Alpha-Omega

MONTHLY REPORT

JANUARY 2024

January 2024

SUMMARY

It's a new year and the Alpha-Omega team is excited to continue our mission of catalyzing security improvements to the most critical open source software projects and ecosystems.

As we discussed in earlier updates, the Alpha-Omega team has been working hard to formalize our governance structure; this work is complete -- Alpha-Omega now operating as a Directed Fund with an updated membership agreement in place. We thank our financial supporters, Amazon Web Services, Microsoft, and Google, for their continued support.

We just released our Annual Report, describing our successes in 2023 and areas of focus for 2024. We're proud of what we were able to accomplish last year and are excited to double down on it this year.

Where we are TODAY

NEW ENGAGEMENTS

We agreed to renew funding for the Node.js project, which includes funding to improve/drive security processes (vulnerability report triage, security releases), security features within the Node.js runtime, and more.

Where we are

TODAY

EXISTING ENGAGEMENTS

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

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

A FEW NOTABLE WORK UPDATES FROM GRANTEES

Rust Foundation

As we pick the security initiative work up for 2024, the highlight of January is that the Crates.io project is now able to replay crate publishing from the past. This provides a retrospective on what new Typomania and Sandpit checks would have found, and thus would find in the future. The project intends to use this to establish a scoring system on potential maliciousness, which — if a crate falls above a given threshold — can feed into deciding whether to quarantine the crate and potentially that user pending further review.

Sandpit is a tool created to scan available crates to try to detect malicious crates based on available heuristics, has been deployed to production on Google Cloud Platform (GCP) and is running at a regular cadence.

Read the Second Security Initiative Report Details Rust Security Advancements

Python Software Foundation (PSF)

Digital Attestations in PyPI: Initial work has been proposed (authored by William Woodruff), reviewed by Seth Larson around digital attestations for PyPI artifacts, enabling a standard mechanism for PyPI to host these attestations for clients to later validate.

Diffoscope for XAR/PKG: CPython publishes PKG files for the macOS platform which use the XAR archive format. The diffoscope tool was indispensable for making CPython's source artifacts reproducible, but didn't have support for XAR/PKG files. As a part of having reproducible builds of macOS the PSF team contributed support for the XAR/PKG format upstream.

ISRG / Prossimo

The Rustls developers spent January primarily building towards the first release with the aws-lc-rs cryptographic back-end as the default, which will include FIPS support. This is one of the most important remaining features that need to be implemented before significantly more widespread adoption is possible. The release with the work can be expected in early February.

The team also merged no-alloc API support in January, which is important for high performance consumers, and have made a number of other miscellaneous improvements.

The team completed, merged, and shipped an excellent benchmarking system, both to catch performance regressions on a per-commit basis and to compare Rustls to OpenSSL. The Prossimo team published a summary of the work and outcomes in this blog post.

OpenRefactory

We continue to work with OpenRefactory to scan the "long tail" of critical open source projects, identify vulnerabilities, triage them, and report them to maintainers to be fixed. This work is important because most open source projects have never undergone any sort of security assessment. At Alpha-Omega, we're continually looking for efficient, effective ways at improving the security for the many thousands of open source projects.

OpenRefactory continued

In the second half of 2023, OpenRefactory completed over 1,400 projects and filed 94 security/reliability issues.

In January 2023, OpenRefactory analyzed 300 projects and reported 8 security/reliability bugs to maintainers. Ten previously reported bugs were fixed.

A spreadsheet containing scan results can be found here.

jQuery

Significant work has been completed in an effort to migrate jQuery Core's testing infrastructure off of deprecated or largely unsupported services and libraries. This includes:

- Migrating the jQuery Core testing scripts from grunt to npm scripts.
- Migrating the jQuery Core test suite from TestSwarm, which runs on an old Jenkins server, to GitHub Actions.
- Migrating the jQuery Core test suite from Karma to using Selenium WebDriver directly for local testing and BrowserStack's REST API for local and CI testing on BrowserStack.
- Building a standalone test server using Express and mock middleware.