Cyberscope

Audit Report

TokenSwap

July 2022

SH256 02af39b877c34a8e3c561de08692e75a84ab561e579b9e8a0d77199b73276582

Audited by © cyberscope

Table of Contents

Contract Review

Contract Name	TokenSwap
Test Deploy	https://testnet.bscscan.com/address/0xa122cDb6DaF69AC9021799724aCe84b6842aE853
Domain	https://hyfinance.net

Audit Updates

Initial Audit	15th July 2022
Corrected	20th July 2022

Source Files

Filename	SHA256
@openzeppelin/contracts/access/Ownable.sol	754825f501dd014526eee0c415687b0f6c600533adfc872f7d45edb4f8b3b053
@openzeppelin/contracts/math/SafeMath.sol	f6d6214aa03f8dd6d6d14b7c15ffa387b3f1ce38ba3a215177baa132a44636e2
@openzeppelin/contracts/token/ERC20/IERC20.sol	c4b741712b8dc93ab3945205554a3ba2f80953e64d684e752d5a0fd07fc93f22
@openzeppelin/contracts/token/ERC20/SafeERC20.sol	74e10f4538df92e1c89140f16654914be8d7e9a66b24d6272ff0f28f89f8728b
@openzeppelin/contracts/utils/Address.sol	a22903d00a93aa211164d90ad11f01ccc7d34648114be89ec38c859fdea0f8d4
@openzeppelin/contracts/utils/Context.sol	eafb62c654640a07832b56e00902b4bf249633346585331af311c738b1c23bc5
contracts/interfaces/JoeRouter.sol	f644fa50a83f151fa7c8927056e5122223dba51741404a1e37617969e947af88
contracts/TokenSwap.sol	02af39b877c34a8e3c561de08692e75a84ab561e579b9e8a0d77199b73276582

Introduction

The TokenSwap contract core functionality is to swap two tokens. The contract is operating as a wrapper between the client and the DEX router. The TokenSwap transfers the tokens temporarily to the contract until the transaction is finished. The swap operation can only be applied by the pool role. The pool role can only be set by the contract owner.

Contract Diagnostics

Critical Medium Minor

Severity	Code	Description	Status
	OCTD	Contract Owner is not able to transfer tokens from specific address	Multi-Sign
	CR	Code Repetition	Acknowledged
	L04	Conformance to Solidity Naming Conventions	Acknowledged

OCTD - Owner Contract Tokens Drain

Criticality	minor
Location	contract.sol#L42
Status	Multi-Sign

Description

The contract owner has the authority to claim all the balance of the contract. The owner may take advantage of it by calling the adminWithdraw function.

```
function adminWithdraw(address token, uint256 amount) external onlyOwner {
        require(IERC20(token).balanceOf(address(this)) >= amount, "Amount too high");
        IERC20(token).safeTransfer(msg.sender, amount);
}
```

Recommendation

The team should carefully manage the private keys of the owner’s account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions. That risk can be prevented by temporarily locking the contract or renouncing ownership.

Updated 20 July 2022

The team has acknowledged that thread and transferred the contract ownership to a multi-sign mechanism.

CR- Code Repetition

Criticality	minor
Location	contract.sol#L50,L74
Status	Acknowledged

Description

There are code segments that are repetitive in the contract. Those segments increase the code size of the contract unnecessarily.

```
path[0] = token1;
path[1] = token2;
IERC20(token1).safeTransferFrom(msg.sender, address(this), amount);
IERC20(token1).approve(router, amount);
.
.
.
uint256 token1Amount = IERC20(token1).balanceOf(address(this));
uint256 token2Amount = IERC20(token2).balanceOf(address(this));
if (token1Amount > 0) {
    IERC20(token1).safeTransfer(msg.sender, token1Amount);
}
if (token2Amount > 0) {
    IERC20(token2).safeTransfer(msg.sender, token2Amount);
}
emit SwapExact(token1, token2, amount);
```

Recommendation

Create an internal function that contains the code segment and remove it from all the sections.

