

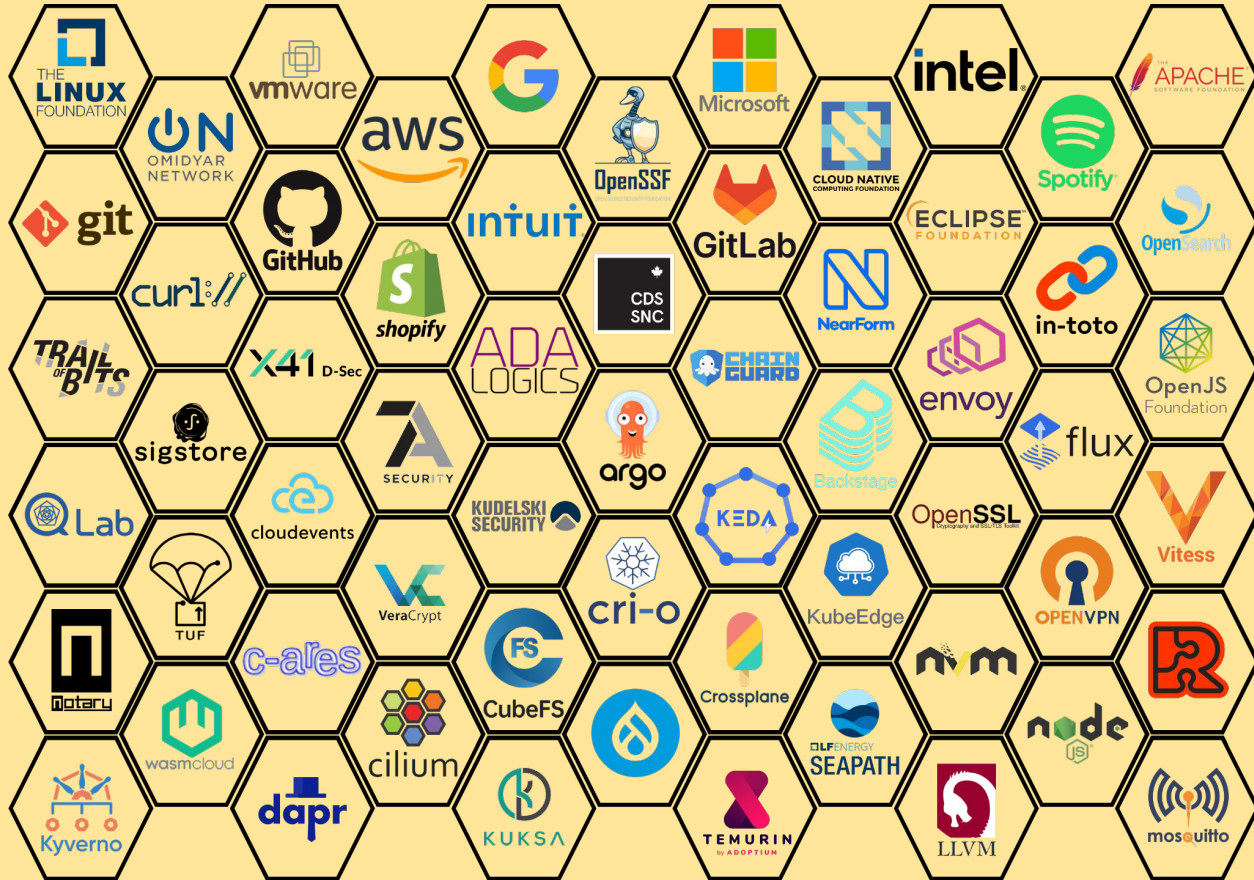


Independent Security Audit Impact Report

Thanks to Funding from Amazon Web Services (AWS)
and The Eclipse Foundation

Prepared by the **Open Source Technology Improvement Fund, Inc**
<https://ostif.org>

Open Source Technology Improvement Fund, Inc



“ Congratulations to OSTIF on the diligent work completing the list of 2023 security audits. Thoroughly reviewing the systems and processes of widely used open source projects is crucial for identifying risks and ensuring the creation of a secure and sustainable environment, primed for innovation.

I commend everyone involved for their commitment to building safer infrastructure through these essential audits, as the diligent work allows use to take appropriate steps to make these systems more secure for our customers.

”

David Nalley

**Director, Open Source Strategy and Marketing
Amazon Web Services**

Contents

A Note from OSTIF	1
The Value of Security Audits	2
2023: By the Numbers	3
Lessons Learned	4
Future Work	5
Feedback From Projects	6
Cost and Funding Breakdown	7
Conclusion and Call to Action	8
Thank You	9
References	10



Helen Woeste, Derek Zimmer, Amir Montazery

A Note from the OSTIF Team

Continuing to grow and directly help critical open source projects.

From September 2022 through November 2023, OSTIF collaborated with Amazon Web Services and Eclipse Foundation on a number of funded projects dedicated to improving security of critical open source projects.

This report provides a high level overview of the work done and some insight into the improvements made to critical projects in the open source ecosystem.

Full details of all the security work covered in this report can be found on the last page.

