OFFSIDE LABS

Exponent Perena Standard

Smart Contract Security Assessment

February 2025

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 January 27th, 2025, and concluding on January 31th, 2025.

Project Overview

The Perena Standard program enables users to mint standard yield tokens that represent deposits in the Perena Numéraire Seed Pool. Which each token representing one USD*. 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 USD* and its value is measured in USD.

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 *perena_standard* program for the *Exponent* project.

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

- *Exponent*
    - Codebase: `https://github.com/exponent-finance/exponent-core`
    - Commit Hash: 381793b79fad93bec6854db637170880d5ec644a

We listed the files we have audited below:

- *Exponent*
    - solana/programs/perena_standard/src/*.rs
    - solana/libraries/perena_cpi/src/*.rs

Findings

The security audit revealed:

- 1 critical issues
- 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	Vulnerability in Exchange Rate Calculation Due to Missing Account Validation	Critical	Fixed
02	Perena Admin Misconfiguration	Informational	Acknowledged

4 Key Findings and Recommendations

4.1 Vulnerability in Exchange Rate Calculation Due to Missing Account Validation

Severity: Critical	Status: Fixed
Target: Smart Contract	Category: Data Validation

Description

In the `to_sy_state` function, the first remaining account is parsed as the LP mint of Perena to extract the LP supply. However, this account is not validated, meaning any token mint account could be passed in to manipulate the supply, ultimately affecting the exchange rate.

```
42 fn to_sy_state(&self, interface_remaining_accounts: &[AccountInfo<'i>]) ->
    ↪ SyState {
43     let emission_indexes = self.get_sy_meta().to_emmission_indexes();
44
45     let mint_data =
        ↪ interface_remaining_accounts[0].try_borrow_data().unwrap();
46     let mint_lp = Mint::try_deserialize(&mut &mint_data[..]).unwrap();
47
48     let exchange_rate =
        ↪ self.get_perena_stable_pool().exchange_index(mint_lp.supply);
```

solana/programs/perena_standard/src/utils.rs#L42-L48

Impact

By manipulating the exchange rate, an attacker could influence the exchange logic within the Exponent core program, allowing them to obtain more output tokens for fewer input tokens, leading to potential fund loss.

Recommendation

Introduce a validation step to ensure the first remaining account is the expected LP mint account.

Mitigation Review Log

Fixed in the commit 6317d3ac3d35410931588a842d4e664fa3d71961.

4.2 Informational and Undetermined Issues

Perena Admin Misconfiguration

Severity: Informational	Status: Acknowledged
Target: Smart Contract	Category: Logic Error

Perena is incorrectly reusing the admin configured for Jito restaking. This should be corrected before the release, or we should consider adopting a universal admin for all standard programs.

```
170     pub fn validate(&self) -> Result<()> {
171         self.admin_state
172             .principles
173             .jito_restaking
174             .is_admin(&self.admin.key)?;
```

solana/programs/perena_standard/src/instructions/admin/init_sy.rs#L170-L174

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.

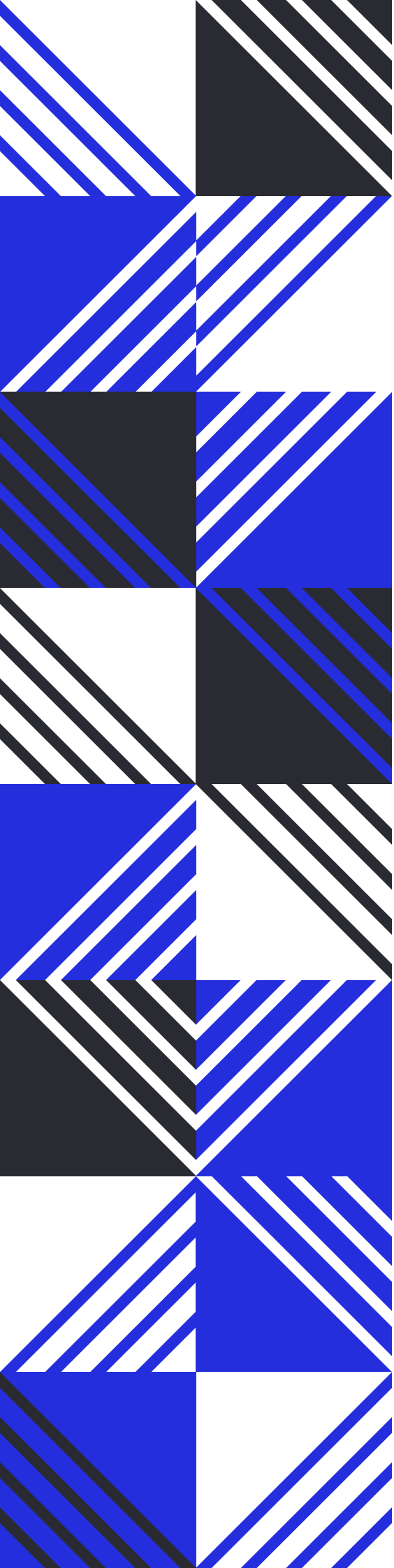
We expressly disclaim any liability for any losses or damages arising from the use of this report or from any security breaches that may occur in the future. We also recommend that our clients engage in multiple independent audits and establish a public bug bounty program as additional measures to bolster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