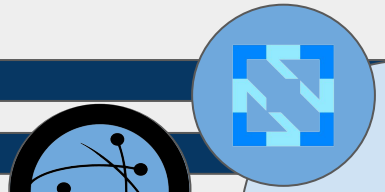


OSTIF

Open Source Technology Improvement Fund

CNCF Managed Audit Program Report 2025

Improving Security Posture of Critical Open Source Projects

ostif.org

Contents

A NOTE FROM OUR DIRECTORS

It's hard to believe that 10 years ago, we started OSTIF with the intention of championing security efforts for critical open source projects.

Now we're making a meaningful impact on the ecosystem, driven by an international and expansive network of advocates, researchers, and maintainer communities.

We can't thank everyone enough who has supported OSTIF: whether collaborating directly on projects, advocating for and funding our work, or participating in meetups and providing feedback.

We hope that in the next 10 years, OSTIF can grow into a sustained organization and be seen as a key partner in improving the ecosystem.

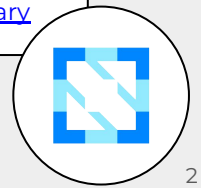
Derek Zimmer, Executive Director

Amir Montazery, Managing Director

As CNCF and OSTIF both celebrate 10 years, it's a powerful moment to reflect on how far open source has come and how essential it's become to the digital world. Open source is the foundation for everything from cloud infrastructure to AI, but that foundation must be secure to scale with confidence. That's where our partnership with OSTIF comes in. Their work strengthens the security behind the code, helping projects and communities thrive. Looking ahead, we're excited to see how OSTIF continues to ensure that as open source grows, it remains safe and secure for everyone.

Chris Aniszczyk
CNCF CTO

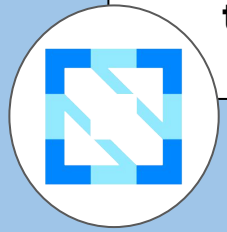
Quote for OSTIF's 10th Anniversary



CNCF Security Audit Program: Building Trust for Graduation

Essential Due Diligence for Cloud Native Project Maturity

- **Goal:** To strengthen **project security**, offer recommendations for **hardening**, and foster **trust** in the community's commitment to security.
- **Partnership:** Audits are conducted through a collaboration with OSTIF as part of the CNCF's significant security investment (**over $3 million**).
- **Impact:** Audits have identified and helped fix over **40 critical, high, and medium severity findings** across 12 projects (2024 & 2025), directly improving the open source security supply chain.
- **Graduation Implication:** Successful audit completion and remediation are crucial for projects to demonstrate the **robust security and trustworthiness** required to reach the **Graduated** maturity stage.



2025 By the Numbers

112

Findings with Security Impact

- 13 Crit/High (100% fixed)
- 25 Medium (100% fixed)
- 74 Low/Informational (95% fixed)

13

CVEs Found & Fixed

8

Security Audits Published

13

Audits Completed or In Process

$500,000+

invested in CNCF project security

CNCF Audit Highlights

linkerd

Scope: Main project repository and proxy APIs

Results:

- 6 Findings with Security Impact
  - 1 High, 6 Hardening Recommendations
- Recommendations for future work

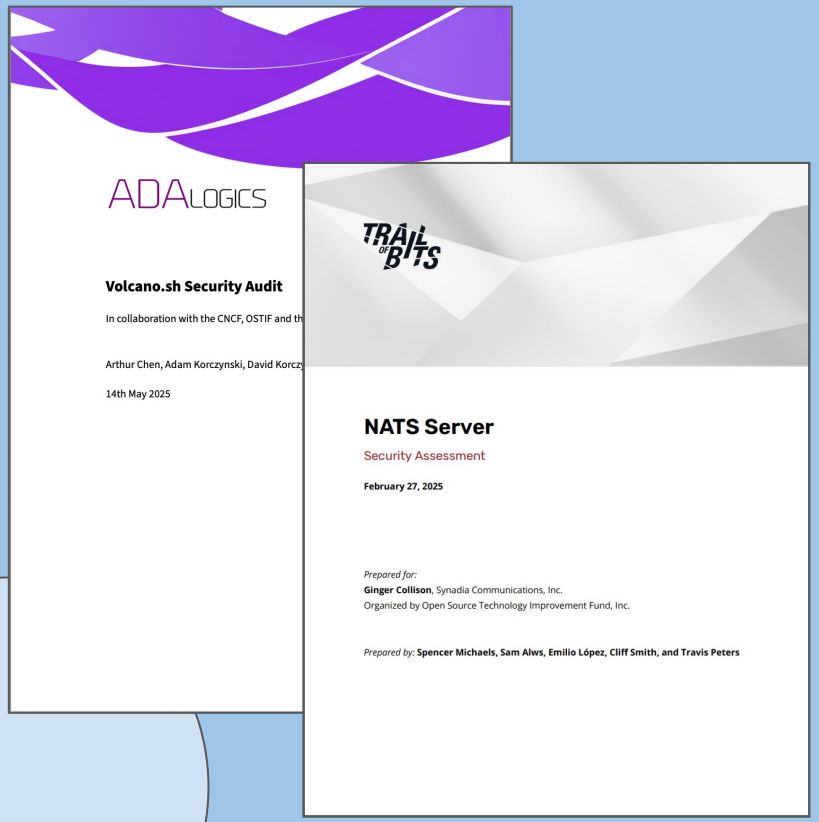
Karmada

Scope: Custom project implementations and third party dependencies

Results:

