2022 Independent Security Audit Impact Report

CLOUD NATIVE
COMPUTING FOUNDATION

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

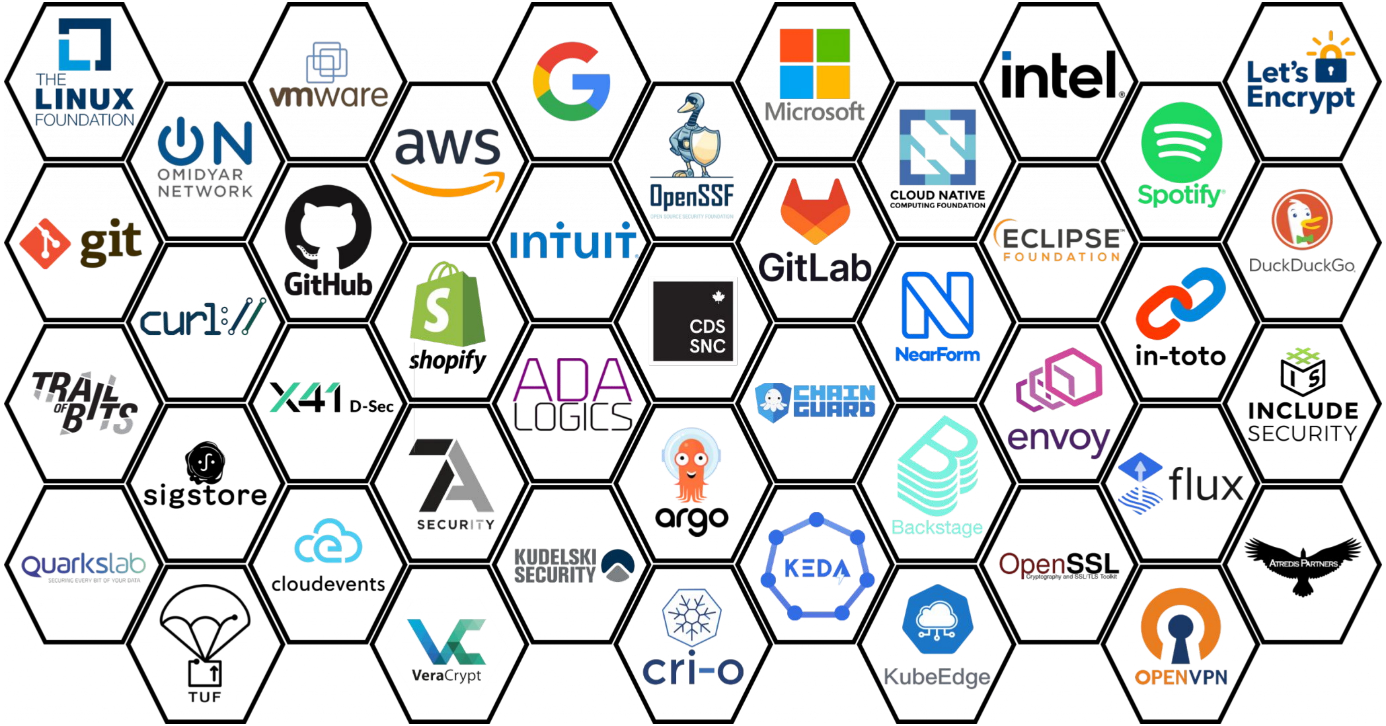
Thanks to support from **Cloud Native Computing Foundation**

Improving Security Posture of Critical Open Source Projects

ostif.org

Open Source Technology Improvement Fund, Inc

Better Security Through A Massive Community



Improving Security Posture of Critical Open Source Projects

ostif.org

Presented in this report is an overview of independent security audits carried out in the second half of 2022 and into early 2023.

This is a follow-up report to the work organized earlier in 2022 and is based on CNCF's 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, share some project feedback, and, finally, discuss associated work and conclude.

The 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.

Project maintainers and contributors work with independent audit experts to identify risks, threat vectors, and implement tools to improve the project’s security posture.

Code reviews typically lead to the finding and fixing of serious issues and classes of bugs, resulting in a more secure project.

A Good Working Partnership

CLOUD NATIVE
COMPUTING FOUNDATION

ostif.org

This impactful work continues as a result of a good working relationship between CNCF and OSTIF.

CNCF continues to provide a strong platform for open source projects to grow and fund security audits for projects who wish to mature to graduated status.

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 Effort for 2022

50

Critical, High or Medium Severity
Findings Fixed

196

Total Security
Improvements Made

73

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

cloudevents envoy Falco cri-o TUF KubeEdge

containerd Istio cilium argo KEDA flux

Feedback From Projects

“ Thanks to the audit we were able to patch some minor vulnerabilities and increase our existing security toolchain to prevent new vulnerabilities from being introduced.”

Tom Kerkhove – KEDA Maintainer, Senior Software Engineer at Microsoft

“We greatly appreciate OSTIF and Trail of Bits for their thorough security audit of KEDA and for the excellent cooperation we received. The KEDA community is constantly striving to make the project better and more secure for our users, the insights provided in the audit will help us achieve that.”

Zbynek Roubalik – KEDA Maintainer, Principal Software Engineer at Red Hat

Associated & Future Work

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

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Google and OpenSSF Impact Report - Highlights a year of security engagements organized by OSTIF.

https://openssf.org/blog/2023/02/01/independent-security-audit-impact-report/

OSTIF is growing and helping more open source projects in 2023 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.

References

OSTIF Audits: https://github.com/ostif-org/OSTIF/blob/main/Completed-Engagements.md

Python TUF: https://ostif.org/our-audit-of-python-tuf-is-complete-multiple-issues-found-and-fixed/

Cloudevents: https://ostif.org/results-of-the-cloudevents-security-assessment/

Istio: https://ostif.org/the-audit-of-istio-is-complete/

Cilium: https://ostif.org/our-audit-of-cilium-is-complete/

KEDA: https://ostif.org/our-audit-of-kubernetes-event-driven-autoscaling-keda-is-complete/

Falco: ETA March 2023

Envoy pt.2: ETA March 2023