COINSCOPE

Audit Report

MoonBoi

January 2022

Type	BEP20
Network	BSC
Address	0x5A965a6a5F18abCB3E0cd747DD6873486Be12AE0
Audited by	© coinscope

Table of Contents

Contract Review

Contract Name	MoonBoi
Compiler Version	v0.8.9+commit.e5eed63a
Optimization	200 runs
Licence	None
Explorer	https://bscscan.com/token/0x5A965a6a5F18abCB3E0cd747DD6873486Be12AE0
Symbol	MoonBoi
Decimals	9
Total Supply	500,000,000,000
Source	contract.sol
Domain	moonboicoin.com

Audit Updates

Initial Audit	30th January 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#L919

Description

The contract owner has the authority to stop all sales excluding the owner. The owner may take advantage of it by setting the `_sellTax` to a high value.

```
if(isSell){
    if(!_excludedFromSellLock.contains(sender)){
            //If seller sold less than sellLockTime(2h 50m) ago, sell is
declined, can be disabled by Team
        require(_sellLock[sender]<=block.timestamp||sellLockDisabled,"Seller in
sellLock");
        //Sets the time sellers get locked(2 hours 50 mins by default)
        _sellLock[sender]=block.timestamp+sellLockTime;
    }
    //Sells can't exceed the sell limit(21,000 Tokens at start, can be updated
to circulating supply)
    require(amount<=sellLimit,"Dump protection");
    tax=_sellTax;


} else if(isBuy){
```

Recommendation

The contract could embody a check for not allowing setting the *_sellTax* to a value that will not allow the transaction to proceed.

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.

ELFM - Exceed Limit Fees Manipulation

Criticality	critical
Location	contract.sol#L1355

Description

The contract owner has the authority to increase over the allowed limit of 25%. The owner may take advantage of it by calling the `TeamSetTaxes` function with a high percentage value to buyTax, sellTax or transferTax.

```
function TeamSetTaxes(uint8 burnTaxes, uint8 liquidityTaxes, uint8
stakingTaxes,uint8 buyTax, uint8 sellTax, uint8 transferTax) public onlyOwner{
    uint8 totalTax=burnTaxes+liquidityTaxes+stakingTaxes;
    require(totalTax==100, "burn+liq+marketing needs to equal 100%");

    _burnTax=burnTaxes;
    _liquidityTax=liquidityTaxes;
    _stakingTax=stakingTaxes;

    _buyTax=buyTax;
    _sellTax=sellTax;
    _transferTax=transferTax;
}
```

Recommendation

The contract could embody a check for the maximum acceptable value.

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 - Unlimited Liquidity to Team Wallet

Criticality	medium
Location	contract.sol#L1438

Description

The contract owner has the authority to remove liquidity pool tokens and transfer them to the dev's wallet. The owner may take advantage by following these steps:

1. Call *TeamRemoveLiquidity(false)*

2. Call *TeamWithdrawALLMarketingBNB()*

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
●	L04	Conformance to Solidity Naming Conventions
●	L09	Dead Code Elimination
●	L07	Missing Events Arithmetic

L01 - Public Function could be Declared External

Criticality	minor
Location	contract.sol#L1469,L1438,L1426 and 30 more

Description

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

```
TeamRemoveRemainingBNB
TeamRemoveLiquidity
TeamReleaseLiquidity
...
```

Recommendation

Use the external attribute for functions never called from the contract

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contract.sol#L1001,L799,L794 and 40 more

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.

```
DistributionMultiplier
PancakeRouter
TeamWallet
...
```

Recommendation

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

L09 - Dead Code Elimination

Criticality	minor
Location	contract.sol#L823,L1281,L728 and 22 more

Description

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

```
_isTeam
XRPWithdraw
remove
...
```

Recommendation

Remove unused functions.

L07 - Missing Events Arithmetic

Criticality	minor
Location	contract.sol#L1379,L1369,L1355 and 4 more

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.

```
balanceLimit = newBalanceLimit
marketingShare = newShare
_burnTax = burnTaxes
...
```

Recommendation

Emit an event for critical parameter changes.

