Alpha-Omega

MONTHLY
REPORT
FEBRUARY 2024

February 2024

SUMMARY

Two brand new engagements this month with FreeBSD and RubyCentral. As is often the case with new grant recipients, we are starting with a mix of audits and short projects.

Our existing engagements continue to have impact. Eclipse's Otterdog project is now enforcing policy and managing over 1000 repos in 90 organizations. This includes 2FA. The Rust Foundation has completed their threat model work. CPython 3.12.2 is the first release to have SBOMs for source artifacts. The Homebrew project will be presenting their work to make Homebrew-core SLSA Build L2 at the Open Source Summit in April.

Where we are

TODAY

NEW ENGAGEMENTS

- FreeBSD
- RubyCentral

OpenRefactory
We also agreed to renew funding for OpenRefactory with a scope focusing on Python projects. OpenRefactory will collect the top 10,000 projectts from PyPi based on the number of downloads over the last year. In addition, generating attestations, working with Python SF to create a mechanism that end users can consume the results.

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
- FreeBSD
- The Rust Foundation
- The Python Software Foundation
- ISRG
- OpenRefactory
- Kernel
- RubyCentral

A FEW NOTABLE WORK UPDATES FROM GRANTEES

Rust Foundation

The primary highlight of February is that all four of the scheduled threat models are now complete and available. In the beginnings of the Foundation's security initiative, we agreed to develop threat models around the crates ecosystem, the crates.io website, Rust project infrastructure and the Rust project itself. These are now all developed and will be used as guides of focus for our security work across all of these potential avenues of maliciousness.

Python Software Foundation (PSF)

CPython 3.12.2 is the first release to have SBOMs for source artifacts!

- Published announcement on the PSF blog
- Adding support for SBOMs for Windows artifacts is complete and awaiting reviews from Windows release managers, pull requests are completed.

Python Software Foundation (PSF) continued

- *Support for macOS artifact SBOMs and Vulnerability Exchange is next after Windows SBOMs are done.*
- Published user documentation for CPython SBOM documents.
- Worked closely with release managers, pip maintainers, and downstream distributors of CPython (mostly Fedora) to create a sustainable workflow.
- Presented on the status and challenges to the OpenSSF SBOM Everywhere SIG.

OpenRefactory

Month	Dec 2023	Jan 2024	Feb 2024
Projects analyzed	328	300	530
Projects with no bugs	293	279	525
Total bugs filed	56	13	7
Security/Reliability bugs filed	15	8	6
Bugs with a fix suggestion	50	10	2
Bugs with a PoC exploit	4	1	2
Fixes merged by maintainers	27	10	5
Security/Reliability fixes merged	6	6	2
Fixes ignored by maintainers	1	1	1
Reports still open	28	2	1

ISRG

We are making great progress. The community is also growing rapidly, with new contributors showing up regularly and largely representing new consumers of Rustls.

We accomplished a major milestone by releasing version 0.23.0.

- It makes AWS's Libcrypto ("aws-lc-rs") cryptography library the default for Rustls, though users can switch between that and ring. Soon, Microsoft's Symcrypt library will be an option, too.
- Libcrypto recently received FIPS support, which serves as a significant validation of its standard of security. FIPS is an important requirement for many potential government and corporate users.

We published a blog post that summarizes this milestone and thanks Alpha-Omega for your support.

