MOVEBIT
Securing the Move Ecosystem

Cetus Concentrated Liquidity Protocol Sui Contract **Audit Report**

https://twitter.com/movebit_

contact@movebit.xyz

Cetus Concentrated Liquidity Protocol Sui Contract Audit Report

1 Executive Summary

1.1 Project Information

Type	DEX
Auditors	MoveBit
Timeline	Mar 27, 2023 – Apr 28, 2023
Languages	Move
Platform	Sui
Methods	Architecture Review, Unit Testing, Manual Review
Source Code	https://github.com/CetusProtocol/cetus-clmm-sui
Commits	11d65f5da993bf0bbc06cfd6591f833a10b842fd 0f6514e922fd9aed0efe9b0bfb57e348de534c0e

1.2 Issue Statistic

Item	Count	Fixed	Acknowledged
Total	18	18	
Minor	12	12	
Medium	3	3	

Major	2	2	
Critical	1	1	

1.3 Issue Level

- **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.

1.4 Issue Status

- **Fixed:** The issue has been 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.

2 Summary of Findings

Cetus is a pioneer DEX and concentrated liquidity protocol built on the Sui and Aptos blockchain. The mission of Cetus is to build a powerful and flexible underlying liquidity network to make trading easier for any users and assets. It focuses on delivering the best trading experience and superior liquidity efficiency to DeFi users through the process of building its concentrated liquidity protocol and a series of affiliate interoperable functional modules.

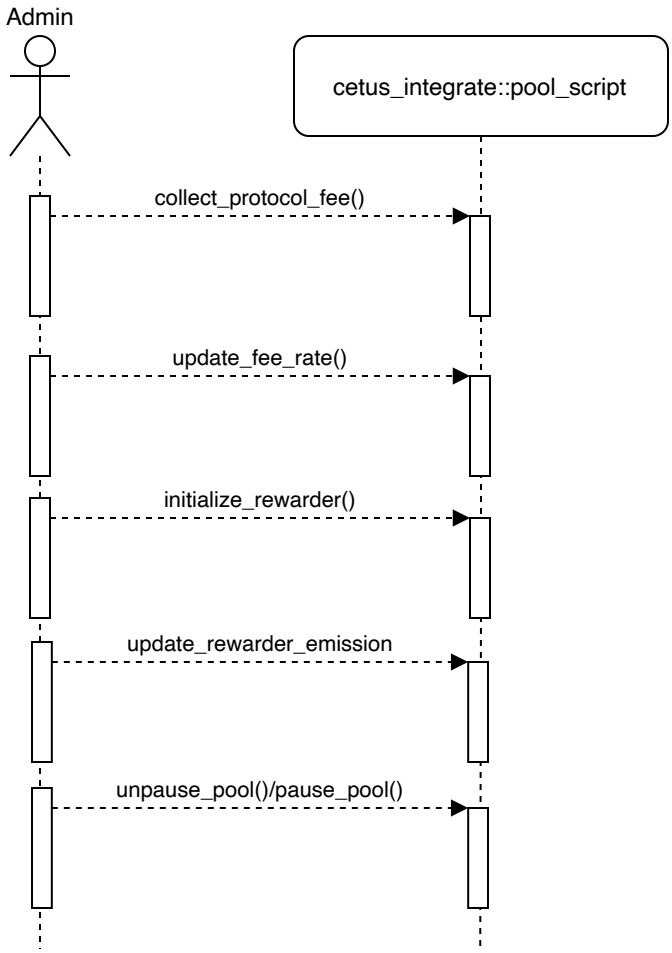
Our team mainly focused on reviewing the code security and normative. During the testing process, our team also maintains close communication with the project team to ensure that we have a correct understanding of business requirements. As a result, our team found a total of **18** issues. The audit and project teams discussed these issues together, and the project solved and confirmed all the issues.