Contract Functions

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
IBEP20	Interface			
	totalSupply	External		-
	decimals	External		-
	symbol	External		-
	name	External		-
	getOwner	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
IPancakeERC20	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	✓	-
IPancakeFacto	Interface			

ry				
	feeTo	External		-
	feeToSetter	External		-
	getPair	External		-
	allPairs	External		-
	allPairsLength	External		-
	createPair	External	✓	-
	setFeeTo	External	✓	-
	setFeeToSetter	External	✓	-
IPancakeRouter01	Interface			
	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	-
	factory	External		-
	WETH	External		-
	quote	External		-
	getamountOut	External		-
	getamountIn	External		-
	getamountsOut	External		-
	getamountsIn	External		-
IPancakeRouter02	Interface	IPancakeRouter01		
	removeLiquidityETHSupportingFeeOnTransferTokens	External	✓	-

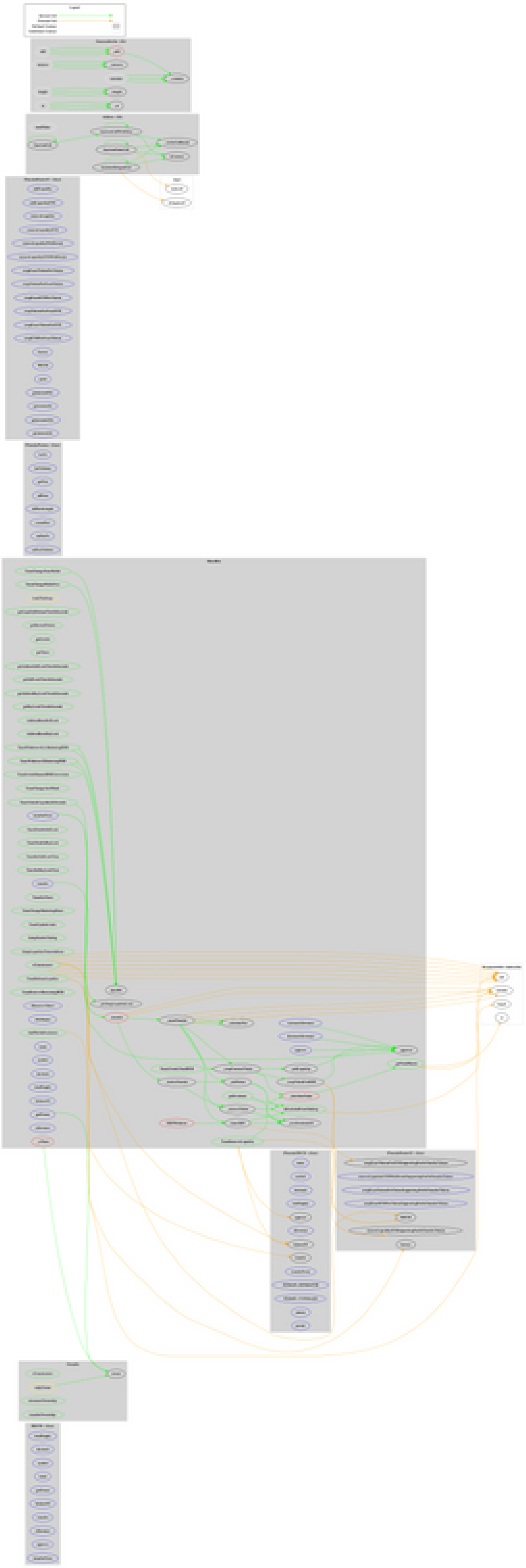
	removeLiquidityETHWithPermitSupportingFeeOnTransferTokens	External	✓	-
	swapExactTokensForTokensSupportingFeeOnTransferTokens	External	✓	-
	swapExactETHForTokensSupportingFeeOnTransferTokens	External	Payable	-
	swapExactTokensForETHSupportingFeeOnTransferTokens	External	✓	-
Ownable	Implementation			
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
Address	Library			
	isContract	Internal		
	sendValue	Internal	✓	
	functionCall	Internal	✓	
	functionCall	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionStaticCall	Internal		
	functionStaticCall	Internal		
	functionDelegateCall	Internal	✓	
	functionDelegateCall	Internal	✓	
	_verifyCallResult	Private		
EnumerableSet	Library			
	_add	Private	✓	
	_remove	Private	✓	
	_contains	Private		
	_length	Private		
	_at	Private		
	add	Internal	✓	
	remove	Internal	✓	

