Alpha-Omega

MONTHLY REPORT

JULY 2024

July 2024

SUMMARY

Alpha Omega held its quarterly roundtable this month, hosting attendees from eleven organizations. OSTIF presented on Security Audits and their impact on open source projects. The Roundtable focused on Improving the security posture and sustainability of open source projects through audits that are collaborative in nature and focus on holistically improving the software. Alpha-Omega (Henri) presented to the OpenSSF TAC on July 9th, and Michael Scovetta and Michael Winser attended the OSPOs for Good conference at the UN with the goal of connecting with other potential sources of funds.

NEW ENGAGEMENTS

IIn July, Alpha Omega granted funds for Apache Airflow PMC to lead review / audit the complete set of dependencies of Airflow using some predefined criteria, including using automation/tooling available. This is the first time that we know of such a comprehensive audit being done across an entire project’s dependencies. The goal of those will be to produce the list of problematic dependencies, and recommended actions ("Fixing", "Forking" (vendoring-in), or "Forgetting" about them and replacing them with other solutions). They will also solve the problems found during the audit and automate monitoring for dependent CVEs. In doing this Airflow will switch to a “Trusted Publisher” workflow which will improve awareness about models of funding supply chain security.

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
- Support of LLVM ports to Debian
- OpenRefactory
- Kernel
- RubyCentral
- ISRG

A FEW NOTABLE WORK UPDATES FROM GRANTEES

Python Software Foundation
This month's primary focus has been in the Python Security Response Team (PSRT) processes and membership policy. Today, this group is fairly loosely organized and doesn't have a membership policy which would be useful for both promoting new members and removing members who are no longer contributing to the PSRT.

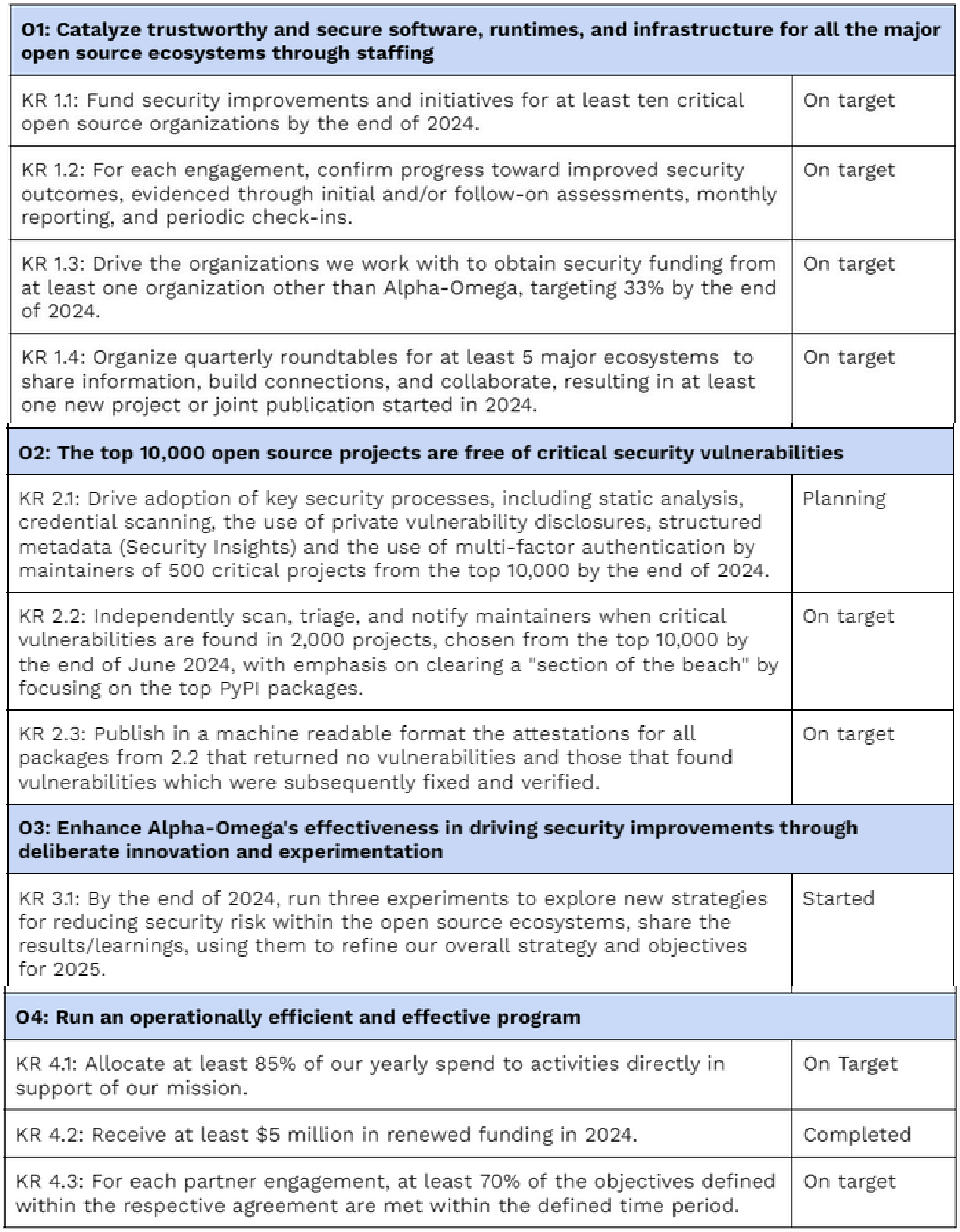
The long-term vision is to adopt GitHub Security Advisories as a ticketing system for tracking vulnerability reports and assign a single "Coordinator" to each ticket to ensure there's clear ownership of each report and who is responsible for taking a report end-to-end through the process, either by marking the report as not a vulnerability or getting a fix and publishing an advisory.

Ruby Central (from the Ruby Central report)
André defined and built the Organization & Membership models, defined their relations, and added administrative views for all of the models. The models are now merged into RubyGems.org, allowing other engineers to be aware of and collaborate on the models whenever their work may overlap. In the meantime, Ian has refined the designs for our onboarding process for new users. We settled on a process that will allow people to use the name of a gem they own as the name of their organization. Allocating org names only by owned gem names will prevent the landrush that PyPI experienced and warned us about. RubyGems.org has been around long enough that most of the desirable gem names are taken. We believe that granting ownership of the same-named org will be a natural progression for most users.

Rust
The Rust team made progress in July in multiple areas: on the engineering side, work continues on verifying provenance on 5,000 crates based on this methodology, with no obvious "red flags" being found. Features were added to crates.io (project RSS feeds, lib/bin detection), and work continues on the larger signing story. On the organization side, the Rust team also welcomed Marco Ieni as their new infrastructure engineer.

Threat models have all been completed and published (Crates Ecosystem, Rust Infrastructure, crates.io, Rust Project). Additional recent updates on crates.io can be found here.

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 August) will be delivered by Monday, September 9th , and our next Alpha-Omega public meeting will take place August 7th. 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 or reach out to one of us directly.

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