediate vulnerabilities  
in CPython and pip projects

# Python Security Response Team

- **Note: Mostly volunteer core developers**
- Revitalize “security-announce” mailing list
- Vulnerability disclosure process
- Experiment with GitHub Security Advisories
- Responsiveness to critical issues (e.g. xz-utils, libwebp)



# PSF CVE Numbering Authority (CNA)

## Why become a CVE Numbering Authority?

- Sensitive information not shared elsewhere
- Right of first refusal for reports
- Control CVE metadata, automation

PSF CNA has published 8 CVEs already!

**[security-announce@python.org](mailto:security-announce@python.org)**



# Open Advisory Database


Database of 125+ vulnerabilities for CPython from 2007 onwards

Open Source Vulnerability format

[github.com/psf/advisory-database](https://github.com/psf/advisory-database)

Thank you, Victor Stinner!

## PSF-2024-2

**Import Source** <https://github.com/psf/advisory-database/blob/main/advisories/PSF-2024-2.json> 

**Aliases** [BIT-python-2024-0450](#)  
[CVE-2024-0450](#)

**Published** 2024-03-19T15:12:07Z

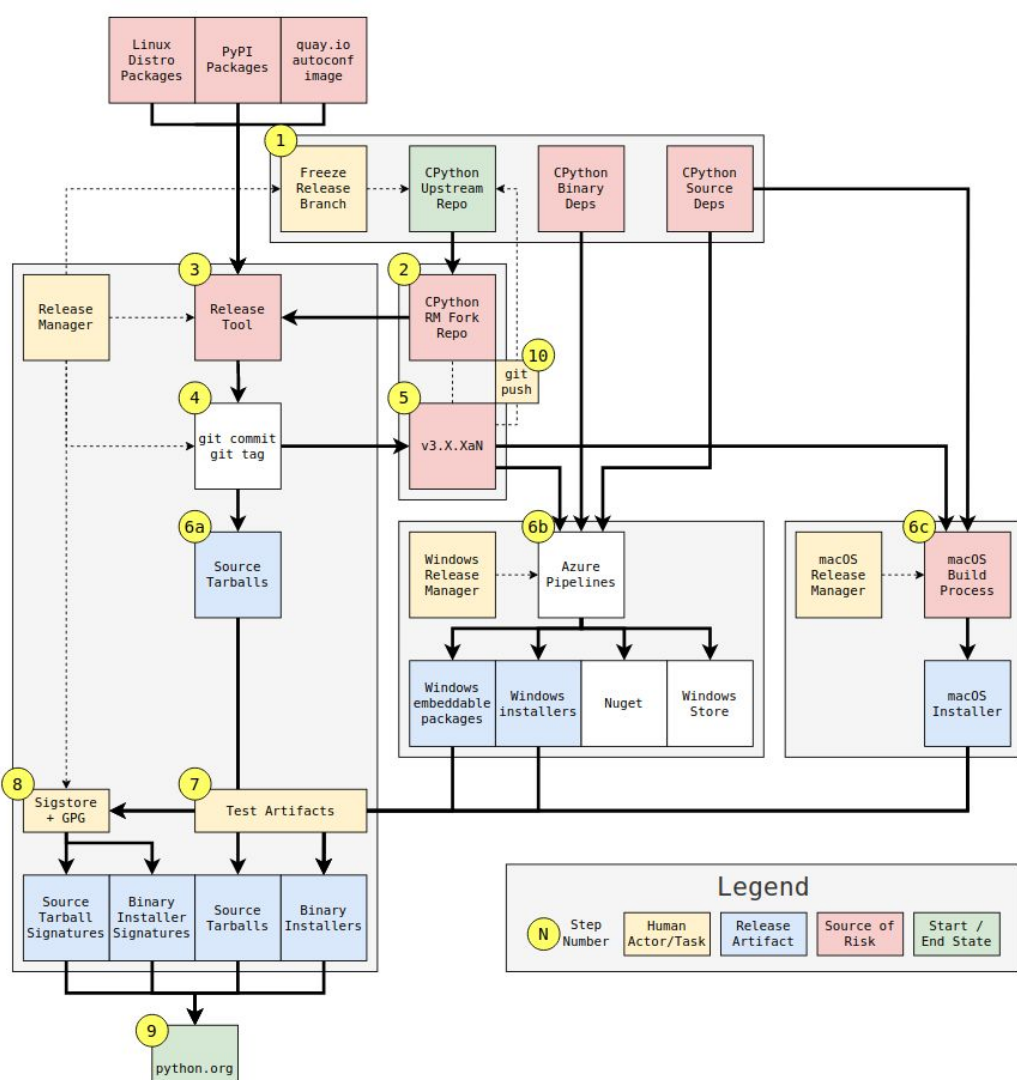
**Modified** 2024-04-03T22:11:43.120887Z

