Sovereign Tech Agency and OSTIF

Report on Open Source Security Audits 2024-2025

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

Code reviews and security audits are among the most effective tools for securing our critical digital infrastructure components and form a key pillar of the Sovereign Tech Resilience program.

We greatly appreciate OSTIF's approach to security audits, which not only helps these critical components identify and address the most pressing threats but also equips them with tools and practices to enhance their long-term security posture.

Tara Tarakiyee
Technologist
Sovereign Tech Agency

The Sovereign Tech Agency is the first public organization in Europe tasked with strengthening critical digital infrastructure. It identifies and invests in foundational open source software components and supports open technologies with broad societal importance. As part of this mission, the agency has established several initiatives, including the Sovereign Tech Resilience Program, which takes a holistic approach to protect critical digital infrastructure by preventing code vulnerabilities.

Security By the Numbers

66

Findings with Security Impact

- 6 Crit/High (100% fixed)
- 21 Medium (100% fixed)
- 39 Low/Informational (95% fixed)

6

Projects underwent fuzzing improvement

8

CVES Found and Fixed

9

Security Audits Published

$642,000

invested in open source security

Sovereign Tech Agency Audit Highlights

conda-forge

Scope: Mac, Windows, and Linux distributions in addition to the core code infrastructure

Results:

- 7 Vulnerabilities
  - 1 Critical, 2 High, 3 Medium, 1 Low, 6 Hardening Recommendations
- Custom Threat Model
- Supply Chain Security Analysis

Click on the report cover page to access each audit report

GNU libmicrohttpd2

curl://

Jackson subprojects

[LOGBACK]

CONDA-FORGE

nghttp3, ngtcp2

log4cxx, log4net

RAILS

Sovereign Tech Agency Audit Highlights

cURL

Scope: HTTP/3 components

Results:

- 2 Informational findings related to code configuration
- Improved existing fuzz tests
- Wrote and contributed additional fuzz tests to increase fuzzing coverage
- Explicit fuzzing and consequential security recommendations

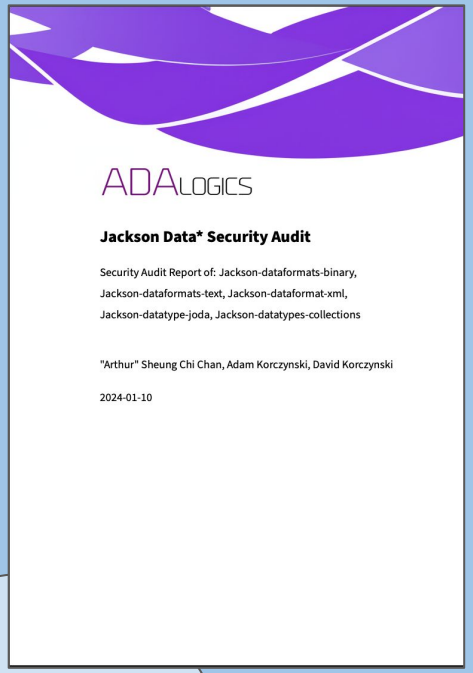
nghttp2, ngtcp2

Scope: Main branches, security related to QUIC

Results:

- 3 Informational findings
- AFL++ fuzz harnesses for four functions
- Recommendations for further testing

Sovereign Tech Agency Audit Highlights



ADALOGICS

Jackson Data* Security Audit

Security Audit Report of: Jackson-dataformats-binary, Jackson-dataformats-text, Jackson-dataformat-xml, Jackson-datatype-joda, Jackson-datatypes-collections

"Arthur" Sheung Chi Chan, Adam Korczynski, David Korczynski

2024-01-10

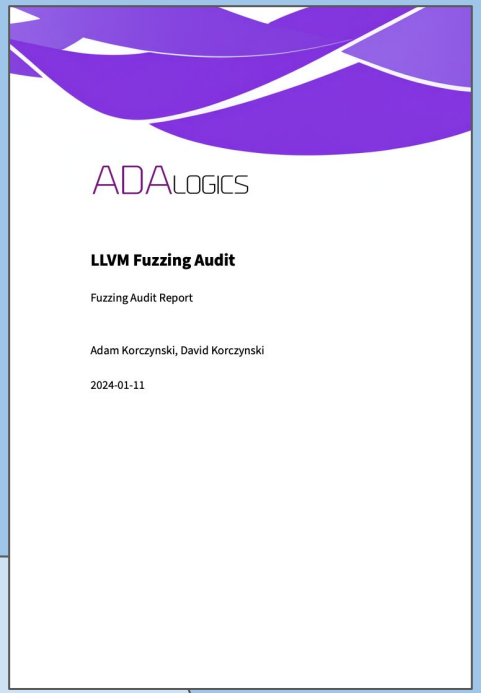
Jackson subprojects

Scope: jackson-dataformats-binary, jackson-dataformats-text, jackson-dataformat-xml, jackson-datatype-joda, and jackson-datatypes-collections

Results:

