G0 Group

Security Review of

Kirobo SafeSwap contract

July 2021

Kirobo SafeSwap contract / July 2020

Files in scope

https://github.com/kiroboio/ki-eth-token/blob/14b800c9581a6afec7de391f49ea39ef4961337c/contracts/SafeSwap.sol

Current status

All reported issues have been fixed by the developer.

Issues

1. depositERC721 doesn't always collect fee

type: Incorrect implementation / Severity: major

When neither `token0` nor `token1` is equal to `address(0)`, `fees0` is not required to be equal to `msg.value` in `depositERC721`, but `swapERC721` assumes this fee is always collected.

status - fixed

The issue is no longer present in

https://github.com/kiroboio/ki-eth-token/blob/bf1efc274158e5e476681c0f5051a2b8f05e245b/contracts/SafeSwap.sol

2. hiddenSwap and hiddenSwapERC721 assumes all deposits are in ETH

type: Incorrect implementation / Severity: major

In `hiddenSwap` and `hiddenSwapERC721` `msg.value` of the original deposit is effectively required to be equal to `info.value0.add(info.fees0)`, but this doesn't make sense if `token0 != address(0)` in that case it should be only equal to `info.fees0`.

status - fixed

The issue is no longer present in

https://github.com/kiroboio/ki-eth-token/blob/bf1efc274158e5e476681c0f5051a2b8f05e245b/contracts/SafeSwap.sol

3. autoRetrieve and autoRetrieveERC721 should transfer the deposit to the original depositor, not to activator

type: Incorrect implementation / Severity: major

`autoRetrieve` and `autoRetrieveERC721` functions should contain a `from` argument, since they are supposed to be called by the activator and not the depositor.

status - fixed

The issue is no longer present in

https://github.com/kiroboio/ki-eth-token/blob/bf1efc274158e5e476681c0f5051a2b8f05e245b/contracts/SafeSwap.sol

4. timedDepositERC721 doesn't collect autoRetrieveFees

type: Incorrect implementation / Severity: medium

`timedDepositERC721` is missing a check to make sure there's enough eth for`autoRetrieveFees`

status - fixed

The issue is no longer present in

https://github.com/kiroboio/ki-eth-token/blob/bf1efc274158e5e476681c0f5051a2b8f05e245b/contracts/SafeSwap.sol

5. timedDepositERC721 is missing the to != msg.sender

type: Incorrect implementation / Severity: minor

`timedDepositERC721` is missing the`to != msg.sender` check that is in other deposit functions

status - fixed

The issue is no longer present in

https://github.com/kiroboio/ki-eth-token/blob/bf1efc274158e5e476681c0f5051a2b8f05e245b/contracts/SafeSwap.sol