Audit Report
PULI INU

January 2022

Type	BEP20
Network	BSC
Address	0xaef0a177c8c329cbc8508292bb7e06c00786bbfc
Audited by	© coinscope

Table of Contents

Contract Review

Contract Name	PULIINU
Compiler Version	v0.8.10+commit.fc410830
Optimization	200 runs
Licence	MIT
Explorer	https://bscscan.com/token/0xAEf0a177c8c329CBC8508292Bb7E06c00786BBfC
Symbol	PULI
Decimals	9
Total Supply	100,000,000
Source	contract.sol
Domain	puli-inu.com

Audit Updates

Initial Audit	26th January 2022
Corrected	17th May 2022

Contract Analysis

● Critical   ● Medium   ● Minor   ● Pass

Severity	Code	Description	Status
●	ST	Contract Owner is not able to stop or pause transactions	Multi-Sign
●	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%)	Multi-Sign
●	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	Multi-Sign

ST - Stop Transactions

Criticality	critical
Location	https://bscscan.com/address/0xaef0a177c8c329cbc8508292bb7e06c00786bbfc#L1588
Status	Multi-Sign

Description

The contract owner has the authority to stop transactions for all users trying to sell their tokens and it will have a honeypot behaviour. The owner may take advantage of it by setting the `maxSellAmount` to zero.

```solidity
        if (recipient == uniswapV2Pair) {
            require(amount <= maxSellAmount, "Sell exceeds limit");
            setSell();
        }
```

The owner can also stop transactions for everyone by setting `maxWalletAmount` to the zero value

```solidity
    if(recipient != uniswapV2Pair){
            require(
                balanceOf(recipient) + amount <= maxWalletAmount,
                "Balance exceeds limit"
            );
        }
```

Recommendation

The contract could embody a check for not allowing setting the `maxSellAmount` less than a reasonable amount. A suggested implementation could check that the maximum amount 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.

Updated 17 May 2022

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

ELFM - Exceed Limit Fees Manipulation

Criticality	critical
Location	https://bscscan.com/address/0xaef0a177c8c329cbc8508292bb7e06c00786bbfc #L1145
Status	Multi-Sign

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 `setSellFee` function with a high percentage value.

```
    function setSellFee(uint16 liq, uint16 market, uint16 reward, uint16 tax)
 external onlyOwner {
        sellFee.liquidityFee = liq;
        sellFee.marketingFee = market;
        sellFee.buybackFee = reward;
        sellFee.taxFee = tax;
    }
```

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.

BC - Blacklisted Contracts

Criticality	medium
Location	https://bscscan.com/address/0xaef0a177c8c329cbc8508292bb7e06c00786bbfc #L1182
Status	Multi-Sign

Description

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

```
function setBlackList(address addr, bool value) external onlyOwner {
    _isBlackListed[addr] = 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.

Updated 17 May 2022

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

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
●	L09	Dead Code Elimination
●	L07	Missing Events Arithmetic

L01 - Public Function could be Declared External

Criticality	minor
Location	contract.sol#L1392,L1182,L1087 and 17 more

Description

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

```
isExcludedFromFee
setSwapAndLiquifyEnabled
excludeFromReward
...
```

Recommendation

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

L02 - State Variables could be Declared Constant

Criticality	minor
Location	contract.sol#L829,L828,L830

Description

Constant state variables should be declared constant to save gas.

```
_symbol
_name
_decimals
```

Recommendation

Add the constant attribute to state variables that never change.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contract.sol#L861,L820,L1357 and 6 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.

```
_marketingWallet
_isBlackListed
_amount
...
```

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#L527,L539,L568 and 17 more

Description

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

```
trySub
tryMul
tryMod
...
```

Recommendation

Remove unused functions.

L07 - Missing Events Arithmetic

Criticality	minor
Location	contract.sol#L1174,L1170,L1166 and 2 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.

