Alpha-Omega

MONTHLY REPORT OCTOBER 2024

February 2024

SUMMARY

The audit of top AI libraries has wrapped up. We will be working with the vendors as they disclose the report and as we look to next steps.

We start Q3 with a review of our OKRs. Most KRs have already met or exceeded their goals. Notably, as we see proposals for 2025 funding we are seeing real progress with KR 1.3: Drive the organizations we work with to obtain security-related funding from at least one organization. Only one KR (2.1: Drive adoption of key security processes) is not on track.

NEW ENGAGEMENTS

In October Alpha-Omega renewed its engagement with OpenJS for 2025 to advance security skills and processes among the contributor and implementer communities. This grant will also strengthen the JavaScript ecosystem broadly, and provide direct support to the most critical projects in the OpenJS project portfolio. Alpha Omega is excited to continue the relationship with OpenJS for a third year.

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

Jenkins

Shlomo has already shipped one CSP fix in the JUnit plugin, proposed another PR that Basil is testing for the Workflow Job, and is in the process of developing/testing a fix for the Subversion Plugin. One important core CSP problem was also fixed by Daniel Beck. The problem was developed over a year ago, has been updated, reviewed, and merged. We have also released CSP fixtures that had been sitting around, like the matrix project, and credentials. It took some work to retest them and get them released.

Prossimo (Rust for Linux)

Prepared and sent the Linux v6.12 rust-fixes PRs: first and second (and likely a third one within October too). Some of these fixes are important for the first major users of Rust in the kernel, particularly Android Binder. Early preparation of the Linux v6.13 rust-next PR is shaping up to be a release with a few major changes, such as the custom alloc series, the lints series and an assortment of other improvements. Some of these features are key to some of the first major use cases of Rust in the kernel as well, such as the Nova GPU driver.

PSF

Seth authored PEP 761, including leading the expected pre-PEP and PEP discussions. The PEP was received positively by CPython core developers and release managers. The discussions included downstream verifiers like Python container image and Linux package distribution maintainers.

During the discussions the feasibility and blockers for these downstream verifiers adopting Sigstore was discussed, including dispelling myths around offline verification, how Sigstore worked, and the availability of tools to verify the signatures. Seth forwarded feedback to Sigstore maintainers. Overall, despite requiring some work by downstream verifiers to adopt Sigstore I believe the discussions were productive.

The earliest version that could remove PGP signatures is Python 3.14 pending a decision from the Python Steering Council.

ISRG

We are making great progress. The community is also growing rapidly, with new contributors showing up regularly and largely representing new consumers of Rustls.

We accomplished a major milestone by releasing version 0.23.0.

- It makes AWS's Libcrypto ("aws-lc-rs") cryptography library the default for Rustls, though users can switch between that and ring. Soon, Microsoft's Symcrypt library will be an option, too.
- Libcrypto recently received FIPS support, which serves as a significant validation of its standard of security. FIPS is an important requirement for many potential government and corporate users.

We published a blog post that summarizes this milestone and thanks Alpha-Omega for your support.

Eclipse

The number of Eclipse Foundation projects incorporating OtterDog has reached 90, marking an increase of 10 since the end of January. OtterDog now manages the configuration of 1,164 repositories.

The GitHub app is now deployed in production: https://otterdog.eclipse.org. All organizations with OtterDog benefit from automatic reviews and deployment of the submitted changes after merging by the security team, for example, see eclipse-tractusx/.eclipsefdn#60.

