Stakekit: PR 41

Security Review

Cantina Managed review by:
MostafaYassin, Security Researcher

June 11, 2026

Contents

1 Introduction **2**
1.1 About Cantina . . . 2
1.2 Disclaimer . . . 2
1.3 Risk assessment . . . 2
1.3.1 Severity Classification . . . 2

2 Security Review Summary **3**
2.1 Scope . . . 3

3 Findings **4**
3.1 Informational . . . 4
3.1.1 Public Allocator Entry Points Cannot Be Paused During Emergencies . . . 4

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 level	Impact: High	Impact: Medium	Impact: Low
Likelihood: high	Critical	High	Medium
Likelihood: medium	High	Medium	Low
Likelihood: low	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

From Jun 7th to Jun 8th the Cantina team conducted a review of borrow-allocator on commit hash f616e399. The team identified a total of **1** 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	1	0	1
Total	**1**	**0**	**1**

2.1 Scope

The security review had the following components in scope for borrow-allocator on commit hash f616e399:

```
src/MorphoAllocator.sol
```

3 Findings

3.1 Informational

3.1.1 Public Allocator Entry Points Cannot Be Paused During Emergencies

Severity: Informational

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

Description: `MorphoAllocator` exposes public user entry points for borrowing, supplying loan assets, and supplying collateral, but it does not include an emergency pause mechanism. There is no active exploit path in the current implementation solely from this design choice.

However, the contract is deployed behind an upgradeable proxy, so future upgrades may introduce new behavior or an unforeseen integration issue. Without a pause control, administrators cannot quickly stop user-facing flows while an issue is investigated or a fix is prepared.

Recommendation: Consider adding an emergency pause mechanism, such as OpenZeppelin's `PausableUpgradeable`.

Stakekit: Acknowledged.

Cantina Managed: Acknowledged.