Panoptic Protocol Security Review

Reviewed by: MrPotatoMagic

January 28th, 2025

Contents

1 About MrPotatoMagic

MrPotatoMagic is an independent smart contract security researcher. Having disclosed over 100 security vulnerabilities across numerous protocol types, he consistently aims to elevate the security of the blockchain ecosystem by offering top quality smart contract security reviews.

2 Disclaimer

A smart contract security review can never verify the complete absence of vulnerabilities. This is a time, resource and expertise bound effort where I try to find as many vulnerabilities as possible. I can not guarantee 100 percent security after the review or even if the review will find any problems with your smart contracts. Subsequent testing, security reviews, bug bounty programs and on-chain monitoring are strongly recommended.

3 Introduction

Panoptic is a permissionless options trading protocol. It enables the trading of perpetual options built on top of UniswapV3 and Uniswap V4.. The Panoptic protocol is noncustodial, has no counterparty risk, offers instantaneous settlement, and is designed to remain fully collateralized at all times.

4 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

4.1 Impact

- High - Leads to significant material loss of assets in the protocol or significant harm to majority of users.
- Medium - Loss/Leakage of small asset amounts or core functionality of the protocol is affected.
- Low - Any kind of unexpected behaviour that is non-critical.

4.2 Likelihood

- High - Almost certain to happen, easy to perform, or not easy but highly incentivized.
- Medium - Only conditionally possible or incentivized, but still relatively likely.
- Low - Involves too many or unlikely assumptions with little-to-no incentive.

4.3 Action required for severity levels

- Critical - Must fix as soon as possible (if already deployed)
- High - Must fix (before deployment if not already deployed)
- Medium - Should fix
- Low - Could fix

5 Executive Summary

Over the course of the security review, Panoptic engaged with MrPotatoMagic to review the panoptic-v1-core and panoptic-v1-helper protocol. In this period of time, a total of 2 issues were found.

Summary

Project Name	Panoptic
Repository	panoptic-v1-core, panoptic-v1-helper
Panoptic V1 Core Pull Requests	PR1, PR2
Panoptic V1 Helper Commit - UniswapMigrator.sol	cb1d1e6....01c63f7
Protocol Type	Perpetual Options, DeFi
Review Timeline	January 20th 2025 - January 25th 2025

Issues Found

Severity	Count	Fixed	Acknowledged
Critical Risk	**0**	**0**	**0**
High Risk	**0**	**0**	**0**
Medium Risk	**0**	**0**	**0**
Low Risk	**0**	**0**	**0**
Non-Critical	**2**	**0**	**2**
Total	**2**	**0**	**2**

6 Findings

6.1 Non-Critical

6.1.1 Allow msg.sender to supply a receiver address instead of directly minting shares

Context: UniswapMigrator.sol#L107

Description: Functions migrateV3() and migrateV4() in UniswapMigrator.sol facilitate the migration from Uniswap LPing to Panoptic LPing. In this process, when we attempt to deposit to the desired collateral vaults, we utilize the msg.sender themselves as the recipient of the shares. While this is particularly not an issue, it is recommended to allow users to supply a recipient address where they can receive their shares. This provides more flexibility during the migration process.

Recommendation: As suggested above, allow users to provide a recipient address as a parameter and supply it as the recipient to the collateral vault's deposit() function call.

6.1.2 Function deposit() calls are prone to slippage during migration

Context: UniswapMigrator.sol#L107

Description: Functions migrateV3() and migrateV4() in UniswapMigrator.sol facilitate the migration from Uniswap LPing to Panoptic LPing. In this process, when we attempt to deposit to the desired collateral vaults, there is no slippage protection offered to users through UniswapMigrator.sol. Due to this, it is possible that the recipient might not receive the amount of shares they expected to receive.

Recommendation: Offer slippage protection through functions migrateV3() and migrateV4() by introducing minAmountOut1 and minAmountOut2 slippage parameters. Following this, the functions can check the pre deposit and post deposit share balance of the receiver to ensure the amount of shares received were greater than or equal to the slippage parameters the user provided.