Shaolin Security Audit

Report Version 0.1

January 25, 2025

Conducted by **Hunter Security**

Table of Contents

1 About Hunter Security

Hunter Security is an industry-leading smart contract security auditing firm. Having conducted over 100 security audits protecting over $1B of TVL, our team always strives to deliver top-notch security services to the best DeFi protocols. For security audit inquiries, you can reach out on Telegram or Twitter at *@georgehntr*.

2 Disclaimer

Audits are a time-, resource-, and expertise-bound effort where trained experts evaluate smart contracts using a combination of automated and manual techniques to identify as many vulnerabilities as possible. Audits can reveal the presence of vulnerabilities, but cannot guarantee their absence.

3 Risk classification

Severity	Impact: High	Impact: Medium	Impact: Low
Likelihood: High	High	High	Medium
Likelihood: Medium	High	Medium	Low
Likelihood: Low	Medium	Low	Low

3.1 Impact

- **High** - leads to a significant loss of assets in the protocol or significantly harms a group of users.
- **Medium** - involves a small loss of funds or affects a core functionality of the protocol.
- **Low** - encompasses any unexpected behavior that is non-critical.

3.2 Likelihood

- **High** - a direct attack vector; the cost is relatively low compared to the potential loss of funds.
- **Medium** - only a conditionally incentivized attack vector, with a moderate likelihood.
- **Low** - involves too many or unlikely assumptions; offers little to no incentive.

3.3 Actions required by severity level

- **High** - client **must** fix the issue.
- **Medium** - client **should** fix the issue.
- **Low** - client **could** fix the issue.

4 Executive summary

Overview

Project Name	Shaolin
Repository	https://github.com/De-centraX/shaolin-contracts
Commit hash	5856224071628d881ddb2f4e914fb0a5ea232453
Resolution	-
Methods	Manual review & testing

Scope

src/pools/LamboPool.sol
src/pools/WBTCPool.sol
src/Mining.sol
src/Shaolin.sol
src/Staking.sol

Issues Found

High risk	0
Medium risk	0
Low risk	1

5 Findings

5.1 Low

5.1.1 Insufficient blacklist validation

Severity: Low

Files: Staking.sol

Description: In *compoundRewards* if a user is blacklisted, they can just approve their tokens to someone else or another address that belongs to them and still perform the forbidden action as the owner of the staking position.

Recommendation: Consider checking whether the owner of the passed position ID is blacklisted.

Resolution: Pending.