Kirobo SafeTransfer contract / November 2020

Files in scope

https://github.com/kiroboio/ki-eth-token/blob/b76d33a8fe91355b92fc8ee3eea8700388e3cf37/contracts/SafeTransfer.sol

Current status

All reported issues have been addressed by the developer.

Issues

1. depositFees collected in timedDeposit function are never added to the s_fees sum of fees withdrawable by the admin

type: usability / Severity: major

`timedDeposit` function enforces transferral of ETH equal to the `depositFees` argument to the contract, these fees should be ultimately either returned to the caller of the caller of the `timedDepost` function, or added to the `s_fees` counter that keeps track of fees that are withdrawable by the contract admin, neither is implemented.

status - fixed

The issue is no longer present in

https://github.com/kiroboio/ki-eth-token/blob/8409e4a05991085c87d22af9d31ba0890ecb4c34/contracts/SafeTransfer.sol

2. Transferral of depositFees is not validated in the timedDepositERC20 and timedDepositERC721 functions

type: usability / Severity: major

`timedDepositERC20` and `timedDepositERC721` are supposed to collect fee equal to the `depositFees` argument the same way `timedDeposit` function does, but the transferral of these fees is not validated.

status - fixed

The issue is no longer present in

https://github.com/kiroboio/ki-eth-token/blob/8409e4a05991085c87d22af9d31ba0890ecb4c34/contracts/SafeTransfer.sol

3. In hiddenCollectERC20 value shouldn't be part of tinfo.id

type: usability / Severity: major

`hiddenCollectERC20` includes the `value` argument in the second variable of the `tinfo.id` hash, this variable is equal to `msg.value` when the hash is constructed in `hiddenDeposit`, so in order for the `hiddenCollectERC20` hash to match the submission hash, the user has to transfer amount of ETH to the contract equal to the amount of ERC20 token that they desire to transfer. This requirement is an implementation error.

status - fixed

The issue is no longer present in

https://github.com/kiroboio/ki-eth-token/blob/8409e4a05991085c87d22af9d31ba0890ecb4c34/contracts/SafeTransfer.sol