



Cyberscope

Audit Report

Shiba Soccer League

October 2022

Type BEP20

Network BSC

Address 0x0872C9b21f1a4463EE8F5a023D25c4d4188eAbf5

Audited by © cyberscope

Table of Contents

Table of Contents	1
Contract Review	3
Source Files	3
Audit Updates	3
Contract Analysis	4
OCTD - Transfers Contract's Tokens	5
Description	5
Recommendation	5
ULTW - Transfers Liquidity to Team Wallet	6
Description	6
Recommendation	6
Contract Diagnostics	7
ZD - Zero Division	8
Description	8
Recommendation	8
L01 - Public Function could be Declared External	9
Description	9
Recommendation	9
L04 - Conformance to Solidity Naming Conventions	10
Description	10
Recommendation	10
L07 - Missing Events Arithmetic	11
Description	11
Recommendation	11
Contract Functions	12
Contract Flow	15

Domain Info	16
Summary	17
Disclaimer	18
About Cyberscope	19

Contract Review

Contract Name	SHIBASOCCERLEAGUE
Compiler Version	v0.8.15+commit.e14f2714
Optimization	200 runs
Licence	Unlicense
Explorer	https://bscscan.com/token/0x0872C9b21f1a4463EE8F5a023D25c4d4188eAbf5
Symbol	SSL
Decimals	4
Total Supply	100,000,000
Domain	https://shibsocaleague.org

Source Files

Filename	SHA256
contract.sol	d78edc408fd2965db78c4cd6875ad5f655c5ffa9f89076126f3a1ba292bb0147

Audit Updates

Initial Audit	5th October 2022
Corrected	

Contract Analysis

● Critical ● Medium ● Minor / Informative ● Pass

Severity	Code	Description	Status
●	ST	Stops Transactions	Passed
●	OCTD	Transfers Contract's Tokens	Unresolved
●	OTUT	Transfers User's Tokens	Passed
●	ELFM	Exceeds Fees Limit	Passed
●	ULTW	Transfers Liquidity to Team Wallet	Unresolved
●	MT	Mints Tokens	Passed
●	BT	Burns Tokens	Passed
●	BC	Blacklists Addresses	Passed

OCTD - Transfers Contract's Tokens

Criticality	minor / informative
Location	contract.sol#L321
Status	Unresolved

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 methods `clearStuckToken` or `bulksend`.

```
function clearStuckToken(address tokenAddress, uint256 tokens) external onlyOwner
returns (bool success) {
    if(tokens == 0){
        tokens = BEP20(tokenAddress).balanceOf(address(this));
    }

    return BEP20(tokenAddress).transfer(msg.sender, tokens);
}
```

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.

ULTW - Transfers Liquidity to Team Wallet

Criticality	minor / informative
Location	contract.sol#L315
Status	Unresolved

Description

The contract owner has the authority to transfer funds without limit to the team wallet. These funds have been accumulated from fees collected from the contract. The owner may take advantage of it by calling the `clearStuckBalance` method.

```
function clearStuckBalance(uint256 amountPercentage) external onlyOwner {  
    uint256 amountBNB = address(this).balance;  
    uint256 amountToClear = ( amountBNB * amountPercentage ) / 100;  
    payable(msg.sender).transfer(amountToClear);  
}
```

Recommendation

The contract could embody a check for the maximum amount of funds that can be swapped. Since a huge amount may volatile the token's price.

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.

Contract Diagnostics

● Critical ● Medium ● Minor / Informative

Severity	Code	Description	Status
●	ZD	Zero Division	Unresolved
●	L01	Public Function could be Declared External	Unresolved
●	L04	Conformance to Solidity Naming Conventions	Unresolved
●	L07	Missing Events Arithmetic	Unresolved

ZD - Zero Division

Criticality	critical
Location	contract.sol#L334
Status	Unresolved

Description

The contract is using variables that may be set to zero as denominators. As a result, the transactions will revert.

The variable `totalFee` can be set to zero and provoke zero division. As a result the transfer transaction will be reverted.

```
function _transferFrom(address sender, address recipient, uint256 amount) internal returns (bool)
{
    //..
    if(shouldSwapBack()){ swapBack(); }

    function swapBack() internal swapping {

        uint256 totalBNBFee = totalFee;

        uint256 amountToLiquify = (swapThreshold * liquidityFee)/(totalBNBFee * 2);
```

Recommendation

The contract should prevent those variables to be set to zero or should not allow to execute the corresponding statements.

