G₀ Group

Security Review of

Flooz Trade

October 2021

Flooz Trade / October 2021

Files in scope

Following files in:

https://github.com/flooz-link/flooz-trade-contracts/tree/a65a97d95b916f1c616d075473c9c3c3ca1bb0ca/contracts/

- FeeReceiver.sol
- FloozRouter.sol
- ReferralRegistry.sol

Current status

All issues have been fixed by the developer. There are no known issues in the relevant contracts in https://github.com/flooz-link/flooz-trade-contracts/tree/89bf471a109471a7f1522f70fa5e4adc7d603171/contracts

Issues

1. Inconsistent fee calculation

type: incorrect implementation / severity: medium

Functions that allow user to specify exact output amount will charge to user lower fee relative to swapped value than functions that specify exact input amount.

status - fixed

Issue has been fixed and is no longer present in

https://github.com/flooz-link/flooz-trade-contracts/tree/89bf471a109471a7f1522f70fa5e4adc7d603171/contracts

2. Functions that swap into ETH return lower amount of ETH than specified in amountOutMin

type: incorrect implementation / severity: medium

Functions that swap into ETH behave slightly differently than other functions, because fee is subtracted from output amount after swap, instead from input amount before swap. One of the effects is that `amountOutMin` doesn't actually specify the minimum output amount, but instead specifies minimum output amount before fees, this is a confusing inconsistency. Similarly in `swapTokensForExactETH` amountOut specifies desired output amount before fees, not the ultimate output amount.

status - fixed

Issue has been fixed and is no longer present in

https://github.com/flooz-link/flooz-trade-contracts/tree/89bf471a109471a7f1522f70fa5e4adc7d603171/contracts

Notes

- `FloozRouter.swapFee` can be changed by the contract owner at any time, hypothetically just before `executeZeroExSwap` call is processed leading to an unexpected fee.
- `FloozRouter.balanceThreshold` can be changed by the contract owner at any time, potentially affecting the utility of the SYA token.
- Owner of `FeeReceiver` contract can intervene into the buyback mechanism, potentially affecting the expected rate of the SYA token appreciation.