Cyberscope

Audit Report

Tea-Fi

June 2025

Files	TeaFiMysteryBoxManager
Sha256	cd8ce3a55ee5f4b1875ef48c97051b50d456f8528e9b247e9fca9969b2e2fbf4
Audited by	© cyberscope

Table of Contents

Risk Classification

The criticality of findings in Cyberscope's smart contract audits is determined by evaluating multiple variables. The two primary variables are:

1. **Likelihood of Exploitation**: This considers how easily an attack can be executed, including the economic feasibility for an attacker.
2. **Impact of Exploitation**: This assesses the potential consequences of an attack, particularly in terms of the loss of funds or disruption to the contract's functionality.

Based on these variables, findings are categorized into the following severity levels:

1. **Critical**: Indicates a vulnerability that is both highly likely to be exploited and can result in significant fund loss or severe disruption. Immediate action is required to address these issues.
2. **Medium**: Refers to vulnerabilities that are either less likely to be exploited or would have a moderate impact if exploited. These issues should be addressed in due course to ensure overall contract security.
3. **Minor**: Involves vulnerabilities that are unlikely to be exploited and would have a minor impact. These findings should still be considered for resolution to maintain best practices in security.
4. **Informative**: Points out potential improvements or informational notes that do not pose an immediate risk. Addressing these can enhance the overall quality and robustness of the contract.

Severity	Likelihood / Impact of Exploitation
● Critical	Highly Likely / High Impact
● Medium	Less Likely / High Impact or Highly Likely/ Lower Impact
● Minor / Informative	Unlikely / Low to no Impact

Review

Audit Updates

Initial Audit	24 Jun 2025

Source Files

Filename	SHA256
TeaFiMysteryBoxManager.sol	cd8ce3a55ee5f4b1875ef48c97051b50d456f8528e9b247e9fca9969b2e2fbf4
interfaces/ITeaFiMysteryBoxManager.sol	935b1ed5a6a7fc67dbf296e41a0d0439e2ffcb3f02dc98944e48651048c61014

Overview

TeaFiMysteryBoxManager Contract

The `TeaFiMysteryBoxManager` smart contract is a solution for managing and validating the opening of mystery boxes within the TeaFi ecosystem. It incorporates security measures, decentralized execution capabilities, and integrates meta-transaction support, ensuring seamless interaction with blockchain users through trusted forwarders.

openMysteryBox Functionalities

The `openMysteryBox` function is responsible for managing the unlocking of mystery boxes. It validates each operation against predefined criteria and ensures that users do not claim boxes more than once per day. Upon successful validation, the contract records the last claimed day for each user, enhancing both operational efficiency and user experience.

Signature Verification and Security Measures

To maintain security, the contract employs signature verification mechanisms, ensuring that only authorized operators can initiate box openings. Each transaction is securely validated using cryptographic signatures. Additionally, nonce management prevents replay attacks and ensures transaction integrity.

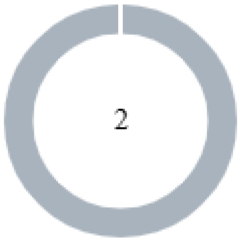
Operator Role and Access Control

The contract uses access control mechanisms to manage operator roles. By assigning the `OPERATOR_ROLE`, the contract restricts access to critical functions, ensuring only authorized operators can perform box openings. This approach safeguards against unauthorized use and maintains operational integrity.

Integration with External Interfaces

The contract supports EIP712 for standardized message signing and verification, enabling smooth interaction with external interfaces. This enhances interoperability and ensures compatibility with other Ethereum-based applications and protocols.

Findings Breakdown



●	Critical	0
●	Medium	0
●	Minor / Informative	2

	Severity	Unresolved	Acknowledged	Resolved	Other
●	Critical	0	0	0	0
●	Medium	0	0	0	0
●	Minor / Informative	2	0	0	0

Diagnostics

● Critical ● Medium ● Minor / Informative

Severity	Code	Description	Status
●	USP	Unused Struct Parameter	Unresolved
●	CCR	Contract Centralization Risk	Unresolved

USP - Unused Struct Parameter

Criticality	Minor / Informative
Location	interfaces/ITeaFiMysteryBoxManager.sol#L30
Status	Unresolved

Description

The struct `OpenBoxParam` has a `receiver` parameter. This address is never used in the contract's functionality or event emission.

```
struct OpenBoxParam {
    //...
    address receiver;
    //...
}
```

Recommendation

Unused parameters should either be removed or utilized in the contract's core functionality.

