morpho-blue-oracles

Security Review

Cantina Managed review by:
Saw-mon-and-Natalie, Lead Security Researcher **Jonah1005**, Lead Security Researcher **StErMi**, Security Researcher

November 14, 2023

Contents

1 Introduction

1.1 About Cantina

Cantina is a security services marketplace that connects top security researchers and solutions with clients. Learn more at cantina.xyz

1.2 Disclaimer

Cantina Managed provides a detailed evaluation of the security posture of the code at a particular moment based on the information available at the time of the review. While Cantina Managed endeavors to identify and disclose all potential security issues, it cannot guarantee that every vulnerability will be detected or that the code will be entirely secure against all possible attacks. The assessment is conducted based on the specific commit and version of the code provided. Any subsequent modifications to the code may introduce new vulnerabilities that were absent during the initial review. Therefore, any changes made to the code require a new security review to ensure that the code remains secure. Please be advised that the Cantina Managed security review is not a replacement for continuous security measures such as penetration testing, vulnerability scanning, and regular code reviews.

1.3 Risk assessment

Severity	Description
Critical	*Must* fix as soon as possible (if already deployed).
High	Leads to a loss of a significant portion (>10%) of assets in the protocol, or significant harm to a majority of users.
Medium	Global losses <10% or losses to only a subset of users, but still unacceptable.
Low	Losses will be annoying but bearable. Applies to things like griefing attacks that can be easily repaired or even gas inefficiencies.
Gas Optimization	Suggestions around gas saving practices.
Informational	Suggestions around best practices or readability.

1.3.1 Severity Classification

The severity of security issues found during the security review is categorized based on the above table. Critical findings have a high likelihood of being exploited and must be addressed immediately. High findings are almost certain to occur, easy to perform, or not easy but highly incentivized thus must be fixed as soon as possible.

Medium findings are conditionally possible or incentivized but are still relatively likely to occur and should be addressed. Low findings a rare combination of circumstances to exploit, or offer little to no incentive to exploit but are recommended to be addressed.

Lastly, some findings might represent objective improvements that should be addressed but do not impact the project's overall security (Gas and Informational findings).

2 Security Review Summary

[PROJECT DESCRIPTION HERE]

From Sep 28th - Oct 16th the Cantina team conducted a review of morpho-blue-oracles on commit hash 9ed193...6f6872. The team identified a total of **3** issues in the following risk categories:

- Critical Risk: 0
- High Risk: 0
- Medium Risk: 0
- Low Risk: 1
- Gas Optimizations: 0
- Informational: 2

3 Findings

3.1 Low Risk

3.1.1 `ChainlinkOracle.constructor` should provide additional sanity checks on the inputs

Severity: Low Risk

Context: ChainlinkOracle.sol#L46-L91

Description: The current implementation of the `ChainlinkOracle constructor` only provides sanity checks for the `vault` and `vaultConversionSample`.

To avoid the deployment of a broken Oracle, Morpho should also provide more sanity checks on the other constructor's parameters:

- at least one feed (`baseFeed1`, `baseFeed2`, `quoteFeed1`, `quoteFeed2`) should not be equal to `address(0)`
- based on the `baseFeed1`, `baseFeed2`, `quoteFeed1`, `quoteFeed2` values, at least one between `baseTokenDecimals` and `quoteTokenDecimals` should not be equal to `0`

Recommendation: Morpho should provide additional sanity checks on the constructor's inputs to avoid the deployment of a broken feed.

Cantina:

The PR `https://github.com/morpho-labs/morpho-blue-oracles/pull/35` reverts the deployment of a `ChainlinkOracle` that has `vaultConversionSample` equal to zero.

Morpho has decided to acknowledge the other suggested changes.

Morpho:

- we think there's a use case for deploying a unit oracle
- the zero base & quote decimals are technically possible and it won't break the oracle

3.2 Informational

3.2.1 Unused endpoints in interfaces can be removed

Severity: Informational

Context:

- AggregatorV3Interface.sol#L9-L16

Description: The endpoints in this context for the relevant `interface` has not been used.

Recommendation: If there is no plan to use these endpoints in the future, it might be best to remove them from the interface to keep the codebase clean.

Morpho:

We acknowledge this issue

3.2.2 Natspec documentation issues: missed parameters, typos or suggested updates

Severity: Informational

Context:

- ChainlinkDataFeedLib.sol#L13-L26
- ChainlinkDataFeedLib.sol#L28-L34
- VaultLib.sol#L6C13-L6C13
- VaultLib.sol#L11-L17

Description: We have found different natspec documentation issues that include missing parameters, typos or in general suggestion to better improve them.

- ChainlinkDataFeedLib.sol#L13-L26: `getPrice` function is missing the `@notice`, `@params` (for all the inputs) and `@return` natspec documentation
- ChainlinkDataFeedLib.sol#L28-L34: `getDecimals` function is missing the `@notice`, `@params` (for all the inputs) and `@return` natspec documentation
- VaultLib.sol#L6C13-L6C13: `VaultLib` natspec `@title` should be changed from `ChainlinkDataFeedLib` to `VaultLib`
- VaultLib.sol#L11-L17: `getAssets` function is missing the `@notice`, `@params` (for all the inputs) and `@return` natspec documentation

Recommendation: Morpho should consider fixing all the listed points to provide a better natspec documentation.

Cantina:

The PR `https://github.com/morpho-org/morpho-blue-oracles/pull/43` correctly rename `VaultLib.sol` contract name to `VaultLib`.

All the remaining recommendations have been acknowledged by Morpho.