Alpha-Omega

MONTHLY REPORT

SEPTEMBER 2024

September 2024

SUMMARY

IAlpha Omega hosted its second in person roundtable at Open Source Summit Europe in Vienna Austria this month. The roundtable was attended by representatives from the Sovereign Tech Fund, OpenSSF, many of our grant recipients, and a smattering of security-minded individuals. Our first session was a lively discussion about how to improve end-of-life transitions for open source projects. The second session was about how Alpha-Omega and our partner organizations can combine on a marketing push to drive awareness of our impact and open source security needs.

NEW ENGAGEMENTS

In September Alpha-Omega provided a grant for three months of full-time work to improve the Jenkins implementation of Content Security Policy (CSP). The improvements will be implemented in October, November, and December of 2024. This work is notable because in 2024, Jenkins does not support CSP! Preventing cross-site scripting from Jenkins Plugins is currently a manual, error-prone, and fragile effort. This work will pave the way for a systematic solution.

EXISTING ENGAGEMENTS

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

- Node.js
- The Eclipse Foundation
- OpenRefactory
- Linux Kernel
- Ruby Central
- Apache Airflow
- FreeBSD
- PHP (Composer, Packagist)
- Rust Foundation
- Python Software Foundation
- ISRG / Prossimo
- Support of LLVM ports to Debian
- Open Source Technology Improvement Fund
- PyPI
- Jenkins

A FEW NOTABLE WORK UPDATES FROM GRANTEES

FreeBSD

The Code Audit is on track. All Critical and High severity vulnerabilities are patched and Security Advisories have been released. Synacktiv Code Audit Report will be released by the end of September, with a FreeBSD-authored Code Audit Report due in October and the Process Audit is on track to begin mid-Oct. Preparations are complete and once the FreeBSD-authored Code Audit Report is published we will start on the process audit.

PyPI

This month we have revived the standards process for Upload 2.0 API for Python Package Repositories and began reviewing the latest draft changes. Coordinating with the PEP's authors/delegates on steps towards finalizing and provisionally accepting the PEP. There has also been pre-PEP discussion for limiting deletions on PyPI. Currently drafting the accompanying PEP.

Rust

A breakthrough occurred at RustConf 2024 - discussion between Foundation security initiative members and some members of the Rust Project agreed in principle that implementing The Update Framework (TUF) for Rust was the best way to move forward with crate signing and mirroring. This would replace the original proposal outlined in the PKI RFC. This agreement in principle amongst the affected parties is actually a big milestone for progress. Now to get all this in writing and hopefully implemented.

There are some technical hurdles to overcome to make this goal of using TUF achievable. One of these hurdles is ensuring that the size of the crate payload metadata is not increased at a noticeable rate. Right now it is estimated that, as-is, 1MB of data would be appended every time the crate index was updated (which is about once a minute), and we want to try to reduce that, if possible. In order to reduce the payload size required to successfully use TUF for Rust, we want to implement TAP16. TAP16 “proposes a method for reducing the size of snapshot metadata a client must download without significantly weakening the security properties of TUF”, by using Merkle trees.

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

COMING UP NEXT MONTH

Our next update (for October) will be delivered by Monday, November 11th and our next Alpha-Omega public meeting will take place Wednesday, November 6th. Our next Roundtable will be held in December.

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, Technical Strategist, Alpha-Omega