Updated 20 July 2022

The team has acknowledged that it is not a security issue.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contracts/TokenSwap.sol#L35,41
Status	Acknowledged

Description

Solidity defines a naming convention that should be followed. Rule exceptions:

- Allow constant variable name/symbol/decimals to be lowercase.
- Allow _ at the beginning of the mixed_case match for private variables and unused parameters.

```
_router
_pool
```

Recommendation

Follow the Solidity naming convention.
https://docs.soliditylang.org/en/v0.4.25/style-guide.html#naming-conventions.

Updated 20 July 2022

The team has acknowledged that it is not a security issue.

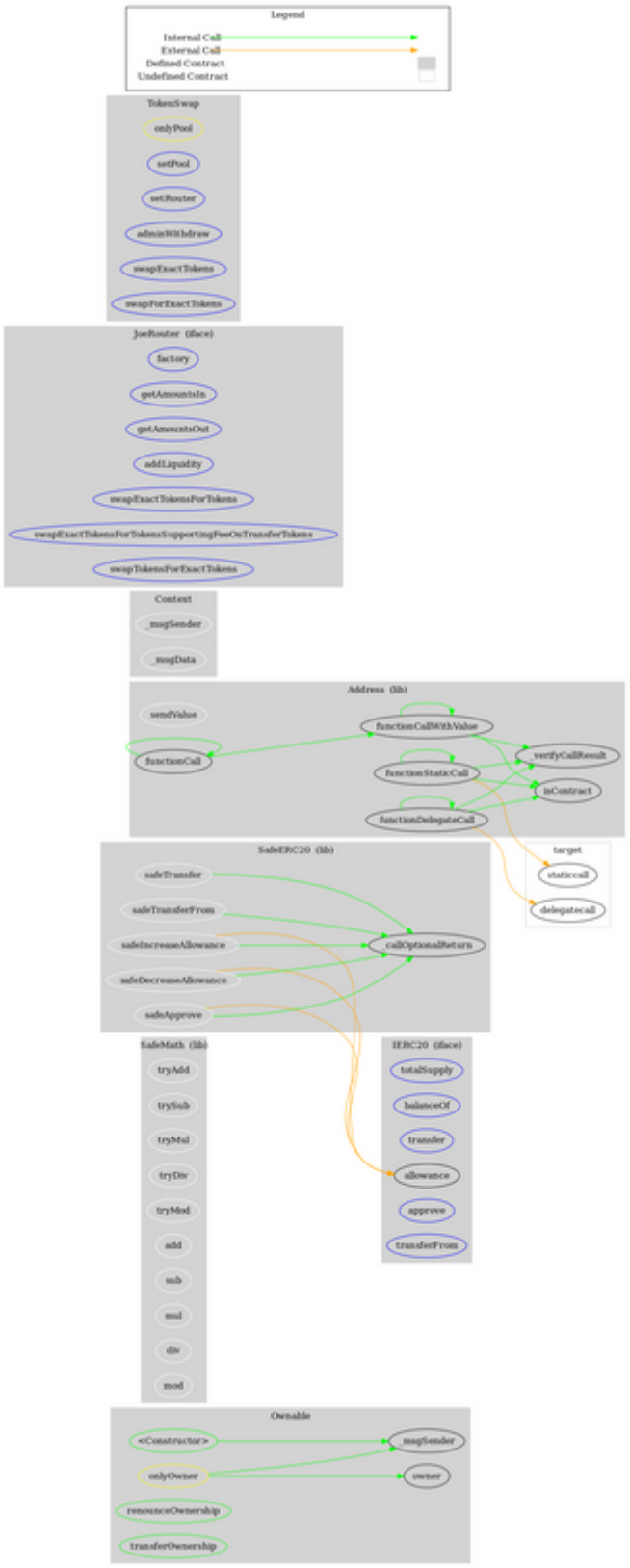
Contract Functions

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
Ownable	Implementation	Context		
	<Constructor>	Internal	✓	
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
SafeMath	Library			
	tryAdd	Internal		
	trySub	Internal		
	tryMul	Internal		
	tryDiv	Internal		
	tryMod	Internal		
	add	Internal		
	sub	Internal		
	mul	Internal		
	div	Internal		
	mod	Internal		
	sub	Internal		
	div	Internal		
	mod	Internal		
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-

