Cyberscope

Audit Report

STEPM

May 2022

Type	BEP20
Network	BSC
Address	0x3c08e6a883eb3d0c279fe7dec4ebb245277ae53c
Audited by	© cyberscope

Table of Contents

Table of Contents 1
Contract Review 3
Source Files 3
Audit Updates 3
Contract Analysis 4
ST - Stop Transactions 5
Description 5
Recommendation 5
BC - Blacklisted Contracts 6
Description 6
Recommendation 6
Contract Diagnostics 7
L01 - Public Function could be Declared External 8
Description 8
Recommendation 8
L02 - State Variables could be Declared Constant 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
L09 - Dead Code Elimination 12
Description 12

Recommendation 12
L11 - Unnecessary Boolean equality 13
Description 13
Recommendation 13
L15 - Local Scope Variable Shadowing 14
Description 14
Recommendation 14
Contract Functions 15
Contract Flow 19
Domain Info 20
Summary 21
Disclaimer 22
About Cyberscope 23

Contract Review

Contract Name	STEPM
Compiler Version	v0.8.7+commit.e28d00a7
Optimization	200 runs
Licence	MIT
Explorer	https://bscscan.com/token/0x3c08e6a883eb3d0c279fe7dec4ebb245277ae53c
Symbol	SST
Decimals	18
Total Supply	1,000,000,000
Domain	stepm.today

Source Files

Filename	**SHA256**
contract.sol	d64d51c7df32801997c367f38dbc1ea937f955424177b84c9a95c796cc3729d8

Audit Updates

Initial Audit	11th May 2022
Corrected	

Contract Analysis

Critical Medium Minor Pass

Severity	Code	Description
Medium	ST	Contract Owner is not able to stop or pause transactions
Pass	OCTD	Contract Owner is not able to transfer tokens from specific address
Pass	OTUT	Owner Transfer User's Tokens
Pass	ELFM	Contract Owner is not able to increase fees more than a reasonable percent (25%)
Pass	ULTW	Contract Owner is not able to increase the amount of liquidity taken by dev wallet more than a reasonable percent
Pass	MT	Contract Owner is not able to mint new tokens
Pass	BT	Contract Owner is not able to burn tokens from specific wallet
Medium	BC	Contract Owner is not able to blacklist wallets from selling

ST - Stop Transactions

Criticality	medium
Location	contract.sol#L1256,1271,1302,1308

Description

The contract does not allow trading of less than 1,000 and more than 100,000 tokens.

```
if(limitSell == true) {
    if(amount < minSell*10**18 || amount > maxSell*10**18) {
        allowToSell = false;
    }
}
```

The contract owner has the authority to stop transactions within one hour. The owner may take advantage of it by setting the `holdTime` to 3600.

```
if(transactionTime == true &&
    lastTransactionTime[sender] <= block.timestamp - holdTime) {
        allowToSell = false;
}
```

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.

BC - Blacklisted Contracts

Criticality	medium
Location	contract.sol#L1249

Description

The contract owner has the authority to stop contracts from transactions. The owner may take advantage of it by calling the `addBlacklist` function.

```
require(!blacklist[sender] && !blacklist[recipient], "BLACKLISTED");
```

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.

Contract Diagnostics

Critical Medium Minor

Severity	Code	Description
	L01	Public Function could be Declared External
	L02	State Variables could be Declared Constant
	L04	Conformance to Solidity Naming Conventions
	L07	Missing Events Arithmetic
	L09	Dead Code Elimination
	L11	Unnecessary Boolean equality
	L15	Local Scope Variable Shadowing

L01 - Public Function could be Declared External

Criticality	minor
Location	contract.sol#L800,808,895,902,909,916,923

Description

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

```
balanceOf
totalSupply
symbol
decimals
name
transferOwnership
renounceOwnership
```

Recommendation

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

L02 - State Variables could be Declared Constant

Criticality	minor
Location	contract.sol#L1159,1158,1157,1151,1153,1140,1152,1154,1156

