YouSUI
Smart Contract
Audit Report

MOVEBIT

contact@movebit.xyz

https://twitter.com/movebit_

05/23/2023

YouSUI Smart Contract Audit Report

1 Executive Summary

1.1 Project Information

Description	A standard coin on Sui.
Type	Token
Auditors	MoveBit
Timeline	May 18, 2023 – May 19, 2023
Languages	Move
Platform	Sui
Methods	Architecture Review, Unit Testing, Manual Review
Source Code	https://github.com/splabs-info/yousui_contract
Commits	0dffe7cbbd3922e9fd4012af38de89094cede48f 0e2d16e0906c152d32e223d162d89a441e1ac943 d08023716f85c40c9d8543c5ca0b4728c8e20568 375e0e19b8b1b1671b38c0df8c37b69877b5b9bf

1.2 Files in Scope

The following are the SHA1 hashes of the last reviewed files.

ID	Files	SHA-1 Hash
XUI	token/sources/xui.move	531ccb4a588c2138c68b4266e73d705e69d263fa

1.3 Issue Statistic

Item	Count	Fixed	Acknowledged
Total	2	1	1
Informational			
Minor			
Medium	1	1	
Major	1		1
Critical			

1.4 MoveBit Audit BreakDown

MoveBit aims to assess repositories for security-related issues, code quality, and compliance with specifications and best practices. Possible issues our team looked for included (but are not limited to):

- Transaction-ordering dependence
- Timestamp dependence
- Integer overflow/underflow by bit operations
- Number of rounding errors
- Denial of service / logical oversights
- Access control
- Centralization of power
- Business logic contradicting the specification
- Code clones, functionality duplication
- Gas usage
- Arbitrary token minting
- Unchecked CALL Return Values
- The flow of capability
- Witness Type

1.5 Methodology

The security team adopted the "**Testing and Automated Analysis**", "**Code Review**" and "**Formal Verification**" strategy to perform a complete security test on the code in a way that is closest to the real attack. The main entrance and scope of security testing are stated in the conventions in the "Audit Objective", which can expand to contexts beyond the scope according to the actual testing needs. The main types of this security audit include:

(1) Testing and Automated Analysis

Items to check: state consistency / failure rollback / unit testing / value overflows / parameter verification / unhandled errors / boundary checking / coding specifications.

(2) Code Review

The code scope is illustrated in section **1.2**.

(3) Formal Verification

Perform formal verification for key functions with the Move Prover.

(4) Audit Process

- Carry out relevant security tests on the testnet or the mainnet;
- If there are any questions during the audit process, communicate with the code owner in time. The code owners should actively cooperate (this might include providing the latest stable source code, relevant deployment scripts or methods, transaction signature scripts, exchange docking schemes, etc.);
- The necessary information during the audit process will be well documented for both the audit team and the code owner in a timely manner.

2 Summary

This report has been commissioned by **SPLabs** to identify any potential issues and vulnerabilities in the source code of the **YouSUI** smart contract, as well as any contract dependencies that were not part of an officially recognized library. In this audit, we have utilized various techniques, including manual code review and static analysis, to identify potential vulnerabilities and security issues.

During the audit, we identified **2** issues of varying severity, listed below.

ID	Title	Severity	Status

XUI-01	Centralization Risk	Major	Acknowledged
XUI-02	Inappropriate transfer of metadata during `XUI` coin registration.	Medium	Fixed

3 Participant Process

Here are the relevant actors with their respective abilities within the **`YouSUI`** Smart Contract:

Deployer

- Deployer can mint unlimited `XUI` through `coin::mint()`.

4 Findings

XUI-01 Centralization Risk

Severity: Major

Status: Acknowledged
Code Location: token/sources/xui.move
Descriptions: There is a risk of centralization, with privileged accounts able to mint unlimited tokens and burn their token.
Suggestion: It is recommended that multi-signature accounts should be set as privileged accounts.

Resolution: The client responded that they need to burn tokens so they decided to keep the `treasury_cap`.

XUI-02 Inappropriate Transfer of Metadata During `XUI` Coin Registration.

Severity: Medium

Status: Fixed
Code Location: token/sources/xui.move

Descriptions: The metadata of registering `XUI` coins should be frozen instead of transferred, which does not comply with the process of registering coins on Sui.
Suggestion: Freeze metadata.

Resolution: The client has followed our suggestion and fixed the issue.

Appendix 1

Issue Level

- **Informational** issues are often recommendations to improve the style of the code or to optimize code that does not affect the overall functionality.
- **Minor** issues are general suggestions relevant to best practices and readability. They don't post any direct risk. Developers are encouraged to fix them.
- **Medium** issues are non-exploitable problems and not security vulnerabilities. They should be fixed unless there is a specific reason not to.
- **Major** issues are security vulnerabilities. They put a portion of users' sensitive information at risk, and often are not directly exploitable. All major issues should be fixed.
- **Critical** issues are directly exploitable security vulnerabilities. They put users' sensitive information at risk. All critical issues should be fixed.

Issue Status

- **Fixed:** The issue has been resolved.
- **Partially Fixed**: The issue has been partially resolved.
- **Acknowledged:** The issue has been acknowledged by the code owner, and the code owner confirms it's as designed, and decides to keep it.

Appendix 2

Disclaimer

This report is based on the scope of materials and documents provided, with a limited review at the time provided. Results may not be complete and do not include all vulnerabilities. The review

and this report are provided on an as-is, where-is, and as-available basis. You agree that your access and/or use, including but not limited to any associated services, products, protocols, platforms, content, and materials, will be at your own risk. A report does not imply an endorsement of any particular project or team, nor does it guarantee its security. These reports should not be relied upon in any way by any third party, including for the purpose of making any decision to buy or sell products, services, or any other assets. TO THE FULLEST EXTENT PERMITTED BY LAW, WE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, IN CONNECTION WITH THIS REPORT, ITS CONTENT, RELATED SERVICES AND PRODUCTS, AND YOUR USE, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NOT INFRINGEMENT.