3 Participant Process

Here are the relevant actors with their respective abilities within the `CetusCLMM` SmartContract :

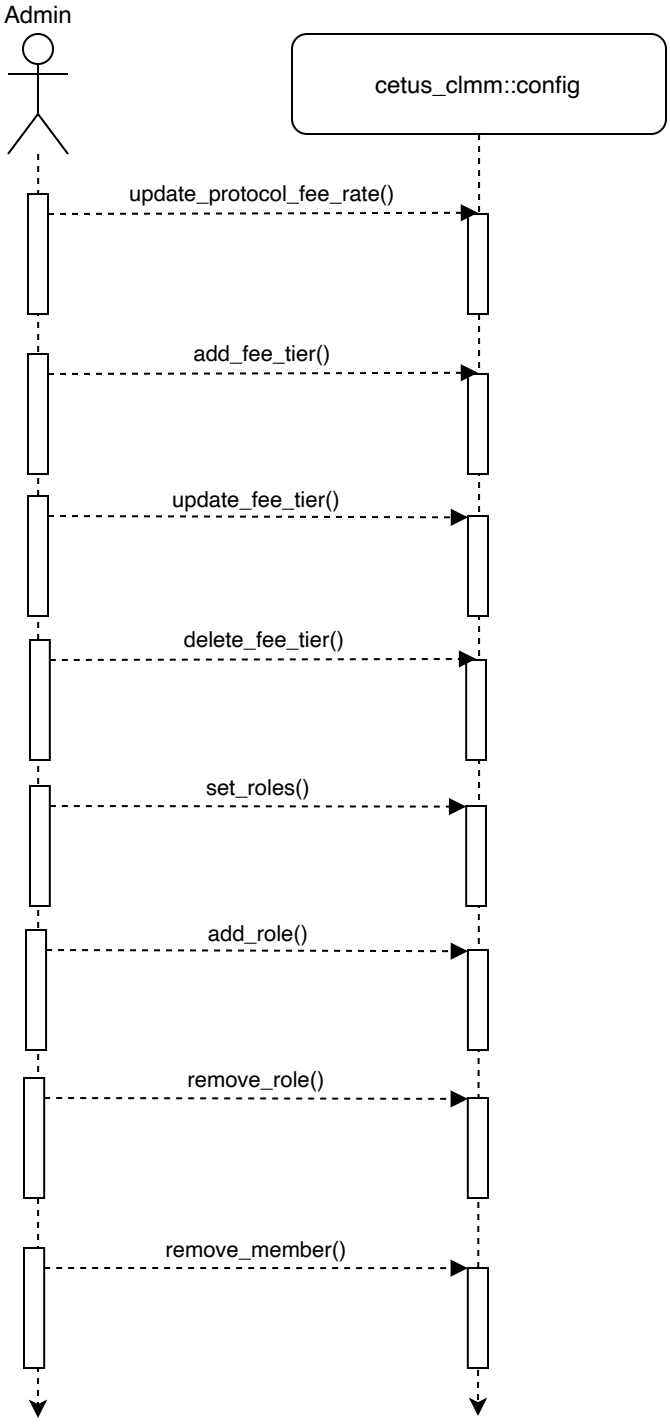
Admin

- Admin can `collect_protocol_fee`
- Admin can `update_fee_rate`
- Admin can `initialize_rewarder`
- Admin can `update_rewarder_emission`
- Admin can `pause_pool` / `unpause_pool`



- Admin can `update_protocol_fee_rate`
- Admin can `add_fee_tier`
- Admin can `delete_fee_tier`
- Admin can `update_fee_tier`
- Admin can `set_roles`

