G$_0$ Group

Security Review of
Symphony Finance
November 2021

Symphony Finance / November 2021

Files in scope

https://github.com/symphony-finance/avalanche-contracts/commit/797af47dd3585caa7b18b12ef94f08ba1e7311a5/contracts/

- adapters/AaveYield.sol
- adapters/BenqiYield.sol
- Symphony.sol
- handlers/PangolinHandler.sol

Current status

All issues have been fixed by the developer. There are no known issues in the relevant contracts in https://github.com/symphony-finance/avalanche-contracts/commit/913e148f25887fbee25f8544e5734dfc9548ba14

Issues

1. Fee and minimal quoteAmount should be calculated from depositPlusYield not inputAmount

type: incorrect implementation / severity: medium

In `fillOrder` `myOrder.inputAmount = depositPlusYield;` should happen before calling a price oracle and calculation of the fee, otherwise fee and minimale quote amount is calculated from original input amount instead from the current value of the deposit.

status - fixed

Issue has been fixed and is no longer present in

https://github.com/symphony-finance/avalanche-contracts/commit/913e148f25887fbee25f8544e5734dfc9548ba14

2. fillOrder doesn't follow checks effects interactions pattern

type: code fragility / severity: minor

It's good practice for functions to follow checks effects interactions pattern whenever possible even where reentrancy guard is used, this is not the case in fillOrder since `orderHash[orderId]` is deleted after external calls.

status - fixed

Issue has been fixed and is no longer present in

https://github.com/symphony-finance/avalanche-contracts/commit/913e148f25887fbee25f8544e5734dfc9548ba14

3. Inactive strategies should have their approval reset to 0

type: security / severity: minor

In case a strategy contract is compromised, it should have it's token approval reset to `0` in `migrateStrategy` after it's deactivated.

status - fixed

Issue has been fixed and is no longer present in

https://github.com/symphony-finance/avalanche-contracts/commit/913e148f25887fbee25f8544e5734dfc9548ba14

4. Executor fee transfer in transferFee should be skipped if protocol fee is 100%

type: incorrect implementation / severity: minor

When protocol fee is set to 100% the executor fee will end up being 0, in that case the token transfer of the executor fee should be skipped.

status - fixed

Issue has been fixed and is no longer present in

https://github.com/symphony-finance/avalanche-contracts/commit/913e148f25887fbee25f8544e5734dfc9548ba14