# Smart Contract Security Audit Report

[2021]

# Table Of Contents

# 1 Executive Summary

On 2021.05.06, the SlowMist security team received the O3 swap team's security audit application for O3 swap, developed the audit plan according to the agreement of both parties and the characteristics of the project, and finally issued the security audit report.

The SlowMist security team adopts the strategy of "white box lead, black, grey box assists" to conduct a complete security test on the project in the way closest to the real attack.

The test method information:

| Test method | Description |
| --- | --- |
| Black box testing | Conduct security tests from an attacker's perspective externally. |
| Grey box testing | Conduct security testing on code modules through the scripting tool, observing the internal running status, mining weaknesses. |
| White box testing | Based on the open source code, non-open source code, to detect whether there are vulnerabilities in programs such as nodes, SDK, etc. |

The vulnerability severity level information:

| Level | Description |
| --- | --- |
| Critical | Critical severity vulnerabilities will have a significant impact on the security of the DeFi project, and it is strongly recommended to fix the critical vulnerabilities. |
| High | High severity vulnerabilities will affect the normal operation of the DeFi project. It is strongly recommended to fix high-risk vulnerabilities. |
| Medium | Medium severity vulnerability will affect the operation of the DeFi project. It is recommended to fix medium-risk vulnerabilities. |
| Low | Low severity vulnerabilities may affect the operation of the DeFi project in certain scenarios. It is suggested that the project party should evaluate and consider whether these vulnerabilities need to be fixed. |
| Weakness | There are safety risks theoretically, but it is extremely difficult to reproduce in engineering. |

| Level | Description |
| --- | --- |
| Suggestion | There are better practices for coding or architecture. |

# 2 Audit Methodology

The security audit process of SlowMist security team for smart contract includes two steps:

Smart contract codes are scanned/tested for commonly known and more specific vulnerabilities using automated analysis tools.

Manual audit of the codes for security issues. The contracts are manually analyzed to look for any potential problems.

Following is the list of commonly known vulnerabilities that was considered during the audit of the smart contract:

- Reentrancy Vulnerability
- Replay Vulnerability
- Reordering Vulnerability
- Short Address Vulnerability
- Denial of Service Vulnerability
- Transaction Ordering Dependence Vulnerability
- Race Conditions Vulnerability
- Authority Control Vulnerability
- Integer Overflow and Underflow Vulnerability
- TimeStamp Dependence Vulnerability
- Uninitialized Storage Pointers Vulnerability
- Arithmetic Accuracy Deviation Vulnerability
- tx.origin Authentication Vulnerability

- "False top-up" Vulnerability
- Variable Coverage Vulnerability
- Gas Optimization Audit
- Malicious Event Log Audit
- Redundant Fallback Function Audit
- Unsafe External Call Audit
- Explicit Visibility of Functions State Variables Aduit
- Design Logic Audit
- Scoping and Declarations Audit

# 3 Project Overview

## 3.1 Project Introduction

O3 Swap is a proprietary cross-chain aggregation protocol built by O3 Labs. The mission of O3 Swap is to provide consumers access to cryptocurrency-based, financial services, allowing them to exchange, or ‘swap’, various digital assets within their O3 Wallet. The benefits of this design can be attributed to the high level of safety and security that is inherent to the decentralized model of asset storage and protection. The platform also provides ‘cross-chain’ swaps to conduct exchange settlements without regard to the limitations of a typical isolated Blockchain network. The term ‘cross-chain’ derives itself from the fact that the exchange is executed after traveling across two or more separate blockchain networks. With a cross-chain swap, the initial asset and the target asset are deployed on two isolated Blockchains that otherwise are non-communicative. In light of the advanced development of decentralized financial protocols (DeFi) and the increasingly mature markets for lending, exchange, derivatives, etc., The O3 Swap protocol, in cooperation with its associated decentralized wallet software, provides a one-stop aggregation &

exchange platform for consumers and offers developers access to an open, distributed, limitless, and secure — trading environment.