**Details** An issue was found in the CPython `zipfile` module affecting versions 3.11.7, 3.10.13, 3.9.18, and 3.8.18 and prior.

The `zipfile` module is vulnerable to “quoted-overlap” zip-bombing in the zip format to create a zip-bomb with a high compression ratio. Older versions of CPython makes the `zipfile` module reject zip archives with entries in the archive.



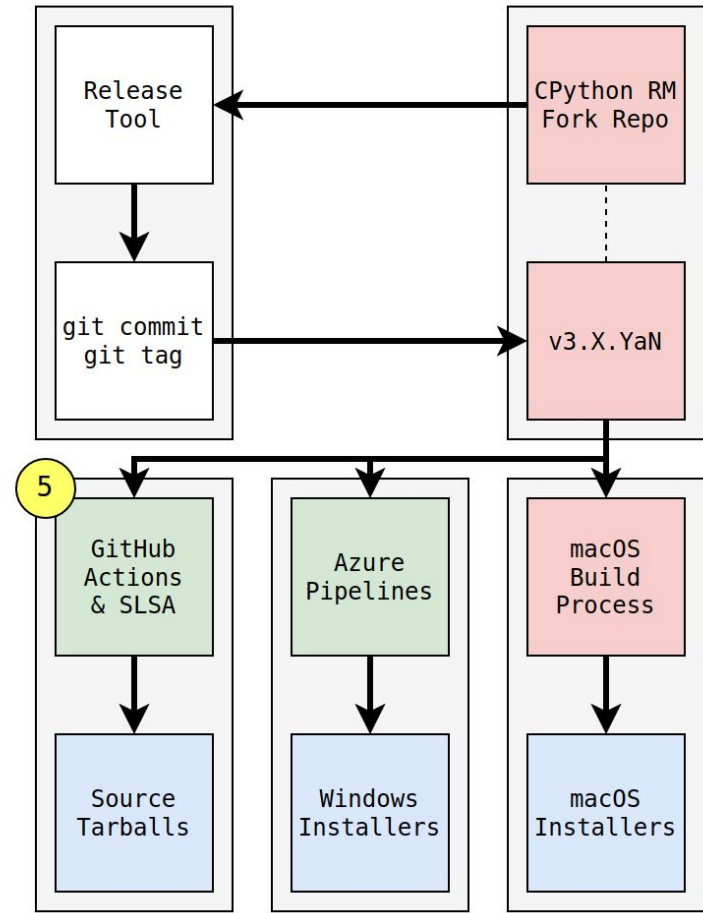
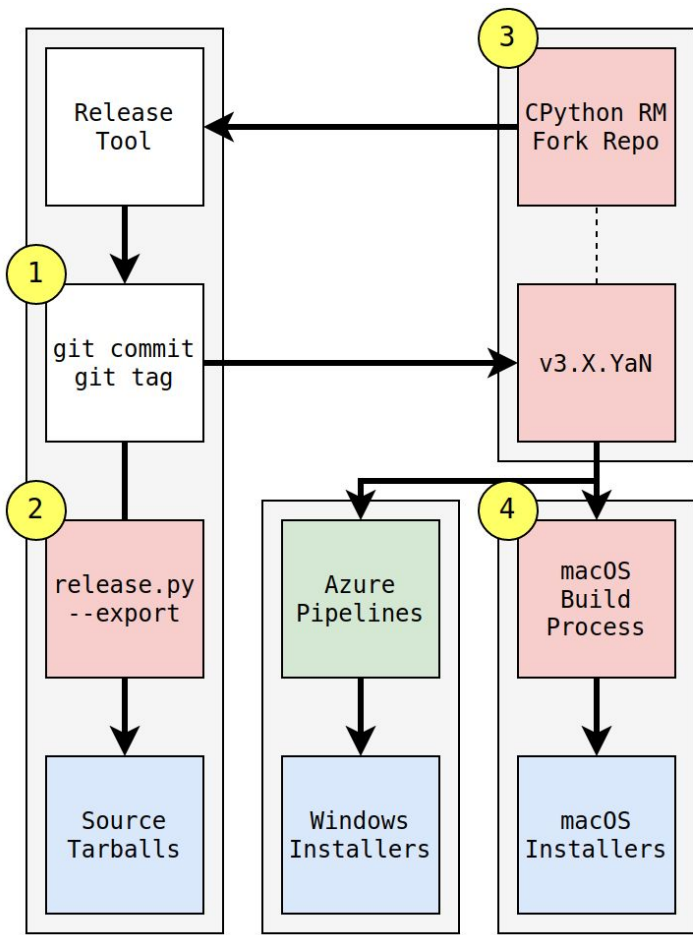
# Hardening the CPython Release Process

