OFFSIDE LABS

Exponent Jito Restaking Standard

Smart Contract Security Assessment

December 2024

Prepared for:

Exponent Finance

Prepared by:

Offside Labs

Ripples Wen

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 *Exponent* smart contracts, starting on December 17th, 2024, and concluding on December 18th, 2024.

Project Overview

The Jito Restaking Standard program enables users to mint standard yield tokens that represent deposits in the Jito Restaking protocol. Which each token representing one KYSOL. Key functionalities include:

1. mint_sy and redeem_sy: Manage deposits into escrow and handle minting or redeeming of standard yield tokens. The deposited token is KYSOL but is treated as SOL with an equivalent value.

2. Emissions Management: Accrues emissions for staked receipt tokens, facilitating easier tracking for the core program. Non-staked emissions are directed to the protocol's treasury.

Audit Scope

The assessment scope contains mainly the smart contracts of the *Jito Restaking Standard* program for the *Exponent* project.

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

- *Jito Restaking Standard*
  - Codebase: `https://github.com/exponent-finance/exponent-core`
  - Commit Hash: 6a6581ce75aa4fe935d186a1f5263ecd6747fec9

We listed the files we have audited below:

- *Jito Restaking Standard*
  - solana/programs/jito_restaking_standard/src/*.rs
  - solana/programs/jito_restaking_interface_spl_stake_pool/src/*.rs
  - solana/libraries/jito_restaking_cpi/src/*.rs

Findings

The security audit revealed:

- 0 critical issue

- 0 high issue
- 0 medium issue
- 0 low issue
- 1 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	Unnecessary CPI Call for jito_restaking_interface _spl_stake_pool	Informational	Fixed

4 Key Findings and Recommendations

4.1 Informational and Undetermined Issues

Unnecessary CPI Call for `jito_restaking_interface_spl_stake_pool`

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

In the `to_sy_state` function, a CPI call is made to the `jito_restaking_interface_spl_stake_pool` to retrieve the exchange rate between JitoSOL and SOL. During this call, the StakePool account is parsed, and the exchange rate is computed as the ratio of `total_lamports` to `pool_token_supply` . However, this computation can be performed directly within the `to_sy_state` function without requiring the CPI call. This optimization would save compute units and reduce the depth of the CPI invoke stack.

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.

OFFSIDE LABS

https://offside.io/

https://github.com/offsidelabs

https://twitter.com/offside_labs