yAudit Euler PendleOracle Review

Review Resources:

- code repository

Auditors:

- HHK
- Panda

Table of Contents

Review Summary

Euler PendleOracle

The Euler PendleOracle adapter provides an Oracle adapter for Pendle tokens to be used within the Euler ecosystem. It will allow deposits of Pendle principal tokens (known as PT tokens) as collateral and/or liability on vaults created with the EVK.

The contracts of the Euler PendleOracle Repo were reviewed over one and a half days. The code review was performed by two auditors between 16 and 17th September 2024. The repository was under active development during the review, but the review was limited to the latest commit, 1582bb4c15b907a0256ec9d649b3eef3ca963739 for the Euler PendleOracle repo, at the start.

Scope

The scope of the review consisted of the following contracts at the specific commit:

```
src/adapter/pendle/PendleOracle.sol
```

After the findings were presented to the Euler team, fixes were made and included in several PRs.

This review is a code review to identify potential vulnerabilities in the code. The reviewers did not investigate security practices or operational security and assumed that privileged accounts could be trusted. The reviewers did not evaluate the security of the code relative to a standard or specification. The review may not have identified all potential attack vectors or areas of vulnerability.

yAudit and the auditors make no warranties regarding the security of the code and do not warrant that the code is free from defects. yAudit and the auditors do not represent nor imply to third parties that the code has been audited nor that the code is free from defects. By deploying or using the code, Euler PendleOracle and users of the contracts agree to use the code at their own risk.

Code Evaluation Matrix

Category	Mark	Description
Access Control	Good	There is no usage of specific access control mechanisms like `Ownable` or `AccessControl`.

Category	Mark	Description
Mathematics	Good	The contract uses simple math.
Complexity	Good	The contract logic is relatively straightforward but involves complex integrations with Pendle protocol components.
Libraries	Good	The reviewed oracle uses the `PendlePYOracleLib`, which is a slightly modified version of `PendlePtOracleLib` that went through security reviews and is used in production by lending protocols such as Silo.
Decentralization	Good	The contract configures immutable variables, ensuring that core parameters cannot be changed after deployment.
Code stability	Good	The code appears stable.
Documentation	Good	The contract is well-documented with clear comments explaining the purpose of functions
Monitoring	Good	No monitoring is in place on this contract, but this is correct. Monitoring isn't required.
Testing and verification	Good	The contract is well tested.

Findings Explanation

Findings are broken down into sections by their respective impact:

- Critical, High, Medium, Low impact
  - These are findings that range from attacks that may cause loss of funds, impact control/ownership of the contracts, or cause any unintended consequences/actions that are outside the scope of the requirements.
- Gas savings
  - Findings that can improve the gas efficiency of the contracts.
- Informational
  - Findings including recommendations and best practices.

Critical Findings

None.

High Findings

None.

Medium Findings

None.

Low Findings

None

Gas Savings Findings

None

Informational Findings

1 Informational - Add a `MAX_TWAP_WINDOW` constant

Technical Details

TWAP oracles rely extensively on the duration window. A duration that is too small can lead to price manipulation, while a window too big can lead to a delay in the price update, as a greater amount of time will have to pass for the twap to reflect the price change. For that reason, it could be interesting to add a `MAX_TWAP_WINDOW` constant.

The Pendle documentation advises for the twap duration to be 15 or 30 minutes, the max constant could be set to 1 hour to make sure no longer window duration is selected.

Impact

Informational.

Recommendation

Consider adding a `MAX_TWAP_WINDOW` constant.

Developer Response

Fixed in https://github.com/euler-xyz/euler-price-oracle/commit/e1bc31ebd2ee2b78bac01271db834dae912d821e.

Final Remarks

After reviewing the PendleOracle adapter, auditors found it well-structured, modular, and effectively utilizing the external oracle. They recommend that vault owners integrating with Pendle carefully review the documentation and select safe parameters to mitigate the risks associated with these multilayered assets—particularly the risks of liquidity shortages, TWAP oracle exploits, and the inherent dangers of underlying yield-bearing assets.