Independent Security Audit Impact Report

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

Thanks to support from Google and OpenSSF

Improving Security Posture of Critical Open Source Projects

ostif.org

Open Source Technology Improvement Fund, Inc

Better Security Through A Massive Community

“

OSTIF helps ensure right focus on priorities by taking away the painstaking task of finding the right partners, project management responsibilities and ascertaining mutually agreeable modus operandi between parties involved.

”

Open Source Project Team Lead

Contents

A Note from the OSTIF Team

From an Idea to a Worldwide Coalition of Advocates & Security Experts

From September 2021 through November 2022, OSTIF collaborated with OpenSSF, Google and the Google Open Source Security Team (GOSST) 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 as a Reference Guide

The Impact of our Work

26

Vulnerabilities & CVEs Found and Fixed

11

Critical/High (CVSS >7.0) Findings Fixed

98

Total Security Improvements Made

20

Tools built or improved to continually monitor Open Source Projects

jackson-core

jackson-databind

4 of the projects audited were identified as critical in the Census II Report.

OSTIF Impact Spotlight: Git audit

- World's most widely-used version control system.
- Underpins not only open source, but the vast majority of public and private software development today.
- Reaches nearly every corner of software development and touches nearly every product that has software.

OSTIF put together a coalition of 7 security experts from 4 different organizations to work on multiple facets of git.

Initial Results:

A total of 35 issues were discovered, including **2 critical severity findings** and a **high severity finding**. Additionally, because of this research, a number of potentially catastrophic security bugs were discovered and resolved internally by the git security team.

Lessons Learned

Auditing an open source project requires a significant amount of coordination and engagement. Due to the nature of open source projects, facilitating and executing an audit requires a high amount of coordination. Contributor and maintainer communities can be varied. Some projects have a “solo maintainer” and some have hundreds if not thousands of contributors. For that reason, appropriate funding and resources need to be allocated to audits to account for the time and effort needed to coordinate resources.

Not all audit attempts will be fruitful. However, projects can be revisited if and when they’re ready. There can be a multitude of reasons why an effort doesn’t materialize. The common denominators are time, resources, and support. Project maintainers and contributors are busy people, they commit time and energy (often without getting paid) to keeping projects up to date to the best of their abilities. More funding for this type of work and support through policy and best practices is necessary in order to successfully audit more projects.

Lessons Learned

Engage the project contributor community directly. As a follow on to Lesson 1, it is absolutely critical to engage with project contributors and maintainers in order to learn about their needs and scope audits accordingly. Furthermore, and this is especially important when contributor communities are large, it shows good faith to approach a project as opposed to asking them to come to you. This can help navigate complexities and find appropriate project representatives when scoping audit work.

Future Work

OSTIF is auditing more projects than ever before in 2023. The curl audit was sponsored by OpenSSF, and we hope that OpenSSF and the greater open source community recognize the value of this work and continue to support it and fund more audits of critical projects.

Feedback From Projects

"We had wanted a security review for almost two years but didn't know where to start. Once OSTIF was brought on board, it happened in a couple of months. The team we worked with was professional, capable, and thorough. The whole process was a breeze, and I certainly would recommend it to any project looking for a similar audit."

Open Source Project Maintainer

"The maintainers and community are very grateful for the work put into this by everyone and the opportunity to grow and improve as a project."

Open Source Project Community Manager

Cost and Funding Breakdown

The following table provides an overview of the cost breakdown for the security work funded by Google and OpenSSF and executed by OSTIF. Figures are aggregated and rounded for simplicity.

GOSST: Security Audits - Annual Audit Program	**$400,000**
Google: Special Project - Triage, Bug Fixing, and Security Coverage Engagements	**$400,000**
Google/OpenSSF: Security Audits - Ad Hoc Project	**$75,000**
OpenSSF: Security Audits - Ad Hoc Project	**$60,000**
Total	**$935,000**

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 log4shell and 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.

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

https://openssf.org/

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

- ❏ Abhishek Arya
- ❏ Brian Behlendorf
- ❏ Bob Calloway
- ❏ Dave Tamasi
- ❏ David A. Wheeler
- ❏ Meder Kydyraliev
- ❏ Kim Lewandowski

References

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

Curl
https://ostif.org/the-ostif-audit-of-curl-with-trail-of-bits-is-complete/

Envoy - ETA Q1 2023

Git
https://ostif.org/the-audit-of-git-is-complete/

Jackson-core & Jackson-databind
https://ostif.org/our-audits-of-jackson-core-and-jackson-databind-are-complete/

Sigstore and slf4j Results
https://openssf.org/blog/2022/07/18/results-of-sigstore-and-slf4j-security-audits/