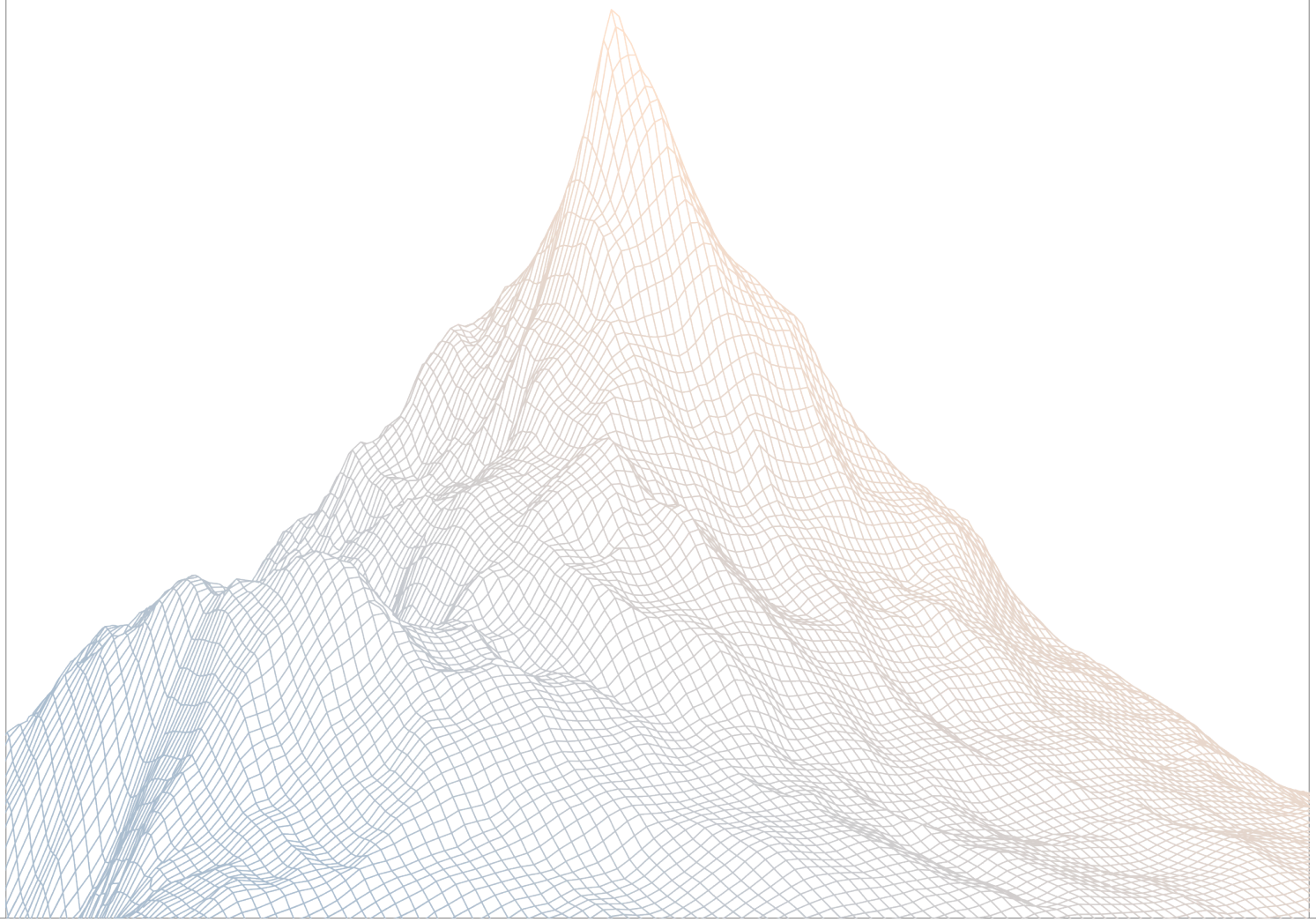
Zenith

Meteora

Smart Contract Security Assessment

VERSION 1.1



AUDIT DATES: January 9th to January 14th, 2026

AUDITED BY: peakbolt

Contents

1 Introduction

1.1 About Zenith

Zenith assembles auditors with proven track records: finding critical vulnerabilities in public audit competitions.

Our audits are carried out by a curated team of the industry's top-performing security researchers, selected for your specific codebase, security needs, and budget.

Learn more about us at https://zenith.security.

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 Meteora

Our mission is to build the most secure, sustainable and composable liquidity layer for all of Solana and DeFi.

By using Meteora's DLMM and Dynamic AMM Pools, liquidity providers can earn the best fees and yield on their capital.

This would help transform Solana into the ultimate trading hub for mainstream users in crypto by driving sustainable, long-term liquidity to the platform. Join us at Meteora to shape Solana's future as the go-to destination for all crypto participants.

2.2 Scope

The engagement involved a review of the following targets:

Target	damm-v2
Repository	https://github.com/MeteoraAg/damm-v2
Commit Hash	`3ff06bd7d3e9c9a92348912e234ee66c7b633654`
Files	`Changes in PR-167`

2.3 Audit Timeline

January 9, 2026	Audit start
January 14, 2026	Audit end
January 14, 2026	Report published

2.4 Issues Found

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

3

Findings Summary

ID	Description	Status
M-1	RATE_LIMITER_STACK_WHITELIST_PROGRAMS enables bypass of the rate-limiter “single swap per tx” check	Acknowledged

4

Findings

4.1 Medium Risk

A total of 1 medium risk findings were identified.

[M-1] `RATE_LIMITER_STACK_WHITELIST_PROGRAMS` enables bypass of the rate-limiter "single swap per tx" check

`SEVERITY:` Medium	`IMPACT:` Medium
`STATUS:` Acknowledged	`LIKELIHOOD:` Medium

Target

- ix_p_swap.rs#L300

Description:

`validate_single_swap_instruction()` is intended to enforce the rate limiter's "single swap per tx" constraint by restricting call-stack patterns. However, `RATE_LIMITER_STACK_WHITELIST_PROGRAMS` is allowed to exceed `stack_height > 2` and fan out into multiple downstream CPIs that each invoke `DAMMv2 swap` on the same pool within one transaction. As OKX smart wallet program is whitelisted, a trader can use it to break down large swap into multiper smaller swaps as follows:

```
whitelisted program
    ⟶ program X1 ⟶ DAMMv2 swap
    ⟶ program X2 ⟶ DAMMv2 swap
    ⟶ program X3 ⟶ DAMMv2 swap
```

That will cause `get_processed_sibling_instruction()` to return none at each swap IX, because they do not share a common parent, effectively bypassing the rate limiter.

Recommendations:

Consider removing the `RATE_LIMITER_STACK_WHITELIST_PROGRAMS` and only allow swaps with `stack_height` $\leqslant 2$.

Meteora: Acknowledged. Whitelisted program is trusted, and they must check this on their side to ensure user doesn't use this to abuse damm-v2 pools.