



Infrared contracts PR 600

Security Review

Cantina Managed review by:

MiloTruck, Lead Security Researcher

Cryptara, Security Researcher

May 8, 2025

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 |
| 3 Findings | 4 |
| 3.1 Informational | 4 |
| 3.1.1 Minor improvements to code and comments | 4 |
| 3.1.2 InfraredV1_5.claimExternalVaultRewards() allows anyone to claim rewards on a user's behalf | 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

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 | <i>Must fix as soon as possible (if already deployed).</i> |
| 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

Infrared simplifies interacting with Proof of Liquidity with liquid staking products such as iBGT and iBERA.

From May 6th to May 7th the Cantina team conducted a review of [infrared-contracts](#) on commit hash [cd2bf2bf](#). 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 | 2 | 0 |
| Total | 2 | 2 | 0 |

3 Findings

3.1 Informational

3.1.1 Minor improvements to code and comments

Severity: Informational

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

Context: See below.

Description/Recommendation:

1. `InfraredV1_5.sol#L7-L9` - The `Errors` and `UUPSUpgradeable` imports are unused and can be removed.
2. `RewardsLib.sol#L434` - Typo, `infarred` → `Infrared`.
3. `RewardsLib.sol#L146` - Typo, `recepient` should be `recipient`.

Recommendation: Fixed in commit [e786416](#).

Cantina: Verified.

3.1.2 `InfraredV1_5.claimExternalVaultRewards()` allows anyone to claim rewards on a user's behalf

Severity: Informational

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

Context: `InfraredV1_5.sol#L23-L26`.

Description: `InfraredV1_5.claimExternalVaultRewards()` does not perform any access control checks on `msg.sender`. This allows anyone to claim BGT rewards on behalf of any user, as long as that user has set the `InfraredV1_5` contract as its operator in a vault.

While this does not cause any issues as the iBGT rewards claimed are still sent to the user, it exposes unnecessary risk to the contract.

Recommendation: Consider including access control in `claimExternalVaultRewards()`. For example, only allow the function to be called by the protocol's keeper through the `onlyKeeper` modifier, which would be consistent with reward functionality in previous versions (e.g. `claimBGTIncentives()` in `InfraredV1_4`).

Recommendation: Fixed in commit [69019f8](#).

Cantina: Verified.