
[H-1] Incorrect fee calculation in TSwapPool::getInputAmountBasedOnOutput causes protocol to take too many tokens from users, resulting in lost fees

Description:

The `getInputAmountBasedOnOutput` function is intended to calculate the amount of tokens a user should deposit given an amount of tokens of output tokens. However, the function currently miscalculates the resulting amount. When calculating the fee, it scales the amount by `10_000` instead of `1_000`.

Impact: Protocol takes more fees than expected from users.

Recommended Mitigation “diff function `getInputAmountBasedOnOutput(uint256 outputAmount, uint256 inputReserves, uint256 outputReserves) public pure revertIfZero(outputAmount) revertIfZero(outputReserves) returns (uint256 inputAmount) { - return ((inputReserves * outputAmount) * 10_000) / ((outputReserves - outputAmount) * 997); + return ((inputReserves * outputAmount) * 1_000) / ((outputReserves - outputAmount) * 997); }`

```
1
2  **Proof of Code/concempt:**
3  ... diff
4  function testFlawedExactOutput() public{
5      uint256 initialLiquidity = 100e18;
6      vm.startPrank(LiquidityProvider);
7      weth.approve(address(pool), initialLiquidity);
8      poolToken.approve(address(pool), initialLiquidity);
9
10     pool.deposit({
11         wethToDeposit: initialLiquidity,
12         minimumLiquidityTokenToMint: 0,
13         maximumPoolTokensDeposit: initialLiquidity,
14         deadline: uint64(block.timestamp),
15     });
16     vm.stopPrank();
17 }
18 ...
19
20 **Recommended Mitigation:**
21 ...diff
22 function getInputAmountBasedOnOutput(
23     uint256 outputAmount,
24     uint256 inputReserves,
25     uint256 outputReserves
26 )
27     public
28     pure
29     revertIfZero(outputAmount)
30     revertIfZero(outputReserves)
31     returns (uint256 inputAmount)
```

```

32     {
33 -         return ((inputReserves * outputAmount) * 10_000) / ((
           outputReserves - outputAmount) * 997);
34 +         return ((inputReserves * outputAmount) * 1_000) / ((
           outputReserves - outputAmount) * 997);
35     }

```

[H-2] Lack of slippage protection in TSwapPool::swapExactOutput causes users to potentially receive way fewer tokens

Description:

The `swapExactOutput` function does not include any sort of slippage protection. This function is similar to what is done in `TSwapPool::swapExactInput`, where the function specifies a `minOutputAmount`, the `swapExactOutput` function should specify a `maxInputAmount`.

Impact: If market conditions change before the transaction processes, the user could get a much worse swap.

Proof of Code/concempt: 1. The price of 1 WETH right now is 1,000 USDC 2. User inputs a `swapExactOutput` looking for 1 WETH

1. inputToken = USDC
2. outputToken = WETH
3. outputAmount = 1
4. deadline = whatever
5. The function does not offer a maxInput amount
6. As the transaction is pending in the mempool, the market changes! And the price moves HUGE
-> 1 WETH is now 10,000 USDC. 10x more than the user expected
7. The transaction completes, but the user sent the protocol 10,000 USDC instead of the expected 1,000 USDC

Recommended Mitigation: We should include a `maxInputAmount` so the user only has to spend up to a specific amount, and can predict how much they will spend on the protocol.

```

1     function swapExactOutput(
2         IERC20 inputToken,
3 +         uint256 maxInputAmount,
4     .
5     .
6     .
7         inputAmount = getInputAmountBasedOnOutput(outputAmount,
           inputReserves, outputReserves);
8 +     if(inputAmount > maxInputAmount){
9 +         revert();

```

```
10 +     }
11     _swap(inputToken, inputAmount, outputToken, outputAmount);
12     }
```

[H-3] ### TSwapPool::sellPoolTokens mismatches input and output tokens causing users to receive the incorrect amount of tokens

Description:

The `sellPoolTokens` function is intended to allow users to easily sell pool tokens and receive WETH in exchange. Users indicate how many pool tokens they're willing to sell in the `poolTokenAmount` parameter. However, the function currently miscalculates the swapped amount.

This is due to the fact that the `swapExactOutput` function is called, whereas the `swapExactInput` function is the one that should be called. Because users specify the exact amount of input tokens, not output.

Impact: Users will swap the wrong amount of tokens, which is a severe disruption of protocol functionality.

