Balanced

Audit Report

contact@bitslab.xyz

https://twitter.com/movebit_

Tue Aug 06 2024

Balanced Audit Report

1 Executive Summary

1.1 Project Information

Description	The Balanced package within the Sui blockchain ecosystem is designed to manage various aspects of the decentralized application (dApp) including asset management, cross-chain communication, and stablecoin operations.
Type	Bridge
Auditors	MoveBit
Timeline	Wed Jul 10 2024 - Tue Aug 06 2024
Languages	Move
Platform	Sui
Methods	Architecture Review, Unit Testing, Manual Review
Source Code	https://github.com/balancednetwork/balanced-move-contracts https://github.com/icon-project/xcall-multi
Commits	https://github.com/balancednetwork/balanced-move-contracts: faf4c7196839a9e50a160843e61997cf5607bbaa2409cca0dd817d161d29d66a6ab5afe107360d58 https://github.com/icon-project/xcall-multi: 7a180af338292da6ae1b3ce9fcd7721ebd5b4ec2ba4eb0dce08a62c2a2a16cefbafd67733b6fdec1

1.2 Files in Scope

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

ID	File	SHA-1 Hash
BDO	balanced_dollar/sources/balanced_dollar.move	8d622a253d6dcbdca7726c683651c63713470cf3
CTR	sources/messages/cross_transfer.move	17efa828f45b07855de5732d1264ab0d554a95ee
CPR	sources/messages/configure_protocol.move	df378e8df29c51e629121b32e1c3c30eadb0d3d6
DRE	sources/messages/deposit_revert.move	547c11e3ba47ba63a0ec78ab80b8648dc2ce5570
CTR1	sources/messages/cross_transfer_revert.move	a8166ab4e55afb00d71d9c87f7f6b598cac03ed8
WTO	sources/messages/withdraw_to.move	d81c7d50378b0518aa8dc0a81c992947db2cc8bc
EXE	sources/messages/execute.move	35af014a14660179c1ecd4bd4073052ee3a8b258
DEP	sources/messages/deposit.move	6a63c19f7e6a7a2216fa4562eb508f011c604596
BDC	sources/balanced_dollar_crosschain.move	6638e21ebed3a896460e7c53322a99042271a343
XMA	sources/xcall_manager.move	f961fc3b63c84b17ee098229e9b190d91fb1ab51
UTI	sources/utils.move	43de6ba33cedef97e2e773d4014e1283dc9f7f5d

AMA	sources/asset_manager.move	916e69e2cb809f5e294c2797ed0898bb903beec3
ENC	contracts/sui/libs/sui_rlp/sources/encoder.move	d076b0dd4766c2fbf3abf0f5be2af5e108b8e09f
DEC	contracts/sui/libs/sui_rlp/sources/decoder.move	48a2a65f103463975df69ff55d9a6bbc9fe50834
UTI	contracts/sui/libs/sui_rlp/sources/utils.move	3d8913de9703e1d6f067d6747a46e96d1bd1e58f
CON	contracts/sui/xcall/sources/connections.move	a0cd3be4bdfc2833066a99ac7f2db428829c185c
MRE	contracts/sui/xcall/sources/types/message_result.move	fb3d682fab5831595d4c7789ec11ed4130d73cd5
CME	contracts/sui/xcall/sources/types/cs_message.move	c0dba1eec486c2b7bac8b9ff4783b78914079187
NAD	contracts/sui/xcall/sources/types/network_address.move	6098e0d668873954e985432e2f718b549bf9c25d
RTI	contracts/sui/xcall/sources/types/rollback_ticket.move	a15db4f2a6da61705eca6b6944c0d56cd46ff78a
ETI	contracts/sui/xcall/sources/types/execute_ticket.move	54caa30bf049de50ff718a2e107a29fd28848ce7
RDA	contracts/sui/xcall/sources/types/rollback_data.move	3f7942bc3b6791c5f19cb7bcf01af6525189a8e5
MRE1	contracts/sui/xcall/sources/types/message_request.move	a25b61dbf40dbb79f63ea613d9ea01d852c548a2
PME	contracts/sui/xcall/sources/messages/persistent_message.move	c9c9653b6a136ea70ec668e2a74e0a4891ffdd8c

ENV	contracts/sui/xcall/sources/messages/envelope.move	e395a3014a048ad47d18e906a604756213917116
CME1	contracts/sui/xcall/sources/messages/call_message.move	a05937b6f8fc29c88b8f4cbad0d964db3af43137
CMR	contracts/sui/xcall/sources/messages/call_message_rollback.move	eddfaeb5a4efe66b543414ce79060d6e7c099719
CEN	contracts/sui/xcall/sources/centralized_connection/centralized_entry.move	739c7f3a1d51eaf3cb7a7efef3dedb414a57bd75
CCO	contracts/sui/xcall/sources/centralized_connection/centralized_connection.move	c4060e54e38184cdcb0359b22f9c5bcf212d89b9
CST	contracts/sui/xcall/sources/centralized_connection/centralized_state.move	f1063290a2b343c189f420a07eb244b026b9b6fd
MAI	contracts/sui/xcall/sources/main.move	ab0a35d23547bd0474a524c8c9b8ac0c3dab03f0
XST	contracts/sui/xcall/sources/states/xcall_state.move	07bdd79cdcb5a130d32183914ea3d1a9775454c9
UTI1	contracts/sui/xcall/sources/utils.move	358496f2e4a9858952789e4554a1baa32e427d4d

1.3 Issue Statistic

Item	Count	Fixed	Acknowledged
Total	8	7	1
Informational	1	1	0
Minor	3	2	1
Medium	2	2	0
Major	2	2	0
Critical	0	0	0

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 Balanced to identify any potential issues and vulnerabilities in the source code of the Balanced 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 8 issues of varying severity, listed below.

