SHERLOCK

Sherlock Security Review For Index

Public contest prepared for: **Index**
Lead Security Expert: **0x52**
Date Audited: **October 14 - October 21, 2024**

Introduction

Utilize the Morpho (formerly Morpho Blue) lending protocol to implement tokenized leverage positions.

Scope

Repository: IndexCoop/index-coop-smart-contracts

Branch: master

Audited Commit: 7202ed7d335c107d51efa5c081fcd68517c310d5

Final Commit: 67b744554b59ea3e7d2c29ff0e15a2995d80bd76

Repository: IndexCoop/index-protocol

Branch: master

Audited Commit: d219221ca97536d74b53b06c2b063ebe3d878b9f

Final Commit: 3718b437d42d14db925a99965ff81c41ffab83ae

For the detailed scope, see the contest details.

Findings

Each issue has an assigned severity:

- Medium issues are security vulnerabilities that may not be directly exploitable or may require certain conditions in order to be exploited. All major issues should be addressed.

- High issues are directly exploitable security vulnerabilities that need to be fixed.

Issues found

Medium	High
1	0

Issues not fixed or acknowledged

Medium	High
0	0

Security experts who found valid issues

0x52   Kirkeelee

Issue M-1: _calculateMaxBorrowCollateral calculates repay incorrectly and can lead to set token liquidation

Source: https://github.com/sherlock-audit/2024-10-morpho-x-index-judging/issues/26

Found by

0x52, Kirkeelee

Summary

When calculating the amount to repay, `_calculateMaxBorrowCollateral` incorrectly applies `unutilizedLeveragePercentage` when calculating `netRepayLimit`. The result is that if the `borrowBalance` ever exceeds `liquidationThreshold*(1-unutilizedLeveragPercentage)` then all attempts to repay will revert. This is nearly identical to the valid issue reported in the last contest that was fixed in the Aave leverage extension.

Root Cause

In MorphoLeverageStrategyExtension.sol:L1124 the borrow limit is reduced by `unutilizedLeveragePercentage` which will cause L1134 to underflow and revert.

Internal pre-conditions

`unutilizedLeveragePercentage` must be a nonzero value. For context this is nonzero for every existing leveraged token currently deployed by Index Coop.

External pre-conditions

The underlying collateral value decreases rapidly in price pushing the set towards liquidation

Attack Path

1. The price of the underlying collateral decreases rapidly causing `liquidationThreshold` to drop

2. `borrowBalance` exceeds `liquidationThreshold*(1-unutilizedLeveragPercentage)`

3. Calls to `MorphoLeverageStrategyExtension#ripcord` will revert due to underflow

4. Set token is liquidated

Impact

Set token suffers losses due to liquidation fee. For most Morpho markets this is at least 5%. Due to the leveraged nature of the set the loss will be multiplicative. This means a 3x leverage token will lose 15% NAV (5% * 3), 5x leverage will lose 25% NAV (5% * 5), etc.

PoC

No response

Mitigation

Don't adjust the max value by `unutilizedLeveragPercentage` when deleveraging

Discussion

sherlock-admin2

The protocol team fixed this issue in the following PRs/commits: https://github.com/IndexCoop/index-coop-smart-contracts/pull/192

Disclaimers

Sherlock does not provide guarantees nor warranties relating to the security of the project.

Usage of all smart contract software is at the respective users' sole risk and is the users' responsibility.