Initial Audit File Informations

Github：

https://github.com/O3Labs/o3swap-aggregator-contracts

commit: c46ed522534fdfc279344a4945e9159241f2c9bf

Github:

https://github.com/O3Labs/o3swap-contracts

commit: 53c009e09ece07328a3a566262dbc4f8a1697478

Fixed Files Informations

Github：

https://github.com/O3Labs/o3swap-aggregator-contracts

commit: ee0b0c395ce165c163449d5db36f83d673a5ef08

Github:

https://github.com/O3Labs/o3swap-contracts

commit: 57884e1ae1d3c7d08b7fc3c61339532d1d9791f0

## 3.2 Vulnerability Information

The following is the status of the vulnerabilities found in this audit:

| NO | Title | Category | Level | Status |
| --- | --- | --- | --- | --- |
| N1 | Did not check whether the pair exists | Others | Suggestion | Fixed |
| N2 | Excessive permissions | Authority Control Vulnerability | Medium | Fixed |

# 4 Code Overview

## 4.1 Contracts Description

The main network address of the contract is as follows:

**The code was not deployed to the mainnet.**

## 4.2 Visibility Description

The SlowMist Security team analyzed the visibility of major contracts during the audit, the result as follows:

| Context | | | |
|---|---|---|---|
| Function Name | Visibility | Mutability | Modifiers |
| _msgSender | internal | - | - |
| _msgData | internal | - | - |

| Ownable | | | |
|---|---|---|---|
| Function Name | Visibility | Mutability | Modifiers |
| _msgSender | internal | - | - |
| _msgData | internal | - | - |
| constructor | internal | can modify state | - |
| owner | public | - | - |
| renounceOwnership | public | can modify state | onlyOwner |
| transferOwnership | public | can modify state | onlyOwner |

| O3SwapBSCPancakeBridge | | | |
|---|---|---|---|
| Function Name | Visibility | Mutability | Modifiers |
| constructor | internal | can modify state | - |
| owner | public | - | - |
| renounceOwnership | public | can modify state | onlyOwner |
| transferOwnership | public | can modify state | onlyOwner |
| _msgSender | internal | - | - |
| _msgData | internal | - | - |
| constructor | public | can modify state | - |
| swapExactTokensForTokensSupportingFeeOnTransferTokens | external | can modify state | ensure |
| swapExactTokensForTokensSupportingFeeOnTransferTokensCrossChain | external | payable | ensure |
| _swapExactTokensForTokensSupportingFeeOnTransferTokens | internal | can modify state | - |
| swapExactETHForTokensSupportingFeeOnTransferTokens | external | payable | ensure |
| swapExactETHForTokensSupportingFeeOnTransferTokensCrossChain | external | payable | ensure |
| _swapExactETHForTokensSupportingFeeOnTransferTokens | internal | can modify state | - |
| swapExactTokensForETHSupportingFeeOnTransferTokens | external | can modify state | ensure |
| _swapExactTokensForETHSupportingFeeOnTransferTokens | internal | can modify state | - |
| _swapSupportingFeeOnTransferTokens | internal | can modify state | - |
| _cross | internal | can modify state | - |

| O3SwapBSCPancakeBridge | | | |
|---|---|---|---|
| receive | external | payable | - |
| setPolySwapperId | external | can modify state | onlyOwner |
| collect | external | can modify state | - |
| setAggregatorFee | external | can modify state | onlyOwner |
| setPancakeFactory | external | can modify state | onlyOwner |
| setPolySwapper | external | can modify state | onlyOwner |
| setWBNB | external | can modify state | onlyOwner |

| ReentrancyGuard | | | |
|---|---|---|---|
| Function Name | Visibility | Mutability | Modifiers |
| constructor | internal | can modify state | - |

| O3Staking | | | |
|---|---|---|---|
| Function Name | Visibility | Mutability | Modifiers |
| constructor | internal | can modify state | - |
| constructor | internal | can modify state | - |
| owner | public | - | - |
| renounceOwnership | public | can modify state | onlyOwner |
| transferOwnership | public | can modify state | onlyOwner |
| _msgSender | internal | - | - |
| _msgData | internal | - | - |

| O3Staking | | | |
|---|---|---|---|
| constructor | public | can modify state | - |
| getTotalProfit | external | - | - |
| getStakingAmount | external | - | - |
| getSharePerBlock | external | - | - |
| setStakingToke | external | can modify state | onlyOwner,*logs* |
| setSharePerBlock | external | can modify state | onlyOwner,*logs* |
| setStartUnstakeBlockIndex | external | can modify state | onlyOwner,*logs* |
| setStartClaimBlockIndex | external | can modify state | onlyOwner,*logs* |
| stake | external | can modify state | nonReentrant,*logs* |
| unstake | external | can modify state | nonReentrant,*logs* |
| claimProfit | external | can modify state | nonReentrant,*logs* |
| _getTotalProfit | internal | can modify state | - |
| _updateUserStakingRecord | internal | can modify state | - |
| _settleCurrentUserProfit | internal | - | - |
| _updateUnitProfitState | internal | can modify state | - |
| _updateUnitProfit | internal | can modify state | - |
| pauseStaking | external | can modify state | onlyOwner,*logs* |
| unpauseStaking | external | can modify state | onlyOwner,*logs* |
| pauseUnstake | external | can modify state | onlyOwner,*logs* |
| unpauseUnstake | external | can modify state | onlyOwner,*logs* |