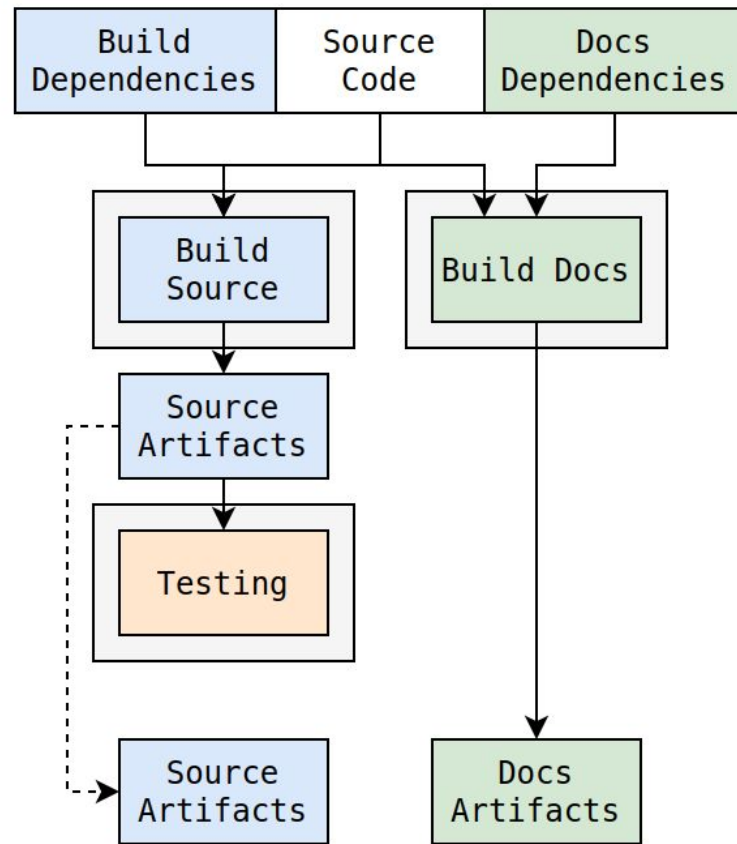
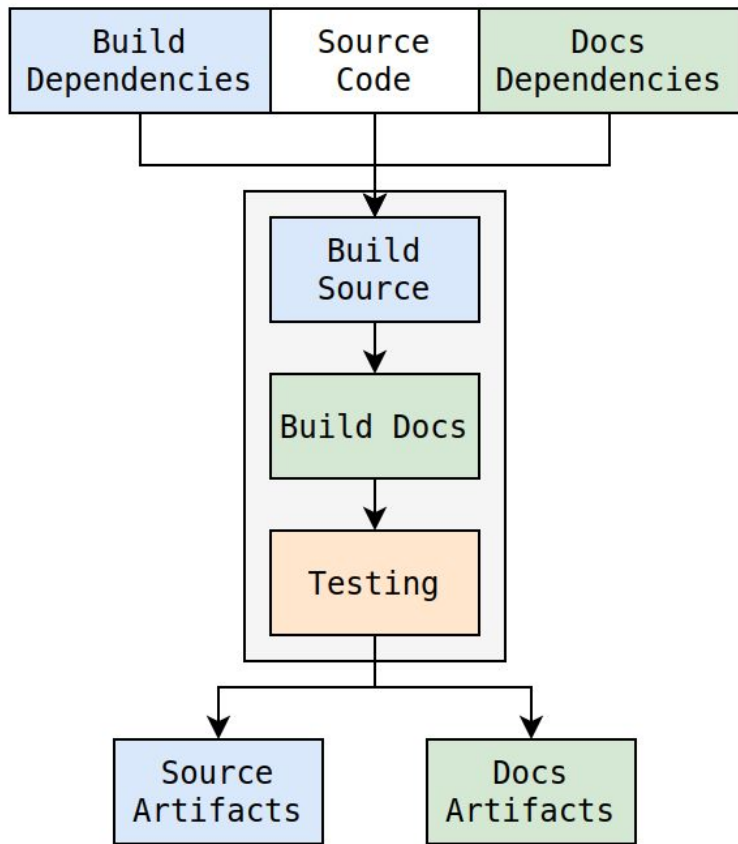


