Index.fun Security Review

Version 2.0

14.01.2025

Conducted by:

MaslarovK, Lead Security Researcher

radev-eth, Lead Security Researcher

Table of Contents

1 About MaslarovK

MaslarovK a Security Reseacher and Co-Founder of Rezolv Solutions.

2 About radev.eth

radev_eth a Security Reseacher and Co-Founder of Rezolv Solutions.

3 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 show the presence of vulnerabilities **but not their absence**.

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** - leads to a significant loss of assets in the protocol or significantly harms a group of users.
- **Medium** - only a small amount of funds can be lost or a functionality of the protocol is affected.
- **Low** - any kind of unexpected behaviour that's not so critical.

4.2 Likelihood

- **High** - direct attack vector; the cost is relatively low to the amount of funds that can be lost.
- **Medium** - only conditionally incentivized attack vector, but still relatively likely.
- **Low** - too many or too unlikely assumptions; provides little or no incentive.

4.3 Actions required by severity level

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

5 Executive summary

Overview

Project Name	Index.fun
Repository	https://github.com/truflation/lot-purchase/tree/main/contracts/contracts
Commit hash	1422726d3ccc5a3ac2e7f25156aef5f5e13c8577
Resolution	ecb9fe19841cf167b4b46da51f097d14dbbff263
Documentation	N/A
Methods	Manual review

Scope

contracts/contracts/BinaryMarket.sol
contracts/contracts/IIndexSlotRegister.sol
contracts/contracts/IndexSlotRegister.sol

Issues Found

Critical risk	0
High risk	3
Medium risk	1
Low risk	2
Informational	5

6 Findings

6.1 High risk

6.1.1 Several problems with fees calculation in BinaryMarket.sol::claim function

6.1.2 No check if the slotId already exist in IndexSlotRegister::createIndex

6.1.3 In the BinaryMarket.sol::setRoundResult, a malicious owner can set the round to not PAID and drain the contact funds

6.2 Medium risk

6.2.1 In the BinaryMarket.sol::placeBet, the chosenOption can't be changed when adding funds to your bet

6.3 Low risk

6.3.1 IndexSlotRegister.sol::adminWithdrawal uses transferFrom instead of transfer

6.3.2 BinaryMarket.sol::changeOracle lacks address(0) check

6.4 Informational risk

6.4.1 IndexSlotRegister.sol::createIndex emits wrong event

6.4.2 IndexSlotRegister.sol::getPrice is not needed

6.4.3 BinaryMarket.sol::_requestYoyInflation is marked as internal and is not used anywhere around the contract

6.4.4 BinaryMarket.sol contains several functions marked as public, but not invoked from inside the contract

6.4.5 Set min and max fees at BinaryMarket.sol::changeFee