Alpha-Omega

MONTHLY REPORT

AUGUST 2024

August 2024

SUMMARY

Our initial “cleaning the entire beach” project with the Apache Airflow project is nearing conclusion and has produced many insights in addition to many fixes. Michael Winser and Jarek Potiuk will be keynoting about the project and supply chain security in general at the upcoming Airflow Summit (Sept 10th in SF).

We're also preparing for the Alpha-Omega roundtable at the Open Source Summit in Vienna. If you're attending the conference and would like to join us, please reach out.

NEW ENGAGEMENTS

In August Alpha Omega granted Trail of Bits funds to improve PyPI's project-level "lifecycle" functionality, including implementing and improving key features related to PyPI's project deletion, project uploading, and project "status" handling. Each of these is proposed as three separate tasks including removal of project deletion in favor of "yanking", project status markers, and project drafting and bulk upload support, via PEP 694. This is a nine month project that includes documentation, testing, and integration time for all engineering tasks.

EXISTING ENGAGEMENTS

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

- Node.js
- The Eclipse Foundation
- Homebrew
- The Rust Foundation
- The Python Software Foundation
- FreeBSD
- PHP (Composer Packagist)
- Apache Airflow
- Support of LLVM ports to Debian
- OpenRefactory
- Kernel
- RubyCentral
- ISRG
- Open Source Technology Improvement Fund
- PyPI

A FEW NOTABLE WORK UPDATES FROM GRANTEES

Airflow

This is the first Monthly report for what has been accomplished during the first month of the “Airflow Beach Cleaning” project. The goal of the project is to perform “Supply chain Analysis” of Apache Airflow and perform actions that aim to improve overall supply chain security for Airflow. Airflow has 700+ Python dependencies, many of which are important part of the “data processing” Python ecosystem and through Apache Airflow being the “user” and “depending” on those, it’s possible to efficiently improve awareness of the need of security improvement and to help Airflow dependencies to improve the security posture and processes.

The project started in August 2024, and during the first month, the Project Meta-Health Audit Concepts document was prepared where idea of “meta-health” of projects was explored and iterated on - a set of scorecards and signals for projects that would provide a general overview of project’s “security health” and indicate the need of prioritizing direct interaction with the project.

Prossimo

Preparation for the Linux v6.12 upcoming merge window, i.e. the `rust-next` branch already contains a few major developments for the cycle, such as the CPU mitigations work, the split of the helpers file to help avoid conflicts for developers and the linked list abstractions series, with more to be added.

The `rust-fixes` PR for v6.11 was sent to Linus and it got merged. A second `rust-fixes` PR is in the works with some more fixes queued for this cycle. Prossimo announced https://rust.docs.kernel.org. The domain contains the generated Rust code documentation. It is intended to help kernel developers (as well as other people) to follow along with the project and explore the Rust abstractions and their source code available in mainline and linux-next. It is ultimately a tool for the kernel community to work with Rust, and thus it should help us achieve the long term goal of getting Rust production drivers merged into the Linux kernel.

Rust

Crate provenance tracking, verifying that a given crate is actually associated with the repository it claims to be, is now running across the entirety of the crates.io corpus. The engineering to get this working across all of crates.io has surfaced various issues in underlying Rust libraries, most notably gitoxide, but these are being worked out and results of the entire corpus work should be available soon.

The crate deletion RFC has been approved and merged. Implementation of the RFC details are now beginning. Recall, the purpose of the RFC is to provide crate owners with a mechanism to delete crates from crates.io under certain conditions. The infra and crates.io teams also worked together on this website, which contains statistics of historic version downloads.

There are two benefits to this the first is moving this info from the crates.io db to a CSV makes the actual crates database faster. And the second, people can download this data and analyze crates.io download statistics.

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.	On target
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.	Planning
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.	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 September) will be delivered by Monday, October 7th and our next Alpha-Omega public meeting will take place Wednesday, October 2nd. Our next Roundtable will be held at Open Source Summit EU on September 17th.

If you have any questions about this update or any of our work, please contact the Alpha-Omega team at info@alpha-omega.dev, reach out to one of us directly, or come say 'hi' on the #alpha_omega channel in the OpenSSF slack.

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