# 2023: Year in Review

A Summary and Discussion of the 2023 Fiscal Year
by an Open Source Security Firm

Prepared by the **Open Source Technology Improvement Fund** https://ostif.org

# Open Source Technology Improvement Fund,Inc

# A Leader in Improving Security Posture for Open Source Projects

Open Source Technology Improvement Fund, Inc (OSTIF) is the nonprofit behind thousands of security improvements to critical projects in the open source ecosystem, over 12,000 hours of organized security work, and the finding of 100 Critical/High vulnerabilities in open source projects.

Since 2015, OSTIF has been building a diverse and deep network of partners and iterating on a repeatable process to effectively improve security posture of projects. Our web of community expands across the globe with a variety of organizations big and small, projects of all implications, and people with diverse security skills.

In 2023, OSTIF scaled up, completing almost 187% more audits than 2022. This report covers our work carried out in the last year.

# Contents



Derek Zimmer

Helen Woeste


Amir Montazery

# A Milestone Year For Independent Security Audits

## Our 2023 Annual Report

Thank you for your time reviewing OSTIF's second annual report. In 2023, OSTIF grew its partner network and collaborated on a record number of projects.

***Our top accomplishments were (1) building on partnerships with Amazon Web Services, Google, Cloud Native Computing Foundation, Eclipse Foundation, and Open Source Security Foundation, (2) improving security posture for critical infrastructure as a result of those partnerships, and (3) continuing to grow and nurture with new communities.***

This report will provide some background on OSTIF, highlight the improvements made to critical projects in the open source ecosystem, and close with a closer look at our accomplishments, financials, and funders.

“

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

# How We Got Here

Open Source Technology Improvement Fund, Inc (OSTIF) launched in 2015 as a corporate non-profit organization with a simple mission: improve the security of Critical Open Source Projects EVERYONE depends on. The goal -- to address the problem of limited resources with regards to security in open source projects. Furthermore, there was a lack of a transparent, systemic process on how to help open source projects in an effective and repeatable way.

## Humble Beginnings

OSTIF built a network of trusted open source security researchers, audit firms, advocates, and project communities from the ground up and honed in on a method to systematically review and audit projects.

This work has culminated in nearly 12,000 hours of expert security work and the finding and remediation of hundreds of critical and high severity security vulnerabilities.

## Amazing Progress

Beginning in 2020, OSTIF started a strategic partnership with Linux Foundation and attended multiple open source conferences around the world. After joining Open Source Security Foundation and having executed on a number of collaborations, OSTIF partnered with Google to scale up and complete more security audits.

Completing more in 2023 than every year before combined, OSTIF has developed an international network based on trust and plans to continue growing into a premier partner and leader in open source security and organizing security engagements.

# OSTIF in 2023: By the Numbers

**118**

Critical, High, and Medium (CVSS >4.0) Severity Findings (100% fixed)

**276**

Total Security Findings (98% fixed)

**35**

Fuzzers built for open source projects (ossfuzz)

**45**

Security Audits Complete or In Progress

(+187% from 2022)

**$1.75 Million** Dollars Raised for Security Audits

## Actualizing Security-How We Do What We Do

OSTIF functions at a high level of productivity, output, and generates actual security work. We turn money into security impact through:

- Varied and Extensive Professional Relationships
- Scoping and Scaling our Audits Accurately
- Emphasis on Communication
- Investment in Open Source Security Testing

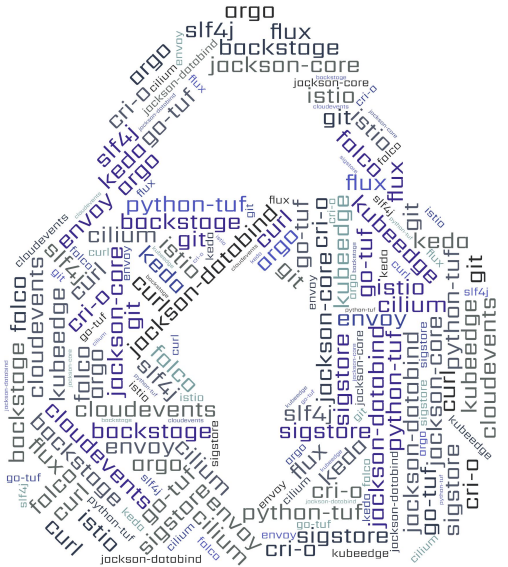
**Finding a vulnerability in an OSTIF audit will cost you a few thousand dollars. A threat actor finding it before us? That cost is immeasurable and varied.**

**Our contractors care about open source projects and their health- and their work to help resolve fixes shows it.**

**OSTIF has a proven process for directing security engagements that promotes open communication, customized scope and objectives, prioritizes project needs, and allows for fixes to be done privately, with further aid given if needed.**

# Impact Spotlight: 50th Audit Milestone

- ❏ OSTIF has completed and published 50 security audits.
- ❏ This work includes 100 Critical/High Vulnerabilities identified and fixed through the auditing process.
- ❏ 91 new fuzzers were created and then donated to projects for continuous security hardening, as well as the improvement of over 50 existing fuzzers.
- ❏ Facilitated and Managed over 12,000 hours of security work.




