Gearbox / Pendle PT Oracle Audit Report

Dec 3, 2024

Table of Contents

Summary

This report has been prepared for Gearbox / 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	**Gearbox / Pendle PT Oracle**
Codebase	**https://github.com/Gearbox-protocol/oracles-v3**
Commit	**4f2b39e0554beeb484d07a53ce90b67f63aaa41d ——— (for v3.0)** **370777f28ba4df7f6465f4deca2a337fece2abb5 ——— (for v3.1)**
Language	**Solidity**

Audit Summary

Delivery Date	**Dec 3, 2024**
Audit Methodology	**Static Analysis, Manual Review**
Total Isssues	**2**

[WP-I1] `PendlePYOracleLib#getPtToAssetRate()` does not correctly handle index fluctuations.

Informational

Issue Description

While the SY's `exchangeRate` is typically monotonically increasing, it is technically possible for the `exchangeRate` to fluctuate for certain assets.

Therefore, `syIndex >= pyIndex` cannot be assumed to always be true.

The official implementation includes a separate branch to handle cases where this invariant does not hold:

```
19  function getPtToAssetRate(IPMarket market, uint32 duration) internal view returns
    (uint256) {
20      (uint256 syIndex, uint256 pyIndex) = getSYandPYIndexCurrent(market);
21      if (syIndex >= pyIndex) {
22          return getPtToAssetRateRaw(market, duration);
23      } else {
24          return (getPtToAssetRateRaw(market, duration) * syIndex) / pyIndex;
25      }
26  }
```

In comparsion, `PendleTWAPPTPriceFeed` does not account for this and incorrectly assumes that `syIndex >= pyIndex` will always hold:

```
72  /// @dev Computes the PT to asset rate from the market implied rate TWAP
73  function _getPTToAssetRate() internal view returns (uint256) {
74      uint256 assetToPTRate =
75          uint256(LogExpMath.exp(int256(_getMarketLnImpliedRate() * (expiry -
    block.timestamp) / SECONDS_PER_YEAR)));
76
77      return FixedPoint.divDown(WAD, assetToPTRate);
78  }
79
80  /// @notice Returns the USD price of the PT token with 8 decimals
81  function latestRoundData() external view override returns (uint80, int256,
    uint256, uint256, uint80) {
```

```
82      int256 answer = _getValidatedPrice(priceFeed, stalenessPeriod, skipCheck);
83
84      if (expiry > block.timestamp) {
85          answer = int256(FixedPoint.mulDown(uint256(answer), _getPTToAssetRate()));
86      }
87
88      return (0, answer, 0, 0, 0);
89  }
```

Recommendation

Consider using or referencing the official `PendlePYOracleLib` for the implementation:

https://github.com/pendle-finance/pendle-core-v2-public/blob/main/contracts/oracles/PendlePYOracleLib.sol

Status

✓ Fixed

[WP-N2] `priceToSy` may not work properly when the SY's `decimals` don't match the yield-bearing token's `decimals` .

Issue Description

The implementation assumes the amount of `SY` matches exactly the yield-bearing token it wraps, which is not guaranteed.

```
128  if (priceToSy) {
129      answer = int256(FixedPoint.divDown(uint256(answer), syIndex));
130  }
```

Status

ⓘ Acknowledged

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.