- Developed threat models for each of the five modules
- Added 1 new OSS-Fuzz project and extended 4 existing OSS-Fuzz Projects
- Created 26 new fuzzers for the Jackson projects
- Performed manual auditing of each of the codebases
- Found and reported 19 issues in Jackson projects
    - 4 of moderate security severity
- Submitted patches for 14 of the issues found

Sovereign Tech Agency Audit Highlights



LLVM

Scope: LLVM's fuzzing suite

Results:

- Performed LLVM OSS-Fuzz Setup, Analysis and Repair to get OSS-Fuzz working again
- Fixed Security-Flagged Issues Reported by OSS-Fuzz
- Expanded Fuzzing Coverage by:
  - Expanding on existing fuzzers to cover additional code
  - Developing new fuzzers that target unexplored code
  - Fixing issues/fuzz blockers that break fuzzers
- Identified Areas for Improvement and Future Work
- Expanded fuzzing coverage from 1.1 million to 2.4 million lines of code
- Extended existing fuzzing suite on OSS-Fuzz and developed three new fuzzers, increasing the fuzzers on OSS-Fuzz by 15
- Fixed 11 Security-Flagged Issues reported by OSS-Fuzz
  - 8 were Memory Corruption Vulnerabilities
- Developed strategy for the next steps of fuzzing LLVM, with a focus on improving fuzzing efficiency

Sovereign Tech Agency Audit Highlights

GNU libmicrohttpd2

Scope: Main branch

Results:

- 5 Findings with Security Impact
  - 1 High, 1 Medium, 3 Low, 2 Informational Findings
- Fuzz Testing Suite
  - 9 custom fuzzers integrated
  - OSS-Fuzz integration
  - 35% code coverage reached
- Recommendations for Future Work

Logback

Scope: Main branch

Results:

- 5 Findings with Security Impact
  - 1 Critical, 1 Medium, 1 Low, 2 Informational
  - Custom Threat Model
  - Supply-chain Levels for Software Artifacts Analysis

Sovereign Tech Agency Audit Highlights

Apache log4cxx, log4net

Scope: Main branch of both projects

Results:

- 8 Findings with Security Impact
  - 4 Medium, 4 Low
- Custom Threat Model
- Log4CXX integrated onto OSS-Fuzz

Ruby on Rails

Scope: Main branch

Results:

- 7 Findings with Security Impact
  - 1 High, 6 Low
- Custom Threat Model

Impact of Auditing

PRESENTING ON OSTIF AUDITS SOVEREIGN TECH AGENCY BUG BOUNTY PANEL, 2024

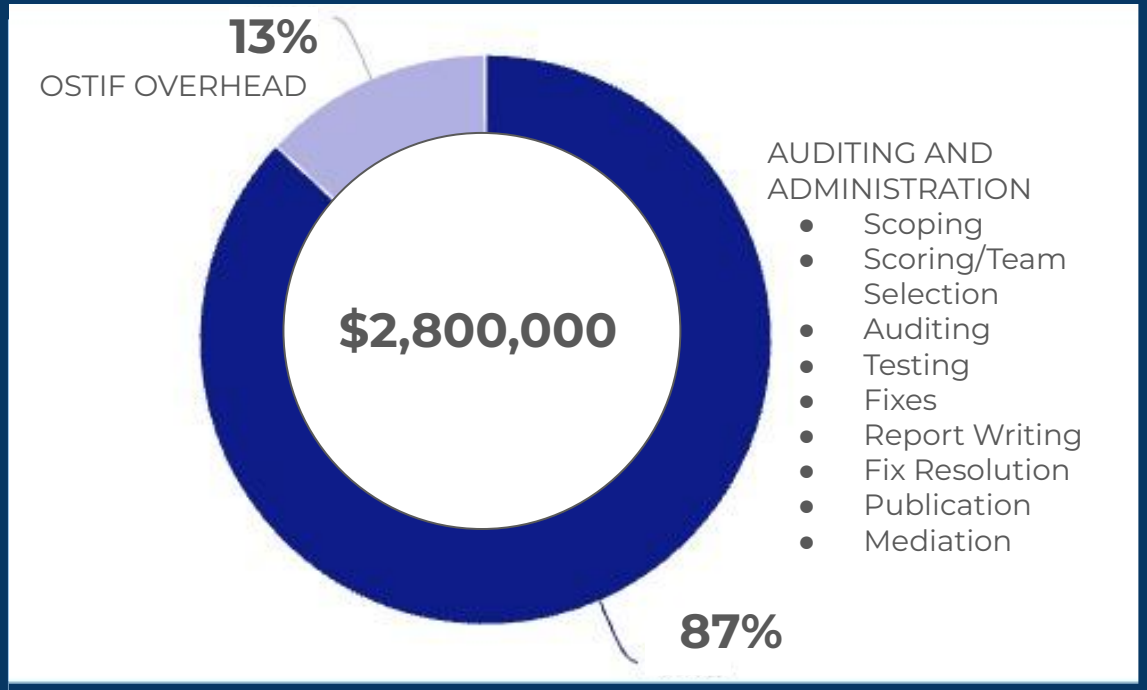
IMMEDIATE

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

LONG-TERM

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

OSTIF 2025 Funding Summary



OSTIF 2025 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 Sovereign Tech Agency Annual Report: 2024