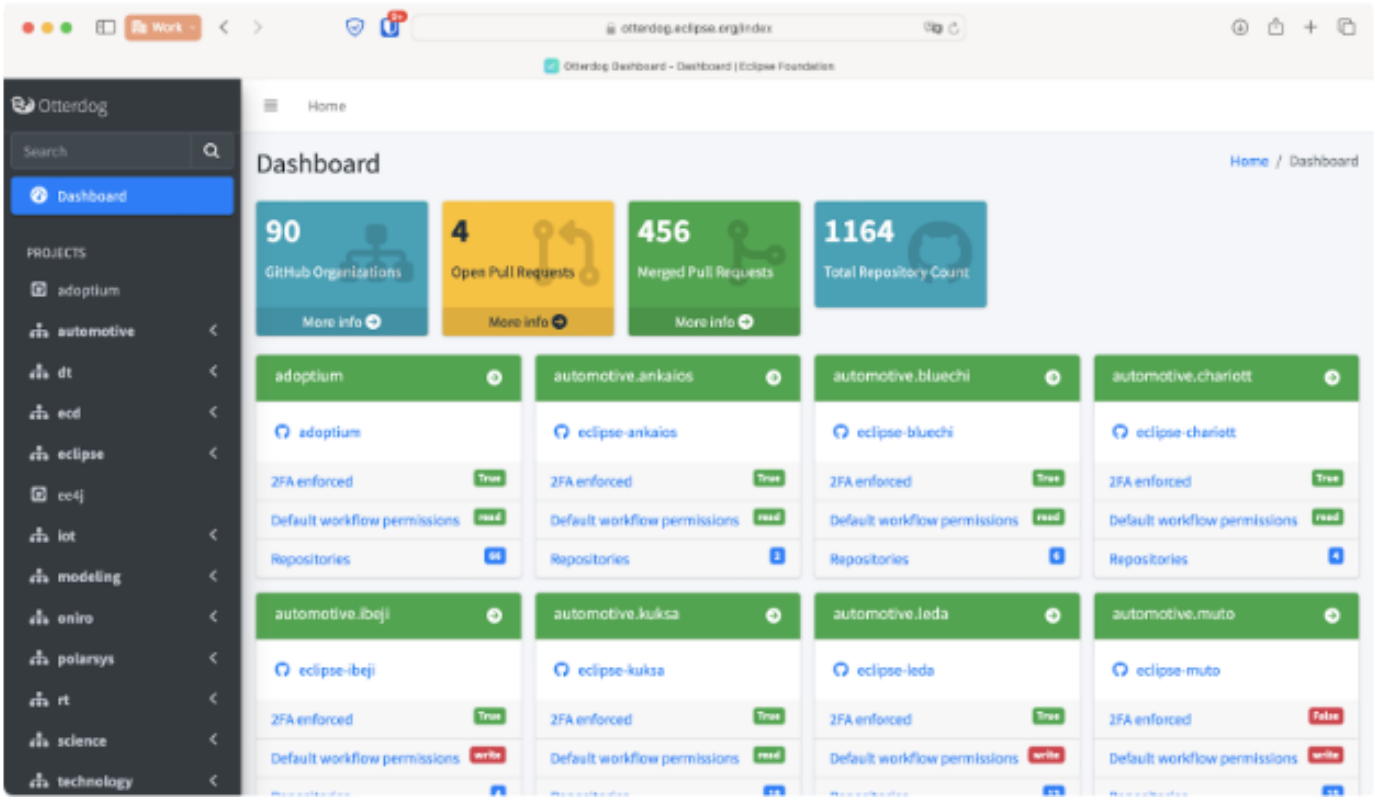
Eclipse

The number of Eclipse Foundation projects incorporating OtterDog has reached 90, marking an increase of 10 since the end of January. OtterDog now manages the configuration of 1,164 repositories.

The GitHub app is now deployed in production: https://otterdog.eclipse.org. All organizations with OtterDog benefit from automatic reviews and deployment of the submitted changes after merging by the security team, for example, see eclipse-tractusx/.eclipsefdn#60.

The dashboard has been revamped and now displays much more information than before. It provides an easy way to capture, at a glance, the security posture of the projects, including important security configurations like 2FA enforcement, default workflow permissions, etc.

Eclipse continued



On February 2nd, we enforced 2FA on all GitHub organizations where all members already had 2FA enabled. Consequently, these organizations were already in full compliance with this new requirement. However, this means that moving forward, all new members will be required to activate 2FA before their invitation to join the GitHub organization can be extended. This action has increased the percentage of Eclipse Foundation-owned organizations with 2FA enabled from 18.5% to 64%.

On February 28th, we also sent a reminder to the 389 accounts without 2FA, informing them that starting April 30th, they will temporarily lose access to their repositories until 2FA is enabled.