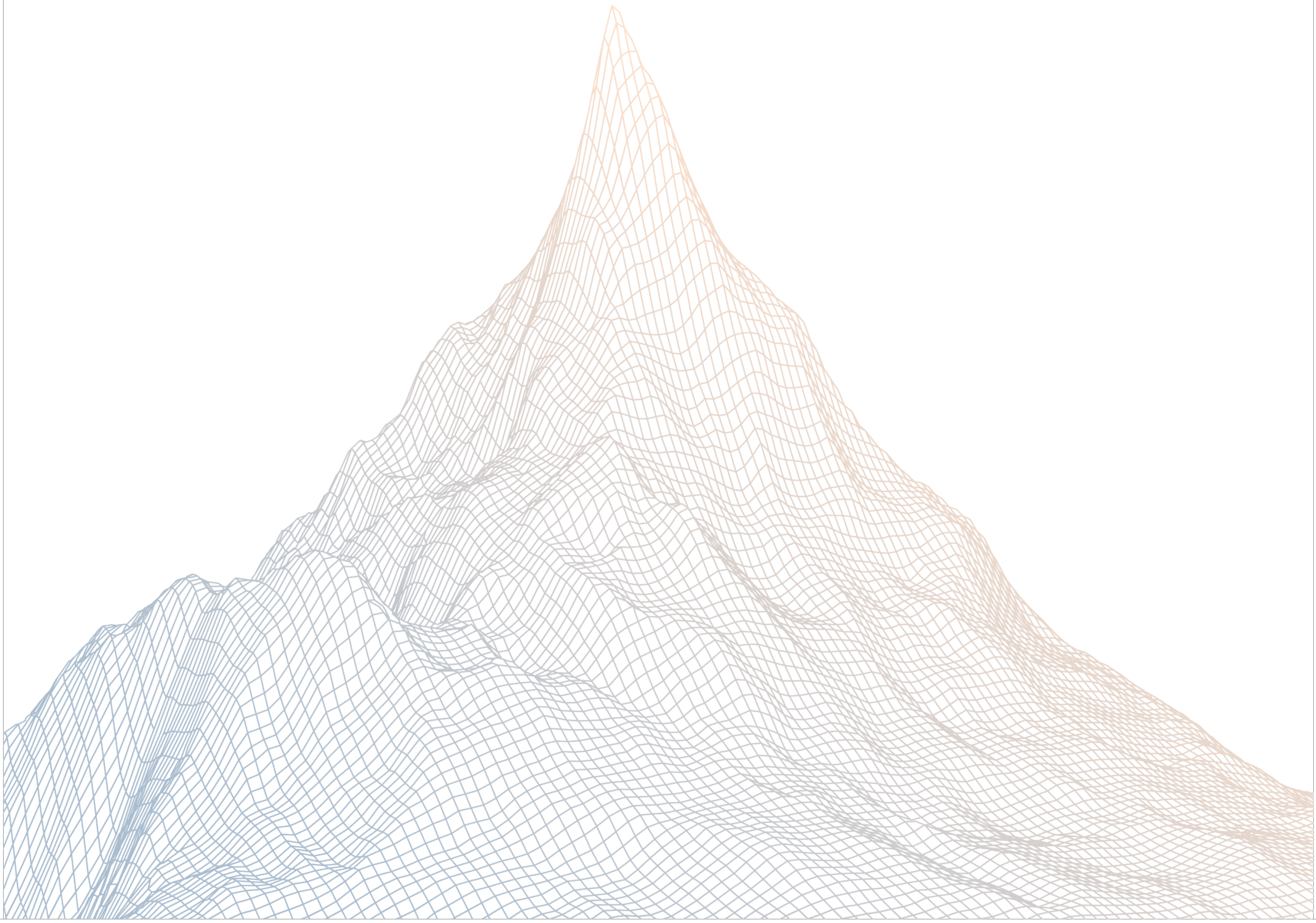
Zenith

Swap.io

Smart Contract Security Assessment

VERSION 1.1



AUDIT DATES:	April 10th to April 12th, 2025
AUDITED BY:	Peakbolt Christian Vari

Contents

1 Introduction

1.1 About Zenith

Zenith is an offering by Code4rena that provides consultative audits from the very best security researchers in the space. We focus on crafting a tailored security team specifically for the needs of your codebase.

Learn more about us at https://code4rena.com/zenith.

1.2 Disclaimer

This report reflects an analysis conducted within a defined scope and time frame, based on provided materials and documentation. It does not encompass all possible vulnerabilities and should not be considered exhaustive.

The review and accompanying report are presented on an "as-is" and "as-available" basis, without any express or implied warranties.

Furthermore, this report neither endorses any specific project or team nor assures the complete security of the project.

1.3 Risk Classification

SEVERITY LEVEL	IMPACT: HIGH	IMPACT: MEDIUM	IMPACT: LOW
Likelihood: High	Critical	High	Medium
Likelihood: Medium	High	Medium	Low
Likelihood: Low	Medium	Low	Low

2

Executive Summary

2.1 About Swap.io

Swap.io CLMM is an open-sourced concentrated liquidity market maker (CLMM) program built for the Solana ecosystem. This project is a fork of Raydium's CLMM, and while it builds upon the original design, it has been adapted and enhanced by the Swap.io team.