L01 - Public Function could be Declared External

Criticality	minor / informative
Location	contract.sol#L444
Status	Unresolved

Description

Public functions that are never called by the contract should be declared external to save gas.

```
getCirculatingSupply
```

Recommendation

Use the external attribute for functions never called from the contract.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor / informative
Location	contract.sol#L152,477,408,474,416,425,121,478,397,381,373,57,389,168,471,435,470,154,243,472,158,476,144,238,155,479
Status	Unresolved

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.

```
totalSupply
config_MaxTransaction
_buy
Set_Wallets
setFees_base1000
_marketingFeeReceiver
WETH
config_TradingStatus
update_fees
...
```

Recommendation

Follow the Solidity naming convention.

<https://docs.soliditylang.org/en/v0.4.25/style-guide.html#naming-conventions>.

L07 - Missing Events Arithmetic

Criticality	minor / informative
Location	contract.sol#L408,416
Status	Unresolved

Description

Detected missing events for critical arithmetic parameters. There are functions that have no event emitted, so it is difficult to track off-chain changes.

```
sellMultiplier = _sell  
liquidityFee = _liquidityFee
```

Recommendation

Emit an event for critical parameter changes.

Contract Functions

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
SafeMath	Library			
	add	Internal		
	sub	Internal		
	sub	Internal		
	mul	Internal		
	div	Internal		
	div	Internal		
BEP20	Interface			
	getOwner	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
Auth	Implementation			
	<Constructor>	Public	✓	-
	authorize	External	✓	onlyOwner
	unauthorize	External	✓	onlyOwner
	isOwner	Public		-
	isAuthorized	Public		-
	transferOwnership	External	✓	onlyOwner
	acceptOwnership	External	✓	-
IDEXFactory	Interface			
	createPair	External	✓	-

IDEXRouter	Interface			
	factory	External		-
	WETH	External		-
	addLiquidityETH	External	Payable	-
	swapExactTokensForETHSupporting FeeOnTransferTokens	External	✓	-
SHIBASOCCE RLEAGUE	Implementation	BEP20, Auth		
	<Constructor>	Public	✓	Auth
	<Receive Ether>	External	Payable	-
	getOwner	External		-
	allowance	External		-
	approve	Public	✓	-
	approveMax	External	✓	-
	transfer	External	✓	-
	transferFrom	External	✓	-
	setMaxWalletPercent_base1000	External	✓	onlyOwner
	setMaxTxPercent_base1000	External	✓	onlyOwner
	_transferFrom	Internal	✓	
	_basicTransfer	Internal	✓	
	takeFee	Internal	✓	
	shouldSwapBack	Internal		
	clearStuckBalance	External	✓	onlyOwner
	clearStuckToken	External	✓	onlyOwner
	tradingEnable	External	✓	onlyOwner
	swapBack	Internal	✓	swapping
	manage_FeeExempt	External	✓	authorized
	manage_TxLimitExempt	External	✓	authorized
	manage_WalletLimitExempt	External	✓	authorized
	update_fees	Internal	✓	
	setMultipliers	External	✓	authorized
	setFees_base1000	External	✓	onlyOwner
	setFeeReceivers	External	✓	onlyOwner
	setSwapBackSettings	External	✓	onlyOwner

	getCirculatingSupply	Public		-
	bulksend	External	✓	authorized

Contract Flow



Domain Info

Domain Name	shibsocaleague.org
Registry Domain ID	fbf7755ebba94377838bfa94fd3c321c-LROR
Creation Date	2022-09-29T21:58:04Z
Updated Date	2022-10-04T21:59:00Z
Registry Expiry Date	2023-09-29T21:58:04Z
Registrar WHOIS Server	http://whois.registrar.amazon.com
Registrar URL	http://registrar.amazon.com
Registrar	Amazon Registrar, Inc.
Registrar IANA ID	468

The domain was created 5 days before the creation of the audit. It will expire in 12 months.

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

Summary

There are some functions that can be abused by the owner like transferring tokens to the team's wallet and transferring funds to the team's wallet. A multi-wallet signing pattern will provide security against potential hacks. Temporarily locking the contract or renouncing ownership will eliminate all the contract threats. There is also a limit of max 10% fees on buy transactions, a max of 12% fee on sell transactions, and a max of 5% transfer fee.

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>