

Smart Contract Security Assessment

Final Report

Sacabam Token

19 December 2023

Table of contents

Table of contents

Disclaimer

1. Overview

- 1.1 Summary
- 1.2 Contract Assessed
- 1.3 Audit Summary
- 1.4 Vulnerability Summary
- 1.5 Audit Scope

2. Findings

- 1.1 SCB-01 | Initial Token Distribution
- 1.2 SCB-02 | Token Ownership

1 Overview

This report has been prepared for Sacabam on the SUI Blockchain. SotaTek provides a user-centered examination of smart contracts to look for vulnerabilities, logic errors or other issues from both an internal and external perspective.


A comprehensive examination has been performed, utilizing Cross Referencing, Static Analysis, In-House Security Tools, and line-by-line Manual Review. The auditing process pays special attention to the following considerations:

- Ensuring contract logic meets the specifications and intentions of the client without exposing the user's funds to risk.
- Testing the smart contracts against both common and uncommon attack vectors.
- Inspecting liquidity and holders' statistics to inform the status to both users and client when applicable.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Verifying contract functions that allow trusted and/or untrusted actors to mint, lock, pause, and transfer assets.
- Thorough line-by-line manual review of the entire codebase by industry experts.

1.1 Summary

Project Name	Sacabam
Type	Token
Platform	Sui Blockchain
Language	Move
Auditors	SotaTek
Timeline	December 10, 2023 – December 19, 2023
Description	Sui Blockchain Native Memecoin

1.2 Contracts Assessed

Name	Contract	Live Code Match
Sacabam	0x9a5502414b5d51d01c8b5641db7436d789fa15a245694b24aa37c25c2a6ce001	

1.3 Audit Summary

Delivery Date	December 18, 2023
Audit Methodology	Static Analysis, Manual Review
URL	https://github.com/Sacabam-Fun/Token-Contract
Commit	d16a7d221590cae1508c7e6af018df5a81653b7d

1.4 Vulnerability Summary

Vulnerability	Total	Pending	Resolved	Acknowledged
Critical	0	0	0	0
Major	0	0	0	0
Medium	1	0	0	1
Informational	0	1	0	1

Classification Of Issues

Severity	Description
Critical	Exploits, vulnerabilities, or errors that will certainly or probabilistically lead towards loss of funds, control, or impairment of the contract and its functions. Issues under this classification are recommended to be fixed with utmost urgency.
Major	Bugs or issues with that may be subject to exploitation, though their impact is somewhat limited. Issues under this classification are recommended to be fixed as soon as possible
Medium	Effects are minimal in isolation and do not pose a significant danger to the project or its users. Issues under this classification are recommended to be fixed nonetheless.
Informational	Consistency, syntax, or style best practices. Generally, pose a negligible level of risk, if any.

1.5 Audit Scope

Delivery Date	December 18, 2023
Audit Methodology	Static Analysis, Manual Review

The following files were made available during the review:

- scb.move

2 Finding

1.1 SCB-01 | Initial Token Distribution

Category	Severity	Location	Status
Centralization / Privilege	Medium	https://github.com/Sacabam-Fun/Token-Contract/blob/d16a7d221590cae1508c7e6af018df5a81653b7d/sources/scb.move#L10	Acknowledged

Description

20B of the 68B max supply is sent to the contract deployer when deploying the contract. This could be a centralization risk as the deployer can distribute XCN tokens without obtaining the consensus of the community.

Recommendation

We recommend the team to be transparent regarding the initial token distribution process, and the team should make enough efforts to restrict the access of the private key.

1.2 SCB-02 | Ownership Issues

Category	Severity	Location	Status
Centralization / Privilege	Information	https://github.com/Sacabam-Fun/Token-Contract/blob/d16a7d221590cae1508c7e6af018df5a81653b7d/sources/scb.move#L10	Acknowledged

Description

Token contracts are owned by normal address. Token contracts should be owned by Governance or Timelock Contract or related like multi-signature contract.

Recommendation

We recommend increasing the security of token contracts by transferring ownership to another delayed action contracts or something similar.

Consider setting the ownership of the contract behind a sufficiently long Timelock, ideally 1 day. This would allow users to monitor the Timelock and react accordingly should this function be queued.

Appendix

Finding Categories

Centralization / Privilege

Centralization / Privilege findings refer to either feature logic or implementation of components that act against the nature of decentralization, such as explicit ownership or specialized access roles in combination with a mechanism to relocate funds.

Logical Issue

Logical Issue findings detail a fault in the logic of the linked code.

Volatile Code

Volatile Code findings refer to segments of code that behave unexpectedly on certain edge cases that may result in a vulnerability.

Language Specific

Language Specific findings are issues that would only arise within Solidity, i.e., incorrect usage of private or deleted.