CANTINA

Vsuite PR 180

Security Review

Cantina Managed review by:

Optimum, Lead Security Researcher

Saw-mon And Natalie, Lead Security Researcher
Akshay Srivastav, Security Researcher

May 15, 2025

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

Kiln is a staking platform you can use to stake directly, or whitelabel staking into your product. It enables users to stake crypto assets, manually or programmatically, while maintaining custody of your funds in your existing solution, such Fireblocks, Copper, or Ledger.

From May 13th to May 15th the Cantina team conducted a review of vsuite on commit hash 50ae19d5. 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	1	0
Total	**1**	**1**	**0**

3 Findings

3.1 Informational

3.1.1 Informational Findings

Severity: Informational

Context: vPool.070525_invalid_report.fix.sol#L37, vPool.070525_invalid_report.fix.sol#L179, vPool.070525_invalid_report.fix.sol#L192-L196, vPool.070525_invalid_report.fix.sol#L466

Description:

- vPool.070525_invalid_report.fix.sol?lines=192,195: More checks can be added to check the pre and post lastReport.activatedCount values.
- vPool.070525_invalid_report.fix.sol?lines=179,179: The last return statement is redundant and can be removed.
- vPool.070525_invalid_report.fix.sol?lines=37,37: The exitingSum parameter of ValidatorsReport struct is named as exiting on onchain vPool contract. Consider renaming it.
- vPool.070525_invalid_report.fix.sol?lines=466,466: Natspec comments should be added for _setReportBounds function, specially the @custom:reference tag.

Kiln: Fixed in commit 87cca770.

Cantina Managed: Fixes verified.