**Just in 2023, OSTIF worked on over 34 projects, with 8 separate security firms, impacting millions of users worldwide**

**What this means for the future of OSTIF and open source security:**

**OSTIF has the capabilities to scale up and manage even more audits simultaneously, while still maintaining quality of work. We look forward to running secondary and tertiary audits of projects proving that consistent oversight and audits of projects leads to more secure projects over time.**

# Cultivating Partnerships

In organizing and managing audits for the Cloud Native Computing Foundation and the funded work by OpenSSF and Amazon Web Services, OSTIF has garnered support in the Open Source and Tech communities.

Link to all of OSTIF's audit reports

Link to all of OSTIF's blog posts

In 2023, 15 CNCF Projects that were looking to mature and improve security did so with OSTIF's help.

CLOUD NATIVE COMPUTING FOUNDATION

aws

ECLIPSE FOUNDATION

Amazon Web Services and Eclipse Foundation, in an effort to secure critical open source projects, funded a number of security audits and associated engagements with OSTIF.

# Growing Our Network

Working with new organizations and across verticals, OSTIF looks towards growth and helping more projects.

**Amazon Web Services**, as part of a greater commitment to supporting security initiatives in open source, supported OSTIF for 10 projects in 2023.

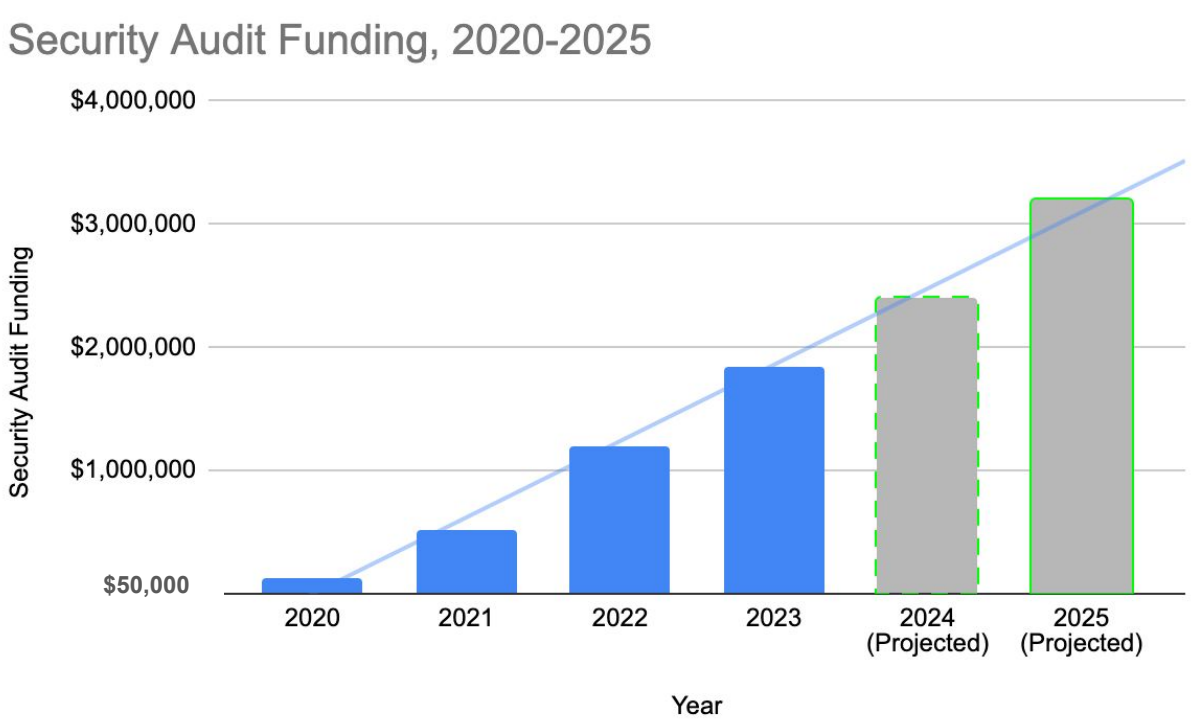
aws


**OpenSSF**, In particular project Alpha, funded OSTIF to facilitate and manage a security audit of a critical component in the open source ecosystem.

**OpenJS Foundation**, following support from the Sovereign Tech Fund, partnered with OSTIF to organize engagements for Impact and At-Large projects.