	contains	Internal		
	length	Internal		
	at	Internal		
	add	Internal	✓	
	remove	Internal	✓	
	contains	Internal		
	length	Internal		
	at	Internal		
	add	Internal	✓	
	remove	Internal	✓	
	contains	Internal		
	length	Internal		
	at	Internal		
MoonBoi	Implementation	IBEP20, Ownable		
	_isTeam	Private		
	<Constructor>	Public	✓	-
	_transfer	Private	✓	
	_taxedTransfer	Private	✓	
	_feelessTransfer	Private	✓	
	_calculateFee	Private		
	isExcludedFromStaking	Public		-
	_getTotalShares	Public		-
	_addToken	Private	✓	
	_removeToken	Private	✓	
	_newDividentsOf	Private		
	_distributeStake	Private	✓	
	claimXRP	Private	✓	
	_swapContractToken	Private	✓	lockTheSwap
	_swapTokenForBNB	Private	✓	
	_addLiquidity	Private	✓	
	getLiquidityReleaseTimeInSeconds	Public		-
	getBurnedTokens	Public		-
	getLimits	Public		-
	getTaxes	Public		-

	getAddressSellLockTimeInSeconds	Public		-
	getSellLockTimeInSeconds	Public		-
	getAddressBuyLockTimeInSeconds	Public		-
	getBuyLockTimeInSeconds	Public		-
	AddressResetSellLock	Public	✓	-
	AddressResetBuyLock	Public	✓	-
	XRPWithdraw	Private	✓	
	getDividents	Public		-
	TeamWithdrawALLMarketingBNB	Public	✓	onlyOwner
	TeamWithdrawXMarketingBNB	Public	✓	onlyOwner
	TeamSwitchManualBNBConversion	Public	✓	onlyOwner
	TeamChangeAntiWhale	Public	✓	onlyOwner
	TeamChangeTeamWallet	Public	✓	onlyOwner
	TeamChangeWalletTwo	Public	✓	onlyOwner
	TeamDisableSellLock	Public	✓	onlyOwner
	TeamDisableBuyLock	Public	✓	onlyOwner
	TeamSetSellLockTime	Public	✓	onlyOwner
	TeamSetBuyLockTime	Public	✓	onlyOwner
	AddWalletExclusion	Public	✓	onlyOwner
	TeamSetTaxes	Public	✓	onlyOwner
	TeamChangeMarketingShare	Public	✓	onlyOwner
	TeamCreateLPandBNB	Public	✓	onlyOwner
	TeamUpdateLimits	Public	✓	onlyOwner
	SetupEnableTrading	Public	✓	onlyOwner
	SetupLiquidityTokenAddress	Public	✓	onlyOwner
	TeamUnlockLiquidityInSeconds	Public	✓	onlyOwner
	_prolongLiquidityLock	Private	✓	
	TeamReleaseLiquidity	Public	✓	onlyOwner
	TeamRemoveLiquidity	Public	✓	onlyOwner
	TeamRemoveRemainingBNB	Public	✓	onlyOwner
	<Receive Ether>	External	Payable	-
	<Fallback>	External	Payable	-
	getOwner	External		-
	name	External		-
	symbol	External		-

	decimals	External		-
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	_approve	Private	✓	
	transferFrom	External	✓	-
	increaseAllowance	External	✓	-
	decreaseAllowance	External	✓	-

Contract Flow



Domain Info

Domain Name	moonboicoin.com
Registry Domain ID	2667378837_DOMAIN_COM-VRSN
Creation Date	2022-01-10T20:47:19Z
Updated Date	2022-01-16T03:41:33Z
Registry Expiry Date	2023-01-10T20:47:19Z
Registrar WHOIS Server	whois.godaddy.com
Registrar URL	http://www.godaddy.com
Registrar	GoDaddy.com, LLC
Registrar IANA ID	146

The domain has been created 20 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

MoonBoi is aiming to build a play-to-earn game. The Project has a friendly and growing community. There are some functions that can be abused by the owner, like manipulating fees, transferring funds to the team’s wallet and stopping transactions. The contract can potentially operate as a honeypot if the contract owner abuses the configuration. 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.

Coinscope 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 Coinscope 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 Coinscope 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 Coinscope team disclaims any liability for the resulting losses.

About Coinscope

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.

Coinscope is aiming to make crypto discoverable and efficient globally. It provides all the essential tools to assist users draw their own conclusions.

The Coinscope.co team

https://www.coinscope.co