



# Morpho Vault v2 & Blue IRM Security Review

Cantina Managed review by:  
**Om Parikh**, Security Researcher  
**Jonatas martins**, Security Researcher

December 5, 2025

# Contents

<b>1</b>	<b>Introduction</b>	<b>2</b>
1.1	About Cantina . . . . .	2
1.2	Disclaimer . . . . .	2
1.3	Risk assessment . . . . .	2
1.3.1	Severity Classification . . . . .	2
<b>2</b>	<b>Security Review Summary</b>	<b>3</b>
2.1	Scope . . . . .	3
<b>3</b>	<b>Findings</b>	<b>4</b>
3.1	Informational . . . . .	4
3.1.1	Inconsistency in marketIds array when burnShares is called . . . . .	4
3.1.2	Burned shares can't be recovered if market gets back to healthy state again . . . . .	4

DRAFT

# 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](https://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 level	Impact: High	Impact: Medium	Impact: Low
<b>Likelihood: high</b>	Critical	High	Medium
<b>Likelihood: medium</b>	High	Medium	Low
<b>Likelihood: low</b>	Medium	Low	Low

### 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 are 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 trustless and efficient lending primitive with permissionless market creation.

From Nov 24th to Dec 6th the Cantina team conducted a review of [morpho-blue-irm PR 139](#) on commit hash `2bce6da3` (tag `2025-11-24`) and [vault-v2 PR 789](#) on commit hash `169044ef` (tag `2025-11-24`). The team identified a total of **2** issues:

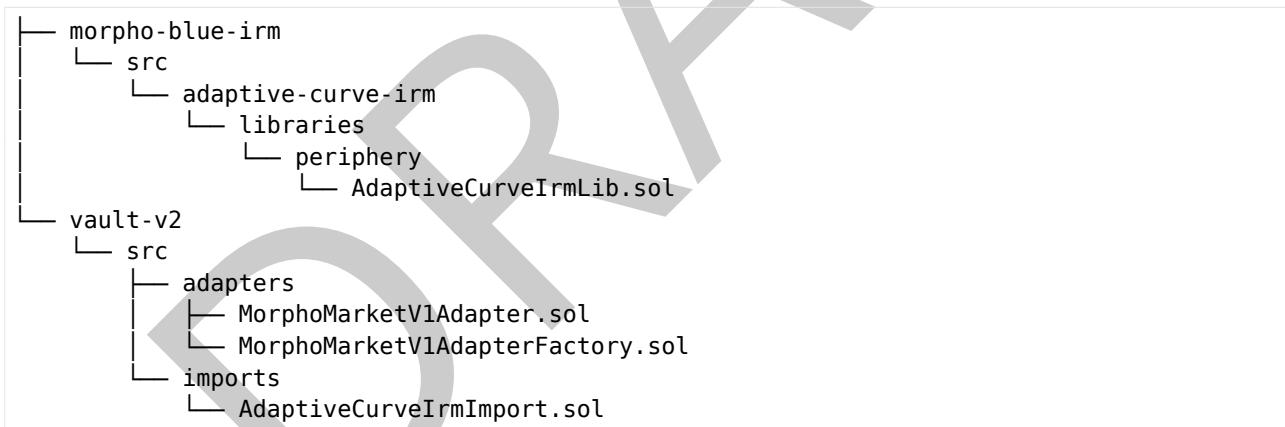
Issues Found

Severity	Count	Fixed	Acknowledged
Critical Risk	0	0	0
High Risk	0	0	0
Medium Risk	0	0	0
Low Risk	0	0	0
Gas Optimizations	0	0	0
Informational	2	1	1
<b>Total</b>	<b>2</b>	<b>1</b>	<b>1</b>

The Cantina Managed team reviewed Morpho's [Morpho vault v2](#) and [blue-irm](#) holistically on commit hash `425f6b1f` (tag `2025-12-04`) and concluded that all findings were addressed and no new vulnerabilities were identified.

### 2.1 Scope

The security review had the following components in scope:



## 3 Findings

### 3.1 Informational

#### 3.1.1 Inconsistency in marketIds array when burnShares is called

**Severity:** Informational

**Context:** MorphoMarketV1Adapter.sol#L105

**Description:** The burnShares function sets supplyShares for a market to zero but does not remove the market from the marketIds array. This creates an inconsistency with the deallocate function, which removes the marketId from the array when the market has no supply.

**Recommendation:** Remove the marketId from the marketIds array to maintain consistency with the deallocate function behavior.

**Morpho:** We don't do it, we think that it's more natural to leave it in deallocate. One would want to call deallocate anyway to update the allocations in the vault.

**Cantina Managed:** Acknowledged.

#### 3.1.2 Burned shares can't be recovered if market gets back to healthy state again

**Severity:** Informational

**Context:** (No context files were provided by the reviewer)

**Description:** When supplied shares for particular morpho market are burned, there is no way to rescue funds or recover funds in case if market gets to healthy state again.

Since morpho shares are not erc20, skimming would not be possible to retrieve them later.

**Recommendation:**

- Consider documenting shares are lost permanently irrespective of market circumstances.
- Add a way to retrieve morpho shares which are burned.

**Morpho:** Fixed in PR 841

**Cantina Managed:** Fix verified.