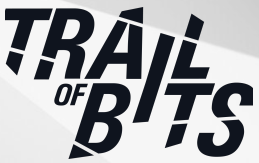

Offchain Reward Distributor Fixes

Security Assessment (Summary Report)

April 18, 2025

Prepared for:
Harry Kalodner, Steven Goldfeder, and Ed Felten
Offchain Labs

Prepared by: **Gustavo Grieco, Simone Monica, Jaime Iglesias, and Nicolas Donboly**

Table of Contents

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:

Jim Miller, Engineering Director, Blockchain
jim.miller@trailofbits.com

The following consultants were associated with this project:

Gustavo Grieco, Consultant
gustavo.grieco@trailofbits.com

Simone Monica, Consultant
simone.monica@trailofbits.com

Jaime Iglesias, Consultant
jaime.iglesias@trailofbits.com

Nicolas Donboly, Consultant
nicolas.donboly@trailofbits.com

Project Timeline

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

Date	Event
April 9, 2025	Delivery of report draft
April 9, 2025	Report readout meeting
April 18, 2025	Delivery of final summary report

Executive Summary

Engagement Overview

Offchain Labs engaged Trail of Bits to review the security of the changes made to the reward distributor contract to support handling of ERC-20 tokens specified at deployment (e.g., WETH). These changes correspond to PR #44 (`fafc251`).

The commits in scope involve a number of changes that allow reward distributor contracts to use ERC-20 tokens to properly reimburse the data availability committee members. Essentially, a set of addresses are paid based on a formula that is computed on-chain (the formula was not modified in the changes in scope). Only the infrastructure smart contract–related changes were in scope, so testing and deployment code was excluded.

A team of four consultants conducted the review from April 7 to April 8, 2025, for a total of four engineer-days of effort. With full access to source code and documentation, we performed a manual review of the code in scope.

Observations and Impact

This engagement did not reveal any issues in the code in scope. However, we provide some recommendations for improving the code quality in the Code Quality Recommendations appendix.

Recommendations

Based on the security review, Trail of Bits recommends that Offchain Labs take the following step:

- Review the items in the Code Quality Recommendations appendix and consider taking action on each one.

A. Code Quality Recommendations

The following is a list of findings that were not identified as immediate security issues but may warrant further investigation.

- **Consider adding documentation on the preconditions for the funds distribution.** For example, the following should be documented:
    - When new recipients are added, the list is not checked for duplicate recipients.
    - When new recipients are added, their assigned weights are not checked to ensure they are nonzero.

  While it is assumed that these checks are performed off-chain and the admin is trusted, the contract code could include some documentation about them.
- **Consider correcting the following typos:**
    - `recieve` should be changed to `receive`.
        - `src/RewardDistributor.sol#L21`
        - `src/FeeRouter/ChildToParentRewardRouter.sol#L10`
    - `OwnerRecieved` should be changed to `OwnerReceived`.
        - `src/RewardDistributor.sol#L43`
        - `src/RewardDistributor.sol#L151`
    - `RecipientRecieved` should be changed to `RecipientReceived`.
        - `src/RewardDistributor.sol#L46`
        - `src/RewardDistributor.sol#L139`
    - `reminder` should be changed to `remainder`.
        - `src/RewardDistributor.sol#L112`
    - `committment` should be changed to `commitment`.
        - `src/RewardDistributor.sol#L183`
        - `src/RewardDistributor.sol#L187`

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.
228 Park Ave S #80688
New York, NY 10003
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.