Proof of Code/concept: Recommended Mitigation: Consider changing the implementation to use `swapExactInput` instead of `swapExactOutput`. Note that this would also require changing the `sellPoolTokens` function to accept a new parameter (ie `minWethToReceive` to be passed to `swapExactInput`)

```
1     function sellPoolTokens(
2         uint256 poolTokenAmount,
3 +         uint256 minWethToReceive,
4         ) external returns (uint256 wethAmount) {
5 -         return swapExactOutput(i_poolToken, i_wethToken,
6 +         return swapExactInput(i_poolToken, poolTokenAmount,
7             poolTokenAmount, uint64(block.timestamp));
            i_wethToken, minWethToReceive, uint64(block.timestamp));
            }
```

[H-4] TSwapPool::deposit is missing deadline check causing transactions to complete even after the deadline

Description:

The `deposit` function accepts a deadline parameter, which according to the documentation is “The deadline for the transaction to be completed by”. However, this parameter is never used. As a consequence, operations that add liquidity to the pool might be executed at unexpected times, in market conditions where the deposit rate is unfavorable.

Impact: Transactions could be sent when market conditions are unfavorable to deposit, even when adding a deadline parameter.

Proof of Concept The deadline parameter is unused **Recommended Mitigation** Consider making the following change to the function.

```
1 function deposit(  
2     uint256 wethToDeposit,  
3     uint256 minimumLiquidityTokensToMint, // LP tokens -> if empty,  
        we can pick 100% (100% == 17 tokens)  
4     uint256 maximumPoolTokensToDeposit,  
5     uint64 deadline  
6 )  
7     external  
8 +     revertIfDeadlinePassed(deadline)  
9     revertIfZero(wethToDeposit)  
10    returns (uint256 liquidityTokensToMint)  
11 {
```

[H-5] In TSwapPool::_swap the extra tokens given to users after every swapCount breaks the protocol invariant of $x * y = k$

Description The protocol follows a strict invariant of $x * y = k$. Where:

x: The balance of the pool token y: The balance of WETH k: The constant product of the two balances
This means, that whenever the balances change in the protocol, the ratio between the two amounts should remain constant, hence the k. However, this is broken due to the extra incentive in the _swap function. Meaning that over time the protocol funds will be drained.

The follow block of code is responsible for the issue.

```
1     swap_count++;  
2     if (swap_count >= SWAP_COUNT_MAX) {  
3         swap_count = 0;  
4         outputToken.safeTransfer(msg.sender, 1  
            _000_000_000_000_000_000);  
5     }
```

Impact: A user could maliciously drain the protocol of funds by doing a lot of swaps and collecting the extra incentive given out by the protocol.

Most simply put, the protocol's core invariant is broken.

Proof of Concept: 1. A user swaps 10 times, and collects the extra incentive of 1_000_000_000_000_000_000 tokens 2. That user continues to swap untill all the protocol funds are drained

Proof of code Place the following into TSwapPool.t.sol.

```

1
2     function testInvariantBroken() public {
3         vm.startPrank(liquidityProvider);
4         weth.approve(address(pool), 100e18);
5         poolToken.approve(address(pool), 100e18);
6         pool.deposit(100e18, 100e18, 100e18, uint64(block.timestamp));
7         vm.stopPrank();
8
9         uint256 outputWeth = 1e17;
10
11        vm.startPrank(user);
12        poolToken.approve(address(pool), type(uint256).max);
13        poolToken.mint(user, 100e18);
14        pool.swapExactOutput(poolToken, weth, outputWeth, uint64(block.
15            timestamp));
16        pool.swapExactOutput(poolToken, weth, outputWeth, uint64(block.
17            timestamp));
18        pool.swapExactOutput(poolToken, weth, outputWeth, uint64(block.
19            timestamp));
20        pool.swapExactOutput(poolToken, weth, outputWeth, uint64(block.
21            timestamp));
22        pool.swapExactOutput(poolToken, weth, outputWeth, uint64(block.
23            timestamp));
24        int256 startingY = int256(weth.balanceOf(address(pool)));
25        int256 expectedDeltaY = int256(-1) * int256(outputWeth);
26
27        pool.swapExactOutput(poolToken, weth, outputWeth, uint64(block.
28            timestamp));
29        vm.stopPrank();
30
31        uint256 endingY = weth.balanceOf(address(pool));
32        int256 actualDeltaY = int256(endingY) - int256(startingY);
33        assertEq(actualDeltaY, expectedDeltaY);
34    }

