CANTINA

Maker DAO: univ2-pool-migrator

Security Review

Cantina Managed review by:
Christoph Michel, Lead Security Researcher
M4rio.eth, Security Researcher
Shung, Associate Security Researcher

July 3, 2024

Contents

1 Introduction

1.1 About Cantina

Cantina is a security services marketplace that connects top security researchers and solutions with clients. Learn more at cantina.xyz

1.2 Disclaimer

Cantina Managed provides a detailed evaluation of the security posture of the code at a particular moment based on the information available at the time of the review. While Cantina Managed endeavors to identify and disclose all potential security issues, it cannot guarantee that every vulnerability will be detected or that the code will be entirely secure against all possible attacks. The assessment is conducted based on the specific commit and version of the code provided. Any subsequent modifications to the code may introduce new vulnerabilities that were absent during the initial review. Therefore, any changes made to the code require a new security review to ensure that the code remains secure. Please be advised that the Cantina Managed security review is not a replacement for continuous security measures such as penetration testing, vulnerability scanning, and regular code reviews.

1.3 Risk assessment

Severity	Description
Critical	*Must* fix as soon as possible (if already deployed).
High	Leads to a loss of a significant portion (>10%) of assets in the protocol, or significant harm to a majority of users.
Medium	Global losses <10% or losses to only a subset of users, but still unacceptable.
Low	Losses will be annoying but bearable. Applies to things like griefing attacks that can be easily repaired or even gas inefficiencies.
Gas Optimization	Suggestions around gas saving practices.
Informational	Suggestions around best practices or readability.

1.3.1 Severity Classification

The severity of security issues found during the security review is categorized based on the above table. Critical findings have a high likelihood of being exploited and must be addressed immediately. High findings are almost certain to occur, easy to perform, or not easy but highly incentivized thus must be fixed as soon as possible.

Medium findings are conditionally possible or incentivized but are still relatively likely to occur and should be addressed. Low findings a rare combination of circumstances to exploit, or offer little to no incentive to exploit but are recommended to be addressed.

Lastly, some findings might represent objective improvements that should be addressed but do not impact the project's overall security (Gas and Informational findings).

2 Security Review Summary

The Maker Protocol, also known as the Multi-Collateral Dai (MCD) system, allows users to generate Dai (a decentralized, unbiased, collateral-backed cryptocurrency soft-pegged to the US Dollar) by leveraging collateral assets approved by the Maker Governance, which is the community organized and operated process of managing the various aspects of the Maker Protocol.

On Jun 12th the Cantina team conducted a review of univ2-pool-migrator on commit hash 106b3255. The team identified a total of **1** issues in the following risk categories:

- Critical Risk: 0
- High Risk: 0
- Medium Risk: 0
- Low Risk: 0
- Gas Optimizations: 0
- Informational: 1

3 Findings

3.1 Informational

3.1.1 Uniswap pool migration pulls all liquidity from old pool

Severity: Informational

Context: UniV2PoolMigratorInit.sol#L59

Description: Almost the entire liquidity (99.97% at time of writing, from $145,000,000 to $40,000) of the MKR <> DAI UniswapV2 pool is held by the `PauseProxy` and will be removed to provide liquidity for the new NGT <> NST UniswapV2 pool.

This could lead to issues for users, bots, or contracts still relying on the old pool:

- Traders swapping in the pool will receive worse prices due to high slippage occurring in low liquidity pools. This could affect contracts or bots that have the pool hardcoded.
- The low liquidity of the MKR <> DAI pool might have second-order trade effects on swap pairs that use the pool as an intermediary to trade through.
- The pool becomes easy to manipulate. This affects any oracles that use the MKR <> DAI pool as a source, for example, to estimate MKR prices in terms of USD.

Recommendation: Communicate and give sufficient notice that the Uniswap MKR <> DAI pool will be deprecated and its liquidity will be removed.

Maker: Acknowledged. Sufficient communication should be done, and possibly other off-chain measures that would make sure there is some minimal external liquidity in the pool for a while.

Cantina Managed: Acknowledged.