Alpha-Omega

MONTHLY REPORT

MARCH & APRIL 2024

March & April 2024

SUMMARY

In early March, Microsoft announced that they were providing an additional $3.2 million to the Alpha-Omega project, and we're pleased to announce that Amazon Web Services recently provided an additional $1.8 million. We're grateful to our stakeholders for standing behind us as we catalyze sustainable security improvements to the most critical open source projects and ecosystems.

In early March, CISA held a roundtable event in Washington, D.C. focused on open source software security. The Alpha-Omega team (and some of our engagement partners) were active participants and we enjoyed connecting with others across the ecosystem.

In mid-April, the Alpha-Omega team hosted our quarterly roundtable at the Open Source Summit in Seattle, bringing together stakeholders, grant recipients, and the larger community together to share lessons and build relationships between security leaders in different ecosystems. The open-ended, "what if" nature of the discussion was well-appreciated, allowing space to explore "wild" ideas rather than just focusing on immediate problems. In addition to our monthly public meetings and quarterly roundtables, we're now planning to host two in-person roundtables per year, preferably at conferences that our partners are already attending.

The Alpha-Omega team also met privately with stakeholders from the Sovereign Tech Fund and the Open Technology Fund, and we plan to connect regularly to share learning and where possible, collaborate.

In addition to the many talks from our friends in OpenSSL, a few recent talks from our direct partners include:

- Embrace the Differences: Securing Open Source Ecosystems Where They Are (Seth Larson, Python Software Foundation)
- Build Provenance: Lessons (so Far) from Homebrew (Joe Sweeney, Trail of Bits)
- Improving the Posture of Critical Open Source Projects (Amir Montazery, OSTIF)
- Effective Vulnerability Management for Over 400 Projects at the Eclipse Foundation (Michael Winser and Marta Rybczynska, Eclipse Foundation)
- Community Engagement and Security Initiatives (Rebecca Rumbul [Rust Foundation] and Deb Nicholson [Python Software Foundation])

NEW ENGAGEMENTS

We recently agreed to fund work through Prossimo to complete development of the Rust-based rav1d AV1 media decoder.

We also agreed to fund a security audit of the PHP Packagist (both server-side code and the infrastructure that hosts packagist.org) and the Composer (client) package management tool.

EXISTING ENGAGEMENTS

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

- Node.js
- jQuery
- The Eclipse Foundation
- OpenSSL
- Homebrew
- FreeBSD
- The Rust Foundation
- The Python Software Foundation
- ISRG
- OpenRefactory
- Kernel
- RubyCentral

A FEW NOTABLE WORK UPDATES FROM GRANTEES

FreeBSD
Our engagement with FreeBSD has just started, but the team has already connected with two organizations to plan out a security audit for the bhyve hypervisor manager and the Capsicum sandboxing framework. The FreeBSD team is also initiating an MFA pilot to determine the best option for their community.

Homebrew
Homebrew reached a milestone recently around adding build provenance to packages. Joe Sweeney (Trail of Bits) presented the work at SOSS Community Day. As a result, all bottles served by homebrew-core will have provenance attestations included. Work continues to complete the other half -- client-side verification of attestations during installation.

Python Software Foundation

Work was recently completed to automate more of the CPython release process, and work has started to separate out the build/test and build/docs phases into separate processes. This will make it harder for supply chain attacks that affect docs dependencies to affect CPython's builds. In addition, CPython now produces SBOMs for Windows builds. Additional artifacts like MSIs and the MacOS installer are coming soon! A Google Summer of Code project for adopting compiler hardening options for C/C++ is now available. Read more at Seth Larson's blog.

ISRG / Prossimo

In addition to our new work with Prossimo described above, existing work continues on the Rustls TLS library, which added support for post-quantum key exchange and the first version of an OpenSSL compatibility layer for Nginx. In addition, the pluggable backend work completed earlier this year was built upon by Microsoft for the rustls-symcrypt backend. Prosimo also drives work related to Rust for Linux, which adds support for the Rust language to the Linux kernel. A set of feature patches were submitted for the Kernel 6.9 merge window. Rust for Linux will also have a micro-conference at the Linux Plumbers Conference in Austria in September.

jQuery

Work has been completed to migrate testing infrastructure on three jQuery projects, including jQuery Core, jQuery Migrate, and jQuery UI.

