LI.FI Security Review

LiFiDEXAggregator(v1.2.0)

Independent Review By:

Sujith Somraaj (somraajsujith@gmail.com)

January 17, 2025

Contents

1   About Researcher

Sujith Somraaj is a distinguished security researcher and protocol engineer with over seven years of comprehensive experience in the Web3 ecosystem.

In addition to working as an external auditor/security researcher with LI.FI, Sujith is a protocol engineer and security researcher at Superform and Spearbit.

Learn more about Sujith on sujithsomraaj.xyz

2   Disclaimer

Note that this security audit is not designed to replace functional tests required before any software release, and does not give any warranties on finding all possible security issues of that given smart contract(s) or blockchain software. i.e., the evaluation result does not guarantee against a hack (or) the non existence of any further findings of security issues. As one audit-based assessment cannot be considered comprehensive, I always recommend proceeding with several audits and a public bug bounty program to ensure the security of smart contract(s). Lastly, the security audit is not an investment advice.

This review is done independently by the reviewer and is not entitled to any of the security agencies the researcher worked / may work with.

3   Scope

- LiFiDEXAggregator.sol(v1.2.0)

4   Risk classification

Severity level	Impact: High	Impact: Medium	Impact: Low
Likelihood: high	Critical	High	Medium
Likelihood: medium	High	Medium	Low
Likelihood: low	Medium	Low	Low

4.1   Impact

High   leads to a loss of a significant portion (>10%) of assets in the protocol, or significant harm to a majority of users.

Medium   global losses <10% or losses to only a subset of users, but still unacceptable.

Low   losses will be annoying but bearable — applies to things like griefing attacks that can be easily repaired or even gas inefficiencies.

4.2   Likelihood

High   almost certain to happen, easy to perform, or not easy but highly incentivized

Medium   only conditionally possible or incentivized, but still relatively likely

Low   requires stars to align, or little-to-no incentive

4.3   Action required for severity levels

Critical   Must fix as soon as possible (if already deployed)

High   Must fix (before deployment if not already deployed)

Medium   Should fix

Low   Could fix

5   Executive Summary

Over the course of 1 hours in total, LI.FI engaged with the researcher to audit the contracts described in section 3 of this document ("scope").

This review focuses solely on the new callback functions (xeiV3SwapCallback, dragonswapV2SwapCallback) and the additional changes added to version v1.1.0, available at Frax. This is not a review of the entire file under audit, as it is an audited fork of Sushiswap.

In this period of time a total of 0 issues were found.

<table>
<tr><th colspan="2">Project Summary</th></tr>
<tr><td>Project Name</td><td align="right">LI.FI</td></tr>
<tr><td>Repository</td><td align="right">lifinance/contracts</td></tr>
<tr><td>Deployed Contract</td><td align="right">0xfdE9CE4e17B650efdcA13d524F132876700d806f</td></tr>
<tr><td>Type of Project</td><td></td></tr>
<tr><td>Audit Timeline</td><td align="right">January 17, 2025</td></tr>
<tr><td>Methods</td><td align="right">Manual Review</td></tr>
</table>

<table>
<tr><th colspan="2">Issues Found</th></tr>
<tr><td>Critical Risk</td><td>0</td></tr>
<tr><td>High Risk</td><td>0</td></tr>
<tr><td>Medium Risk</td><td>0</td></tr>
<tr><td>Low Risk</td><td>0</td></tr>
<tr><td>Gas Optimizations</td><td>0</td></tr>
<tr><td>Informational</td><td>0</td></tr>
<tr><td>Total Issues</td><td>0</td></tr>
</table>

6 Findings