OFFSIDE Labs

Mind Network Restaking

Smart Contract Security Assessment

June 2024

Prepared for:

Mind Network

Prepared by:

Offside Labs

Tim Li

Allen Xu

Siji Feng

Contents

1 About Offside Labs

Offside Labs is a leading security research team, composed of top talented hackers from both academia and industry.

We possess a wide range of expertise in modern software systems, including, but not limited to, *browsers*, *operating systems*, *IoT devices*, and *hypervisors*. We are also at the forefront of innovative areas like *cryptocurrencies* and *blockchain technologies*. Among our notable accomplishments are remote jailbreaks of devices such as the **iPhone** and **PlayStation 4**, and addressing critical vulnerabilities in the **Tron Network**.

Our team actively engages with and contributes to the security community. Having won and also co-organized *DEFCON CTF*, the most famous CTF competition in the Web2 era, we also triumphed in the **Paradigm CTF 2023** within the Web3 space. In addition, our efforts in responsibly disclosing numerous vulnerabilities to leading tech companies, such as *Apple*, *Google*, and *Microsoft*, have protected digital assets valued at over **$300 million**.

In the transition towards Web3, Offside Labs has achieved remarkable success. We have earned over **$9 million** in bug bounties, and **three** of our innovative techniques were recognized among the **top 10 blockchain hacking techniques of 2022** by the Web3 security community.

https://offside.io/

https://github.com/offsidelabs

https://twitter.com/offside_labs

2 Executive Summary

Introduction

Offside Labs completed a security audit of *Mind Network Restaking* smart contracts, starting on June 25, 2024, and concluding on June 25, 2024.

Project Overview

This project consists of Solidity smart contracts that facilitate users in restaking their LRT (Liquid Restaking Tokens) and LST (Liquid Staking Tokens) to the *Mind Network*. The purpose of these contracts is to enhance network security by allowing token holders to actively participate in network operations through restaking.

Audit Scope

The assessment scope contains mainly the smart contracts of the *Restaking Contract* program for the *Mind Network* project.

The audit is based on the following specific branches and commit hashes of the codebase repositories:

- mind-restaking-contracts
  - Branch: main
  - Commit Hash: 9aa3d8221fcf73a0c14ab0b7e3f34f5b7f007b18
  - Codebase Link

We listed the files we have audited below:

- mind-restaking-contracts
  - contracts/strategies/Strategy.sol
  - contracts/strategies/MToken.sol
  - contracts/strategies/FixedStrategy.sol

Findings

The security audit revealed:

- 2 informational issues

Further details, including the nature of these issues and recommendations for their remediation, are detailed in the subsequent sections of this report.

3 Summary of Findings

ID	Title	Severity	Status
01	Strategy Contract Unable to Directly Burn User's Token	Informational	Fixed
02	Unused Error Revert in FixedStrategy Contract	Informational	Fixed

4 Key Findings and Recommendations

4.1 Informational and Undetermined Issues

Strategy Contract Unable to Directly Burn User's Token

Severity: Informational	Status: Fixed
Target: Smart Contract	Category: Gas Optimization

The strategy contract cannot directly burn a user's token and must instead call `burnFrom()` , which requires the user to grant additional approval. This increases user interaction cost and on-chain gas usage.

Override `burnFrom()` to check the caller has the `MINTER` role, allowing the strategy to burn tokens without extra approval. The strategy contract has the `MINTER` role already. This will eliminate the need for user approval and reduce costs.

Unused Error Revert in FixedStrategy Contract

Severity: Informational	Status: Fixed
Target: Smart Contract	Category: Unused Code

The error `DepositOnlyDuringCampaign` should be used in the `deposit` function of the `FixedStrategy` contract. However, it reverts with an unexpected empty error message.

5 Disclaimer

This audit report is provided for informational purposes only and is not intended to be used as investment advice. While we strive to thoroughly review and analyze the smart contracts in question, we must clarify that our services do not encompass an exhaustive security examination. Our audit aims to identify potential security vulnerabilities to the best of our ability, but it does not serve as a guarantee that the smart contracts are completely free from security risks.

We expressly disclaim any liability for any losses or damages arising from the use of this report or from any security breaches that may occur in the future. We also recommend that our clients engage in multiple independent audits and establish a public bug bounty program as additional measures to bolster the security of their smart contracts.

It is important to note that the scope of our audit is limited to the areas outlined within our engagement and does not include every possible risk or vulnerability. Continuous security practices, including regular audits and monitoring, are essential for maintaining the security of smart contracts over time.

Please note: we are not liable for any security issues stemming from developer errors or misconfigurations at the time of contract deployment; we do not assume responsibility for any centralized governance risks within the project; we are not accountable for any impact on the project's security or availability due to significant damage to the underlying blockchain infrastructure.

By using this report, the client acknowledges the inherent limitations of the audit process and agrees that our firm shall not be held liable for any incidents that may occur subsequent to our engagement.

This report is considered null and void if the report (or any portion thereof) is altered in any manner.