2.2 Scope

The engagement involved a review of the following targets:

Target	swap-io-clmm
Repository	https://github.com/swap-dot-io/swap-io-clmm
Commit Hash	`e7a51f1bd4cd3886091316ef0e11cb80796c7fe7`
Files	`Changes on top of the fork`

2.3 Audit Timeline

April 10th, 2025	Audit start
April 12th, 2025	Audit end
April 24th, 2025	Report published

2.4 Issues Found

SEVERITY	COUNT
Critical Risk	0
High Risk	0
Medium Risk	2
Low Risk	1
Informational	2
Total Issues	**5**

3

Findings Summary

ID	Description	Status
M-1	reward_token_vault can be frozen to prevent LP owners from removing their liquidity	Resolved
M-2	get_metadata_data() returns the incorrect metadata for position NFTs	Resolved
L-1	The admin is not able to remove support_mint_associated accounts	Resolved
I-1	Constant strings were not updated	Resolved
I-2	Hardcoded API key in configuration file exposing Helius RPC access	Resolved

4 Findings

4.1 Medium Risk

A total of 2 medium risk findings were identified.

[M-1] reward_token_vault can be frozen to prevent LP owners from removing their liquidity

SEVERITY: Medium	IMPACT: Low
STATUS: Resolved	LIKELIHOOD: Low

Target

- pool.rs#L239-L309

Description:

`initialize_rewards()` can by called by the global admin or pool owners to provide a `reward_token_mint` and start a new reward distribution for the pool to incentivize liquidity provisioning.

However, it fails to ensure that `reward_token_mint` does not have a freeze authority. That will allow the freeze authority of `reward_token_mint` to freeze the `reward_token_vault` token account and and cause claiming of the reward tokens via `collect_rewards()` to always fail.

As `collect_rewards()` is called within `decrease_liquidity()`, this issue will also prevent LP owners from removing their liquidity, leading them to be locked in the pool.

Recommendations:

Ensure the `reward_token_mint` does not have a freeze authority as shown in this commit, which only allows freeze authority on mint when it is eitherwhitelisted, a token in the pool or is set by global admin.

Swap.io: Resolved with @30d35b287ba...

Zenith: Verified. Resolved by applying the fix commit from raydium.

[M-2] `get_metadata_data()` returns the incorrect metadata for position NFTs

SEVERITY: Medium	IMPACT: Low
STATUS: Resolved	LIKELIHOOD: Low

Target

- open_position.rs#L814-L823

Description:

The `get_metadata_data()` returns the incorrect metadata for position NFTs, which will always point to the wrong URL, and show the wrong name and symbol.

```
fn get_metadata_data(personal_position_id: Pubkey) -> (String, String,
    String) {
    return (
        String::from("Raydium Concentrated Liquidity"),
        String::from("RCL"),
        format!(
            "https://dynamic-ipfs.raydium.io/clmm/position?id={}",
            personal_position_id.to_string()
        ),
    );
}
```

Recommendations:

Update `get_metadata_data()` with the correct metadata information.

Swap.io: Resolved with @f63e889333...

Zenith: Verified. Resolved with updated metadata.

4.2 Low Risk

A total of 1 low risk findings were identified.

[L-1] The admin is not able to remove `support_mint_associated` accounts

SEVERITY: Low	IMPACT: Low
STATUS: Resolved	LIKELIHOOD: Low

Target

- programs/amm/src/instructions/admin/create_support_mint_associated.rs

Description:

The program currently lacks a mechanism remove `support_mint_associated` accounts once created.

This design flaw prevents the admin from dynamically managing the list of supported mint addresses. The inability to deprecate or remove accounts compromises protocol hygiene and hampers effective governance, particularly if mint entries become compromised or are no longer valid.

Recommendations:

We recommend implementing a dedicated close instruction, such as `close_support_mint_associated`, that performs the following:

- Validates caller authorization, ensuring only the admin can invoke the closure.
- Utilizes the close attribute within the #[account] macro to transfer lamports from the closed account to a designated recipient.

Swap.io: Resolved with @b4b154b66c...

Zenith: Verified

4.3 Informational

A total of 2 informational findings were identified.

[I-1] Constant strings were not updated

SEVERITY: Informational	IMPACT: Informational
STATUS: Resolved	LIKELIHOOD: Low

Target

- collect_remaining_rewards.rs#L11
- decrease_liquidity.rs#L14

Description:

The following constant string in `collect_remaining_rewards()` and `decrease_liquidity()` are not updated to swap.io.

```
/// Memo msg for collect remaining
pub const COLLECT_REMAINING_MEMO_MSG: &'static [u8]
    = b"raydium_collect_remaining";
```

```
/// Memo msg for decrease liquidity
pub const DECREASE_MEMO_MSG: &'static [u8] = b"raydium_decrease";
```

Recommendations:

Consider updating them or remove if not required.

Swap.io: Resolved with @e26aea7ab1...

Zenith: Verified. Constant string has be updated.

[I-2] Hardcoded API key in configuration file exposing Helius RPC access

SEVERITY: Informational	IMPACT: Informational
STATUS: Resolved	LIKELIHOOD: Low

Target

- client_config.ini

Description:

The project repository contains the exposure of sensitive credentials. Specifically, a Helius RPC API key is hardcoded directly within the configuration file `client_config.ini`. This exposure occurs in both the HTTP and WebSocket URLs, granting access to Helius services.

This enables malicious actors to extract the API key directly from the source repository or its historical commits. Once obtained, the key can be used to perform unauthorized API operations, potentially incurring significant costs, enabling service abuse, or causing operational disruptions.

Recommendations:

We recommend revoking and rotating the exposed Helius API key to prevent unauthorized access. API keys should be managed through environment variables or a dedicated secrets management system. The project documentation must be updated to provide clear instructions for developers on securely configuring their environments.

Swap.io: Resolved with @0baa163bb08...

Zenith: Verified