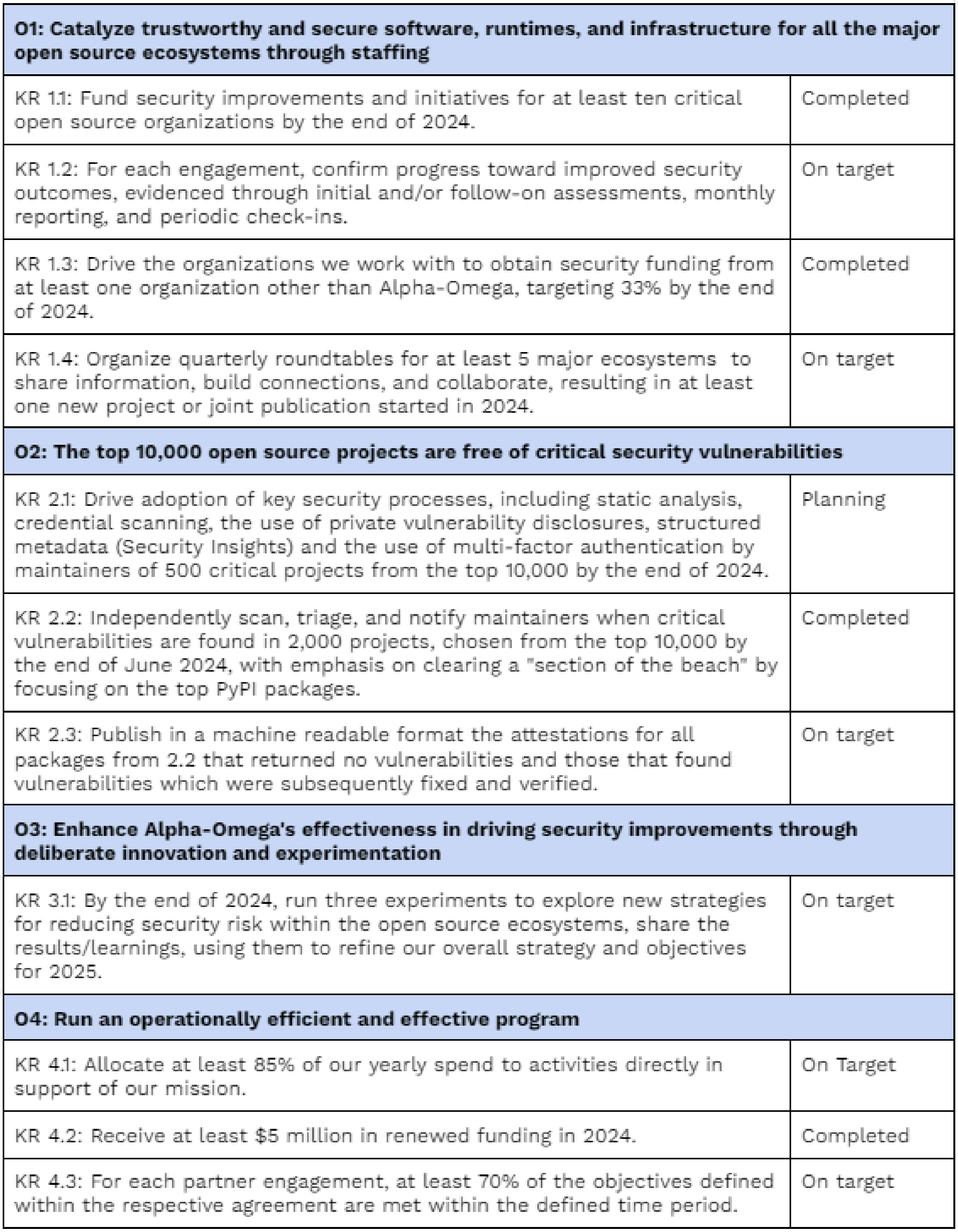
The dashboard has been revamped and now displays much more information than before. It provides an easy way to capture, at a glance, the security posture of the projects, including important security configurations like 2FA enforcement, default workflow permissions, etc.

Rust Foundation

Jon has publicly posted his draft version of the C++/Rust Interop initiative problem statement and high level strategy to the Rust Project. Jon is receiving feedback and starting to move towards implementing this strategy, which will be a heavy focus on 2025.

Also, as part of defining what we need to do for C++/Rust Interop, we are asking questions about unsafe since that is a key barrier between the two languages. There is a discussion happening around the definition of unsafety and undefined behavior, safety critical coding guidelines and unsafe coding guidelines research and writing.

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.	Completed
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.	Completed
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.	Completed
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.	On target
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 November) will be delivered by Monday, December 9th and our next Alpha-Omega public meeting will take place Wednesday, December 4th. 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