Canto Solo Audit by Ghoul.sol Findings & Analysis Report

2022-07-10

Table of contents

Overview

About C4

Code4rena (C4) is an open organization consisting of security researchers, auditors, developers, and individuals with domain expertise in smart contracts.

A C4 Solo Audit is a single-warden or single-team audit performed by a top Code4rena contributor.

During the Solo Audit outlined in this document, C4 conducted an analysis of the Canto code. The audit took place between July 8—10, 2022.

Wardens

Ghoul.sol is a senior Solidity developer and has served as a Code4rena judge for a dozen audit contests.

Final report assembled by sock.

Summary

The Solo Audit yielded 4 vulnerabilities. Of those vulnerabilities, 3 received a risk rating of HIGH severity and 1 received a risk rating of MEDIUM. 1 informational finding was also reported.

4 vulnerabilities have been fixed and 1 information finding has been acknowledged.

The codebase in question had already undergone two prior Code4rena contests. This code review had a targeted nature which included 30 lines of code modified following prior Code4rena audits. Only specific functions outlined were reviewed.

Code review was focused on critical issues only. Improvements and optimizations were not reported.

Scope

Code reviewed consisted of the following files:

- BaseV1-core.sol
- BaseV1-periphery.sol

Following functions were reviewed:

- BaseV1Router01.getUnderlyingPrice
- BaseV1Pair._update
- BaseV1Pair.quote
- BaseV1Pair.sample
- BaseV1Pair.reserves
- BaseV1Pair.sampleReserves
- BaseV1Pair.totalSupplyAvg
- BaseV1Pair.sampleSupply

Severity Criteria

C4 assesses the severity of disclosed vulnerabilities according to a methodology based on OWASP standards.

Vulnerabilities are divided into three primary risk categories: high, medium, and low/non-critical.

High-level considerations for vulnerabilities span the following key areas when conducting assessments:

- Malicious Input Handling
- Escalation of privileges
- Arithmetic
- Gas use

Further information regarding the severity criteria referenced throughout the submission review process, please refer to the documentation provided on the C4 website.

High Risk Findings (3)

[H-01] Wrong LP price calculated

`TotalSupply` amount is read directly from storage.

Attacker can manipulate that amount using a flash loan and change the calculated LP token price. This is also an issue during regular calculation because the TVL is calculated based on time-averaged values but total supply is a current block value which will result consistently incorrect results.

https://github.com/Canto-Network/lending-updates/blob/06a77049bb1bb41b32c1eed1fcdcc23587696f62/src/Swap/BaseV1-periphery.sol#L544

STATUS: Mitigated

[H-02] Loss of precision resulting in wrong value for price ratio

Price ratio was calculated by division of price0 and price1. Both prices are normalized to 18 decimal points. Division at best case would return 0 which would cause division by zero revert. At worst case it returns single digit which will make calculations of fair reserves incorrect.

https://github.com/Canto-Network/lending-updates/blob/8f1e624a74ea67e63400209dded2bb716d92e472/src/Swap/BaseV1-periphery.sol#L573

STATUS: Mitigated

[H-03] Wrong reserves calculated for non-19 decimals points tokens

As part of `calculateFairReserves` function, a square root of each reserve is calculated and divided by 1e18 to normalized the value to 18 decimals. However, there is evidence that reserves are 18 decimals value in the first place which will result in a wrong value calculated for pairs with tokens that do not have 18 decimal points.

https://github.com/Canto-Network/lending-updates/blob/8f1e624a74ea67e63400209dded2bb716d92e472/src/Swap/BaseV1-periphery.sol#L568

STATUS: Mitigated

Medium Risk Findings (1)

[M-01] Typo in price1 calculation.

`price1` calculation used `stable0` value instead of `stable1`. It will cause `pairFor` function to return wrong address and most likely cause a revert. In extreme scenario it could return wrong price. https://github.com/Canto-Network/lending-updates/blob/8f1e624a74ea67e63400209dded2bb716d92e472/src/Swap/BaseV1-periphery.sol#L539

STATUS: Mitigated

Informational Findings (1)

[Info-1] Hardcoded prices for stablecoins

Hardcoding price of USDT and USDC as 1 may open some arbitrage opportunities when real price for each token is a little bit different. Also, in case of UST-style collapse, the protocol will not be able to liquidate bad loans.

https://github.com/Canto-Network/lending-updates/blob/a19b1648decd705d9349317ae37cc072e5342a49/src/Swap/BaseV1-periphery.sol#L509

STATUS: Acknowledged

Disclosures

C4 is an open organization governed by participants in the community.

C4 does not provide any guarantee or warranty regarding the security of this project. All smart contract software should be used at the sole risk and responsibility of users.