OpenSSL

While the OpenSSL audit was completed a few months ago, a few remaining issues are being worked through by the OpenSSL team; a public report is expected shortly, once the issues have all been resolved.

OpenRefactory

Through our engagement with OpenRefactory, we've scanned over 3,700 projects for critical security vulnerabilities (e.g. injection or cryptographic flaws), focused primarily on the PyPI ecosystem. When vulnerabilities are found, OpenRefactory discloses them privately to the maintainer and works with them as needed on a fix. To date we've had 40 security vulnerabilities fixed. As part of this effort, we're publishing signed attestations that can be used during package consumption.

OpenRefactory Cont.

Month	Aug 2023	Sep 2023	Oct 2023	Nov 2023	Dec 2023	Jan 2024	Feb 2024	Mar 2024	Apr 2024
Projects analyzed	132	458	809	1,079	1,407	1,707	2,237	3,017	3,729
Projects with no bugs	98	398	718	938	1,231	1,510	2,035	2,811	3,519
Total bugs filed	33	75	113	168	224	237	244	251	255
Security/Reliability bugs filed	12	23	43	79	94	102	108	113	115
Total high severity bugs filed*	-	-	-	-	25	29	34	39	40
Bugs with a fix suggestion	26	64	94	140	190	200	202	204	208
Bugs with a PoC exploit	6	13	18	22	26	27	29	32	32
Fixes merged by maintainers	15 (45%)	38 (51%)	54 (48%)	76 (45.3%)	103 (46%)	113 (47.7%)	118 (48.4%)	121 (48.2%)	125 (49.01%)
Security/Reliability fixes merged	Not measured	Not measured	13 (30%)	25 (31.6%)	31 (32.9%)	37 (36.2%)	39 (36.1%)	40 (35.4%)	40 (34.78%)
Fixes ignored by maintainers	Not measured	8 (11%)	7 (6%)	9 (5.3%)	10 (4.5%)	11 (4.6%)	12 (4.9%)	12 (4.78%)	14 (5.5%)
Reports still open	Not measured	29 (39%)	52 (46%)	83 (49.4%)	111 (49.5%)	113 (47.7%)	114 (46.7%)	118 (47.01%)	116 (45.49%)

RubyGems

The RubyGems team met with Trail of Bits to plan their upcoming security and process audit, and are iterating on the proposal. They also onboarded a project manager to drive work to implement namespaces within the RubyGems ecosystem and will soon be meeting with the PyPI team to learn from their experiences.

Rust Foundation

Work continues on the crates.io administrator functionality. A recent PR adds a concept of "sudo mode" for admins logged into crates.io. Actions that require admin privileges will be disabled by default unless the admin explicitly turns on admin actions from the user menu, at which point they will be given privileges for six hours or until they disable admin actions again from the user menu.
With the user functionality and the ability to delete crates, that is about 95% of the rapid response scenarios covered.

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.	Not measured *ETA next month*
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

CHALLENGES AND OPPORTUNITIES

The xz backdoor drove many discussions around advanced adversaries targeting open source ecosystems, including a recent report by the OpenJS Foundation calling attention to what appeared to be a similar social engineering attack. While these types of insider attacks are fundamentally hard to defend against, we believe we have the right focus: hardening the most critical parts of the ecosystem, encouraging provenance and transparency, strong authentication, hardening build systems, and (in some places) adopting memory safe languages.

Sustainability within the open source ecosystem (e.g. maintainer burnout, etc.) continues to be a challenge without an obvious solution - there's an opportunity for OpenSSF to drive meaningful conversations and action to address this risk.

FOCUS FOR NEXT MONTH

Over the next month, we'll be working to finalize our plan on assessing the security of open source AI libraries, and evaluating a few grant requests.

We'll also be having discussions with GitHub on the most feasible approach to encourage more maintainers (particularly those of popular projects) to leverage available tooling (i.e. static analysis, secret detection, dependency management, and private vulnerability reporting).

Our next update (for May) will be delivered by Monday, June 10, and our next Alpha-Omega public meeting will take place on Wednesday, May 1st. 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.