2023 Independent Security Audit Impact Report

ostif.org

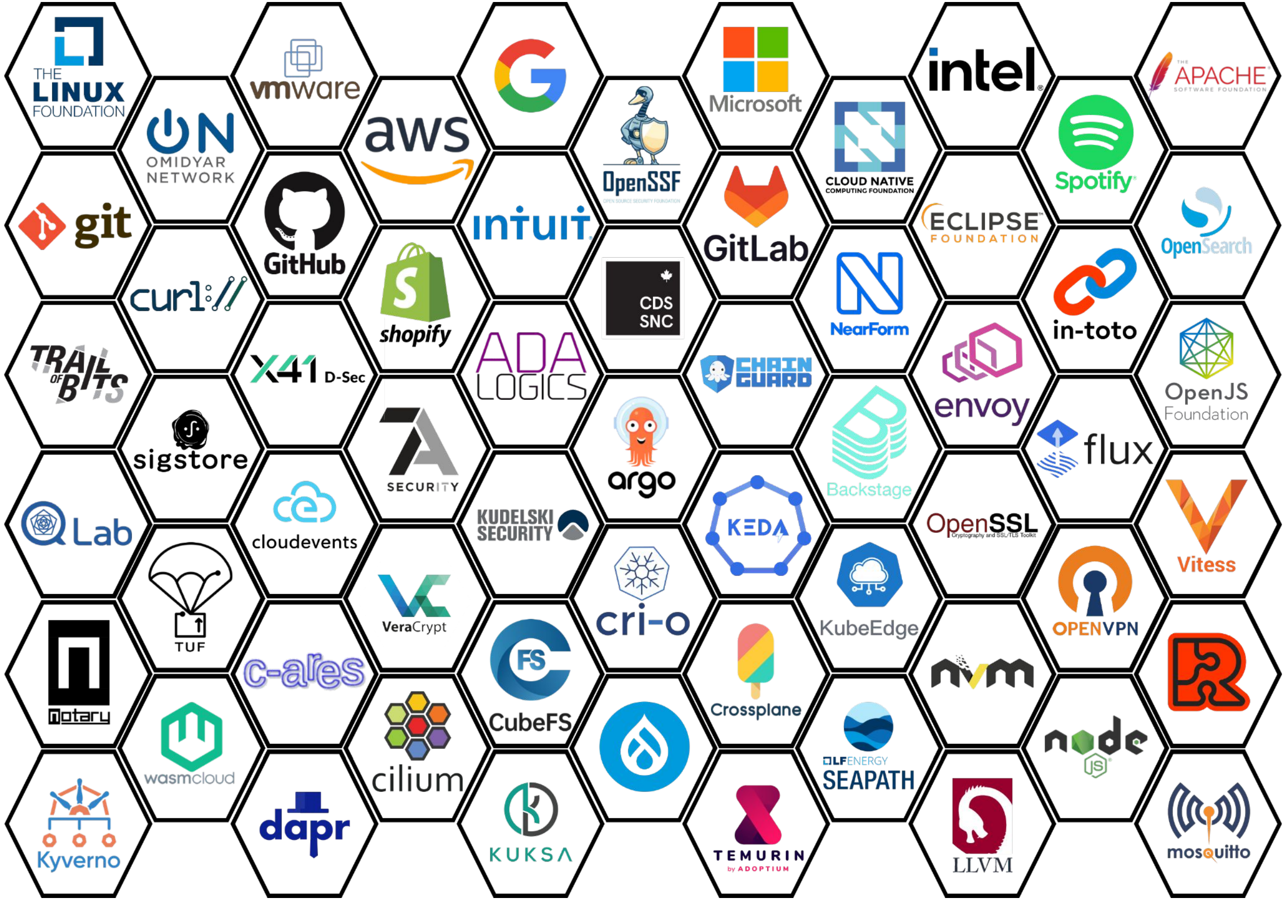
CLOUD NATIVE
COMPUTING FOUNDATION

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

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

Improving Security Posture of Critical Open Source Projects

The Open Source Technology Improvement, Fund



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 2023

Contents

Summary

This is a follow-up report to the work organized earlier in 2022. In funding these security engagements, the Cloud Native Computing Foundation (CNCF) is exhibiting a strong commitment to improving the security posture of projects, a sound guiding policy and project maturity model, and a repeatable process for executing audits with the help of strategic partner Open Source Technology Improvement Fund (OSTIF).

