Alpha-Omega

MONTHLY
REPORT
MAY 2024

May 2024

SUMMARY

This month we met with GitHub on the most feasible approach to encourage more maintainers (particularly those of popular projects) to leverage available tooling (i.e. static analysis, secret detection, dependency management, and private vulnerability reporting).

We also met with KForce and the Open Source Technology Improvement Fund (OSTIF) to scope the evaluation of all open source AI packages/libraries. The expected outcome of this initiative is intended to: Relieve the time needed from Engineering teams to evaluate vulnerabilities when using specific AI tools and provide an overview of implementation flaws, vulnerabilities, etc. for each AI package. Alpha Omega has a set budget and goal to complete this scope by the end of 2025.

We also had the first in a series of regular meetings with the Open Technology Fund and the Sovereign Tech Fund, to build better connections, share learnings, and to the extent possible, collaborate on funding critical open source projects.

We've also decided to hold our next in-person roundtable for Alpha-Omega engagement partners and friends at the Open Source Summit EU in September. We'll share additional information when it's available.

EXISTING ENGAGEMENTS

Our existing engagements provide monthly updates to us through our public GitHub repository:

- Node.js
- jQuery
- The Eclipse Foundation
- OpenSSL
- Homebrew
- FreeBSD
- The Rust Foundation
- The Python Software Foundation
- ISRG
- OpenRefactory
- Kernel
- RubyCentral

A FEW NOTABLE WORK UPDATES FROM GRANTEES

Security Audits

One of Alpha-Omega's four "buckets" of focus are on security audits; this month, we had two such audits complete:

- Eclipse Kuksa: This project provides shared building blocks for Software Defined Vehicles, and the audit covered the data broker and the Python client, conducted by Quarkslab and managed by the Open Source Technology Improvement Fund. There were two high severity findings and about a dozen lower severity findings, all addressed in the latest version. Download the full report.
- OpenSSL: This security audit focused on the libcrypto component of OpenSSL 3.1, and was conducted by Trail of Bits and managed by the Open Source Technology Improvement Fund. There were four medium and six low severity findings. Download the full report.

Python Software Foundation (PSF)

PyCon US 2024 was held this month, with Seth Larson and Michael Winser delivering a talk, State of Python Supply Chain Security to a packed conference room.

CPython's Hardened Compiler Options Guide for C/C++ project was accepted to Google's Summer of Code 2024, and Seth is mentoring the contributor.

On the build side, work has been completed to separate the build, test, and documentation stages, reducing dependencies of the source build by about 660. Windows artifacts distributed on python.org will have SBOMs available after the next release.

OpenRefactory

Link to results: Results from Scan and Audit Performed by OpenRefactory

May

Month	Dec 2023	Jan 2024	Feb 2024	Mar 2024	Apr 2024	May 2024
Projects analyzed	328	300	530	780	712	785
Projects with no bugs	293	279	525	776	708	784
Total bugs filed	56	13	7	7	4	7
Security/Reliability bugs filed	15	8	6	5	2	5
Bugs with a fix suggestion	50	10	2	2	4	0
Bugs with a PoC exploit	4	1	2	3	0	0
Fixes merged by maintainers	27	10	5	3	4	0
Security/Reliability fixes merged	6	6	2	1	0	0
Fixes ignored by maintainers	1	1	1	0	2	0
Reports still open	28	2	1	4	0	7

Homebrew

Last November, we engaged with the Homebrew team and Trail of Bits to add build provenance to Homebrew. The core part of this work now live (public beta): homebrew-core is now cryptographically attesting to all bottles built in the official Homebrew CI. You can verify these attestations with the (currently external, but soon upstreamed) brew verify command. This means that, from now on, each bottle built by Homebrew will come with a cryptographically verifiable statement binding the bottle's content to the specific workflow and other build-time metadata that produced it. This metadata includes (among other things) the git commit and GitHub Actions run ID for the workflow that produced the bottle, making it a SLSA Build L2-compatible attestation.

OKR UPDATES

O1: Catalyze trustworthy and secure software, runtimes, and infrastructure for all the major open source ecosystems through staffing	
KR 1.1: Fund security improvements and initiatives for at least ten critical open source organizations by the end of 2024.	On target
KR 1.2: For each engagement, confirm progress toward improved security outcomes, evidenced through initial and/or follow-on assessments, monthly reporting, and periodic check-ins.	On target
KR 1.3: Drive the organizations we work with to obtain security funding from at least one organization other than Alpha-Omega, targeting 33% by the end of 2024.	Not measured
KR 1.4: Organize quarterly roundtables for at least 5 major ecosystems to share information, build connections, and collaborate, resulting in at least one new project or joint publication started in 2024.	On target
O2: The top 10,000 open source projects are free of critical security vulnerabilities	
KR 2.1: Drive adoption of key security processes, including static analysis, credential scanning, the use of private vulnerability disclosures, structured metadata (Security Insights) and the use of multi-factor authentication by maintainers of 500 critical projects from the top 10,000 by the end of 2024.	Not started
KR 2.2: Independently scan, triage, and notify maintainers when critical vulnerabilities are found in 2,000 projects, chosen from the top 10,000 by the end of June 2024, with emphasis on clearing a "section of the beach" by focusing on the top PyPI packages.	On target
KR 2.3: Publish in a machine readable format the attestations for all packages from 2.2 that returned no vulnerabilities and those that found vulnerabilities which were subsequently fixed and verified.	On target
O3: Enhance Alpha-Omega's effectiveness in driving security improvements through deliberate innovation and experimentation	
KR 3.1: By the end of 2024, run three experiments to explore new strategies for reducing security risk within the open source ecosystems, share the results/learnings, using them to refine our overall strategy and objectives for 2025.	Not started
O4: Run an operationally efficient and effective program	
KR 4.1: Allocate at least 85% of our yearly spend to activities directly in support of our mission.	On Target
KR 4.2: Receive at least $5 million in renewed funding in 2024.	Completed
KR 4.3: For each partner engagement, at least 70% of the objectives defined within the respective agreement are met within the defined time period.	On target

WHAT'S NEXT

Our next update (for June) will be delivered by Monday, July 8th, and our next Alpha-Omega public meeting will take place on Wednesday, July 3rd. If you have any questions about this update or any of our work, please contact the Alpha-Omega team at info@alpha-omega.dev or reach out to one of us directly.

Bob Callaway, Google
Henri Yandell, AWS
Michael Scovetta, Microsoft
Michael Winser, Alpha-Omega