Cyberscope

Audit Report

1Healthy

June 2022

Type	BEP20
Network	BSC
Address	0xd9007290D1c8040da203B938D3f02d650875Bebb
Audited by	© cyberscope

Table of Contents

Contract Review

Contract Name	Healthy
Compiler Version	v0.8.4+commit.c7e474f2
Optimization	200 runs
Licence	OSL-3.0
Explorer	https://bscscan.com/token/0xd9007290D1c8040da203B938D3f02d650875Bebb
Symbol	1Healthy
Decimals	9
Total Supply	240,000,000
Domain	1healthy-healthy.com

Source Files

Filename	**SHA256**
contract.sol	87752801e7e21f38db031df96d74444e2aefa0592098b65fce876a667ac0c77f

Audit Updates

Initial Audit	6th June 2022
Corrected	

Contract Analysis

Critical Medium Minor Pass

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

ST - Stop Transactions

Criticality	critical
Location	contract.sol#L561,962,1064

Description

The contract owner has the authority to stop transactions for all users excluding the owner. The contract owner can also stop transactions by setting the killblock to a very big amount.

```
if (sender == uniswapPair) {
          if (block.number <= launchedBlock + killblock) {
            addBot(recipient);
          }
        }
```

Another action that can stop transactions is setting _totalDistributionShares to 0. This will make swapAndLiquify function to fail.

```
        uint256 tokensForLP =
tAmount.mul(_liquidityShare).div(_totalDistributionShares).div(2);
```

Recommendation

The contract could embody a check for not allowing setting the _totalDistributionShares to zero or the killblock very high value. A suggested implementation could check that the related variables should be more than a fixed percentage of the total supply.

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#L922

Description

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

```
    function writeAntiwhale(address recipient, bool value) public onlyOwner {
    _isAntiwhaleed[recipient] = value;
  }
```

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
	MC	Missing Check
	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

MC - Missing Check

Criticality	minor
Location	contract.sol#L561

Description

The contract is processing variables that have not properly sanitized and checked that they form the proper shape. These variables may produce vulnerability issues. The contract should check not to allow the _totalDistributionShares to be zero.

```
    function setDistributionSettings(uint256 newLiquidityShare, uint256
newMarketingShare, uint256 newTeamShare) external onlyOwner() {
        _liquidityShare = newLiquidityShare;
        _marketingShare = newMarketingShare;
        _teamShare = newTeamShare;

        _totalDistributionShares =
_liquidityShare.add(_marketingShare).add(_teamShare);
    }
```

Recommendation

The contract should properly check the variables according to the required specifications.

L01 - Public Function could be Declared External

Criticality	minor
Location	contract.sol#L162,167,173,485,489,493,497,505,509,514,519,523,536,541,557,581,587,591,599,621,626,632,640,644

Description

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

```
writeAntiwhale
setKillBlock
isAntiwhale
transferFrom
transfer
changeRouterVersion
getCirculatingSupply
setSwapAndLiquifyByLimitOnly
setSwapAndLiquifyEnabled
...
```

Recommendation

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

L02 - State Variables could be Declared Constant

Criticality	minor
Location	contract.sol#L403,404,405,385,383,407,408,409,384

Description

Constant state variables should be declared constant to save gas.

```
_symbol
_sellTeamFee
_sellMarketingFee
_sellLiquidityFee
_name
_decimals
_buyTeamFee
_buyMarketingFee
_buyLiquidityFee
```

Recommendation

Add the constant attribute to state variables that never change.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contract.sol#L209,210,226,245,536,581,394,403,404,405,407,408,409,411,412,413,415,416,417

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.

```
_totalDistributionShares
_totalTaxIfSelling
_totalTaxIfBuying
_teamShare
_marketingShare
_liquidityShare
_sellTeamFee
_sellMarketingFee
_sellLiquidityFee
...
```

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#L561,569,640

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.

```
killblock = num
minimumTokensBeforeSwap = newLimit
_liquidityShare = newLiquidityShare
```

Recommendation

Emit an event for critical parameter changes.

L09 - Dead Code Elimination

Criticality	minor
Location	contract.sol#L122,105,109,113,117,85,97

Description

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

```
sendValue
isContract
functionCallWithValue
functionCall
_functionCallWithValue
```

Recommendation

Remove unused functions.

Contract Functions

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
SafeMath	Library			
	add	Internal		
	sub	Internal		
	sub	Internal		
	mul	Internal		
	div	Internal		
	div	Internal		
	mod	Internal		
	mod	Internal		
Address	Library			
	isContract	Internal		
	sendValue	Internal	✓	
	functionCall	Internal	✓	
	functionCall	Internal	✓	
	functionCallWithValue	Internal	✓	