```
maxWalletAmount = value * 10 ** _decimals
maxSellAmount = value * 10 ** _decimals
maxBuyAmount = value * 10 ** _decimals
...
```

Recommendation

Emit an event for critical parameter changes.

Contract Functions

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
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	✓	-
IUniswapV2Factory	Interface			
	feeTo	External		-
	feeToSetter	External		-
	getPair	External		-
	allPairs	External		-
	allPairsLength	External		-
	createPair	External	✓	-
	setFeeTo	External	✓	-
	setFeeToSetter	External	✓	-
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
Ownable	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	_setOwner	Private	✓	
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		
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
PULIINU	Implementation	Context, IERC20, Ownable		
	<Constructor>	Public	✓	-
	name	Public		-
	symbol	Public		-
	decimals	Public		-
	totalSupply	Public		-

	balanceOf	Public		-
	transfer	Public	✓	-
	allowance	Public		-
	approve	Public	✓	-
	transferFrom	Public	✓	-
	increaseAllowance	Public	✓	-
	decreaseAllowance	Public	✓	-
	isExcludedFromReward	Public		-
	totalFees	Public		-
	checkBlock	Public		-
	deliver	Public	✓	-
	reflectionFromToken	Public		-
	tokenFromReflection	Public		-
	excludeFromReward	Public	✓	onlyOwner
	includeInReward	External	✓	onlyOwner
	excludeFromFee	External	✓	onlyOwner
	includeInFee	External	✓	onlyOwner
	launch	External	✓	onlyOwner
	controlBuyBack	External	✓	onlyOwner
	setBuyFee	External	✓	onlyOwner
	setSellFee	External	✓	onlyOwner
	setNumTokensSellToAddToLiquidity	External	✓	onlyOwner
	updateRouter	External	✓	onlyOwner
	setMaxBuyAmount	External	✓	onlyOwner
	setMaxSellAmount	External	✓	onlyOwner
	setMaxWallet	External	✓	onlyOwner
	setBlackList	External	✓	onlyOwner
	setSwapAndLiquifyEnabled	Public	✓	onlyOwner
	triggerBuyBack	External	✓	onlyOwner
	claimStuckTokens	External	✓	onlyOwner
	<Receive Ether>	External	Payable	-
	_reflectFee	Private	✓	
	_getValues	Private		
	_getTValues	Private		
	_getRValues	Private		

	_getRate	Private		
	_getCurrentSupply	Private		
	_takeLiquidity	Private	✓	
	_takeBuyBackAndMarketing	Private	✓	
	calculateTaxFee	Private		
	calculateLiquidityFee	Private		
	calculatebuybackFee	Private		
	calculateMarketingFee	Private		
	removeAllFee	Private	✓	
	setBuy	Private	✓	
	setSell	Private	✓	
	setAntiBot	Private	✓	
	isExcludedFromFee	Public		-
	_approve	Private	✓	
	_transfer	Private	✓	
	swapAndLiquify	Private	✓	
	swapAndSendFee	Private	✓	
	swapTokensForEth	Private	✓	lockTheSwap
	swapETHForTokens	Private	✓	lockTheSwap
	addLiquidity	Private	✓	lockTheSwap
	_tokenTransfer	Private	✓	
	_transferStandard	Private	✓	
	_transferToExcluded	Private	✓	
	_transferFromExcluded	Private	✓	
	_transferBothExcluded	Private	✓	

Contract Flow

Domain Info

Domain Name	puli-inu.com
Registry Domain ID	2665936265_DOMAIN_COM-VRSN
Creation Date	2022-01-04T16:23:05Z
Updated Date	2022-01-04T16:23:06Z
Registry Expiry Date	2023-01-04T16:23:05Z
Registrar WHOIS Server	whois.wix.com
Registrar URL	http://www.wix.com
Registrar	Wix.com Ltd.
Registrar IANA ID	3817

The domain has been created 22 days before the creation of the audit. It will expire in 11 months.

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

Summary

PULI INU is an interesting project with a friendly and growing community. The Smart Contract analysis reported no compiler error, but a few critical issues. There are some functions that can be abused by the owner, like manipulating fees up to 100%, blacklisting wallets from selling and stopping all transactions. A multi-wallet signing pattern will provide security against potential hacks. Temporarily locking the contract or renouncing ownership will eliminate all the contract threats.

Updated 17 May 2022

The team has acknowledged the threats and 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.

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