Alpha-Omega

MONTHLY REPORT OCTOBER 2023

October 2023

SUMMARY

Each of our Alpha engagement partners continue to make substantial progress each month, delivering security improvements that benefit billions of end-users each month.

NEW ENGAGEMENTS

We agreed to fund Rust for a second year to support the Rust Foundation Security Initiative (announcement).

We provided funds to the Homebrew team to add provenance and package signing to the ecosystem, announced on alpha-omega.dev and by Trail of Bits (Homebrew's technology partner).

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 (announcement)
- The Rust Foundation
- The Python Software Foundation
- ISRG
- OpenRefactory

A FEW NOTABLE WORK UPDATES FROM GRANTEES

Rust Foundation

Progress on the four threat models being developed by the Rust Foundation:

1. Crates ecosystem: Published.
2. Rust Infrastructure: Published.
3. crates.io: Potential threats identified.
4. Rust Project: Threat outline developed.

Python Software Foundation (PSF)

Wrote and published the report for Q3 in the Security Developer-in-Residence role. Included all the highlighted accomplishments in the role; such as the PSF becoming a CNA, storing advisories in an OSV database, improvements to the Python Security Response Team, and more.

Python Software Foundation (PSF)continued

Three areas of focus for the next quarter:

- Securing the CPython release process
- Metadata for bundled projects in Python packages
- SBOM for CPython release artifacts

ISRG / Prossimo

The pluggable cryptography implementation started to land in August and work is under way to add support for aws-lc-rs. This has been a huge amount of work. We expect the pluggable cryptography implementation and aws-lc-rs integration to be completed in October. We are waiting on guidance from the aws-lc-rs team regarding finalizing FIPS support. Adolfo Ochogavia is making great progress on benchmarking and his benchmarking tools are already being used by Rustls developers to improve performance. Ferrous Systems has largely completed an RFC for caller managed buffers, asynchronous APIs, and no-std support. Implementation has started.

OpenRefactory

OpenRefactory continues to analyze critical open source projects using automated tools, triage, and private reporting, analyzing around 300-350 projects per month. They've reported 20 security bugs in October (43 in total), and continue to follow up with maintainers to encourage fixes to be merged.

Additional details are available in OpenRefactory's monthly reports.

FOCUS FOR NEXT MONTH

We're actively exploring improving information sharing between Alpha engagement partners, separately from the public meetings we've held since our inception. We plan to publish a 2023 annual report, similar to the one we published last year.

If you have any questions about this update or any of our work, please contact the Alpha-Omega team at info@alpha-omega.dev.