Honey
Security Review

Cantina Managed review by:

Noah Marconi, Lead Security Researcher
Ladboy233, Security Researcher

April 9, 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

Berachain is an EVM-identical L1 turning liquidity into security powered by Proof Of Liquidity.

On Apr 4th the Cantina team conducted a review of honey on commit hash PR 605. The team identified a total of **3** 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	3	0	0
Total	**3**	**0**	**0**

3 Findings

3.1 Informational

3.1.1 Trust assumptions around `custodyAddress` account

Severity: Informational

Context: CollateralVault.sol#L324

Description: It's worth noting some of the trust assumptions surrounding the custody account:

- The account will not misappropriate the funds.
- The account will max approve the `CollateralVault` to enable normal operations.
- The account will not move funds to another address without a corresponding update to `setCustodyInfo` occuring to enable the new address.

If the funds in the custody account are transferred out by the account owner, then the invariant check is broken and reverts the asset `deposit`, `withdraw` and `liquidation` transactions.

If more funds are transferred to the custody account, the additional funds that belong to other users can be transferred back to the vault when the admin resets the `_isCustodyVault` flag to `false`.

The above trust assumptions are similar to the trust assumptions surrounding the upgradeability of contracts in the system with one major difference being access control moving from the onchain governance to the custodian and custody client.

3.1.2 Tokens with 0 value transfer restrictions temporarily block `setCustodyInfo` calls

Severity: Informational

Context: CollateralVault.sol#L131

Description: A minor annoyance is possible for tokens that revert on 0 asset transfers. In the case where a custody address holds 0 assets and needs to be removed, the caller would need to send 1 wei in order to set a new `custodyAddress` to get past 0 value transfer restrictions.

3.1.3 Fee on transfer tokens would be problematic

Severity: Informational

Context: CollateralVault.sol#L314-L327

Description: Currently none of the assets are fee on transfer tokens. Any upgradeable token, or token with a fee switch included, would be problematic for the protocol if fee on transfer were to be enabled.

Recommendation: Ensure no fee on transfer token is added to the system. Monitor any upgradeable tokens, or tokens with a fee switch, to ensure fee on transfer is not encountered.