Overview

About audit

This audit was requested through C4 and audited by C4 warden: *rvierdiiev* as Solo Audit. During the Solo Audit outlined in this document, warden conducted an analysis of the Rodeo code. The audit took place between August 11—15, 2023.

Summary

The Solo Audit yielded 1 HIGH severity vulnerability. Also 3 informational finding was found.

Scope

Code reviewed consisted of the following files inside *audit-2308* branch:

- StrategyJonesUsdc.sol
- StrategyCamelot.sol
- StrategyPendleLSD.sol
- StrategyPendleCamelot.sol

Severity Criteria

C4 assesses the severity of disclosed vulnerabilities according to a methodology based on OWASP standards.

Vulnerabilities are divided into three primary risk categories: high, medium, and low/non-critical.
High-level considerations for vulnerabilities span the following key areas when conducting assessments:

- Malicious Input Handling
- Escalation of privileges
- Arithmetic
- Gas use

Further information regarding the severity criteria referenced throughout the submission review process, please refer to the documentation provided on the C4 website.

High Risk Findings (1)

[H-01] Exchange rate dilution

_rate function applies *redeemFee* that will be collected by JonesDao vault. Such fee should be only applied to rate calculation for withdraws. When new user deposits into the StrategyJonesUsdc, then he provides less amount of assets in order to mint shares. As result, each new deposit makes exchange rate to decrease, which means lose of funds for depositors.

https://github.com/rodeofi/rodeo/blob/audit-2308/contracts/src/strategies/StrategyJonesUsdc.sol#L72
https://github.com/rodeofi/rodeo/blob/audit-2308/contracts/src/strategies/StrategyJonesUsdc.sol#L82

STATUS: Mitigated

Informational Findings (2)

[Info-01] PartnerProxy is not payable

PartnerProxy contract is intended to be able to work with native payment. But because call function is not payable and contract doesn't have *receive* or *fallback*, it's not possible to top up it.

https://github.com/rodeofi/rodeo/blob/audit-2308/contracts/src/PartnerProxy.sol#L19

STATUS: Mitigated

[Info-02] Lack of slippage protection

earn function in *StrategyPendleCamelot* and *StrategyPendleLSD* contracts is going to be called by authorized actor periodically. This function will claim all rewards and swap them to the target asset. After it's done, *addPendleLiquidity* will be called, which will provide target asset to the pendle market. This function doesn't use slippage protection, which allows attacker to sandwich earn calls to make profit.

This is marked as low severity, because currently it's not possible to sandwhich txs on arbitrum chain.

https://github.com/rodeofi/rodeo/blob/audit-2308/contracts/src/strategies/StrategyPendleCamelot.sol#L170
https://github.com/rodeofi/rodeo/blob/audit-2308/contracts/src/strategies/StrategyPendleLSD.sol#L144

STATUS: Mitigated

[Info-03] Inefficient use of funds in StrategyJonesUsdc

earn function in *StrategyJonesUsdc* tries to leave 10% of users funds in the contract for withdraws. In case if funds were redeemed for JonesDao, then function doesn't update current balance of funds and request withdraw again. This can lead to more than 10% funds to be withdrawn from JonesDao and those funds will not earn yields.

https://github.com/rodeofi/rodeo/blob/audit-2308/contracts/src/strategies/StrategyJonesUsdc.sol#L126-L132

STATUS: Mitigated

Disclosures

C4 is an open organization governed by participants in the community.
C4 does not provide any guarantee or warranty regarding the security of this project. All smart contract software should be used at the sole risk and responsibility of users.