Description

Constant state variables should be declared constant to save gas.

```
poolAddress
minSell
minBuy
maxSupply
maxSell
maxBuy
marketingAddress
developmentAddress
airdropAddress
```

Recommendation

Add the constant attribute to state variables that never change.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contract.sol#L27,1191,1198,1217,1146,1150

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.

```
BuyFee
SellFee
_sec
_mktFee
_lqdtFee
_poolFee
_adFee
_devFee
WETH
...
```

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
Location	contract.sol#L1191,1198,1217

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.

```
holdTime = _sec
poolBuy = _poolFee
developmentSell = _devFee
```

Recommendation

Emit an event for critical parameter changes.

L09 - Dead Code Elimination

Criticality	minor
Location	contract.sol#L350,360,379,393,439,449,412,422,325,466,1120

Description

Functions that are not used in the contract, and make the code's size bigger.

```
_burnFrom
verifyCallResult
sendValue
functionStaticCall
functionDelegateCall
functionCallWithValue
functionCall
...
```

Recommendation

Remove unused functions.

L11 - Unnecessary Boolean equality

Criticality	minor
Location	contract.sol#L1205,1217,1241

Description

The comparison to boolean constants is redundant. Boolean constants can be used directly and do not need to be compared to true or false.

```
enableTax == true
antiBot == true && recipient == uniswapV2Pair && sender != address(this)
sender.isContract() == true
transactionTime == true && lastTransactionTime[recipient] <= block.timestamp -
holdTime
recipient.isContract() == true
allowToBuy == true
transactionTime == true && lastTransactionTime[sender] <= block.timestamp -
holdTime
limitBuy == true
require(bool,string)(allowToTransfer == true,Not Allow to Transfer)
...
```

Recommendation

Remove the equality to the boolean constant.

L15 - Local Scope Variable Shadowing

Criticality	minor
Location	contract.sol#L878,1169

Description

The are variables that are defined in the local scope containing the same name from an upper scope.

```
_symbol
_name
symbol
name
```

Recommendation

The local variables should have different names from the upper scoped variables.

Contract Functions

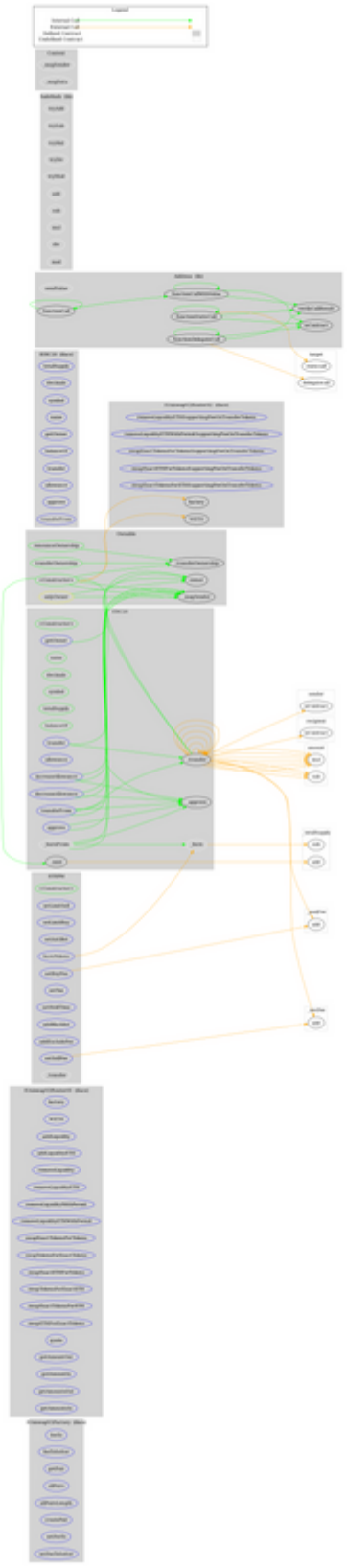
Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
IUniswapV2Factory	Interface			
	feeTo	External		-
	feeToSetter	External		-
	getPair	External		-
	allPairs	External		-
	allPairsLength	External		-
	createPair	External	✓	-
	setFeeTo	External	✓	-
	setFeeToSetter	External	✓	-
IUniswapV2Router01	Interface			
	factory	External		-
	WETH	External		-
	addLiquidity	External	✓	-
	addLiquidityETH	External	Payable	-
	removeLiquidity	External	✓	-
	removeLiquidityETH	External	✓	-
	removeLiquidityWithPermit	External	✓	-
	removeLiquidityETHWithPermit	External	✓	-
	swapExactTokensForTokens	External	✓	-
	swapTokensForExactTokens	External	✓	-
	swapExactETHForTokens	External	Payable	-
	swapTokensForExactETH	External	✓	-
	swapExactTokensForETH	External	✓	-
	swapETHForExactTokens	External	Payable	-
	quote	External		-
	getAmountOut	External		-