## CPython Release Process

- Human-involved process
- Reduce supply chain risk
- Reproducibility
- Artifact integrity

Diagram of PEP 101 process, Sept 2023





*50% faster with 660 fewer dependencies*

# CPython Software Bill-of-Materials

# Software Bill-of-Materials (SBOM) for CPython

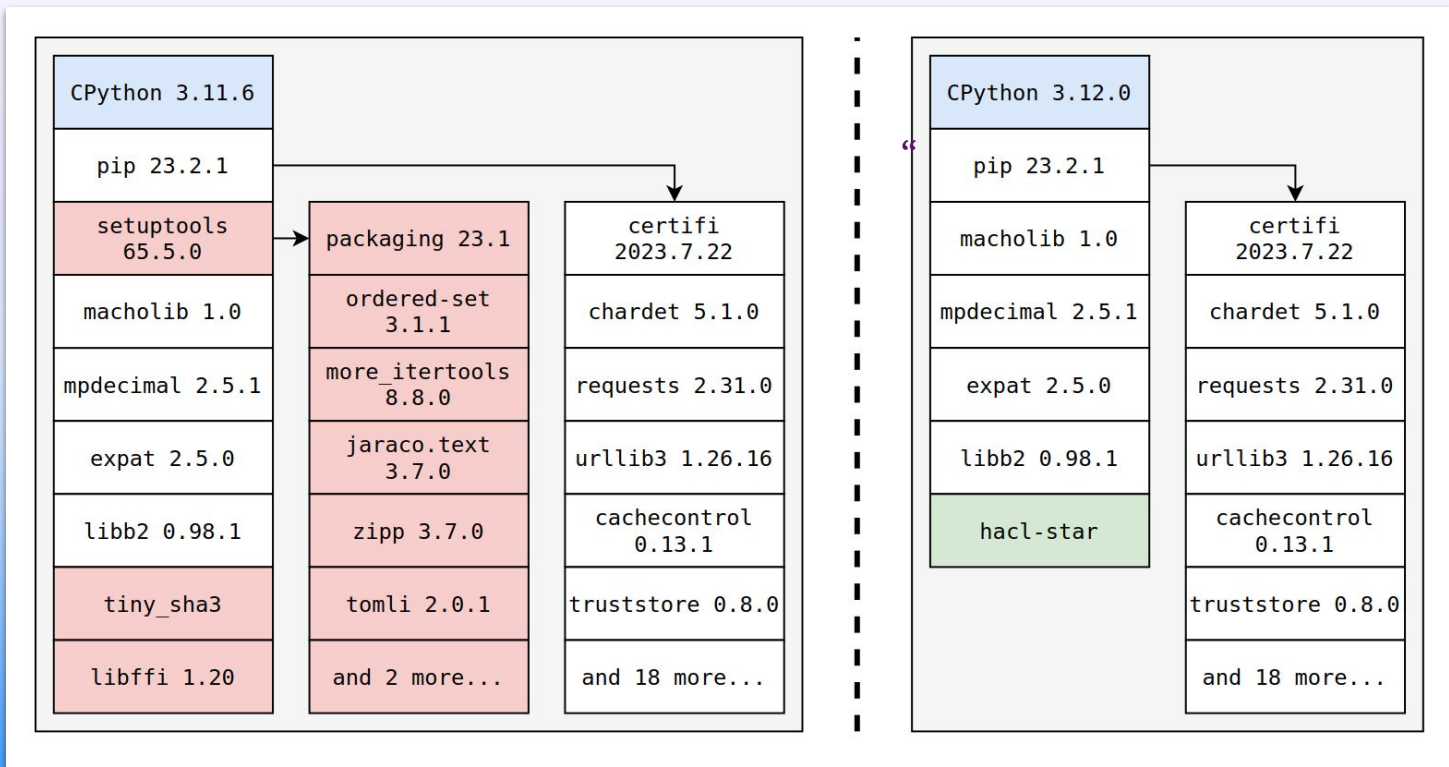
**What?** “List of ingredients”