| O3Staking | | | |
|---|---|---|---|
| pauseClaimProfit | external | can modify state | onlyOwner,*logs* |
| unpauseClaimProfit | external | can modify state | onlyOwner,*logs* |
| collect | external | can modify state | nonReentrant,onlyOwner,*logs* |
| _pushToken | internal | can modify state | - |
| _pushShareToken | internal | can modify state | - |
| _pullToken | internal | can modify state | - |

| O3SwapETHUniswapBridge | | | |
|---|---|---|---|
| Function Name | Visibility | Mutability | Modifiers |
| constructor | internal | can modify state | - |
| owner | public | - | - |
| renounceOwnership | public | can modify state | onlyOwner |
| transferOwnership | public | can modify state | onlyOwner |
| _msgSender | internal | - | - |
| _msgData | internal | - | - |
| constructor | public | can modify state | - |
| swapExactTokensForTokensSupportingFeeOnTransferTokens | external | can modify state | ensure |
| swapExactTokensForTokensSupportingFeeOnTransferTokensCrossChain | external | payable | ensure |
| _swapExactTokensForTokensSupportingFeeOnTransferTokens | internal | can modify state | - |
| swapExactETHForTokensSupportingFeeOnTransferTokens | external | payable | ensure |

| O3SwapETHUniswapBridge | | | |
|---|---|---|---|
| swapExactETHForTokensSupportingFeeOnTransferTokensCrossChain | external | payable | ensure |
| _swapExactETHForTokensSupportingFeeOnTransferTokens | internal | can modify state | - |
| swapExactTokensForETHSupportingFeeOnTransferTokens | external | can modify state | ensure |
| _swapExactTokensForETHSupportingFeeOnTransferTokens | internal | can modify state | - |
| _swapSupportingFeeOnTransferTokens | internal | can modify state | - |
| _cross | internal | can modify state | - |
| receive | external | payable | - |
| setPolySwapperId | external | can modify state | onlyOwner |
| collect | external | can modify state | - |
| setAggregatorFee | external | can modify state | onlyOwner |
| setUniswapFactory | external | can modify state | onlyOwner |
| setPolySwapper | external | can modify state | onlyOwner |
| setWETH | external | can modify state | onlyOwner |

| O3SwapHecoMdexBridge | | | |
|---|---|---|---|
| Function Name | Visibility | Mutability | Modifiers |
| constructor | internal | can modify state | - |
| owner | public | - | - |
| renounceOwnership | public | can modify state | onlyOwner |
| transferOwnership | public | can modify state | onlyOwner |

| O3SwapHecoMdexBridge | | | |
|---|---|---|---|
| _msgSender | internal | - | - |
| _msgData | internal | - | - |
| constructor | public | can modify state | - |
| swapExactTokensForTokensSupportingFeeOnTransferTokens | external | can modify state | ensure |
| swapExactTokensForTokensSupportingFeeOnTransferTokensCrossChain | external | payable | ensure |
| _swapExactTokensForTokensSupportingFeeOnTransferTokens | internal | can modify state | - |
| swapExactETHForTokensSupportingFeeOnTransferTokens | external | payable | ensure |
| swapExactETHForTokensSupportingFeeOnTransferTokensCrossChain | external | payable | ensure |
| _swapExactETHForTokensSupportingFeeOnTransferTokens | internal | can modify state | - |
| swapExactTokensForETHSupportingFeeOnTransferTokens | external | can modify state | ensure |
| _swapExactTokensForETHSupportingFeeOnTransferTokens | internal | can modify state | - |
| _swapSupportingFeeOnTransferTokens | internal | can modify state | - |
| _cross | internal | can modify state | - |
| receive | external | payable | - |
| setPolySwapperId | external | can modify state | onlyOwner |
| collect | external | can modify state | - |
| setAggregatorFee | external | can modify state | onlyOwner |
| setMdexFactory | external | can modify state | onlyOwner |