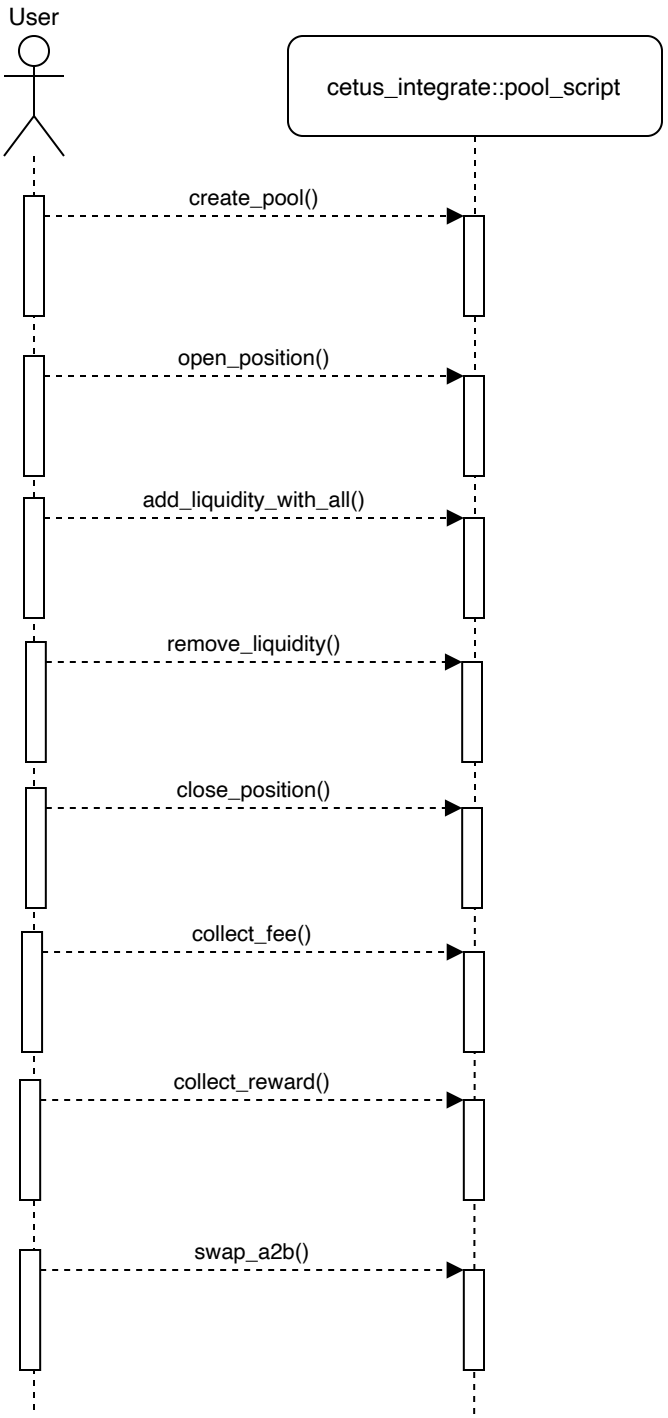
- Admin can `add_role`
- Admin can `remove_role`
- Admin can `remove_member`



User

- User can `create_pool`
- User can `open_position`
- User can `add_liquidity_with_all`

- User can `remote_liquidity`
- User can `close_position`
- User can `collect_fee`
- User can `collect_reward`
- User can `swap_a2b`



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

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

Code scope sees **Appendix 1**.

(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.

6 Findings

6.1 Unused Private Functions

Severity: **Minor**
Status: **Fixed**

Descriptions: There is a private function `remove_tick` in the tick module that is not used.

Code Location: clmmpool/sources/tick.move:153

Suggestion: Remove function `remove_tick` .

6.2 Functions Operating The Pool Do Not Check The Pool Status

Severity: **Medium**
Status: **Fixed**

Descriptions: In the module `clmmpool::pool` , some public functions for modifying the pool do not determine whether the current pool is suspended. If the pool is in an emergency and the administrator suspends the pool, some data in the pool can still be modified, causing the pool to be abnormal. Functions include `repay_flash_swap` , `repay_flash_swap_with_partner` , `update_pool_url` , `update_fee_rate` .

Code Location: clmmpool/sources/pool.move:588,638,745,756

Suggestion: Add `assert` to verify the state in the pool.

6.3 Swap Gas Optimization

Severity: Minor

Status: Fixed

Descriptions: When the index of `next_sqrt_price` and pool's `current_sqrt_price` are equal, there is no need to update `current_sqrt_price`, they only need to update when they are not equal.

Code Location: clmmpool/sources/pool.move:1343

Suggestion: Change `else` to `else if`.

6.4 Unused Module

Severity: Minor

Status: Fixed

Descriptions: `dl_list_table` module is not used.

Code Location: clmmpool/sources/dl_list_table.move

Suggestion: Delete this module.

6.5 The Calculation Of `reward` And `point` May Be Inaccurate

Severity: Medium

Status: Fixed

Descriptions: When executing/running/invoking these methods(`pool::collect_reward`, `pool::calculate_and_update_rewards`, `pool::calculate_and_update_points`), rewards are not recalculated except in some special cases. This can lead to inaccurate reward and point calculations.