- 6 Findings with security impact
  - 1 High, 1 Medium, 2 Low, 2 Informational
- Recommendations for future work

CNCF Audit Highlights



Volcano

Scope: Main branch

Results:

- 10 Findings with security impact
  - 1 High, 5 Medium, 4 Low or Informational
- Threat Model
- Integrated onto OSS-Fuzz

NATS.io

Scope: Main branch

Results:

- 10 Findings with security impact
  - 3 Medium, 1 Low, 6 Informational
- Threat Model
- Recommendations for future work

CNCF Audit Highlights

Notary

Scope: two new cryptographic features
Results:

- 11 Findings with security impact
  - 1 Medium, 1 Low, 9 Informational
- Recommendations for future work
- Custom documentation

Backstage

*Published December 2024
Scope: Main branch
Results:

- 11 Findings with security impact
  - 3 High, 1 Medium, 7 Informational
- Recommendations for future work
- Custom documentation

CNCF Audit Highlights

Istio

Scope: ztunnel implementation

Results:

- 3 Findings with Security Impact
  - 1 Medium, 2 Informational
- CI/CD review and recommendations

KubeVirt

Scope: Main branch

Results:

- 15 Findings with Security Impact
  - 1 High, 7 medium, 4 Low, 3 Informational
- Threat Model
- Fix recommendations

Managed Audit Program Class of 2025

Kubernetes

Releasing 2026

Auditors: Shielder

Scope: Popular non-core components

Amir keynoting at kubecon na Atlanta, GA, Nov. 2025

48% of all CNCF projects have been audited by OSTIF

13 Incubating CNCF projects who received OSTIF audits

20 Graduated CNCF projects who received OSTIF audits

2021-2025

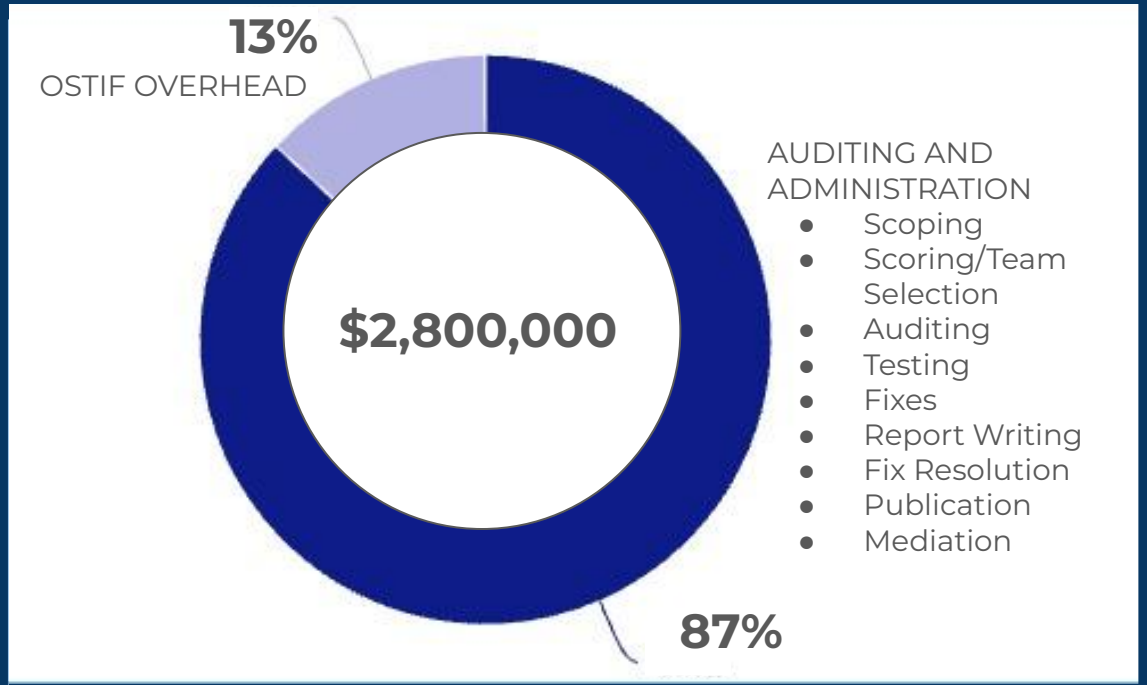
131 Critical & High Issues Discovered and Fixed

404 Medium, Low, & Informational Issues Reported

to date

Managed Audit Program Stats

OSTIF 2025 Funding Summary



2025 General Audit Program Funding Ratio

OSTIF leverages industry knowledge, experience, and relationships to source world class security teams for competitive prices on behalf of open source.

OSTIF saves all parties involved labor, time, and money by utilising custom scoping, cost-splitting, follow-on work, and open source tooling.

Where OSTIF shines

Cost + quality controls

Access to our network of security expertise

Custom scoping and administration

High standard of transparency

OSTIF

CELEBRATING 10 YEARS!

We are a small team of friends from Chicago, Illinois, working together to preserve and protect global digital infrastructure in open source.

Are you interested in contributing to OSTIF's mission? Email us at contactus@ostif.org.

Previous OSTIF-CNCF Annual Reports: 2024, 2023, 2022