Smart Contract Security Assessment

Final Report

SUI PEARL

26 December 2023

Table of contents

1 Overview

This report has been prepared for Sui Pearl Fi on the SUI Blockchain. SotaTek 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	Sui Pearl Fi
Type	Yield Aggregator

Platform	Sui Blockchain
Language	Move
Auditors	SotaTek
Timeline	Oct 20, 2023 – Oct 27, 2023
Description	Sui Pearl is a yield aggregator platform which allow user to maximize their yield earnings through different farming strategies on the Sui Network.

1.2 Contracts Assessed

Name	**Contract**	**Live Code Match**
Sui Pearl	0xf794e590fb6a42aee87837631e6ff9c006397503d64a1d3f69bfb3938a118b9e	✓

1.3 Audit Summary

Delivery Date	October 26, 2023
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	2	0	0	2
Informational	0	2	0	2

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	October 26, 2023
Audit Methodology	Static Analysis, Manual Review

The following files were made available during the review:

- cage/sources/custodian.move
- cage/sources/fee_collector.move
- cage/sources/fee_collector_registry.move
- cage/sources/fetcher.move
- cage/sources/operator.move
- cage/sources/pool.move
- cage/sources/pool_registry.move
- cage/sources/position.move
- cage/sources/position_registry.move
- cage/sources/state.move

2 Finding

1.1 SPF-01 | Redundant Test Function

Category	Severity	Location	Status
Redundant	Informational	Multiple location	Acknowledged

Description

Test functions are not removed when deploying. We recommend removing these functions when deploying. Redundant found in:

1. cage/sources/custodian.move
2. cage/sources/fee_collector.move
3. cage/sources/fee_collector_registry.move
4. cage/sources/operator.move
5. cage/sources/pool.move
6. cage/sources/pool_registry.move
7. cage/sources/position.move
8. cage/sources/position_registry.move
9. cage/sources/state.move

Recommendation

We recommend the team to be remove these functions from the repository.

1.2 SPF-02 | Ownership Issues

Category	Severity	Location	Status
Centralization / Privilege	Medium	/cage/sources/fee_collector.move#lines-46	Acknowledged

Description

During every calculation, the contract takes percentage variables from the Fee Collector, and divides it by 100. However, there are no validations in setters of fee that percentage variables are less than 100. Thus, calculated values can be greater than 100%. In any case, the SuiPearl team should verify the behavior.

Recommendation

Validate that percentage values don't exceed 100 OR verify that percentage values can exceed 100.

1.3 SPF-03 | Ownership Issues

Category	Severity	Location	Status
Centralization / Privilege	Medium	cage/sources/operator.move#lines-417	Acknowledged

Description

The contract owner has the power to stop distributing rewards to staked users, and no further rewards will be distributed after that.

Recommendation

The contract owner has implemented a delayed action mechanism like TimeLock.

1.4 SPF-04 | Validation Issues

Category	Severity	Location	Status
Centralization / Privilege	Informational	cage/sources/operator.move#lines-226	Acknowledged

Description

Function receives allocpoint, fee rate, clock as function input but not validated any parameters.

Recommendation

Validate these parameters to ensure function behavior.

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.