Alpha-Omega

MONTHLY REPORT

JUNE 2024

June 2024

SUMMARY

We're active and healthy. Our team consists of Michael Scovetta (Microsoft), Henri Yandell (Amazon Web Services), Bob Callaway (Google), supported by Michael Winser (contractor) and Michelle Martineau and Tracy Li from the Linux Foundation. We've received over $5M in funding so far in 2024 and are actively meeting with new potential engagement partners. Our team meets weekly, we also meet with at least a few partners and grantees a week to gather updates and review proposals. The first half of the year has resulted in over 4M in grants that have helped catalyze sustainable security improvements to the world's most critical open source projects and ecosystems. Our goal is to match this investment in the second half of 2024.

EXISTING ENGAGEMENTS

In June Alpha Omega developed a plan to understand the security posture of the 100 most-interesting open source AI libraries, with particular focus on those characteristics unique to AI and generative AI. Alpha Omega has partnered with OSTIF to assist in this initiative. The methodology will evolve over time as new threats are identified and analysis techniques are refined. You can review a full list of proposed libraries here. 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.

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

Debian/Ubuntu LLVM Packaging

- New Features and Improvements: Added support for Ubuntu Noble, packaging of llvmlibc, made libpolly available as a separate package, improved automation for patch handling and integrated mold as a linker for faster builds
- Toolchain Updates: Pushed numerous updates across LLVM Toolchain versions 16, 17, 18 and 19 - Debian, Ubuntu and apt.llvm.org
- Issues Reported and Fixed: Reported multiple upstream issues and resolved several significant ones. Improving the builds on all platforms.
- Additional Changes: Implemented a workaround for Bookworm in llvm.sh and continued to refine the automation processes, and improved the documentation of the processes.

ISRG

AV1 Media decoders have historically been fertile ground for memory safety vulnerabilities. This is because they are complex, heavily used, and commonly processing untrusted data from networks. AV1 is set to become one of the most important media formats on the Internet. Prossimo is building a high-performance and memory safe AV1 decoder, called Rav1d.

At this point in the project, the Rust code is functionally equivalent to the original C code. In June, the team focused primarily on:

- Performance profiling and optimization
- Integration and polish

Performance work has focused on identifying regressions and addressing them. Optimizations included profiling and improving runtime performance in the latest safe code. In addition, the team worked on improving the memory overhead by porting upstream dav1d (the C AV1 decoder from which rav1d was transpiled) changes.

The team is currently seeking to close the ~11% performance delta between the original C code and the transpiled Rust code. ISRG has made outside advisors available to consult on this issue.

OpenRefactory

June

Month	Dec 2023	Jan 2024	Feb 2024	Mar 2024	Apr 2024	May 2024	Jun 2024
Projects analyzed	328	300	530	780	712	785	1,198
Projects with no bugs	293	279	525	776	708	784	1,198
Total bugs filed	56	13	7	7	4	7	1
Security/Reliability bugs filed	15	8	6	5	2	5	2 *[1]
Bugs with a fix suggestion	50	10	2	2	4	0	1
Bugs with a PoC exploit	4	1	2	3	0	0	0
Fixes merged by maintainers	27	10	5	3	4	0	1
Security/Reliability fixes merged	6	6	2	1	0	0	0
Fixes ignored by maintainers	1	1	1	0	2	0	2
Reports still open	28	2	1	4	0	7	0

Ruby Central

- We have refactored a large portion of our authorization system, using rails best practices (a gem known as "Pundit").
- We are continuing to work on the API authorization system, which adds an extra layer but is not blocking yet.
- In the meantime, we have devised a roadmap for the upcoming features for Organizations.

Excerpt:
In order to eventually support namespaces for gems, we must first establish a clear, useful organizational structure. The structure must be in place before namespaces so that management of the namespace is owned by a well defined organizational structure with effective permission control.

We eventually aim to provide a solution that supports the following namespace and ownership related goals:

- Reduce customer confusion for tools and services spanning multiple gems. It is not uncommon for an organization to distribute many packages, such as Rails with the active/action packages, AWS with SDK clients, Ruby standard library gems, etc.
- Help clarify ownership of gems so typosquatting is less effective.
- Allow for a better gem owner permissions model that ensures the security of gems by controlling ownership and access.
- Increase security by allowing teams to collaborate or automate processes without requiring shared accounts and credentials.
- Increase transparency around actions taken by team members by recording and reporting events for any actions performed by a member of the organization.

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.	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 July) will be delivered by Monday, August 12th, and our next Alpha-Omega public meeting will take place on Wednesday, August 7th. 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