The Value of Security Audits

A security audit is a collaborative engagement in which independent experts examine a project's code, review tooling and practices, and work with project maintainers on findings and fixes to improve security posture holistically. Every open source project is different, so it is important to tailor the audit to project needs and scope the audit accordingly.



Immediate Benefits

- ❑ Security Exercise for Contributors/Maintainers
- ❑ Threat Modeling and Risk Assessment
- ❑ Finding and Fixing of Vulnerabilities
- ❑ Audit Report Documenting the Process

Long-term Benefits

- ❑ Closed classes of Bugs with Improved Tooling
- ❑ Hardened Supply Chain
- ❑ Threat Modeling and Audit Documentation as a Reference Guide

2023: By The Numbers

88

Vulnerabilities & CVEs Found and Fixed

19

Critical/High (CVSS >7.0) Findings Fixed

24

Tools built or improved to continually monitor Open Source Projects



Worked with teams and communities across three continents and ten countries.

\$2,400,000

Conservative Estimate of Cost Savings to Projects and Funders

10 Projects

jetty://

OpenSearch

c-ares



mosquitto



Equinox p2, libcap, simpleJSON, libjpegturbo



Lessons Learned

Security Audits and associated work directly help project's security posture.

There is a correlation between a supported, frequently reviewed and maintained project and a project with fewer security issues. When a project undergoes an audit, it receives detailed recommendations for future work as well as documentation and tooling that is invaluable for a second round of review. Examples are threat models, supply chain security tests, automated testing like fuzzers, and fix recommendations.

Proactive security work heavily benefits projects, and is cost effective.

Efficiencies are possible with increased funding. When multiple projects are financed from a single source, OSTIF is able to save on administrative work and time cost by bundling similar work engagements. Offering multiple relevant projects to a singular security firm can result in discounted person days or hourly rates and faster audit execution timelines.



Lessons Learned

Projects of all sizes, support levels, and maturity can benefit from Security Audits.

Projects at all points of their lifecycle are excellent candidates for a security audit. We have assisted projects ranging from 20+ year old projects, like [git](#) (audit completed January 2023) and cURL, to nascent projects earlier on in their lifecycle. Essentially, there are few to no examples of projects that would not benefit from customized security work.



Future Work

OSTIF audited more projects than any year prior in 2023. Our ability to scale up is directly dependent on funding and resources made available to us. We can do more, with more.

Feedback From Projects and Partners

“OSTIF streamlines the initiation of security audits by assisting us in defining the audit's scope relative to our budget and eliminating the challenging task of seeking appropriate partners.”

“Generally speaking, OSTIF as well as the maintainers of the library deserve a lot of praise for their overall support and assistance. It was a pleasure for the testing team working with them.”

Mikael Barbero
Head of Security, Eclipse Foundation

Security Audit Team
Manager

Cost and Funding Breakdown

The following table provides an overview of the cost breakdown for the security work funded by Amazon Web Services and Eclipse Foundation and executed by OSTIF. Figures are aggregated and rounded for simplicity.


Amazon Web Services - Security Audits - Annual Audit Program **\$500,000**

Eclipse Foundation - Security Audits - Security Audit Bundle **\$240,000**

Total \$740,000

Average Cost Per Engagement **\$74,000**

Average cost per bug fix/tool implementation **\$6,592**



Conclusion & Call to Action

A considerable amount of attention and funding has gone into open source security the last few years in the wake of numerous supply chain attacks in the ecosystem. OSTIF's proactive, people-first approach and refined process thanks to 8+ years of experience is one of the most effective ways to improve the security posture of critical open source projects. OSTIF urges all organizations who wish to really make a difference in improving security in open source to collaborate and fund security work and continue doing so, as evidenced by this report and the long track record of successful audits and security improvements.

Audits are a tried and true method for helping projects holistically with security needs. OSTIF has, to date, **impacted over 50 open source projects** and communities. OSTIF is capable of further scaling and production of audits, allowing for further reach and impact in open source security.

Thank you for your support of our mission!

Thank you to the following organizations for funding the security engagements covered in this report:



Further thanks to the teams that worked on these engagements with us:

[X41 D-Sec](#)

[Include Security](#)

[Trail of Bits](#)

Thank you to the following individuals for contributing to make these funded engagements a reality:

David
Nalley

Aaron
Leung

Mikael
Barbero

References

OSTIF Audits

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

simplejson <https://ostif.org/our-audit-of-simplejson-is-complete/>

libcap <https://ostif.org/our-audit-of-libcap-is-complete/>

c-ares <https://ostif.org/our-audit-of-c-ares-is-complete/>

libjpegturbo <https://ostif.org/our-audit-of-libjpeg-turbo-is-complete/>

Equinox p2 <https://ostif.org/2023-15/>

JKube <https://ostif.org/jkube-audit/>

OpenSearch <https://ostif.org/opensearch-audit/>

Jetty <https://ostif.org/ostif-has-completed-an-audit-of-jetty/>

Rustvmm <https://ostif.org/rustvmm-audit-complete/>

Mosquitto- <https://ostif.org/mosquitto-security-audit/>