

Protocol Audit Report

6pillz

june 14, 2024



TSwap Protocol Audit Report

Version 1.0

Cyfrin.io

June 14, 2024

Protocol Audit Report

6pillz

june 14, 2024

Prepared by: 6pillz Lead Auditors: -

Table of Contents

- Table of Contents
- Protocol Summary
- Disclaimer
- Risk Classification
- Audit Details
 - Scope
 - Roles
- Executive Summary
 - Issues found
- Findings
- Aderyn Analysis Report
- Table of Contents
- Summary
 - Files Summary
 - Files Details
 - Issue Summary
- Low Issues
 - L-1: **public** functions not used internally could be marked **external**
 - L-2: Define and use **constant** variables instead of using literals
 - L-3: Event is missing **indexed** fields
 - L-4: PUSH0 is not supported by all chains
 - L-5: Large literal values multiples of 10000 can be replaced with scientific notation
 - L-6: Unused Custom Error
 - High
 - * [H-1] **TSwapPool::deposit** is missing deadline check causing transactions to complete even after the deadline
 - * [H-2] Incorrect fee calculation in **TSwapPool::getInputAmountBasedOnOutput** causes protocol to take too many tokens from users, resulting in lost fees

- * [H-3] Lack of slippage protection in `TSwapPool::swapExactOutput` causes users to potentially receive way fewer tokens
- * [H-4] `TSwapPool::sellPoolTokens` mismatches input and output tokens causing users to receive the incorrect amount of tokens
- * [H-5] In `TSwapPool::_swap` the extra tokens given to users after every `swapCount` breaks the protocol invariant of $x * y = k$
- Low
 - * [L-1] `TSwapPool::LiquidityAdded` event has parameters out of order
 - * [L-2] Default value returned by `TSwapPool::swapExactInput` results in incorrect return value given
- Informationals
 - * [I-1] `PoolFactory::PoolFactory__PoolDoesNotExist` is not used and should be removed
 - * [I-2] Lacking zero address checks
 - * [I-3] `PoolFactory::createPool` should use `.symbol()` instead of `.name()`
 - * [I-4] Event is missing `indexed` fields

Protocol Summary

Disclaimer

The YOUR_NAME_HERE team makes all effort to find as many vulnerabilities in the code in the given time period, but holds no responsibilities for the findings provided in this document. A security audit by the team is not an endorsement of the underlying business or product. The audit was time-boxed and the review of the code was solely on the security aspects of the Solidity implementation of the contracts.

Risk Classification

		Impact		
Likelihood	High	High	Medium	Low
	Medium	H/M	M	M/L
	Low	M	M/L	L

We use the CodeHawks severity matrix to determine severity. See the documentation for more details.

Audit Details

Scope

Roles

Executive Summary

Issues found

Severtity	Number of issues found
High	4
Medium	2
Low	2
Info	9
Total	17

Findings

Aderyn Analysis Report

This report was generated by Aderyn, a static analysis tool built by Cyfrin, a blockchain security company. This report is not a substitute for manual audit or security review. It should not be relied upon for any purpose other than to assist in the identification of potential security vulnerabilities. # Table of Contents

- Summary
 - Files Summary
 - Files Details
 - Issue Summary
- Low Issues
 - L-1: `public` functions not used internally could be marked `external`
 - L-2: Define and use `constant` variables instead of using literals
 - L-3: Event is missing `indexed` fields
 - L-4: PUSH0 is not supported by all chains
 - L-5: Large literal values multiples of 10000 can be replaced with scientific notation
 - L-6: Unused Custom Error

Summary

Files Summary

Key	Value
.sol Files	2
Total nSLOC	350

Files Details

Filepath	nSLOC
src/PoolFactory.sol	35
src/TSwapPool.sol	315
Total	350

Issue Summary

Category	No. of Issues
High	0
Low	6

Low Issues

L-1: public functions not used internally could be marked external

Instead of marking a function as `public`, consider marking it as `external` if it is not used internally.

1 Found Instances

- Found in src/TSwapPool.sol Line: 298

```
function swapExactInput(
```

L-2: Define and use constant variables instead of using literals

If the same constant literal value is used multiple times, create a constant state variable and reference it throughout the contract.

