



Security Assessment Report

# Wormhole Fast Transfer PR193

September 12, 2024

# Summary

The Sec3 team (formerly Soteria) was engaged to conduct a thorough security analysis of the PR#193 in the Wormhole Fast Transfer repository.

The artifact of the audit was the source code of the following programs, excluding tests, in <https://github.com/wormhole-foundation/example-liquidity-layer>.

| Repository              | PR / commit            |
|-------------------------|------------------------|
| example-liquidity-layer | <a href="#">PR#193</a> |

We have reviewed the "example-liquidity-layer" codebase ([commit 78d6f22](#)) in a previous audit. This was an incremental review focusing on a small refactor atop that.

No issue was found in this review.

# Table of Contents

Result Overview ..... 3

Findings in Detail ..... 4

Appendix: Methodology and Scope of Work ..... 5

# Result Overview

| Issue                          | Impact | Status |
|--------------------------------|--------|--------|
| EXAMPLE-LIQUIDITY-LAYER PR#193 |        |        |
| No issues found                |        |        |

## Findings in Detail

No issues found.

## Appendix: Methodology and Scope of Work

Assisted by the Sec3 Scanner developed in-house, the manual audit particularly focused on the following work items:

- Check common security issues.
- Check program logic implementation against available design specifications.
- Check poor coding practices and unsafe behavior.
- The soundness of the economics design and algorithm is out of scope of this work

# DISCLAIMER

The instance report ("Report") was prepared pursuant to an agreement between Coderect Inc. d/b/a Sec3 (the "Company") and Wormhole Foundation (the "Client"). This Report solely includes the results of a technical assessment of a specific build and/or version of the Client's code specified in the Report ("Assessed Code") by the Company. The sole purpose of the Report is to provide the Client with the results of the technical assessment of the Assessed Code. The Report does not apply to any other version and/or build of the Assessed Code. Regardless of the contents of the Report, the Report does not (and should not be interpreted to) provide any warranty, representation or covenant that the Assessed Code: (i) is error and/or bug free, (ii) has no security vulnerabilities, and/or (iii) does not infringe any third-party rights. Moreover, the Report is not, and should not be considered, an endorsement by the Company of the Assessed Code and/or of the Client. Finally, the Report should not be considered investment advice or a recommendation to invest in the Assessed Code and/or the Client.

This Report is considered null and void if the Report (or any portion thereof) is altered in any manner.

# ABOUT

The Sec3 audit team comprises a group of computer science professors, researchers, and industry veterans with extensive experience in smart contract security, program analysis, testing, and formal verification. We are also building automated security tools that incorporate static analysis, penetration testing, and formal verification.

At Sec3, we identify and eliminate security vulnerabilities through the most rigorous process and aided by the most advanced analysis tools.

For more information, check out our [website](#) and follow us on [twitter](#).