# Fundraising

- **Almost 20x growth from 2020 to 2023.**
- **Approximately 1.8 Million USD in funding raised for security audits in 2023.**
- **187% increase in audits between 2022-2023.**



# OSTIF's Value*

35 Critical/High Findings (CVSS > 7.0) from a total 2023 budget of $1.75 million = **~$5K per Critical/High Vulnerability Found and Fixed**

**Cost of Vulnerabilities/Breached Data**

**log4shell**- estimated cost of $90,000 per organization affected.

**Heartbleed**- estimates between $10s of millions-$100s of millions.

**Solarwinds**- exceeds $100 million which includes legal costs and damage to company's market value.

**Equifax**- approx. $1.7 billion, including legal costs, regulatory fines, and improved cybersecurity.

**At minimum- we save organizations tens of thousands of dollars. The maximum- incalculable.**

***See last slide for references found in this slide.**

# Funding Support

Premier Supporters Amazon Web Services and Linux Foundation supported OSTIF by funding security audits for open source projects.

Platinum Supporter Eclipse Foundation supported OSTIF by funding security audits for projects under the EF umbrella, along with OpenSSF's funding of the OpenSSL security audit.

Gold Supporters Google and OpenJS Foundation supported OSTIF by funding security audit engagements to open source projects.

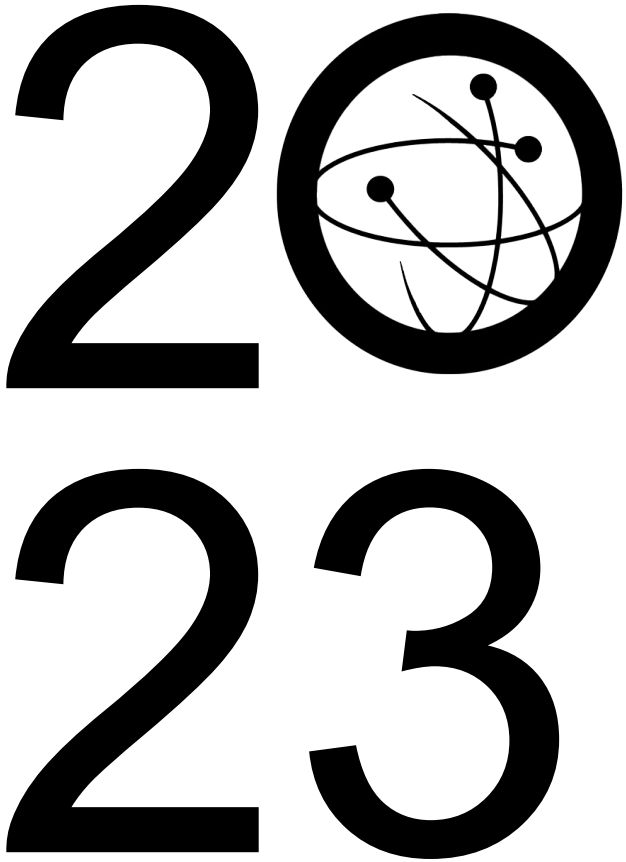
Silver Supporter DuckDuckGo supported OSTIF by providing funding to help with overhead costs and operations.

**Premier Supporters (>$400k)**

**Platinum Supporters (>$100k)**

**Gold Supporters ($50k)**

**Silver Supporters ($25k)**




# SUPPORT OUR WORK

Thank you to everyone who supported and helped OSTIF grow. We are extremely grateful to have such a diverse, generous, and passionate team of contributors- from individual oss project communities, top open-source researchers, to executives at the world's largest technology companies and foundations.

Our mission is more critical than ever, with larger-reaching and more devastating digital attacks happening every year. Help protect and secure open source with us through a donation or financing of an engagement.

*Thanks for your support!*

*Derek Amir Helen*

To learn more about OSTIF, check out https://www.ostif.org or contact amir@ostif.org

# References


OSTIF's Value

Solarwinds-"Cleaning up the SolarWinds hack may cost as much as 100 billion" Gopal Ratnam, 2021

https://rollcall.com/2021/01/11/cleaning-up-solarwinds-hack-may-cost-as-much-as-100-billion/

Heartbleed-"Heartbleed SSL Flaw's True Cost Will Take Time to Tally" Sean Michael Kerner, 2014

https://www.eweek.com/security/heartbleed-ssl-flaw-s-true-cost-will-take-time-to-tally/

Equifax-"Equifax expects to pay out another $100 million for data breach" Ben Lane, 2020

https://www.housingwire.com/articles/equifax-expects-to-pay-out-another-100-million-for-data-breach/#:~:text=Overall%2C%20the%20breach%20cost%20Equifax,million%20on%20that%20insurance%20policy.

Log4shell-"4 Lessons Learned from Log4shell" SOCRadar Research, 2023

https://socradar.io/4-lessons-learned-from-log4shell/#:~:text=According%20to%20research%2C%20the%20average,Alphv%2FBlackCat%20(12%25).