4 Found Instances

- Found in src/TSwapPool.sol Line: 276

```
uint256 inputAmountMinusFee = inputAmount * 997;
```

- Found in src/TSwapPool.sol Line: 295

```
((outputReserves - outputAmount) * 997);
```

- Found in src/TSwapPool.sol Line: 454

```
1e18,
```

- Found in src/TSwapPool.sol Line: 463

```
1e18,
```

L-3: Event is missing indexed fields

Index event fields make the field more quickly accessible to off-chain tools that parse events. However, note that each index field costs extra gas during emission, so it's not necessarily best to index the maximum allowed per event (three fields). Each event should use three indexed fields if there are three or more fields, and gas usage is not particularly of concern for the events in question. If there are fewer than three fields, all of the fields should be indexed.

4 Found Instances

- Found in src/PoolFactory.sol Line: 35

```
event PoolCreated(address tokenAddress, address poolAddress);
```

- Found in src/TSwapPool.sol Line: 52

```
event LiquidityAdded(
```

- Found in src/TSwapPool.sol Line: 57

```
event LiquidityRemoved(
```

- Found in src/TSwapPool.sol Line: 62

```
event Swap(
```

L-4: PUSH0 is not supported by all chains

Solc compiler version 0.8.20 switches the default target EVM version to Shanghai, which means that the generated bytecode will include PUSH0 opcodes. Be sure to select the appropriate EVM version in case you intend to deploy on a chain other than mainnet like L2 chains that may not support PUSH0, otherwise deployment of your contracts will fail.

2 Found Instances

- Found in src/PoolFactory.sol Line: 15

```
pragma solidity 0.8.20;
```

- Found in src/TSwapPool.sol Line: 15

```
pragma solidity 0.8.20;
```

L-5: Large literal values multiples of 10000 can be replaced with scientific notation

Use **e** notation, for example: **1e18**, instead of its full numeric value.

3 Found Instances

- Found in src/TSwapPool.sol Line: 45

```
uint256 private constant MINIMUM_WETH_LIQUIDITY = 1_000_000_000;
```
- Found in src/TSwapPool.sol Line: 294

```
((inputReserves * outputAmount) * 10000) /
```
- Found in src/TSwapPool.sol Line: 402

```
outputToken.safeTransfer(msg.sender, 1_000_000_000_000_000_000);
```

L-6: Unused Custom Error

it is recommended that the definition be removed when custom error is unused

1 Found Instances

- Found in src/PoolFactory.sol Line: 22

```
error PoolFactory__PoolDoesNotExist(address tokenAddress);
```

High

[H-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 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.

```
function deposit(
    uint256 wethToDeposit,
    uint256 minimumLiquidityTokensToMint, // LP tokens -> if empty, we can pick 100% (1000000000000000000)
    uint256 maximumPoolTokensToDeposit,
    uint64 deadline
)
```



```

        external
+       revertIfDeadlinePassed(deadline)
        revertIfZero(wethToDeposit)
        returns (uint256 liquidityTokensToMint)
    }

```

[H-2] 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:

```

    function getInputAmountBasedOnOutput(
        uint256 outputAmount,
        uint256 inputReserves,
        uint256 outputReserves
    )
        public
        pure
        revertIfZero(outputAmount)
        revertIfZero(outputReserves)
        returns (uint256 inputAmount)
    {
-       return ((inputReserves * outputAmount) * 10_000) / ((outputReserves - outputAmount)
+       return ((inputReserves * outputAmount) * 1_000) / ((outputReserves - outputAmount)
    }

```

[H-3] 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 Concept: 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` 3. The

function does not offer a `maxInput` amount 4. 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 5. 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.

```
function swapExactOutput(
    IERC20 inputToken,
+    uint256 maxInputAmount,
    .
    .
    .
    inputAmount = getInputAmountBasedOnOutput(outputAmount, inputReserves, outputReserve
+    if(inputAmount > maxInputAmount){
+        revert();
+    }
    _swap(inputToken, inputAmount, outputToken, outputAmount);
```

