Tea Token

Security Review

Cantina Managed review by:

Om Parikh, Security Researcher
High Byte, Security Researcher

November 14, 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 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

Tea is a decentralized protocol for open-source developers to capture the value they create.

From Nov 2nd to Nov 4th the Cantina team conducted a review of tea-token on commit hash 9b3e637e. 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	2	2	0
Gas Optimizations	0	0	0
Informational	1	1	0
Total	**3**	**3**	**0**

3 Findings

3.1 Low Risk

3.1.1 Incorrect recovered address when signer's `fallback` function is triggered

Severity: Low Risk

Context: ERC20PermitWithERC1271.sol#L154-L157

Description: If signer has `fallback` when `isValidSignature` function is not present, then it will return arbitrary data and not the magic value. This case returns false correctly. however, the recovered variable would not be correct as it will be the address recovered from ECDSA logic.

Recommendation: Consider explicitly setting `recovered` address to `address(0)`.

```
  try IERC1271(signer).isValidSignature(digest, signature) returns (bytes4 magicValue) {
      if (magicValue == IERC1271.isValidSignature.selector) {
          return (true, address(0));
+     } else {
+         return (false, address(0)); // or recovered = address(0)
      }
  } catch {
      return (false, recovered);
```

Tea.xyz: Fixed in PR 4.

Cantina Managed: Fix verified.

3.1.2 Increase & decrease allowance can be removed

Severity: Low Risk

Context: Tea.sol#L127-L135

Summary: increase & decrease allowance functionalities were removed from openzeppelin for security reasons. hence I recommend to remove them here as well.

Recommendation: unless strictly required, it is advised to conform to modern security standards and also simplify the contract by removing this funcitonality.

Tea.xyz: Fixed in PR 4.

Cantina Managed: Fix verified.

3.2 Informational

3.2.1 Unused structs, variables & imports

Severity: Informational

Context: EIP3009.sol#L30-L77, ERC20PermitWithERC1271.sol#L13-L43, Tea.sol#L19, Tea.sol#L36-L38

Description: At various places linked below, these variables, structs & imports are not used anywhere:

- ERC20PermitWithERC1271.sol#L13-L43.
- EIP3009.sol#L30-L77.
- Tea.sol#L36-L38.
- Tea.sol#L19.

Recommendation: Consider removing them.

Tea.xyz: Fixed in PR 4.

Cantina Managed: Fix verified.