**Why?** US and EU regulations, vuln management

- NTIA Minimum Elements for SBOM
- SBOMs for source code for CPython 3.12.2+
- **New in 3.13.0b1: SBOM for Windows installers**
- Coming soon: SBOM for macOS installer



# Software Bill-of-Materials (SBOM) for CPython



# Software Bill-of-Materials (SBOM) for CPython

```
$ grype sbom:Python-3.12.2.tgz.spdx.json
```

- ✓ Vulnerability DB [no update available]
- ✓ Scanned for vulnerabilities [7 vulnerability matches]
  - └─ by severity: 0 critical, 3 high, 4 medium, 0 low, 0 negligible
  - └─ by status: 2 fixed, 5 not-fixed, 0 ignored

| NAME    | INSTALLED | FIXED-IN | TYPE   | VULNERABILITY       | SEVERITY |
|---------|-----------|----------|--------|---------------------|----------|
| CPython | 3.12.2    |          |        | CVE-2023-6597       | High     |
| CPython | 3.12.2    |          |        | CVE-2024-0450       | Medium   |
| expat   | 2.5.0     |          |        | CVE-2023-52425      | High     |
| expat   | 2.5.0     |          |        | CVE-2023-52426      | Medium   |
| idna    | 3.4       | 3.7      | python | GHSA-jjg7-2v4v-x38h | Medium   |
| pip     | 24.0      |          | python | CVE-2018-20225      | High     |
| urllib3 | 1.26.17   | 1.26.18  | python | GHSA-g4mx-q9vg-27p4 | Medium   |



# What's in flight today?

- **Release process and SBOMs for macOS**
- Sigstore “workload identity” for CPython artifacts
- Automating CVE Numbering Authority processes



# Engaging with the Community

# “Rising tides lift all boats”

## Reviewer of security PEPs

- PEP 740: Index Support for Digital Attestations
- PEP 543: CPython support for alternate TLS backends
- PEP 639: SPDX License Expressions for Python packages
- PEP 665: Lock Files for Python packages