[H-4] `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 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`)

```
function sellPoolTokens(
    uint256 poolTokenAmount,
+    uint256 minWethToReceive,
    ) external returns (uint256 wethAmount) {
```

```

-         return swapExactOutput(i_poolToken, i_wethToken, poolTokenAmount, uint64(block.timestamp));
+         return swapExactInput(i_poolToken, poolTokenAmount, i_wethToken, minWethToReceive, poolTokenAmount);
    }

```

Additionally, it might be wise to add a deadline to the function, as there is currently no deadline. (MEV later)

[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.

```

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

```

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.

```

function testInvariantBroken() public {
    vm.startPrank(liquidityProvider);
    weth.approve(address(pool), 100e18);
    poolToken.approve(address(pool), 100e18);
    pool.deposit(100e18, 100e18, 100e18, uint64(block.timestamp));
    vm.stopPrank();

    uint256 outputWeth = 1e17;

    vm.startPrank(user);

```

```

poolToken.approve(address(pool), type(uint256).max);
poolToken.mint(user, 100e18);
pool.swapExactOutput(poolToken, weth, outputWeth, uint64(block.timestamp));
pool.swapExactOutput(poolToken, weth, outputWeth, uint64(block.timestamp));
pool.swapExactOutput(poolToken, weth, outputWeth, uint64(block.timestamp));
pool.swapExactOutput(poolToken, weth, outputWeth, uint64(block.timestamp));
pool.swapExactOutput(poolToken, weth, outputWeth, uint64(block.timestamp));
pool.swapExactOutput(poolToken, weth, outputWeth, uint64(block.timestamp));
pool.swapExactOutput(poolToken, weth, outputWeth, uint64(block.timestamp));
pool.swapExactOutput(poolToken, weth, outputWeth, uint64(block.timestamp));
pool.swapExactOutput(poolToken, weth, outputWeth, uint64(block.timestamp));

int256 startingY = int256(weth.balanceOf(address(pool)));
int256 expectedDeltaY = int256(-1) * int256(outputWeth);

pool.swapExactOutput(poolToken, weth, outputWeth, uint64(block.timestamp));
vm.stopPrank();

uint256 endingY = weth.balanceOf(address(pool));
int256 actualDeltaY = int256(endingY) - int256(startingY);
assertEq(actualDeltaY, expectedDeltaY);
}

```

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.

```

-     swap_count++;
-     // Fee-on-transfer
-     if (swap_count >= SWAP_COUNT_MAX) {
-         swap_count = 0;
-         outputToken.safeTransfer(msg.sender, 1_000_000_000_000_000);
-     }

```

Low

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

Description: When 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:

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

Recommended Mitigation:

```
{
    uint256 inputReserves = inputToken.balanceOf(address(this));
    uint256 outputReserves = outputToken.balanceOf(address(this));

-    uint256 outputAmount = getOutputAmountBasedOnInput(inputAmount, inputReserves, outputReserves);
+    output = getOutputAmountBasedOnInput(inputAmount, inputReserves, outputReserves);

-    if (output < minOutputAmount) {
-        revert TSwapPool__OutputTooLow(outputAmount, minOutputAmount);
+    if (output < minOutputAmount) {
+        revert TSwapPool__OutputTooLow(outputAmount, minOutputAmount);
    }

-    _swap(inputToken, inputAmount, outputToken, outputAmount);
+    _swap(inputToken, inputAmount, outputToken, output);
}
```

Informationals

[I-1] PoolFactory::PoolFactory__PoolDoesNotExist is not used and should be removed

```
- error PoolFactory__PoolDoesNotExist(address tokenAddress);
```

[I-2] Lacking zero address checks

```
constructor(address wethToken) {
+    if(wethToken == address(0)) {
+        revert();
+    }
    i_wethToken = wethToken;
}
```

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

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

[I-4] Event is missing indexed fields

Index event fields make the field more quickly accessible to off-chain tools that parse events. However, note that each index field costs extra gas during emission, so it's not necessarily best to index the maximum allowed per event (three fields). Each event should use three indexed fields if there are three or more fields, and gas usage is not particularly of concern for the events in question. If there are fewer than three fields, all of the fields should be indexed.

- Found in src/TSwapPool.sol: Line: 44
- Found in src/PoolFactory.sol: Line: 37
- Found in src/TSwapPool.sol: Line: 46
- Found in src/TSwapPool.sol: Line: 43