Code Location: clmmpool/sources/pool.move

Suggestion: Call the `settle` functions to recalculate the rewards and points for all the branches.

6.6 Unused Return Value

Severity: Minor

Status: Fixed

Descriptions: The function `position::increase_liquidity` has a return value of type u128, but it is not used.

Code Location: clmmpool/sources/position.move:143

Suggestion: Have a check on the return value, or just remove the return value of the function `position::increase_liquidity`.

6.7 Unused Function

Severity: Minor

Status: Fixed

Descriptions: The method `borrow_mut_tick_for_swap` exists but is not used anywhere in the entire contract. It is also public, which poses a security risk.

Code Location: clmmpool/sources/tick.move:178

Suggestion: This function is not used and can be removed, or can be modified for private visibility.

6.8 Logic Repetition

Severity: Minor

Status: Fixed

Descriptions: The verification logic for positive and negative numbers in the function `cmp` is consistent.

Code Location: integer_mate/sui/sources/i32.move:159

Suggestion: Delete code `if (sign(num1) == 0)`.

6.9 Redundant Functions

Severity: Minor

Status: Fixed

Descriptions: The two functions `contains` and `is_some_and_eq` are logically the same.

Code Location: move-stl/sources/option_u64.move:49

Suggestion: Delete one of those functions.

6.10 Recursive Function

Severity: Major
Status: Fixed

Descriptions: The function `collect_fee_and_rewards` calls itself again, resulting in repeated calls to `collect_fee`, the transaction can never be executed successfully, resulting in gas loss.

Code Location: integrate/sources/pool.move:309

Suggestion: Replace `collect_fee_and_rewards` in the function with `collect_rewards`.

6.11 `Description` Cannot Be Modified

Severity: Minor
Status: Fixed

Descriptions: The `description` of `open_position` is specified as an empty string when the position is created, it is not passed through function parameters, and there is no function that can modify the description in other functions of the position.

Code Location: clmmpool/sources/position.move:99

Suggestion: Specify the value of `description` through parameters.

6.12 List Structure Design Flaws

Severity: Minor
Status: Fixed

Descriptions: The `list` is a data structure in the form of a linked list. The storage node uses the dynamic field in the Sui to store the node. The `dynamic_field` in the Sui can not have multiple key-value pairs with the same key. When the same `key` is inserted, an error will be reported. Although In this project will not have the same `key`, the list data structure itself should determine whether the `key` exists.

Code Location: move-stl/sources/list.move:98

Suggestion: Determine whether `key` exists before `push_back` and `insert` operations.

6.13 Function Parameter Error

Severity: Critical

Status: Fixed

Descriptions: The parameters of the `cross_by_swap` function are passed in the wrong order, which can cause the swap result to be wrong.

Code Location: clmmpool/sources/pool.move:1332

Suggestion: Modify to the correct order of parameters.

6.14 Multiple Coin Object Support

Severity: Minor

Status: Fixed

Descriptions: Because each token of Sui is independent, it is recommended to support `vector<Coin<CoinTypeA>>`, `vector<Coin<CoinTypeB>>` in functions `pool_script::create_pool_with_liquidity*`, `pool_script::open_position_with_liquidity*`, `pool_script::add_liquidity*`, `pool_script::swap*`, and follow-up operations after merging.

Code Location: integrate/sources/pool.move:58

Suggestion: Modify to support the coin vector.

6.15 Remaining TODO

Severity: Minor

Status: Fixed

Descriptions: There is still a part of `TODO` in the code, it is recommended to check whether the functions are complete.

Code Location: clmmpool/sources/math/clmm_math.move:133,178,215

Suggestion: Check whether the functions are complete, and update the comments.

6.16 Random Design Flaws

Severity: Major

Status: Fixed

Descriptions: When the parameter seed of the function seed and `seed_rand` is 0, all random numbers will be 0. Currently used in `skip_list`, if misused with seed 0, it will lead to an infinite loop of `skip_list`.

