MMT Finance CLMM

Audit Report

MOVEBIT

✉ contact@bitslab.xyz

https://twitter.com/movebit_

Fri Feb 28 2025

MMT Finance CLMM Audit Report

1 Executive Summary

1.1 Project Information

Description	Move contracts for clmm.
Type	DEX
Auditors	MoveBit
Timeline	Mon Feb 17 2025 - Fri Feb 28 2025
Languages	Move
Platform	Sui
Methods	Architecture Review, Unit Testing, Manual Review
Source Code	https://github.com/mmt-finance/core-contract/
Commits	44c2a59d0b129cb4536528e0b43b0726427b8397 51df090a96a534da34e907fc3cf0fc715295b297

1.2 Files in Scope

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

ID	File	SHA-1 Hash
MOV	contracts/clmm/move.toml	e0f69505d4c1f9d46513887e407098accbb82d10
SMA	contracts/clmm/sources/utils/swap_math.move	a41c40c18b93bf385c2b184072dcae2b199e87a8
LMA	contracts/clmm/sources/utils/liquidity_math.move	da0c20339e7f5b133c4a0c139e92ec839ddc8897
CON	contracts/clmm/sources/utils/constants.move	8ac1c8fb8cd53a8f2debe2ec080b52616361a715
COM	contracts/clmm/sources/utils/comparator.move	7492134f2e8f389d8a61c55cd25e78ee06175157
SPM	contracts/clmm/sources/utils/sqrt_price_math.move	c2b44da04ec253fdf79a402d305b06cd0f7117c2
ORA	contracts/clmm/sources/utils/oracle.move	06cf84379f4f91f450e16ae75f1f8c2cfde39526
UTI	contracts/clmm/sources/utils/utils.move	37d7b68be4cb01cfa716c442605c72452ffe3bc8
BMA	contracts/clmm/sources/utils/bit_math.move	597b417598ffe3854ad145008dede97b9f7a9bab
TMA	contracts/clmm/sources/utils/tick_math.move	9a4dc9333f6ca5cacebf3f72eed323b265ad970a
ADM	contracts/clmm/sources/actions/admin.move	16db914eae03d13821702a6dcbec519eed569a12

TRA	contracts/clmm/sources/actions/trade.move	09274964f73d4c31ee621fe7998432a1c079f1eb
LIQ	contracts/clmm/sources/actions/liquidity.move	9b992aad2d517d18d5e486eaaeb7fb5c62f8128f
COL	contracts/clmm/sources/actions/collect.move	3f2dcf07e71f593f0b65eacc35611429440377e0
CPO	contracts/clmm/sources/actions/create_pool.move	1268613b57fe2a0ed6d6d1b398f7b729f5e3c9e0
MU2	contracts/clmm/sources/integer-mate/math_u256.move	eb4716bc638c0d659379fbf4861815c38a5fc745
MU1	contracts/clmm/sources/integer-mate/math_u128.move	2af22e4216db18f4652a6ec603e9ea4566e1a0d4
FMU6	contracts/clmm/sources/integer-mate/full_math_u64.move	0e3d6f23bc3cf31365eafddeb245168a174708e0
FMU1	contracts/clmm/sources/integer-mate/full_math_u128.move	d419157097cec362605f7a9a352e06878fb536d8
I32	contracts/clmm/sources/integer-mate/i32.move	88a81906d82e1f9e3d8f3176b4295ab19b0b40b5
I12	contracts/clmm/sources/integer-mate/i128.move	932eb48697485eb34d5d9edbb7113bee1249f8a4
I64	contracts/clmm/sources/integer-mate/i64.move	62544d24cdeb852be58965c5ef1f4c09d068456d
MU6	contracts/clmm/sources/integer-mate/math_u64.move	87339b525a68a62c177f82d1084209b294b922f4
POS	contracts/clmm/sources/storage/position.move	910763fe040277aded593c481319cea53081a7d5

GCO	contracts/clmm/sources/storage/global_config.move	950bd0e70a8c27fccd99b79af56058e4fc12151e
TBI	contracts/clmm/sources/storage/tick_bitmap.move	e95caf5595933e16585d2a0d024b8b76b78409c4
POO	contracts/clmm/sources/storage/pool.move	aff6b769f9e8c198b7bf1df0c98c878ad78f68f1
TIC	contracts/clmm/sources/storage/tick.move	0f766b0d0abec653295f1bb751ea514543d02952
ERR	contracts/clmm/sources/error.move	cd7ab57f2c92e118ce739a194e311005f1efb929
APP	contracts/clmm/sources/app.move	2f413170bb41b408a23ddc2a815758f0c7cdb158
CVE	contracts/clmm/sources/version/current_version.move	8b718d67355e4866f3082b3b48e41632b9354066
VER	contracts/clmm/sources/version/version.move	98c83e32408eba3110a0cab2abf5afa7d0d1b4d4

1.3 Issue Statistic

Item	Count	Fixed	Acknowledged
Total	2	2	0
Informational	0	0	0
Minor	2	2	0
Medium	0	0	0
Major	0	0	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(Optional)

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 MMT Finance to identify any potential issues and vulnerabilities in the source code of the MMT Finance CLMM 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
APP-1	Lack of Events Emit	Minor	Fixed
CPO-1	Missing Pool Token Type Check	Minor	Fixed

3 Participant Process

Here are the relevant actors with their respective abilities within the MMT Finance CLMM Smart Contract :

Admin

- The `Admin` can add and initialize a reward to a pool through `initialize_pool_reward()` .
- The `Admin` can collect protocol fee from a pool through `collect_protocol_fee()` .
- The `Admin` can extend the period of a reward of a pool through `add_seconds_to_reward_emission()` .
- The `Admin` can add more reward to a pool through `add_balance_to_reward_emission()` .
- The `Admin` can set the protocol fee rate through `set_protocol_fee_rate()` .
- The `Admin` can grow the observations through `increase_observation_cardinality_next()` .

User

- The `User` can withdraw coins from owned position through `fee()` .
- The `User` can claim rewards from owned position through `reward()` .
- The `User` can open a position through `open_position()` .
- The `User` can close a position when it is empty through `close_position()` .
- The `User` can remove liquidity through `remove_liquidity()` .
- The `User` can add liquidity through `add_liquidity()` .
- The `User` can swap tokens and get a swap receipt through `flash_swap()` .
- The `User` can repay swap receipt through `repay_flash_swap()` .
- The `User` can get a flash loan and get a flashloan receipt through `flash_loan()` .
- The `User` can repay a flashloan receipt through `repay_flash_loan()` .

4 Findings

APP-1 Lack of Events Emit

Severity: Minor

Status: Fixed

Code Location:

contracts/clmm/sources/app.move#26,31;

contracts/clmm/sources/storage/global_config.move#253,278

Descriptions:

Some functions in the contract lacks appropriate events for monitoring operations, which could make it difficult to track sensitive actions or detect potential issues.

Suggestion:

It is recommended to emit events for the function.

Resolution:

This issue has been fixed. The client has adopted our suggestions.

CPO-1 Missing Pool Token Type Check

Severity: Minor

Status: Fixed

Code Location:

contracts/clmm/sources/actions/create_pool.move#27

Descriptions:

When creating a pool, the token type is not checked, which allows pools with the same token type to be created.

Suggestion:

It is recommended to ensure that this is in accordance with the protocol design.

Resolution:

This issue has been fixed. The client has adopted our suggestions.

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.

MOVEBIT VERIFIED

MOVEBIT