

Smart Contract Security Assessment

Final Report

FLOWX FINANCE

15 January 2024

Table of contents

Table of contents

Disclaimer

1. Overview

- 1.1 Summary
- 1.2 Contract Assessed
- 1.3 Audit Summary
- 1.4 Vulnerability Summary
- 1.5 Audit Scope

2. Findings

- 1.1 FLX-01 | Logical Issue in Fee Rate Function
- 1.2 FLX-02 | Ownership Issues
- 1.3 FLX-03 | Ownership Issues

1 Overview

This report has been prepared for FlowX Finance on the SUI Blockchain. SotaLabs provides a user-centered examination of smart contracts to look for vulnerabilities, logic errors or other issues from both an internal and external perspective.

A comprehensive examination has been performed, utilizing Cross Referencing, Static Analysis, In-House Security Tools, and line-by-line Manual Review. The auditing process pays special attention to the following considerations:



- Ensuring contract logic meets the specifications and intentions of the client without exposing the user's funds to risk.
- Testing the smart contracts against both common and uncommon attack vectors.
- Inspecting liquidity and holders' statistics to inform the status to both users and client when applicable.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Verifying contract functions that allow trusted and/or untrusted actors to mint, lock, pause, and transfer assets.
- Thorough line-by-line manual review of the entire codebase by industry experts.

1.1 Summary

Project Name	FlowX Finance
Type	Decentralize Exchange

Platform	Sui Blockchain
Language	Move
Auditors	Sota Labs
Timeline	Oct 20, 2023 – Jan 15, 2023
Description	FlowX is the ultimate destination for all your trading needs, designed to provide a seamless, user-friendly experience for all.

1.2 Contracts Assessed

Name	Contract	Live Code Match
AMM Package	0xba153169476e8c3114962261d1edc70de5ad9781b83cc617ecc8c1923191cae0	
FLX	0x6dae8ca14311574fdfe555524ea48558e3d1360d1607d1c7f98af867e3b7976c	

1.3 Audit Summary

Delivery Date	Jan 15, 2024
Audit Methodology	Static Analysis, Manual Review

1.4 Vulnerability Summary

Vulnerability	Total	Pending	Resolved	Acknowledged
Critical	0	0	0	0
Major	0	0	0	0
Medium	3	0	0	3
Informational	0	2	0	0

Classification Of Issues

Severity	Description
Critical	Exploits, vulnerabilities, or errors that will certainly or probabilistically lead towards loss of funds, control, or impairment of the contract and its functions. Issues under this classification are recommended to be fixed with utmost urgency.
Major	Bugs or issues with that may be subject to exploitation, though their impact is somewhat limited. Issues under this classification are recommended to be fixed as soon as possible
Medium	Effects are minimal in isolation and do not pose a significant danger to the project or its users. Issues under this classification are recommended to be fixed nonetheless.
Informational	Consistency, syntax, or style best practices. Generally, pose a negligible level of risk, if any.

1.5 Audit Scope

Delivery Date	Jan 15, 2024
Audit Methodology	Static Analysis, Manual Review

The following files were made available during the review:

- exchange/factory.move
- exchange/pair.move
- exchange/router.move
- exchange/treasury.move
- utils/comparator.move
- utils/math.move
- utils/swap_utils.move
- utils/type_helper.move
- flx/sources/flx.move
- flx/sources/minter_role.move

2 Finding

1.1 FLX-01 | Logical Issue in Fee Rate Function

Category	Severity	Location	Status
Logical Issue	Medium	exchange/factory.move#lines-140	Acknowledged

Description

1. Set_fee_rate function is not validate new_fee_rate input. This parameter can go from 0 to FEE_PRECISION.

Recommendation

We recommend the team to be set minimum value and maximum value for this parameter.

1.2 FLX-02 | Ownership Issues

Category	Severity	Location	Status
Centralization / Privilege	Medium	exchange/pair.move#lines-141	Acknowledged

Description

Some functions in pair package can be called by owner of the factory package.

Recommendation

To reduce the centralization of the package, owner should be controlled as multisig-wallet or using action delay function like Timelock,...

1.3 FLX-03 | Ownership Issues

Category	Severity	Location	Status
Centralization / Privilege	Medium	/flx/sources/flx.move#lines-62	Acknowledged

Description

The contract owner has the power to mint token from package. The token is limited by total supply is “10000000000000000u64” value

Recommendation

The contract owner has implemented a delayed action mechanism like TimeLock or using multisig-wallet to enhanced security.

Appendix

Finding Categories

Centralization / Privilege

Centralization / Privilege findings refer to either feature logic or implementation of components that act against the nature of decentralization, such as explicit ownership or specialized access roles in combination with a mechanism to relocate funds.

Logical Issue

Logical Issue findings detail a fault in the logic of the linked code.

Volatile Code

Volatile Code findings refer to segments of code that behave unexpectedly on certain edge cases that may result in a vulnerability.

Language Specific

Language Specific findings are issues that would only arise within Solidity, i.e., incorrect usage of private or deleted.

Sota Labs