Pendle PT Oracle Audit Report

May 26, 2023

Table of Contents

Summary **2**

Overview **3**

Issues **4**

[WP-H1] When the real index (`SY.exchangeRate()`) is less than `YT.pyIndexCurrent()` , PendlePtOracle may not be working as expected 4

Appendix **6**

Disclaimer **7**

Summary

This report has been prepared for Pendle PT Oracle smart contract, to discover issues and vulnerabilities in the source code of their Smart Contract as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing Static Analysis and Manual Review techniques.

The auditing process pays special attention to the following considerations:

- Testing the smart contracts against both common and uncommon attack vectors.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Overview

Project Summary

Project Name	**Pendle PT Oracle**
Codebase	**https://github.com/pendle-finance/pendle-core-v2-public**
Commit	**02a503a849b35482a06003b2c89a7934e81dc02f**
Language	**Solidity**

Audit Summary

Delivery Date	**May 26, 2023**
Audit Methodology	**Static Analysis, Manual Review**
Total Isssues	**1**

[WP-H1] When the real index (`SY.exchangeRate()`) is less than `YT.pyIndexCurrent()` , PendlePtOracle may not be working as expected

High

Issue Description

https://github.com/pendle-finance/pendle-core-v2-public/blob/a9c731ce2168547a09362ba7a90e3e330737192a/contracts/offchain-helpers/Oracles/PendlePtOracle.sol#L32-L38

```
function getPtToAssetRate(
    address market,
    uint32 duration
) external view returns (uint256 ptToAssetRate) {
    ptToAssetRate = IPMarket(market).getPtToAssetRate(duration);
}
```

https://github.com/pendle-finance/pendle-core-v2-public/blob/a9c731ce2168547a09362ba7a90e3e330737192a/contracts/offchain-helpers/Oracles/samples/PendlePtUsdChainlinkOracle.sol#L39-L43

```
function getPtPrice() external view virtual returns (uint256) {
    uint256 ptRate = IPPtOracle(ptOracle).getPtToAssetRate(market, twapDuration);
    uint256 assetPrice = _getUnderlyingAssetPrice();
    return (assetPrice * ptRate) / Math.ONE;
}
```

When PT expires and gets redeemed to SY, if the current value of the SY index (`SY.exchangeRate()`) is not at its historical high index (`YT.pyIndexCurrent()`), then PT cannot be exchanged to Asset at a 1:1 ratio.

For example:

If historical high index `YT.pyIndexCurrent() == 2` and the actual index is `1` , then 1 PT can only exchange for 0.5 SY. However, the value of 0.5 SY does not amount to 1 Asset, but only 0.5 Asset.

To handle this situation, PT first needs to be converted to SY using the current index (`YT.pyIndexCurrent()`) and then to Asset using the actual exchange rate (the `SY.exchangeRate()` as in `SY.redeem()`).

Thus, the correct result should be that PT is worth 0.5 SY and each SY is worth 1 Asset, such that each PT is worth `0.5 * 1 == 0.5 Asset` .

The same applies to cases where PT has not yet expired, but the current index is lower than the historical high index (`YT.pyIndexCurrent()`). In such cases, the result returned by the market needs to be converted again using the actual index to determine the real value of the PT in Asset.

Status

✓ Fixed

Appendix

Timeliness of content

The content contained in the report is current as of the date appearing on the report and is subject to change without notice, unless indicated otherwise by WatchPug; however, WatchPug does not guarantee or warrant the accuracy, timeliness, or completeness of any report you access using the internet or other means, and assumes no obligation to update any information following publication.

Disclaimer

This report is based on the scope of materials and documentation provided for a limited review at the time provided. Results may not be complete nor inclusive of all vulnerabilities. The review and this report are provided on an as-is, where-is, and as-available basis. You agree that your access and/or use, including but not limited to any associated services, products, protocols, platforms, content, and materials, will be at your sole risk. Smart Contract technology remains under development and is subject to unknown risks and flaws. The review does not extend to the compiler layer, or any other areas beyond the programming language, or other programming aspects that could present security risks. A report does not indicate the endorsement of any particular project or team, nor guarantee its security. No third party should rely on the reports in any way, including for the purpose of making any decisions to buy or sell a product, service or any other asset. To the fullest extent permitted by law, we disclaim all warranties, expressed or implied, in connection with this report, its content, and the related services and products and your use thereof, including, without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. We do not warrant, endorse, guarantee, or assume responsibility for any product or service advertised or offered by a third party through the product, any open source or third-party software, code, libraries, materials, or information linked to, called by, referenced by or accessible through the report, its content, and the related services and products, any hyperlinked websites, any websites or mobile applications appearing on any advertising, and we will not be a party to or in any way be responsible for monitoring any transaction between you and any third-party providers of products or services. As with the purchase or use of a product or service through any medium or in any environment, you should use your best judgment and exercise caution where appropriate. FOR AVOIDANCE OF DOUBT, THE REPORT, ITS CONTENT, ACCESS, AND/OR USAGE THEREOF, INCLUDING ANY ASSOCIATED SERVICES OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, INVESTMENT, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.