ID	Title	Severity	Status
AMA-1	`send_call` Issue	Major	Fixed
AMA-2	Some Functions Missing Version Checks	Medium	Fixed
AMA-3	`calculate_limit` Calculation Problem	Minor	Fixed
AMA-4	Meaningless Calculation	Informational	Fixed
BDO-1	Lack of Events Emit	Minor	Acknowledged
CME-1	Missing `test_only` Modifier	Medium	Fixed
EXE-1	`execute decode` Function Problem	Minor	Fixed
XST-1	Functions Return Mutable References Directly	Major	Fixed

3 Participant Process

Here are the relevant actors with their respective abilities within the Balanced Smart Contract :

Owner

- The owner can call the `register_token` function to register an wrapper token.
- The owner can call the `configure_rate_limit` to set token rate.
- The owner can call the `whitelist_action` function to set the whitelist action.
- The owner can use the `configure` function to set global config.

User

- Users can call the `deposit` function to send deposit message.
- Users can call the `execute_call` to execute the message.
- Users can call the `execute_rollback` to execute the message which is fail.
- Users can call the `cross_transfer` to send cross transfer message.

4 Findings

AMA-1 `send_call` Issue

Severity: Major

Status: Fixed

Code Location:

sources/asset_manager.move;

sources/balanced_dollar_crosschain.move

Descriptions:

The various `wrap_*` methods are public and the user can construct any parameter they want and due to `idcap` is public function, user can get the config's `idcap` from the function, then construct the envelope and bypassing the deposit coin to the AssetManager, fianlly user can call the `send_call` method directly.

Suggestion:

It is recommended to change `idcap` to a package function.

AMA-2 Some Functions Missing Version Checks

Severity: Medium

Status: Fixed

Code Location:

sources/asset_manager.move#114-118;

sources/balanced_dollar_crosschain.move#89 93;

sources/xcall_manager.move#93 97

Descriptions:

There is no version checking when calling the functions for example `get_xcall_manager_id` function, so when the object is upgraded or the code of those functions is modified, the user can still call the old function to deposit profit which may lead to unexpected results.

Suggestion:

It is recommended to add a version check.

AMA-3 `calculate_limit` Calculation Problem

Severity: Minor

Status: Fixed

Code Location:

sources/asset_manager.move#187

Descriptions:

There is an issue with the comparison of `rate_limit.current_limit` and `allowed_withdrawal` in the `calculate_limit` calculation which may cause incorrect update of limit.

Suggestion:

It is recommended to change to correct logic.

AMA-4 Meaningless Calculation

Severity: Informational

Status: Fixed

Code Location:

sources/asset_manager.move#146

Descriptions:

There are meaningless calculations in the `register_token` function when creating `current_limit` in RateLimit, `current_limit` defaults to 0. Since the number of balances in the first `AssetManager` creation is 0, the result of the current_limit `calculation` will still be 0.

Suggestion:

It is recommended to remove the meaningless calculations.

BDO-1 Lack of Events Emit

Severity: Minor

Status: Acknowledged

Code Location:

balanced_dollar/sources/balanced_dollar.move#25;

sources/xcall_manager.move;

sources/asset_manager.move

Descriptions:

The contract lacks appropriate events for monitoring sensitive operations, which could make it difficult to track sensitive actions or detect potential issues. For example, when receiving message `WithdrawMsg` , `Withdraw all` and `MinBalanceMsg` .

Suggestion:

It is recommended to emit events for those important functions.

CME-1 Missing `test_only` Modifier

Severity: Medium

Status: Fixed

Code Location:

contracts/sui/xcall/sources/types/cs_message.move#83;

contracts/sui/xcall/sources/types/network_address.move#63

Descriptions:

If the `test_only` modifier is missing, the test code will be compiled into the bytecode of the module. The modifier is not only needed for functions but also for test modules.

Suggestion:

It is recommended to add modifiers to the test module.

EXE-1 `execute decode` Function Problem

Severity: Minor

Status: Fixed

Code Location:

sources/messages/execute.move#26

Descriptions:

When deserializing `warp_execute` in the decode function, the data is incorrectly obtained from `decoder::decode(vector::borrow(&decoded, 4));` , but Execute has only two fields, which causes decoding to fail.

Suggestion:

It is recommended to change to the correct decode logic.

Resolution:

The client removed this piece of code.

XST-1 Functions Return Mutable References Directly

Severity: Major

Status: Fixed

Code Location:

contracts/sui/xcall/sources/states/xcall_state.move#235

Descriptions:

Return mutable variables in a module by a public function are usually considered dangerous if the associated modifier function exists and the user can modify the object at will.

Suggestion:

It is recommended to change the permissions of the function to `package`.

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.