	getAmountIn	External		-
	getAmountsOut	External		-
	getAmountsIn	External		-
IUniswapV2Router02	Interface	IUniswapV2Router01		
	removeLiquidityETHSupportingFeeOnTransferTokens	External	✓	-
	removeLiquidityETHWithPermitSupportingFeeOnTransferTokens	External	✓	-
	swapExactTokensForTokensSupportingFeeOnTransferTokens	External	✓	-
	swapExactETHForTokensSupportingFeeOnTransferTokens	External	Payable	-
	swapExactTokensForETHSupportingFeeOnTransferTokens	External	✓	-
IERC20	Interface			
	totalSupply	External		-
	decimals	External		-
	symbol	External		-
	name	External		-
	getOwner	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
Address	Library			
	isContract	Internal		
	sendValue	Internal	✓	
	functionCall	Internal	✓	
	functionCall	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionStaticCall	Internal		

	functionStaticCall	Internal		
	functionDelegateCall	Internal	✓	
	functionDelegateCall	Internal	✓	
	verifyCallResult	Internal		
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		
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
Ownable	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	_transferOwnership	Internal	✓	
ERC20	Implementation	Context, IERC20, Ownable		
	<Constructor>	Public	✓	-
	getOwner	External		-

	name	Public		-
	decimals	Public		-
	symbol	Public		-
	totalSupply	Public		-
	balanceOf	Public		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
	increaseAllowance	External	✓	-
	decreaseAllowance	External	✓	-
	_transfer	Internal	✓	
	_mint	Internal	✓	
	_burn	Internal	✓	
	_approve	Internal	✓	
	_burnFrom	Internal	✓	
STEPM	Implementation	ERC20		
	<Constructor>	Public	✓	ERC20
	setLimitSell	External	✓	onlyOwner
	setLimitBuy	External	✓	onlyOwner
	setAntiBot	External	✓	onlyOwner
	setSellFee	External	✓	onlyOwner
	setBuyFee	External	✓	onlyOwner
	setTax	External	✓	onlyOwner
	setHoldTime	External	✓	onlyOwner
	addBlacklist	External	✓	onlyOwner
	addExcludeFee	External	✓	onlyOwner
	burnTokens	External	✓	onlyOwner
	_transfer	Internal	✓	

Contract Flow



Domain Info

Domain Name	stepm.today
Registry Domain ID	792cf4a2b0d84a4abd83bca40f57eb4b-DONUTS
Creation Date	2022-05-11T03:58:03Z
Updated Date	2022-05-11T03:58:04Z
Registry Expiry Date	2023-05-11T03:58:03Z
Registrar WHOIS Server	whois.networksolutions.com
Registrar URL	http://www.networksolutions.com
Registrar	Network Solutions, LLC
Registrar IANA ID	2

The domain has been created about 5 hours 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 stopping transactions with some conditions and blacklisting addresses. A multi-wallet signing pattern will provide security against potential hacks. Temporarily locking the contract or renouncing ownership will eliminate all the contract threats.

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 provides all the essential tools to assist users draw their own conclusions.

The Cyberscope team

https://www.cyberscope.io