Clave Ztake

Security Review

Cantina Managed review by:
Blockdev, Security Researcher
Windhustler, Associate Security Researcher

July 5, 2024

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

Clave is an easy-to-use non-custodial smart wallet powered by Account Abstraction and the Hardware Elements (e.g Secure Enclave, Android Trustzone etc...), offering a unique onboarding process.

From Jun 21st to Jun 25st the Cantina team conducted a review of ZtaKe on commit hash 1790faf4. The team identified a total of **2** issues in the following risk categories:

- Critical Risk: 0
- High Risk: 0
- Medium Risk: 0
- Low Risk: 2
- Gas Optimizations: 0
- Informational: 0

3 Findings

3.1 Low Risk

3.1.1 Insufficient reward balance check

Severity: Low Risk

Context: ZtaKe.sol#L139-L142

Description: As `notifyRewardAmount` gets called to extend the reward finish time, the only check is if the balance of the `ZK` token minus the total staked amount is greater than or equal to the future rewards.

```
require(
    rewardRate * duration <= ZK.balanceOf(address(this)) - totalSupply,
    'reward amount > balance'
);
```

The intended functionality is transferring the needed reward amount of `ZK` token into the `ZtaKe` contract and then calling `notifyRewardAmount`.

However, the contract might contain rewards that belong to some users but have not been withdrawn yet. The balance check is not sufficient to ensure that the transferred rewards are enough to cover everyone.

As a result, the contract might end up in a state where some users are unable to claim their rewards.

Recommendation: Consider using `transferFrom` inside the `notifyRewardAmount` function to immediately transfer the ZK tokens intended for rewards into the `ZtaKe` contract.

Clave: Acknowledged.

Cantina Managed: Acknowledged.

3.1.2 `owner` cannot be updated

Severity: Low Risk

Context: ZtaKe.sol#L12

Description: `owner` cannot be updated after contract deployment. If the private key or access to the owner is at the risk of being stolen, you will not be able to update `owner`.

`owner` has the privilege of withdrawing all the rewards and configuring user and total limit for deposits.

Recommendation: Consider using OpenZeppelin's `Ownable2Step` to manage contract ownership.

Clave: Acknowledged. We are using the contract now, so not a big issue to migrate.

Cantina Managed: Acknowledged.