SafeERC20	Library			
	safeTransfer	Internal	✓	
	safeTransferFrom	Internal	✓	
	safeApprove	Internal	✓	
	safeIncreaseAllowance	Internal	✓	
	safeDecreaseAllowance	Internal	✓	
	_callOptionalReturn	Private	✓	
Address	Library			
	isContract	Internal		
	sendValue	Internal	✓	
	functionCall	Internal	✓	
	functionCall	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionStaticCall	Internal		
	functionStaticCall	Internal		
	functionDelegateCall	Internal	✓	
	functionDelegateCall	Internal	✓	
	_verifyCallResult	Private		
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
JoeRouter	Interface			
	factory	External		-
	getAmountsIn	External		-
	getAmountsOut	External		-
	addLiquidity	External	✓	-
	swapExactTokensForTokens	External	✓	-
	swapExactTokensForTokensSupportingFeeOnTransferTokens	External	✓	-
	swapTokensForExactTokens	External	✓	-

TokenSwap	Implementation	Ownable		
	<Constructor>	Public	✓	-
	setPool	External	✓	onlyOwner
	setRouter	External	✓	onlyOwner
	adminWithdraw	External	✓	onlyOwner
	swapExactTokens	External	✓	onlyPool
	swapForExactTokens	External	✓	onlyPool

Contract Flow



Domain Info

Domain Name	hyfinance.net
Registry Domain ID	2683607355_DOMAIN_NET-VRSN
Creation Date	2022-03-22T21:24:53.00Z
Updated Date	0001-01-01T00:00:00.00Z
Registry Expiry Date	2023-03-22T21:24:53.00Z
Registrar WHOIS Server	whois.namecheap.com
Registrar URL	http://www.namecheap.com
Registrar	NAMECHEAP INC
Registrar IANA ID	1068

The domain was created 8 months before the creation of the audit.

There is no public billing information, the creator is protected by the privacy settings.

Summary

The TokenSwap operates as a wrapper between the user and the exchange router. It does not keep fees, thus the ‘adminWithdraw’ method is safe. This audit investigates the security aspects and mentions some potential improvements.

Updated 20 July 2022

The team has transferred the contract ownership to a multi-sign mechanism.

Disclaimer

All the content provided in this document is for general information only and should not be used as financial advice or a reason to buy any investment.

Cyberscope team provides no guarantees against the sale of team tokens or the removal of liquidity by the project audited in this document. Always Do your own research and protect yourselves from being scammed.

The Cyberscope team has audited this project for general information and only expresses their opinion based on similar projects and checks from popular diagnostic tools. Under no circumstances did Cyberscope receive a payment to manipulate those results or change the awarding badge that we will be adding in our website.

Always Do your own research and protect yourselves from scams. This document should not be presented as a reason to buy or not buy any particular token.

The Cyberscope team disclaims any liability for the resulting losses.

About Cyberscope

Coinscope audit and K.Y.C. service has been rebranded to Cyberscope.

Coinscope is the leading early coin listing, voting and auditing authority firm. The audit process is analyzing and monitoring many aspects of the project. That way, it gives the community a good sense of security using an informative report and a generic score.

Cyberscope and Coinscope are aiming to make crypto discoverable and efficient globally. They provide all the essential tools to assist users draw their own conclusions.

The Cyberscope team

https://www.cyberscope.io