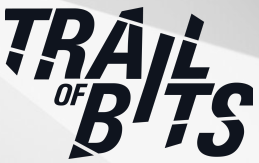

RegisterAndSetArbCustomGateway Governance Action

Security Assessment (Summary Report)

September 26, 2024

Prepared for:
Offchain Labs

Prepared by: **Gustavo Grieco, Priyanka Bose, and Michael Colburn**

About Trail of Bits

Founded in 2012 and headquartered in New York, Trail of Bits provides technical security assessment and advisory services to some of the world's most targeted organizations. We combine high-end security research with a real-world attacker mentality to reduce risk and fortify code. With 100+ employees around the globe, we've helped secure critical software elements that support billions of end users, including Kubernetes and the Linux kernel.

We maintain an exhaustive list of publications at https://github.com/trailofbits/publications, with links to papers, presentations, public audit reports, and podcast appearances.

In recent years, Trail of Bits consultants have showcased cutting-edge research through presentations at CanSecWest, HCSS, Devcon, Empire Hacking, GrrCon, LangSec, NorthSec, the O'Reilly Security Conference, PyCon, REcon, Security BSides, and SummerCon.

We specialize in software testing and code review projects, supporting client organizations in the technology, defense, and finance industries, as well as government entities. Notable clients include HashiCorp, Google, Microsoft, Western Digital, and Zoom.

Trail of Bits also operates a center of excellence with regard to blockchain security. Notable projects include audits of Algorand, Bitcoin SV, Chainlink, Compound, Ethereum 2.0, MakerDAO, Matic, Uniswap, Web3, and Zcash.

To keep up to date with our latest news and announcements, please follow @trailofbits on Twitter and explore our public repositories at https://github.com/trailofbits. To engage us directly, visit our "Contact" page at https://www.trailofbits.com/contact, or email us at info@trailofbits.com.

Trail of Bits, Inc.
497 Carroll St., Space 71, Seventh Floor
Brooklyn, NY 11215
https://www.trailofbits.com
info@trailofbits.com

Notices and Remarks

Copyright and Distribution

Test Coverage Disclaimer

All activities undertaken by Trail of Bits in association with this project were performed in accordance with a statement of work and agreed upon project plan.

Security assessment projects are time-boxed and often reliant on information that may be provided by a client, its affiliates, or its partners. As a result, the findings documented in this report should not be considered a comprehensive list of security issues, flaws, or defects in the target system or codebase.

Trail of Bits uses automated testing techniques to rapidly test the controls and security properties of software. These techniques augment our manual security review work, but each has its limitations: for example, a tool may not generate a random edge case that violates a property or may not fully complete its analysis during the allotted time. Their use is also limited by the time and resource constraints of a project.

Table of Contents

About Trail of Bits 1
Notices and Remarks 2
Table of Contents 3
Project Summary 4
Project Targets 5
Executive Summary 6

Project Summary

Contact Information

The following project manager was associated with this project:

Mary O'Brien, Project Manager
mary.obrien@trailofbits.com

The following engineering director was associated with this project:

Josselin Feist, Engineering Director, Blockchain
josselin.feist@trailofbits.com

The following consultants were associated with this project:

Gustavo Grieco, Consultant
gustavo.grieco@trailofbits.com

Priyanka Bose, Consultant
priyanka.bose@trailofbits.com

Michael Colburn, Consultant
michael.colburn@trailofbits.com

Project Timeline

The significant events and milestones of the project are listed below.

Date	Event
September 3, 2024	Delivery of report draft
September 26, 2024	Delivery of summary report

Project Targets

The engagement involved a review and testing of the following target.

RegisterAndSetCustomGateway action

Repository	https://github.com/ArbitrumFoundation/governance/pull/308
Version	`c39fdf3c5bcdad117adbd616c255761f33a5a8d5`
Type	Solidity
Platform	EVM

Executive Summary

Engagement Overview

Offchain Labs engaged Trail of Bits to review the security of the governance `RegisterAndSetArbCustomGateway` governance action implemented in this PR. This governance action performs the migration for the RARI token to use a custom gateway when bridging tokens from L1 to L2.

A team of three consultants conducted the review on August 30, 2024 for a total of three engineer-days of effort. With full access to source code and documentation, we performed manual review of the code.

Observations and Impact

The code review uncovered no issues.

We focused our efforts on checking the correct procedure to safely modify the configuration of the token bridge. We also checked if external users could block or delay the action, and looked for any exceptional behavior in the (re)execution of retryable tickets needed to complete this configuration change.

We did not review any of the RARI codebase nor its on-chain configuration. This audit focused on the correct interaction between the governance action and the token bridge.

Recommendations

Despite the lack of identified issues, Offchain Labs should be careful when executing this governance action, since the RARI contract configuration could suddenly change or become misconfigured before triggering the action.