
LI.FI Security Review

WithdrawablePeriphery(v1.0.0)

Independent Review By:

Sujith Somraaj (somraajsujith@gmail.com)

October 14, 2024

Contents

1 About Researcher 2

2 Disclaimer 2

3 Scope 2

4 Risk classification 2

4.1 Impact 2

4.2 Likelihood 2

4.3 Action required for severity levels 3

5 Executive Summary 3

6 Findings 4

6.1 Informational 4

6.1.1 Add indexed keyword to TokensWithdraw event 4

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

- src/Helpers/WithdrawablePeriphery.sol

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 hour in total, [LI.FI](#) engaged with the [researcher](#) to audit the contracts described in section 3 of this document ("scope").

In this period of time a total of 1 issues were found.

Project Summary	
Project Name	LI.FI
Repository	lifinance/contracts
Commit Hashes	b03e658b35.....a7c107ba462a
Type of Project	
Audit Timeline	September 16, 2024
Methods	Manual Review

Issues Found	
Critical Risk	0
High Risk	0
Medium Risk	0
Low Risk	0
Gas Optimizations	0
Informational	1
Total Issues	1

6 Findings

6.1 Informational

6.1.1 Add indexed keyword to TokensWithdraw event

Context: [WithdrawablePeriphery.sol#L12](#)

Description: The TokensWithdraw event is emitted when the owner successfully recovers locked tokens from the WithdrawablePeriphery contract. However, the parameters of this event are not indexed for easier off-chain indexing/querying.

Recommendation: Add the indexed keyword to the TokensWithdraw event.

LI.FI: Thanks for pointing it out but we will not need this keyword for this particular case as it's an admin-function only.

Researcher: Acknowledged.