2024 Independent Security Audit Impact Report

CLOUD NATIVE
COMPUTING FOUNDATION

OSTIF

Prepared by the **Open Source Technology Improvement Fund**

Thanks to support from **Cloud Native Computing Foundation**

Improving Security Posture of Critical Open Source Projects

ostif.org

This report is an overview of independent security audits published or carried out in the calendar year of 2024.

Contents

Summary

This deck is a summary of the working relationship between the Cloud Native Computing Foundation (CNCF) and the Open Source Technology Improvement Fund (OSTIF) in the year 2024.

These two organizations work together to bring real and impactful security work to CNCF projects that help create the foundation of our digital world.

Improving Security Posture of Critical Open Source Projects

ostif.org

> “As open source permeates every industry and technology across the world, it's of utmost importance to ensure high quality security practices for critical projects. We are proud of our high impact partnership with OSTIF that has yielded multitudes of security improvements across some of the most widely used cloud native open source projects.”

Chris Aniszczyk
CTO, Cloud Native Computing Foundation

Impact of a Professional & Independent Security Audit

Security audits are a great exercise for open source projects and a powerful tool for improving security posture. Audits, as compared to other security solutions, are uniquely able to provide tailored security work, offer long-term hardening recommendations and can include new or updated fuzz testing for the project.

Project maintainers and contributors work with independent audit experts to identify risks, threat vectors, and implement tools to improve the project's security posture. While there time commitment can be low, their impact upon the success of audits is high. They ultimately can have a deeper understanding of their project and its security having participated in the audit process.

Code reviews typically lead to the finding and fixing of serious issues and classes of bugs, resulting in a more secure project. Furthermore, the documentation generated by audits positively contributes to the longevity and health of projects.

Cumulative Statistics for 2024*

* able to be publicly shared as of November 2024

28

Critical, High or Medium Severity Findings

80

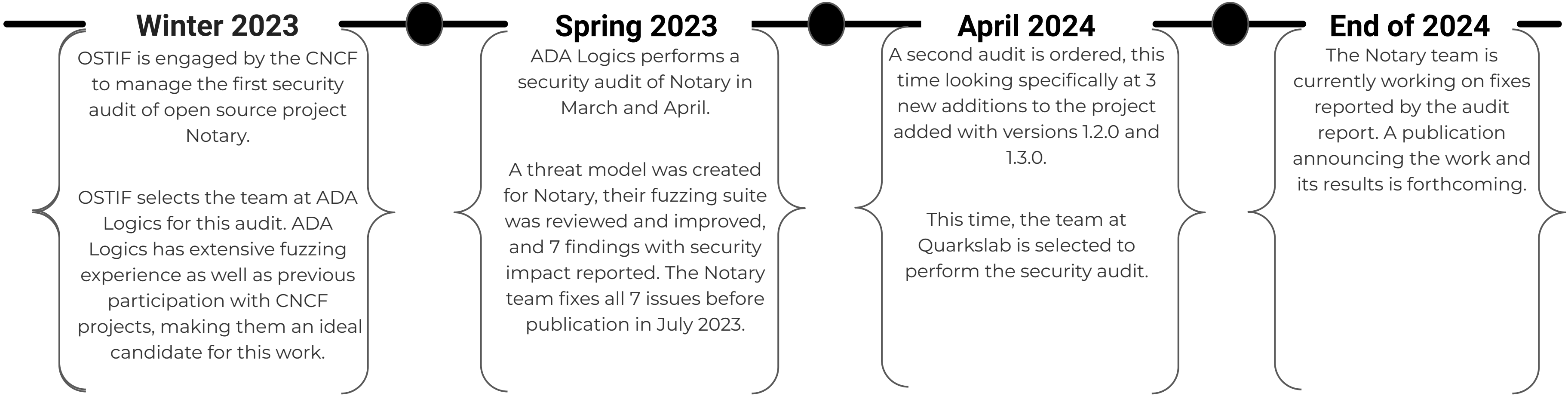
Total Security Recommendations Made

3,000+

Hours of review and audit work by security experts

A Case Study Supporting the Efficacy Open Source Security Audits

Notary has now undergone a second security audit with OSTIF. Projects that receive follow-up audits tend to exhibit signs of more robust security, with less severe vulnerabilities reported than the first audit and more secure development practices.



Winter 2023

OSTIF is engaged by the CNCF to manage the first security audit of open source project Notary.

OSTIF selects the team at ADA Logics for this audit. ADA Logics has extensive fuzzing experience as well as previous participation with CNCF projects, making them an ideal candidate for this work.

Spring 2023

ADA Logics performs a security audit of Notary in March and April.

A threat model was created for Notary, their fuzzing suite was reviewed and improved, and 7 findings with security impact reported. The Notary team fixes all 7 issues before publication in July 2023.

April 2024

A second audit is ordered, this time looking specifically at 3 new additions to the project added with versions 1.2.0 and 1.3.0.

This time, the team at Quarkslab is selected to perform the security audit.

End of 2024

The Notary team is currently working on fixes reported by the audit report. A publication announcing the work and its results is forthcoming.

Project Feedback

“From the development process perspective, the security audit helps us write more secure code and increase the quality of code.

Additionally, the security audit forces our developers and maintainers to become more aware of security (such as threat modeling), which provides a better security foundation for the engineering design, implementation, and future development of the project.”

Feynman Zhou, Notary maintainer

We Graduated with OSTIF!

Falco

Istio

CertManager

Vitess

KEDA

Dapr

Cilium

Python-TUF/Go-TUF

Flux

Envoy

Argo

KubeEdge

Cri-O

Associated & Future Work

OSTIF is grateful to help open source projects, foundations, and organizations improve security posture and protect against supply chain attacks.

Coming in 2025: Backstage, LinkerD, Karmada, Volcano, and Kubernetes

Sovereign Tech Agency

OpenSSF

OSTIF collaborates with global funds like the Sovereign Tech Agency and OpenSSF to bring impact to open source projects looking to improve their security and resilience.

OSTIF is growing and helping more open source projects in 2025 than ever before. Stay tuned to https://ostif.org/news/ for up to date information.

Thank You

A big thank you to Chris Aniszczyk and the Cloud Native Computing Foundation for their continued trust and support. We are grateful for the continued opportunity to work with CNCF members.

Also, special thanks to the diverse set of fantastic maintainers and contributors of the projects mentioned in this report. Your efforts are what make the positive impact of this work feasible.

Last but not least, thank you to our independent audit teams and experts; like the fantastic folks at ADA Logics, X41 D-Sec, Trail of Bits, Shielder, and Quarkslab.

From OSTIF

References

OSTIF website: ostif.org
OSTIF X: https://x.com/OSTIFofficial
OSTIF LinkedIn: https://www.linkedin.com/company/ostif/
CNCF: https://www.cncf.io/
Graduated projects: https://www.cncf.io/projects/

Audit Reports:
CubeFS: https://ostif.org/cubefs-audit-complete/
Certmanager: https://ostif.org/cert-manager-audit-complete/
CloudCustodian: https://ostif.org/cc-audit-complete/
Buildpacks: https://ostif.org/buildpacks-audit-complete/
OpenTelemetry: https://ostif.org/otel-audit-complete/
LitmusChaos: https://ostif.org/litmuschaos-audit-complete/