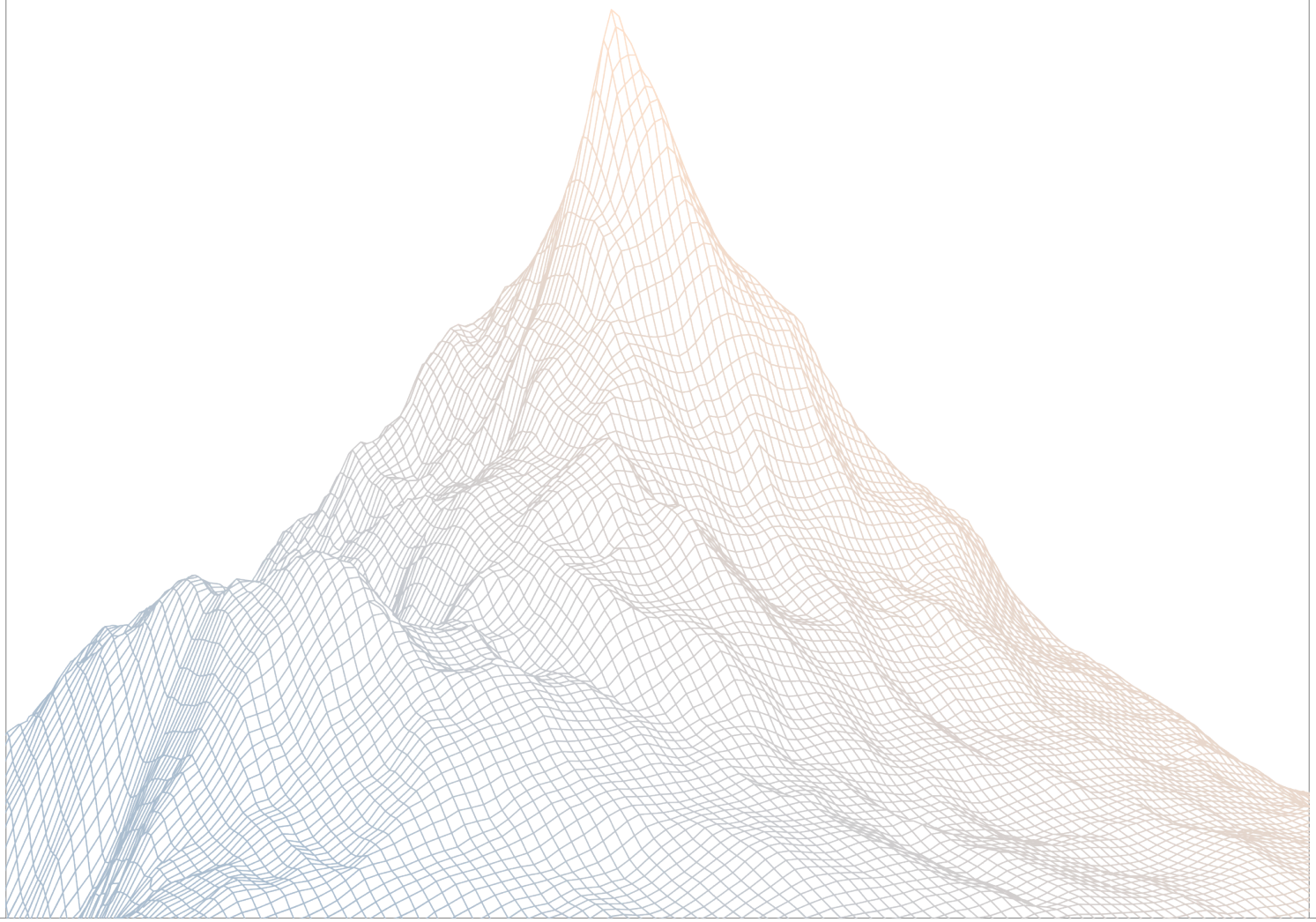
Zenith

Meteora

Smart Contract Security Assessment

VERSION 1.1



AUDIT DATES: January 8th to January 9th, 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	Meteora Zap Program
Repository	https://github.com/MeteoraAg/zap-program
Commit Hash	`4a48c48a1ad8ea1daec86a0d4f50dda452d7101d`
Files	`Changes in PR-41`

Target	Meteora Zap Program Mitigation Review
Repository	https://github.com/MeteoraAg/zap-program
Commit Hash	`020f3d23b114a662b946c384996a911a26811e60`
Files	`Changes in PR-41`

2.3 Audit Timeline

January 8, 2026	Audit start
January 9, 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	Missing Instructions sysvar in swap2 CPI within zap_in_damm_v2 breaks swaps on rate-limited DAMM v2 pools	Resolved

4

Findings

4.1 Medium Risk

A total of 1 medium risk findings were identified.

[M-1] Missing `Instructions` sysvar in `swap2` CPI within `zap_in_damm_v2` breaks swaps on rate-limited DAMM v2 pools

`SEVERITY:` Medium	`IMPACT:` Medium
`STATUS:` Resolved	`LIKELIHOOD:` Medium

Target

- ix_zap_in_damm_v2.rs#L83-L107

Description:

`zap_in_damm_v2` performs a CPI into DAMM v2 `swap2` as part of the zap in flow.

However, when the rate limiter is enabled, DAMM v2 `swap2` calls `validate_single_swap_instruction()` and reads the `Instructions` sysvar from `remaining_accounts[0]`, but the zap's `swap2` CPI passes no `remaining_accounts` at all.

As a result, zapping in to rate-limiter enabled pools could fail due to the swap error.

Recommendations:

Update the `swap2` CPI in `zap_in_damm_v2` to pass the `Instructions` sysvar as remaining_accounts when rate limiter is enabled.

Meteora: Resolved with PR-44.

Zenith: Verified. Resolved by passing in `ctx.remaining_accounts as part of swap2 CPI in` zap_in_damm_v2'.