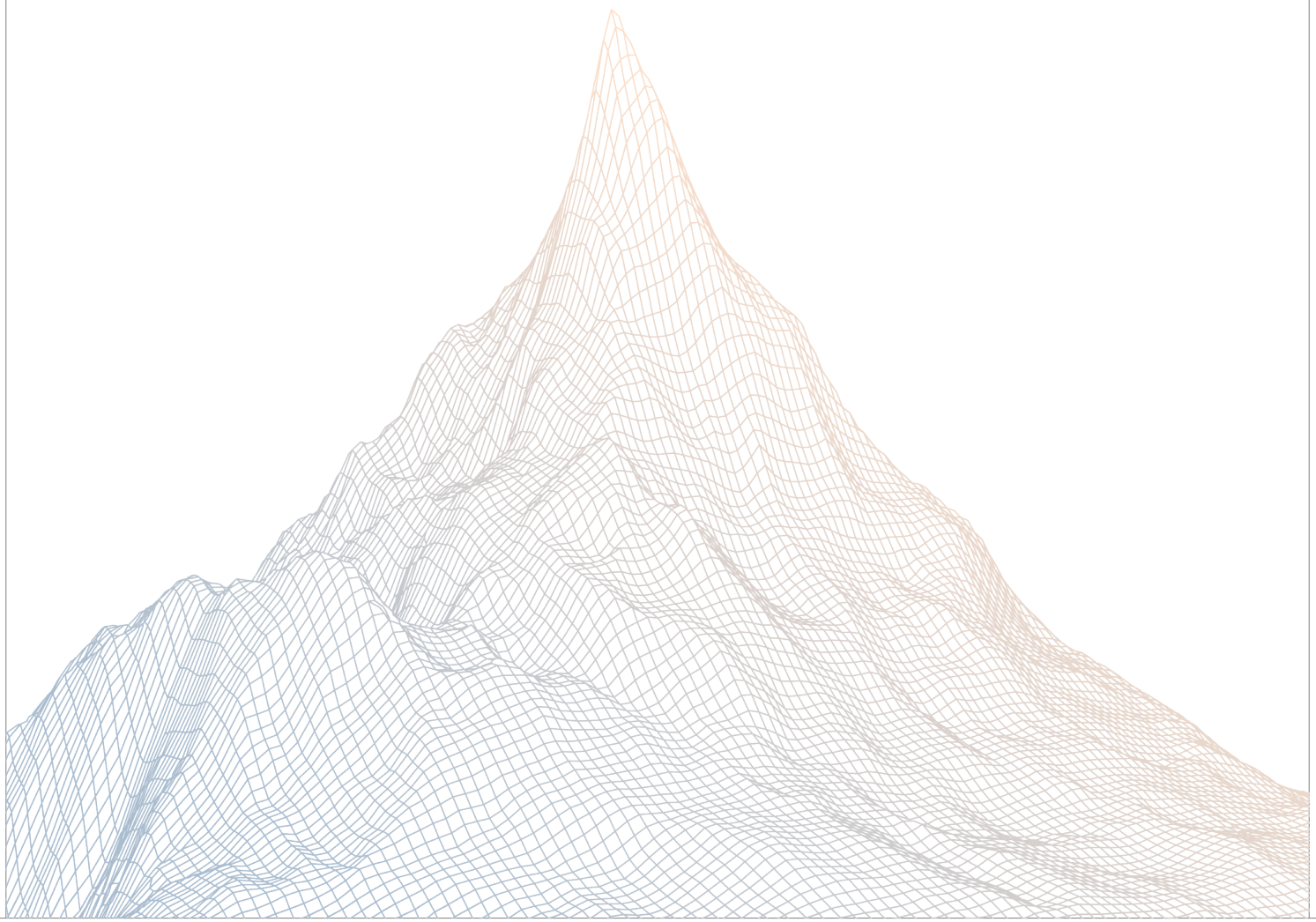
Zenith

Mitosis

Smart Contract Security Assessment

VERSION 1.1



AUDIT DATES: August 15th to August 15th, 2025

AUDITED BY: DadeKuma
Matte

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 Mitosis

Mitosis introduces a protocol that transforms DeFi liquidity positions into programmable components while solving fundamental market inefficiencies. In current DeFi systems, when users provide liquidity to protocols, they encounter two significant limitations. First, their positions become static and illiquid - once assets are committed, they can't be effectively used elsewhere. Second, the most profitable opportunities remain exclusive to large investors who can negotiate private agreements, creating an uneven playing field that mirrors traditional finance systems.

2.2 Scope

The engagement involved a review of the following targets:

Target	TMITO
Repository	https://github.com/mitosis-org/TMITO.git
Commit Hash	`7f9598ba48ab2bc5980b7b38ede5b64fb62cdcc7`
Files	`src/TMITO.sol`

2.3 Audit Timeline

August 15, 2025	Audit start
August 15, 2025	Audit end
August 18, 2025	Report published

2.4 Issues Found

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

3

Findings Summary

ID	Description	Status
L-1	Users can redeem with an unfinalized ratio when the lockup period has ended	Resolved
L-2	redeem may revert in some scenarios	Resolved

4

Findings

4.1 Low Risk

A total of 2 low risk findings were identified.

[L-1] Users can redeem with an unfinalized ratio when the lockup period has ended

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

Target

- src/TMITO.sol

Description:

An edge case exists in the redemption process where:

1. The lockup period has ended
2. The redemption ratio remains unfinalized by admin
3. Users can still initiate redemption transactions

This creates potential inconsistency where redemptions occur without a finalized ratio. While unlikely, this scenario violates the intended protocol flow where ratio finalization should precede any redemptions.

Recommendations:

Consider requiring that the ratio is finalized when `redeem` is called.

Mitosis: Resolved with @e3284c0252...

Zenith: Verified.

[L-2] `redeem` may revert in some scenarios

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

Target

- src/TMITO.sol

Description:

Using the `transfer` function for an address leads to transaction failure when:

- Target contract lacks a payable function.
- Target contract has a payable fallback using over 2300 gas units.
- Target contract's payable fallback needs less than 2300 gas units but is called through a proxy, exceeding the gas limit.
- Some multisig wallets may require gas higher than 2300.

Recommendations:

Consider using `call` instead of `transfer`.

Mitosis: Resolved with @4d22e5f4ed...

Zenith: Verified.