SWO-01 | MISSING VALIDATION ON MULTI-SWAP

Category	Severity	Location	Status
Logical Issue	● Critical	sources/swap_router.move (06/12-reward-fix): 169	● Resolved

Description

Contract commit: 43d97c84923065996d31758c4ea858096b92f331 File: `swap_router.move`

The module `swap_router` is working as an interface to help users access the swap service. It mainly provides two kinds of swap:

1. single swap, for example, from SUI to TURBOS.
2. multi swap, for example, from SUI to TURBOS, then from TURBOS to USDC.

The single swap will invoke `pool::swap` to calculate the swap result, which updates the pool, and then invoke `pool::swap_coin` to process the coin change.

For multiswap, it will invoke `pool::swap` twice. Taking the exact out mode as an example:

1. swaps `step2_in` token y for `step2_out` token z
2. swaps `step1_in` token x for `step1_out` token y

Then the function `pool::swap_coin` processes the balance changes.

However, in the scenario that a pool does not have enough liquidity, which leads to `step1_out` possibly not equalling `step2_in`, an imbalanced swap can be generated.

Recommendation

We recommend the team adding validations on the `pool::swap` result to ensure the swap result is consistent during the multi swap methods.

Alleviation

[**Turbos Finance**, 07/31/2023]: The team heeded the advice and resolved the issue in commit bad211723bb3f8a67e7919265627f2f3528f90fc by adding validation on swap results inside the multi swap methods.