CCR - Contract Centralization Risk

Criticality	Minor / Informative
Location	TeaFiMysteryBoxManager.sol#L46,47,106
Status	Unresolved

Description

The contract's functionality and behavior are heavily dependent on external parameters or configurations. While external configuration can offer flexibility, it also poses several centralization risks that warrant attention. Centralization risks arising from the dependence on external configuration include Single Point of Control, Vulnerability to Attacks, Operational Delays, Trust Dependencies, and Decentralization Erosion.

```
_grantRole(DEFAULT_ADMIN_ROLE, owner);
_grantRole(OPERATOR_ROLE, operator);
...
if (!hasRole(OPERATOR_ROLE, operator) || operator ==
address(0))
```

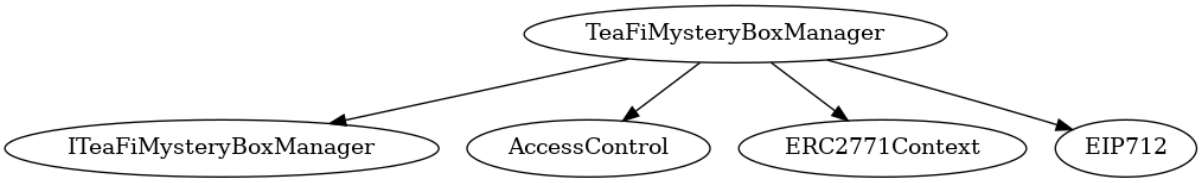
Recommendation

To address this finding and mitigate centralization risks, it is recommended to evaluate the feasibility of migrating critical configurations and functionality into the contract's codebase itself. This approach would reduce external dependencies and enhance the contract's self-sufficiency. It is essential to carefully weigh the trade-offs between external configuration flexibility and the risks associated with centralization.

Functions Analysis

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
TeaFiMysteryBoxManager	Implementation	ITeaFiMysteryBoxManager, AccessControl, ERC2771Context, EIP712		
		Public	✓	ERC2771Context EIP712
	openMysteryBox	External	✓	-
	_validateInput	Private	✓	
	_verifySignature	Internal	✓	
	hashTypedDataV4	External		-
	_msgSender	Internal		
	_msgData	Internal		
	_contextSuffixLength	Internal		
ITeaFiMysteryBoxManager	Interface			
	openMysteryBox	External	✓	-

Inheritance Graph



Summary

Tea-Fi contract implements a utility and rewards mechanism. This audit investigates security issues, business logic concerns and potential improvements.

Disclaimer

The information provided in this report does not constitute investment, financial or trading advice and you should not treat any of the document's content as such. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes nor may copies be delivered to any other person other than the Company without Cyberscope's prior written consent. This report is not nor should be considered an “endorsement” or “disapproval” of any particular project or team. This report is not nor should be regarded as an indication of the economics or value of any “product” or “asset” created by any team or project that contracts Cyberscope to perform a security assessment. This document does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors' business, business model or legal compliance. This report should not be used in any way to make decisions around investment or involvement with any particular project. This report represents an extensive assessment process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk Cyberscope's position is that each company and individual are responsible for their own due diligence and continuous security Cyberscope's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies and in no way claims any guarantee of security or functionality of the technology we agree to analyze. The assessment services provided by Cyberscope are subject to dependencies and are under continuing development. You agree that your access and/or use including but not limited to any services reports and materials will be at your sole risk on an as-is where-is and as-available basis Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives false negatives and other unpredictable results. The services may access and depend upon multiple layers of third parties.

About Cyberscope

Cyberscope is a blockchain cybersecurity company that was founded with the vision to make web3.0 a safer place for investors and developers. Since its launch, it has worked with thousands of projects and is estimated to have secured tens of millions of investors' funds.

Cyberscope is one of the leading smart contract audit firms in the crypto space and has built a high-profile network of clients and partners.

The Cyberscope team

cyberscope.io