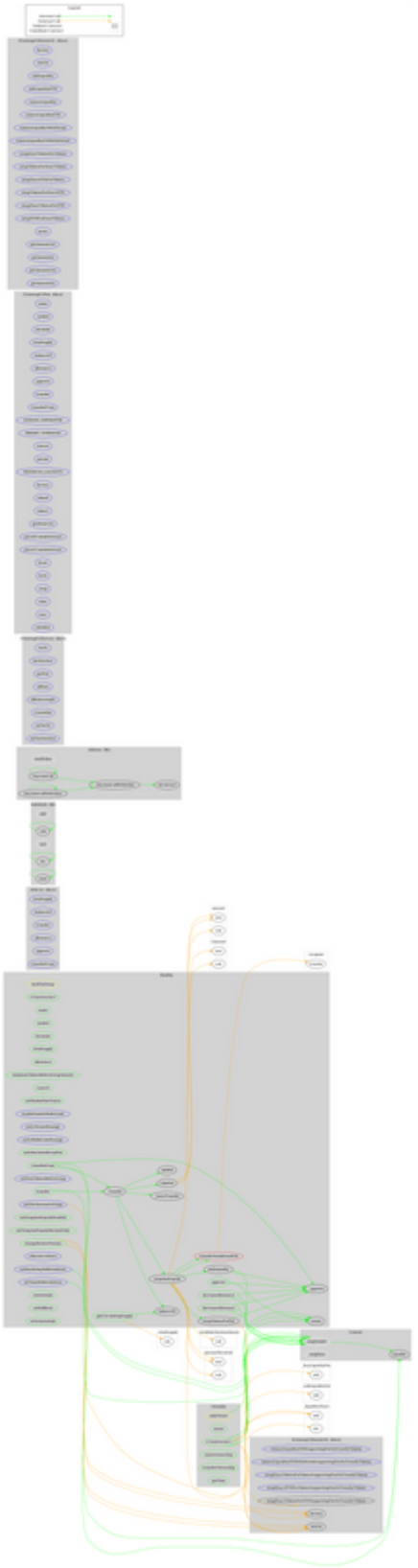
	functionCallWithValue	Internal	✓	
	_functionCallWithValue	Private	✓	
Ownable	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	waiveOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	getTime	Public		-
IUniswapV2Factory	Interface			
	feeTo	External		-
	feeToSetter	External		-
	getPair	External		-
	allPairs	External		-
	allPairsLength	External		-
	createPair	External	✓	-
	setFeeTo	External	✓	-
	setFeeToSetter	External	✓	-
IUniswapV2Pair	Interface			
	name	External		-
	symbol	External		-
	decimals	External		-
	totalSupply	External		-
	balanceOf	External		-
	allowance	External		-
	approve	External	✓	-
	transfer	External	✓	-
	transferFrom	External	✓	-
	DOMAIN_SEPARATOR	External		-
	PERMIT_TYPEHASH	External		-
	nonces	External		-
	permit	External	✓	-

	MINIMUM_LIQUIDITY	External		-
	factory	External		-
	token0	External		-
	token1	External		-
	getReserves	External		-
	price0CumulativeLast	External		-
	price1CumulativeLast	External		-
	kLast	External		-
	burn	External	✓	-
	swap	External	✓	-
	skim	External	✓	-
	sync	External	✓	-
	initialize	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	✓	-
Healthy	Implementation	Context, IERC20, Ownable		
	<Constructor>	Public	✓	-
	name	Public		-
	symbol	Public		-
	decimals	Public		-
	totalSupply	Public		-
	balanceOf	Public		-
	allowance	Public		-
	increaseAllowance	Public	✓	-
	decreaseAllowance	Public	✓	-
	minimumTokensBeforeSwapAmount	Public		-
	approve	Public	✓	-
	_approve	Private	✓	
	Launch	Public	✓	onlyOwner
	setMarketPairStatus	Public	✓	onlyOwner
	enableDisableWalletLimit	External	✓	onlyOwner
	setIsTxLimitExempt	External	✓	onlyOwner
	setIsWalletLimitExempt	External	✓	onlyOwner
	setIsExcludedFromFee	Public	✓	onlyOwner
	setDistributionSettings	External	✓	onlyOwner
	setNumTokensBeforeSwap	External	✓	onlyOwner
	setMarketingWalletAddress	External	✓	onlyOwner

	setTeamWalletAddress	External	✓	onlyOwner
	setSwapAndLiquifyEnabled	Public	✓	onlyOwner
	setSwapAndLiquifyByLimitOnly	Public	✓	onlyOwner
	getCirculatingSupply	Public		-
	transferToAddressETH	Private	✓	
	changeRouterVersion	Public	✓	onlyOwner
	<Receive Ether>	External	Payable	-
	transfer	Public	✓	-
	transferFrom	Public	✓	-
	isAntiwhale	Public		-
	addBot	Internal	✓	
	setKillBlock	Public	✓	onlyOwner
	writeAntiwhale	Public	✓	onlyOwner
	_transfer	Private	✓	
	_basicTransfer	Internal	✓	
	swapAndLiquify	Private	✓	lockTheSwap
	swapTokensForEth	Private	✓	
	addLiquidity	Private	✓	
	takeFee	Internal	✓	

Contract Flow



Domain Info

Domain Name	1healthy-healthy.com
Registry Domain ID	2700254500_DOMAIN_COM-VRSN
Creation Date	2022-05-30T07:00:00Z
Updated Date	2022-05-31T07:00:00Z
Registry Expiry Date	2023-05-30T07:00:00Z
Registrar WHOIS Server	whois.namesilo.com
Registrar URL	https://www.namesilo.com/
Registrar	NameSilo, LLC
Registrar IANA ID	1479

The domain has been created 7 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 stopping transactions and blacklisting addresses. The contract can be converted into a honeypot and prevent users from selling if the owner abuses the admin functions. 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 provide all the essential tools to assist users draw their own conclusions.

The Cyberscope team

https://www.cyberscope.io