Custodia Security

Size v1.6.1 Review

Conducted By: Ali Kalout, Ali Shehab

Contents

1. Disclaimer

A smart contract security review cannot ensure the absolute absence of vulnerabilities. This process is limited by time, resources, and expertise and aims to identify as many vulnerabilities as possible. We cannot guarantee complete security after the review, nor can we assure that the review will detect every issue in your smart contracts. We strongly recommend follow-up security reviews, bug bounty programs, and on-chain monitoring.

2. Introduction

Custodia conducted a security assessment of Size's smart contract following the implementation of v1.6.1, ensuring its proper implementation.

3. About Size

Size is a lending marketplace with unified liquidity across maturities.

Size is built on an order book model where offers are expressed as yield curves, allowing efficient and continuous pricing of fixed-rate products while maintaining unified liquidity.

4. Risk Classification

Severity	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: Results in a substantial loss of assets within the protocol or significantly impacts a group of users.
- Medium: Causes a minor loss of funds (such as value leakage) or affects a core functionality of the protocol.
- Low: Leads to any unexpected behavior in some of the protocol's functionalities, but is not critical.

4.2. Likelihood

- High: The attack path is feasible with reasonable assumptions that replicate on-chain conditions, and the cost of the attack is relatively low compared to the potential funds that can be stolen or lost.
- Medium: The attack vector is conditionally incentivized but still relatively likely.
- Low: The attack requires too many or highly unlikely assumptions, or it demands a significant stake by the attacker with little or no incentive.

4.3. Action required for severity levels

- Critical: Must fix as soon as possible
- High: Must fix
- Medium: Should fix
- Low: Could fix

5. Security Assessment Summary

Duration: 11/02/2025 - 12/02/2015
Repository: SizeCredit/size-solidity
Commit: 3dbb7cc541a001ef6469d757a3b6125670978755

- src/*

6. Executive Summary

Throughout the security review, Ali Kalout and Ali Shehab engaged with Size's team to review Size. During this review, one issue was uncovered.

Findings Count

Severity	**Amount**
Critical	N/A
High	N/A
Medium	N/A
Low	1
Total Finding	**1**

Summary of Findings

ID	Title	Severity	Status
L-01	`validateCopyLimitOrders` doesn't validate if the max APR is greater than the min	Low	Resolved

7. Findings

7.1. Low Findings

[L-01] `validateCopyLimitOrders` doesn't validate if the max APR is greater than the min

Severity:
Low

Description:
`validateCopyLimitOrders` allows users to copy limit orders while providing min and max APRs, however, it doesn’t validate that min APR is < max APR. Allowing users to copy limit orders and have them unusable.

Recommendations:
Enforce min APR <= max APR.

7.2. Informational Findings

1. `copyLimitOrders` shouldn’t allow users to copy their limit orders.