```

Recommended Mitigation Remove the extra incentive mechanism. If you want to keep this in, we should account for the change in the $x * y = k$ protocol invariant. Or, we should set aside tokens in the same way we do with fees.

```

1 -     swap_count++;
2 -     // Fee-on-transfer

```

```

3 -         if (swap_count >= SWAP_COUNT_MAX) {
4 -             swap_count = 0;
5 -             outputToken.safeTransfer(msg.sender, 1
6 -                 _000_000_000_000_000_000);

```

Medium

[M-1] TSwapPool::deposit is missing deadline check causing transactions to complete even after the deadline

Description: The `deposit` function accepts a deadline parameter, which according to the documentation is “The deadline for the transaction to be completed by”. However, this parameter is never used. As a consequence, operations that add liquidity to the pool might be executed at unexpected times, in market conditions where the deposit rate is unfavorable. **Impact:** Transactions could be sent when market conditions are unfavorable, even when adding a deadline parameter.

Proof of Concept: The `deadline` parameter is unused.

```

1 Warning (5667): Unused function parameter. Remove or comment out the
  variable name to silence this warning.
2 --> src/TSwapPool.sol:96:9:
3   |
4 96 |         uint64 deadline
5   |         ^^^^^^^^^^^^^^^^^

```

Recommended Mitigation: Consider making the following change to the function:

```

1 function deposit(
2     uint256 wethToDeposit,
3     uint256 minimumLiquidityTokensToMint,
4     uint256 maximumPoolTokensToDeposit,
5     uint64 deadline
6 )
7     external
8 +     revertIfDeadlinePassed(deadline)
9     revertIfZero(wethToDeposit)
10    returns (uint256 liquidityTokensToMint)
11    {...}

```

[L-1] ### TSwapPool::LiquidityAdded event has parameters out of order .

Description:

What the `LiquidityAdded` event is emitted in the `TSwapPool::_addLiquidityMintAndTransfer`

function, it logs values in an incorrect order. The `poolTokensToDeposit` value should go in the third parameter position, whereas the `wethToDeposit` value should go second.

Impact: Event emission is incorrect, leading to off-chain functions potentially malfunctioning.

Recommended Mitigation:

```
1 - emit LiquidityAdded(msg.sender, poolTokensToDeposit, wethToDeposit);
2 + emit LiquidityAdded(msg.sender, wethToDeposit, poolTokensToDeposit);
```

[L-2] Default value returned by `TSwapPool::swapExactInput` results in incorrect return value given

Description:

The `swapExactInput` function is expected to return the actual amount of tokens bought by the caller. However, while it declares the named return value `output` it is never assigned a value, nor uses an explicit return statement.

Impact: The return value will always be 0, giving incorrect information to the caller.

Proof of Code/concept: Recommended Mitigation:

```
1 {
2     uint256 inputReserves = inputToken.balanceOf(address(this));
3     uint256 outputReserves = outputToken.balanceOf(address(this));
4
5 -     uint256 outputAmount = getOutputAmountBasedOnInput(inputAmount
6 +     , inputReserves, outputReserves);
7     output = getOutputAmountBasedOnInput(inputAmount,
8     inputReserves, outputReserves);
9
10 -     if (output < minOutputAmount) {
11 -         revert TSwapPool__OutputTooLow(outputAmount,
12         minOutputAmount);
13 +     if (output < minOutputAmount) {
14 +         revert TSwapPool__OutputTooLow(outputAmount,
15         minOutputAmount);
16 }
17 }
```

[S-#] TITLE (Root cause + Impact)

Description:

Impact: Proof of Code/concempt: Recommended Mitigation:

[S-#] TITLE (Root cause + Impact)

Description:

Impact: Proof of Code/concempt: Recommended Mitigation:

[S-#] TITLE (Root cause + Impact)

Description:

Impact: Proof of Code/concempt: Recommended Mitigation:

Informationals

[I-1] poolFactory:: PoolFactory__PoolAlreadyExists error is not being

```
1 - error PoolFactory__PoolAlreadyExists(address tokenAddress);
```

[I-2] Lacking zero address checks

```
1 constructor(address wethToken) {  
2 + if(wethToken == address(0)){  
3     revert();  
4 }  
5 -     i_wethToken = wethToken;  
6 }
```

[I-3] poolFactory:: createPool should use .symbol() instead of .name()

```
1 - string memory liquidityTokenSymbol = string.concat("ts", IERC20(  
    tokenAddress).name());  
2  
3 + string memory liquidityTokenSymbol= string.concat("ts", IERC20(  
    tokenAddress).symbol());
```