Code Location: move-stl/sources/random.move:13,27

Suggestion: The restriction parameter cannot be 0 when initializing the `seed` and generating random numbers.

6.17 Gas Optimization

Severity: Medium

Status: Fixed

Descriptions: A while loop in `position::is_empty` can return `false` when the `amount_owned` of one of the vector elements is not 0. In addition, in the return value `&&` expression, there is no check of `position_info.points_owned==0`.

Code Location: clmmpool/sources/position.move:352

Suggestion: Return `false` when the `amount_owned` of one of the vector elements is not 0.

6.18 Time Parameter Check

Severity: Minor

Status: Fixed

Descriptions: The `start_time` created and updated by `create_partner` may be smaller than the current time, and should be greater than or equal to the current time.

Code Location: clmmpool/sources/partner.move:103,211

Suggestion: Refactor the time check asserts.

Appendix 1 – Files in Scope

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

Files	SHA-1 Hash
./integrate/sources/utils.move	05a5a2016f86190245eb267fdd0c14c4d08c61b5
./integrate/sources/rewarder.move	68622b33642fbd3734fadf34753d055ea9b3224c
./integrate/sources/fetcher.move	79064f8a49b10e62387b64ddc57081759a4d9c9c
./integrate/sources/pool.move	f101f4d86ce26f31c65804d600b7a51d29a39857
./integrate/sources/tests/pool_tests.move	22f9e6775536a5d324f4fb6080658b10536dc27c
./integrate/sources/partner.move	6668f311af5b6d38d732fc8e6a74c9db98f426dd
./integrate/sources/config.move	c2a85e3ade352e895cf318e61513d39fe3273f96
./clmmpool/sources/factory.move	a78dded9d770f8f176bef2a5ab8c2f38df8855ba
./clmmpool/sources/utils.move	c0b0e8815734f1146c25587446ac076d7af86572
./clmmpool/sources/rewarder.move	425098b207c79b5174e23d9f2b0f4202bd899456
./clmmpool/sources/pool.move	8c87175e44d3e4e6d25fbcabf38799d2c889f3c0
./clmmpool/sources/tick.move	be70ac296c7a1969e874006f02e608f11eee12b3
./clmmpool/sources/tests/factory_tests.move	961ec95f1d55a3e97c0a39ade32670e0ccab6ced
./clmmpool/sources/tests/pool_tests.move	894da26ddc9d7ab397576bb0bb191eb023a01a7d
./clmmpool/sources/tests/config_tests.move	2934a90f6e60bef795965fbde4b977a048bd38f7
./clmmpool/sources/tests/swap_tests.move	582e55e00198e8a19e98a66d02401099dbbf434b
./clmmpool/sources/tests/rewarder_tests.move	9b9eb313b1e14e41bd36cafa60abfe370bbafed9

./clmmpool/sources/math/tick_math.move	1f8fe025c78d067ffcbaf31baf8beaae806ac968
./clmmpool/sources/math/clmm_math.move	aebbaa7a51686088ad613346b0413bc24345c965
./clmmpool/sources/partner.move	651b3c847129eef8ed09fa634e201df3bc2c36e7
./clmmpool/sources/acl.move	448993946dc1fe86a2006c4bf083b41a329d4ceb
./clmmpool/sources/config.move	46f77a9b6b724d9aca738f54a1d4a5349e3e634e
./clmmpool/sources/position.move	3f195f354513cc5a5bdfcc29397a2183a81bc177
./integrate/Move.toml	93226b12a8fd5d2fe9dbab7655d451661200c6b6
./clmmpool/Move.toml	76bdacd0b87fd29fa8249ceeff1c150b374c43aa
./sui/sources/skip_list.move	bb09e61f776b05d51b0eb0e895d54cd1556cd74c
./sui/sources/linked_table.move	9026901182f5bb5a581f565f1490cab717e0c95d
./sui/sources/option_u64.move	ae9f08d8842f0eaa5df357ee8721e1a917a501ed
./sui/sources/random.move	5b9994182540a864dd661a45a7105644a13f446d
./sui/Move.toml	71370e3568fe586f83577802ec1ca80f2c3a8c9d

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

Securing the Move Ecosystem

https://twitter.com/movebit_

contact@movebit.xyz