| O3SwapHecoMdexBridge | | | |
|---|---|---|---|
| setPolySwapper | external | can modify state | onlyOwner |
| setWHT | external | can modify state | onlyOwner |

| ERC20 | | | |
|---|---|---|---|
| Function Name | Visibility | Mutability | Modifiers |
| totalSupply | external | - | - |
| balanceOf | external | - | - |
| transfer | external | can modify state | - |
| allowance | external | - | - |
| approve | external | can modify state | - |
| transferFrom | external | can modify state | - |
| _msgSender | internal | - | - |
| _msgData | internal | - | - |
| constructor | public | can modify state | - |
| name | public | - | - |
| symbol | public | - | - |
| decimals | public | - | - |
| totalSupply | public | - | - |
| balanceOf | public | - | - |
| transfer | public | can modify state | - |

| ERC20 | | | |
|---|---|---|---|
| allowance | public | - | - |
| approve | public | can modify state | - |
| transferFrom | public | can modify state | - |
| increaseAllowance | public | can modify state | - |
| decreaseAllowance | public | can modify state | - |
| _transfer | internal | can modify state | - |
| _mint | internal | can modify state | - |
| _burn | internal | can modify state | - |
| _approve | internal | can modify state | - |
| _setupDecimals | internal | can modify state | - |
| _beforeTokenTransfer | internal | can modify state | - |

| O3 | | | |
|---|---|---|---|
| Function Name | Visibility | Mutability | Modifiers |
| constructor | internal | can modify state | - |
| getUnlockFactor | external | - | - |
| getUnlockBlockGap | external | - | - |
| totalUnlocked | external | - | - |
| unlockedOf | external | - | - |
| lockedOf | external | - | - |

| O3 | | | |
|---|---|---|---|
| getStaked | external | - | - |
| getUnlockSpeed | external | - | - |
| claimableUnlocked | external | - | - |
| setUnlockFactor | external | can modify state | - |
| setUnlockBlockGap | external | can modify state | - |
| stake | external | can modify state | - |
| unstake | external | can modify state | - |
| claimUnlocked | external | can modify state | - |
| setAuthorizedMintCaller | external | can modify state | - |
| removeAuthorizedMintCaller | external | can modify state | - |
| mintUnlockedToken | external | can modify state | - |
| mintLockedToken | external | can modify state | - |
| totalSupply | external | - | - |
| balanceOf | external | - | - |
| transfer | external | can modify state | - |
| allowance | external | - | - |
| approve | external | can modify state | - |
| transferFrom | external | can modify state | - |
| constructor | internal | can modify state | - |
| owner | public | - | - |

| O3 | | | |
|---|---|---|---|
| renounceOwnership | public | can modify state | onlyOwner |
| transferOwnership | public | can modify state | onlyOwner |
| _msgSender | internal | - | - |
| _msgData | internal | - | - |
| constructor | public | can modify state | - |
| name | public | - | - |
| symbol | public | - | - |
| decimals | public | - | - |
| totalSupply | public | - | - |
| balanceOf | public | - | - |
| transfer | public | can modify state | - |
| allowance | public | - | - |
| approve | public | can modify state | - |
| transferFrom | public | can modify state | - |
| increaseAllowance | public | can modify state | - |
| decreaseAllowance | public | can modify state | - |
| _transfer | internal | can modify state | - |
| _mint | internal | can modify state | - |
| _burn | internal | can modify state | - |
| _approve | internal | can modify state | - |

| O3 | | | |
|---|---|---|---|
| _setupDecimals | internal | can modify state | - |
| _beforeTokenTransfer | internal | can modify state | - |
| constructor | public | can modify state | - |
| getUnlockFactor | external | - | - |
| getUnlockBlockGap | external | - | - |
| totalUnlocked | external | - | - |
| unlockedOf | external | - | - |
| lockedOf | public | - | - |
| getStaked | external | - | - |
| getUnlockSpeed | external | - | - |
| claimableUnlocked | external | - | - |
| transfer | public | can modify state | - |
| transferFrom | public | can modify state | - |
| setUnlockFactor | external | can modify state | onlyOwner |
| setUnlockBlockGap | external | can modify state | onlyOwner |
| stake | external | can modify state | nonReentrant |
| unstake | external | can modify state | nonReentrant |
| claimUnlocked | external | can modify state | nonReentrant |
| _updateStakeRecord | internal | can modify state | - |
| mintUnlockedToken | external | can modify state | onlyAuthorizedMintCaller |

| O3 | | | |
|---|---|---|---|
| mintLockedToken | external | can modify state | onlyAuthorizedMintCaller |
| setAuthorizedMintCaller | external | can modify state | onlyOwner |
| removeAuthorizedMintCaller | external | can modify state | onlyOwner |
| _settleUnlockAmount | internal | - | - |
| _mintUnlocked | internal | can modify state | - |
| _getUnlockSpeed | internal | - | - |
| _unlockTransfer | internal | can modify state | - |
| _pullToken | internal | can modify state | - |
| _pushToken | internal | can modify state | - |

