CANTINA

Morpho - bundlers-public-allocator Security Review

Cantina Managed review by:
Emanuele Ricci, Lead Security Researcher
Jonah1005, Lead Security Researcher

March 11, 2024

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

Morpho is a lending pool optimizer. It improves the capital efficiency of positions on existing lending pools by seamlessly matching users peer-to-peer.

Morpho's rates stay between the supply rate and the borrow rate of the pool, reducing the interests paid by the borrowers while increasing the interests earned by the suppliers. It means that you are getting boosted peer-to-peer rates or, in the worst case scenario, the APY of the pool. Morpho also preserves the same experience, liquidity and parameters (collateral factors, oracles, ...) as the underlying pool.

From Feb 19th to Feb 23rd the Cantina team conducted a review of morpho-blue-bundlers on commit hash 26fcc30f. The team identified a total of **1** issue in the following risk category:

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

3 Findings

3.1 Informational

3.1.1 NatSpec documentation issues: missed parameters, typos or suggested updates

Severity: Informational

Context: MorphoBundler.sol#L246-L247

Description: Various NatSpec documentation issues were found, that include missing parameters, typos or that allow general suggestions for improval:

- MorphoBundler.sol#L246-L247: In `PublicAllocator.reallocateTo` the `withdrawals` and `supplyMarketParams` parameters have some strict requirements. Items in `withdrawals` must be sorted ASC and not contain duplicates, and the market identified by `supplyMarketParams` must not be contained in the markets listed in `withdrawals`. Given such strict requirements, it's worth documenting them also in the `MorphoBundler.reallocateTo` function as natspec `@dev` comments.

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

Morpho: Acknowledged. The other functions in the bundler do not mention the requirement of the function they are calling. This is because otherwise it would basically add all the requirements and specification of all the contracts that the bundler is calling. So for consistency I think we should not add those comments, but a redirection (in the `README` for example) to the corresponding repositories could serve the same purpose.

Cantina Managed: Acknowledged.