The report will highlight the impact audits can have, overview the CNCF projects audited, and share some project feedback. Also included is a discussion of associated work and a reference page.

> “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 well 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.

Our Partnership

This impactful work continues as a result of a good working relationship between CNCF and OSTIF. Between 2022 and 2023, 23 projects have received security audits sponsored by CNCF funding.

CNCF provides a platform and strong guidance for open source projects to grow and mature. By sponsoring the projects security audit for OSTIF to realize, the CNCF is enriching the open source community in both resources and security research. It's a win-win situation for everyone involved.

OSTIF continues to build partnerships with security teams that understand open source, and iterate on processes that deliver tangible improvements to the open source ecosystem while maintaining full transparency.

Cumulative Statistics for 2023

54

Critical, High or Medium Severity Findings Fixed

16 CVEs

156

Total Security Improvements Made

50

Tools built or improved to continually monitor Open Source Projects for security issues

Kyverno KEDA Notary Falco Dragonfly TUF

Crossplane Istio cilium flux dapr

A Case Study Supporting the Efficacy Open Source Security Audits

Flux

November 2021

Flux undergoes security audit thanks to CNCF funding, OSTIF facilitation, and ADA Logics researchers.

Project finds and fixes its first CVE. Multiple other improvements such as addition of fuzz testing and improved documentation are a result of the audit.

November 2022

Flux team expresses interest in follow on work on changes and new focus areas.

November 2023

A second audit is completed. Executed by a different audit team, results showed that the project had demonstrated improved security posture and testing.

There were half as many findings (10 compared to 22 previously), all low or informational issues.

2024

Thanks to improvements to code and testing practices from the first audit, the second audit yielded exclusively low/informational findings for five different categories.

Project Feedback

"The results of the audit not only validate the architecture and security posture of wasmCloud but also exemplifies our commitment to transparency, security, and open-source excellence in our community."

Bailey Hayes, Chief Technology Officer, Cosmonic

“Thanks to our collaboration with OSTIF, we've been able to improve and validate our security posture. Working with OSTIF not just once, but twice, has been an outstanding experience and we look forward to future collaborations to further strengthen our security efforts.”

Hidde Beydals, Flux Core Maintainer, Staff Engineer at Weaveworks

Associated & Future Work

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

OSTIF Audit Reports - Link to all security audits conducted by OSTIF in 2023, including the 2023 Annual Report.

OSTIF is growing and helping more open source projects in 2024 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 the continued trust and support.

Also special thanks to the diverse set of fantastic maintainers and contributors of the projects mentioned in this report.

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, and Quarkslab.

From OSTIF

References

OSTIF Audits: https://github.com/ostif-org/OSTIF/blob/main/Completed-Engagements.md
Istio: https://ostif.org/the-audit-of-istio-is-complete/
KEDA: https://ostif.org/our-audit-of-kubernetes-event-driven-autoscaling-keda-is-complete/
Cilium: https://ostif.org/our-audit-of-cilium-is-complete/
Falco: https://ostif.org/our-review-of-falco-is-complete/
in-toto: https://ostif.org/our-audit-of-in-toto-is-complete/
Vitess: https://ostif.org/our-audit-of-vitess-is-complete/
go-tuf: https://ostif.org/go-tuf-on-bugs-ostifs-audit-of-go-tuf/
Notation: https://ostif.org/2023-14/
Crossplane: https://ostif.org/crossplane-audit-complete/
Dapr: https://ostif.org/dapr-audit/
Dragonfly2: https://ostif.org/dragonfly-audit/
wasmCloud: https://ostif.org/ostif-has-completed-a-security-audit-of-wasmcloud/
Flux: https://ostif.org/flux-audit-complete/
Knative: https://ostif.org/knative-audit-complete/
Kyverno: https://ostif.org/kyverno-audit-complete/

CubeFS, CertManager: ETA December 2023/January 2024