## 4.3 Vulnerability Summary

**[N1] [Suggestion] Did not check whether the pair exists**

**Category: Others**

**Content**

The _swapSupportingFeeOnTransferTokens function of the O3swapBSCPancakeBridge / O3swapETHUniswapBridge / O3swapHecoMdexBridge contract did not verify the existence of the pair, which caused the exchange to fail

```
function _swapSupportingFeeOnTransferTokens(address[] memory path, address _to)
internal virtual {
        for (uint i; i < path.length - 1; i++) {
            (address input, address output) = (path[i], path[i + 1]);
            (address token0,) = PancakeLibrary.sortTokens(input, output);
            //SlowMist// There is no check to see if the pair exists, which causes
the exchange to fail
```

```
            IPancakePair pair = IPancakePair(PancakeLibrary.pairFor(pancakeFactory,
input, output));
            uint amountInput;
            uint amountOutput;
            { // scope to avoid stack too deep errors
            (uint reserve0, uint reserve1,) = pair.getReserves();
            (uint reserveInput, uint reserveOutput) = input == token0 ? (reserve0,
reserve1) : (reserve1, reserve0);
            amountInput = IBEP20(input).balanceOf(address(pair)).sub(reserveInput);
            amountOutput = PancakeLibrary.getAmountOut(amountInput, reserveInput,
reserveOutput);
            }
            (uint amount0Out, uint amount1Out) = input == token0 ? (uint(0),
amountOutput) : (amountOutput, uint(0));
            address to = i < path.length - 2 ? PancakeLibrary.pairFor(pancakeFactory,
output, path[i + 2]) : _to;
            pair.swap(amount0Out, amount1Out, to, new bytes(0));
        }
    }
```

**Solution**

It is recommended to add a check

**Status**

Fixed

### [N2] [Medium] Excessive permissions

**Category: Authority Control Vulnerability**

**Content**

The collect function of the O3 staking contract can transfer any tokens in the contract, including the user's assets.

There is a problem of excessive authority. It is recommended to limit the token != stakingToken

```
    function collect(address token, address to) external nonReentrant onlyOwner
_logs_ {
        //SlowMist// Excessive authority issues,  should be restricted token !=
staking Token
        uint balance = IERC20(token).balanceOf(address(this));
        _pushToken(token, to, balance);
    }
```

**Solution**

Restricted transfer of tokens cannot be stakingToken

**Status**

Fixed

# 5 Audit Result

| Audit Number | Audit Team | Audit Date | Audit Result |
| --- | --- | --- | --- |
| 0X002105140003 | SlowMist Security Team | 2021.05.06 - 2021.05.14 | Passed |

Summary conclusion: The SlowMist security team use a manual and SlowMist team's analysis tool to audit the project, during the audit work we found 1 medium risk, 1 low risk. And 1 medium risk, 1 low risk were confirmed and being fixed; . The code was not deployed to the mainnet.

# 6 Statement

SlowMist issues this report with reference to the facts that have occurred or existed before the issuance of this report, and only assumes corresponding responsibility based on these.

For the facts that occurred or existed after the issuance, SlowMist is not able to judge the security status of this project, and is not responsible for them. The security audit analysis and other contents of this report are based on the documents and materials provided to SlowMist by the information provider till the date of the insurance report (referred to as "provided information"). SlowMist assumes: The information provided is not missing, tampered with, deleted or concealed. If the information provided is missing, tampered with, deleted, concealed, or inconsistent with the actual situation, the SlowMist shall not be liable for any loss or adverse effect resulting therefrom. SlowMist only conducts the agreed security audit on the security situation of the project and issues this report. SlowMist is not responsible for the background and other conditions of the project.

**Official Website**

www.slowmist.com

**E-mail**

team@slowmist.com

**Twitter**

@SlowMist_Team

**Github**

https://github.com/slowmist