## Google Summer of Code mentor

Adopting Hardened Compiler Options for CPython



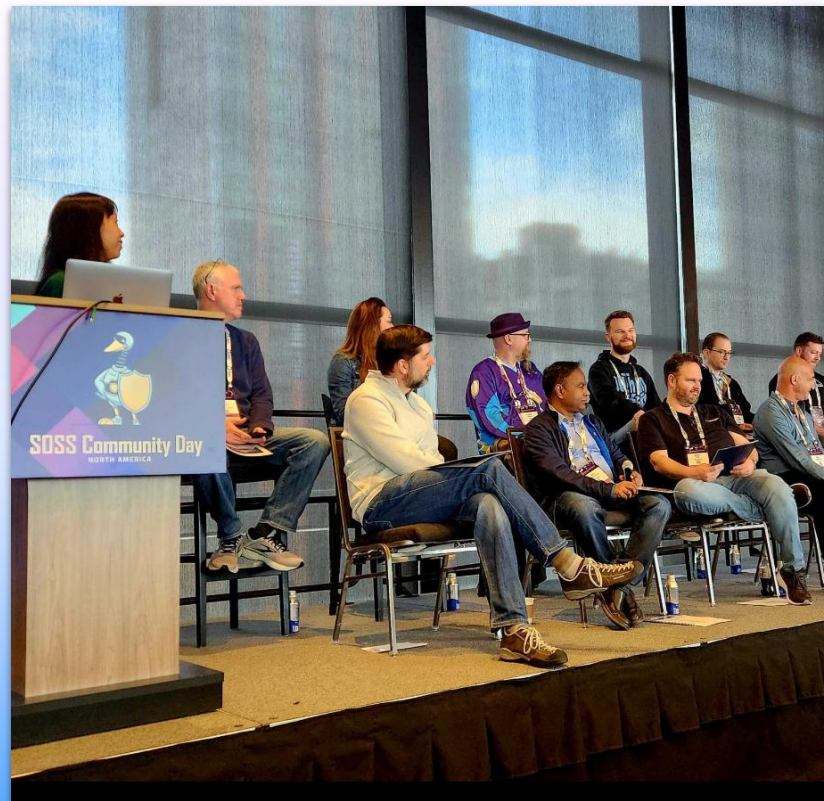
# “Rising tides lift all boats”

## Community Outreach

40+ blog posts, 4 conference talks  
OpenSSF and CVE working groups  
The New Stack, The Register, podcasts

## Alpha-Omega cohort

Eclipse, FreeBSD, Homebrew, NodeJS,  
OpenRefactory, OpenSSL, Prossimo,  
RubyCentral, Rust Foundation, jQuery



Tabletop Session, SOSS Community Day



# OpenSSF

OPEN SOURCE SECURITY FOUNDATION

## Guide for Open Source Projects Becoming a CVE Numbering Authority



# OpenSSF

OPEN SOURCE SECURITY FOUNDATION

## Linux Kernel Achieves CVE Numbering Authority Status

“I’d like to point out the great work that the Python project has done in supporting this effort”

– Greg Kroah-Hartman



CURL AND LIBCURL

### CURL IS A CNA

🕒 JANUARY 16, 2024 👤 DANIEL STENBERG 💬 3 COMMENTS

[The curl project](#) has been accepted as a [CVE Numbering Authority](#) (CNA) for vulnerabilities in all products directly made or managed by the project. If I’m counting correctly, we are the 351st CNA.

# What's next for Python Supply Chain Security?

# What's next for Python Supply Chain Security?

**Focus on the community of Python users and maintainers!**

Python packaging tools and workflows

**Build Provenance** and **SBOMs**  
for Python packages

Adoption of security best practices



*Let's keep Python secure!*



# What's next for Python Supply Chain Security?

## Want to help? Here's what to do today:

- Add **Trusted Publishers** to PyPI packages  
GitHub, GitLab, GCB, and ActiveState
- Use a lock file with hashes  
like **pip-compile** or **Poetry**
- Test and adopt new security features



*Let's keep Python secure!*

# Learn more and get involved!

Python Software Foundation Blog

<https://pyfound.blogspot.com>

- **New and Completed Projects**
- Policy, Standards, Grants, Staffing



# Learn more and get involved!

Python Package Index Blog

<https://blog.pypi.org>

- **New Security Features for PyPI**
- PyPI Sec Engineer, Mike Fiedler



# Learn more and get involved!

Python Packaging Discussion forum

<https://discuss.python.org>

- **Packaging Tools and Standards**
- Projects affecting Python packaging
- *Maintainers and users welcome!*



Stickers, we've got stickers!



# Thank you! ❤️

## Q&A, have a Python security question?

Email: [seth@python.org](mailto:seth@python.org)

Image credits:

- <https://xkcd.com/2347>
- <https://slsa.dev/spec/v1.0/threats-overview>
- Wikipedia for logos

