2024 Sovereign Tech Agency Security Audit Impact Report

OSTIF

Sovereign Tech Agency

Prepared by the Open Source Technology Improvement Fund

https://ostif.org

www.sovereign.tech

Improving Security Posture of Critical Open Source Projects

ostif.org

Contents

A Note from the OSTIF Team

Our goal: continuing to grow and directly help critical open source projects.

L-R: Helen Woeste, Amir Montazery, Derek Zimmer (FOSDEM 2024)

Working with the Sovereign Tech Agency is a dream come true for OSTIF. As we enter our 10th year working to provide and promote open source security audits, a partnership with a government agency dedicated to underpinning the digital infrastructure of our world is a match of ideals with funding.

We would like to call out the maintainers and audit teams who worked with us to create real security impact for their projects. These efforts would not have been possible or as impactful without their enthusiastic involvement.

Thank you to the Sovereign Tech Agency team for supporting our mission and the opportunities for collaboration. We look forward to future engagements together improving open source security.

The Value of Security Audits

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 and Audit Documentation as a Reference Guide

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.

For those reasons and many more, the Sovereign Tech Agency incorporated security audits into their Sovereign Tech Resilience Program and partnered with OSTIF to direct and manage those engagements. View the links above to read more about the program and its impact on our digital infrastructure.

2024: By The Numbers

50	100+	1,865
Security Issues Found and Fixed	Security Tools Built or Improved	Hours of review and audit work by security experts

These engagements brought together audit teams and maintainers spanned across 10+ countries.

7 Projects:

cURL, Jackson subprojects, Node.js, Express, Fastify, LLVM, and nvm

Financials for the 7 Projects Funded by Sovereign Tech Agency

Sovereign Tech Resilience Program funding	**$322,000**USD
Funding via OpenJS Foundation	**$150,000**USD

Total Funding: **$472,000**USD

Average cost per fixed finding/tool implemented*: $3,000USD

Average cost of exploited vulnerability: $4,880,000USD **(IBM Cost of Data Breach Report 2024**)

*(total cost/total findings+tools)

Lessons Learned

Maintainer buy-in and participation is essential for a successful security audit.

Establishing expectations, setting communication channels, and aligning schedules are all practices that can help improve maintainer participation.

Research is needed on audits and supply-chain security.

Differences on opinion around supply-chain security caused disputes around audit results. More information is needed about the importance and best practices of supply-chain security in order to create a baseline of expectations for projects to follow. Similarly, research about the long-term impact of audits would be helpful in understanding the investment payoff for maintainers and funders in participating and sourcing security audits.

Lessons Learned, cont.

Projects of all sizes, support levels, and maturity can benefit from Security Audits.

Projects at all points of their lifecycle are excellent candidates for a security audit. We have assisted projects ranging from 20+ year old projects, like git (audit completed January 2023) and cURL, to nascent projects earlier on in their lifecycle. Essentially, **there are few to no examples of projects that would not benefit from customized security work.**

Future Work

OSTIF will be undertaking another 7 audits for the Sovereign Tech Agency before the end of 2024. These audits will help a variety of projects with their security, and includes a project that will be a second collaboration between Gitlab and OSTIF.

Partner Feedback

> “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

Conclusion & Call to Action

There is no end point to cybersecurity.

Every completed audit or engagement is another step towards moving goalposts. That might sound like what we do is aimless in the face of thousands of vulnerabilities and hackers working against us, but in fact it is the opposite. Without efforts to harden the security of our digital world, we place the data and livelihood of the globe at risk. Every effort and each dollar towards cybersecurity helps to close the gap between where we are now and where we can be with regards to digital security.

Join us, the Sovereign Tech Agency, and many others in working towards a future where open source is not only the cheapest software but the most secure one. Fund open source security work through OSTIF to help strengthen our current and future digital world.

Panel: Public Sector's Role in Public Bug Bounty Programs
Dr. Ryan Ellis, Associate Professor, Northeastern University
Amir Montazery, Managing Director, OSTIF
Yona Raekow, Section Head IT Systems, BSI
Dr. Aïmad Berady, VP Product, YesWeHack
Moderated by:
Tara Tarakiyee
Technologist, Sovereign Tech Fund

Amir Montazery, Managing Director of OSTIF (second from left) participating in a panel discussion hosted by the Sovereign Tech Agency in Berlin, September 2024, with panel moderation by Tara Tarakiyee.

Thank you for your support of our mission!

A special thank you to all the maintainers who worked with us on these engagements:

Chris de Almeida, Jon Church, Matteo Collina, Michael Dawson, Ulises Gascón, Daniel Stenberg, Tatu Saloranta, Wes Todd, and many more.

Further thanks to the teams that worked on these engagements with us:

Ada Logics
Trail of Bits

Thank you to the following organizations for contributing to make these security audits a reality:

Sovereign Tech Agency

OpenJS Foundation

References

OSTIF Audits : https://github.com/ostif-org/OSTIF/blob/main/Completed-Engagements.md
Sovereign Tech Agency: sovereign.tech
OpenJS Foundation: openjsf.org

IBM Report: https://www.ibm.com/reports/data-breach

Jackson: https://ostif.org/dataformatsdatatypes-audit-complete/
LLVM: https://ostif.org/llvm-audit-complete/
cURL: https://ostif.org/curl-audit-complete/
Fastify: https://ostif.org/fastify-audit-complete/
Node.js: https://ostif.org/node-js-fuzzing-audit-complete/
Express.js: https://ostif.org/express-audit-complete/