2022: Year in Review

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

Open Source Technology Improvement Fund, Inc

Improving Security Through A Massive Community

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.

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.

In 2022, OSTIF scaled significantly. This report covers our work carried out in the last year.

“

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 Milestone Year For Independent Security Audits

Our Work & First Annual Report

Thank you for your time reviewing OSTIF's first annual report. In 2022, OSTIF grew its partner network and collaborated on a record number of projects.

Our top accomplishments were (1) building on partnerships with top open-source organizations Google, Cloud Native Computing 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.

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 10,000 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 exponentially more security audits.

Completing more in 2022 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 2022: By the Numbers

34

Critical/High (CVSS >7.0) Severity Findings (100% fixed)

220

Total Security Findings (98% fixed)

80

Fuzzers built for open source projects (ossfuzz)

24

Security Audits Complete or In Progress

$1.2 Million Dollars Raised for Security Audits

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.

Cultivating Partnerships

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

CNCF Projects that are looking to mature and improve security do so with OSTIF's help.

https://www.cncf.io/blog/2023/03/13/an-overview-of-the-cncf-and-ostif-impact-report-for-the-second-half-of-2022-and-early-2023/

CLOUD NATIVE COMPUTING FOUNDATION

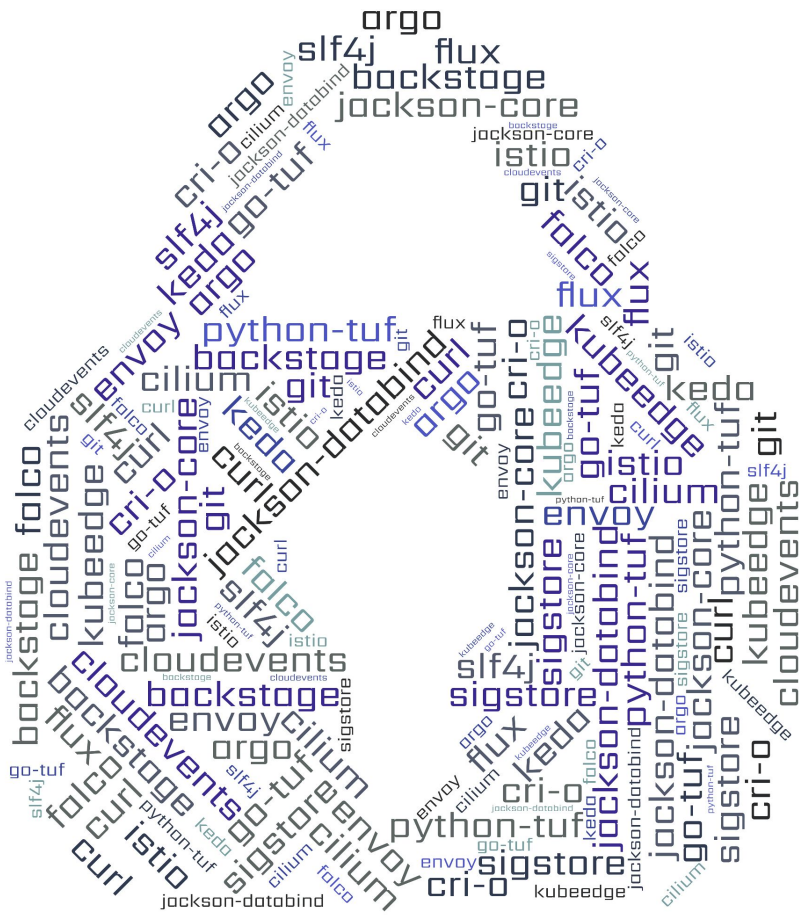
Google and OpenSSF, in an effort to secure critical open source projects, funded a number of security audits and associated engagements with OSTIF

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

Securing Critical Projects

OSTIF's leadership led to significant security improvements on numerous widely adopted and critical open source projects.

Link to all of OSTIF's work: https://github.com/ostif-org/OSTIF/blob/main/Completed-Engagements.md



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 2023.

Omidyar Network, as part of a number of commitments to open source initiatives, supported OSTIF in 2022. This is OSTIF's first support from a technology philanthropy.

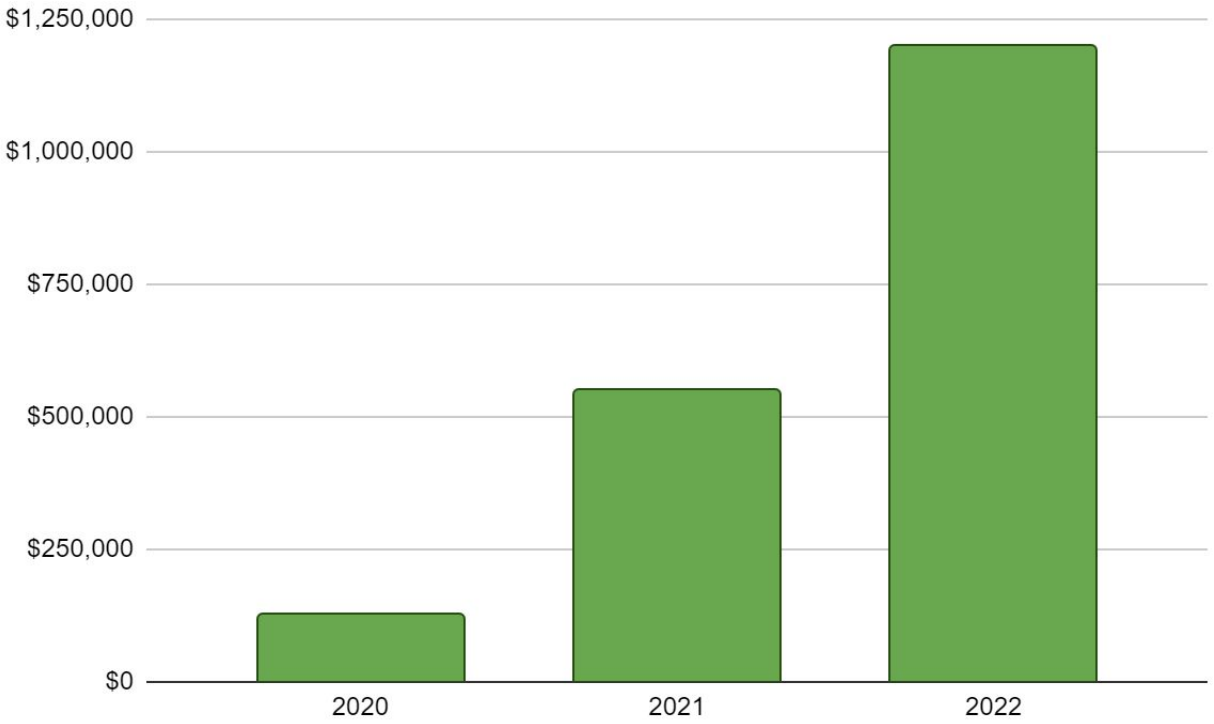
Eclipse Foundation, following support from OpenSSF Project Alpha-Omega, worked with OSTIF to organize engagements for EF projects.

A Closer Look

A closer look at funding raised by OSTIF in 2022.

10x growth since 2020

Increase of 800% in projects completed per year



Funding Support

Premier Supporters Amazon Web Services, Linux Foundation & Google 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.

Gold Supporter Omidyar Network supported OSTIF by providing funding to improve operations, branding, and help support key staff.

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)

2022

SUPPORT OUR WORK

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

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