Audit Report

Equity

February 2022

Type	ERC20
Network	MATIC MUMBAI
Address	0x96C240d8d043727d0527100A3f76ebd5D583FFCd
Audited by	© coinscope

Table of Contents

Contract Review

Contract Name	Equity
Compiler Version	v0.8.10+commit.fc410830
Optimization	500 runs
Licence	
Explorer	https://mumbai.polygonscan.com/token/0x96c240d8d043727d0527100a3f76ebd5d583ffcd
Symbol	Equity
Decimals	18
Total Supply	1,020,000
Source	Equity.sol ReflectiveToken.sol IReflective.sol IReflectionTracker.sol SharedOwnable.sol IUniswapV2Router02.sol IUniswapV2Router01.sol IUniswapV2Factory.sol draft-EIP712.sol ECDSA.sol Strings.sol Counters.sol Context.sol draft-IERC20Permit.sol draft-ERC20Permit.sol IERC20Metadata.sol IERC20.sol ERC20.sol Ownable.sol

Audit Updates

Initial Audit	17th February 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

Contract Diagnostics

Critical Medium Minor

Severity	Code	Description
	L12	Using Variables before Declaration
	L14	Uninitialized Variables in Local Scope
	L13	Divide before Multiply Operation

L12 - Using Variables before Declaration

Criticality	minor
Location	contract/ReflectiveToken.sol#L336

Description

The contract is using a variable before the declaration. This is usually happening either if it has not been declared yet or the variable has been declared in a different scope.

```
gasUsed
lastProcessedIndex
iterations
claims
```

Recommendation

The variables should be declared before any usage of them.

L14 - Uninitialized Variables in Local Scope

Criticality	minor
Location	contract/ReflectiveToken.sol#L336

Description

The are variables that are defined in the local scope and are not initialized.

```
lastProcessedIndex
claims
iterations
gasUsed
```

Recommendation

All the local scoped variables should be initialized.

L13 - Divide before Multiply Operation

Criticality	minor
Location	contract/ReflectiveToken.sol#L302,413

Description

Performing divisions before multiplications may cause lose of prediction.

```
number = (seed - ((seed / 100) * 100))
feeAmount = (amount / 100) * feePercentage
_swapAndSendReflections((_minimumTokenBalanceForSwapAndSendReflections / 100) *
_getRandomNumber())
```

Recommendation

The multiplications should be prior to the divisions.

Contract Functions

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
Counters	Library			
	current	Internal		
	increment	Internal	✓	
	decrement	Internal	✓	
	reset	Internal	✓	
EIP712	Implementation			
	<Constructor>	Public	✓	-
	_domainSeparatorV4	Internal		
	_buildDomainSeparator	Private		
	_hashTypedDataV4	Internal		
ERC20Permit	Implementation	ERC20, IERC20Permit, EIP712		
	<Constructor>	Public	✓	EIP712
	permit	Public	✓	-
	nonces	Public		-
	DOMAIN_SEPARATOR	External		-
	_useNonce	Internal	✓	
IERC20Permit	Interface			
	permit	External	✓	-
	nonces	External		-
	DOMAIN_SEPARATOR	External		-

ECDSA	Library			
	_throwError	Private		
	tryRecover	Internal		
	recover	Internal		
	tryRecover	Internal		
	recover	Internal		
	tryRecover	Internal		
	recover	Internal		
	toEthSignedMessageHash	Internal		
	toEthSignedMessageHash	Internal		
	toTypedDataHash	Internal		
Equity	Implementation	ReflectiveToken		
	<Constructor>	Public	✓	ReflectiveToken
ERC20	Implementation	Context, IERC20, IERC20Metadata		
	<Constructor>	Public	✓	-
	name	Public		-
	symbol	Public		-
	decimals	Public		-
	totalSupply	Public		-
	balanceOf	Public		-
	transfer	Public	✓	-
	allowance	Public		-
	approve	Public	✓	-
	transferFrom	Public	✓	-
	increaseAllowance	Public	✓	-
	decreaseAllowance	Public	✓	-
	_transfer	Internal	✓	
	_mint	Internal	✓	
	_burn	Internal	✓	

	_approve	Internal	✓	
	_beforeTokenTransfer	Internal	✓	
	_afterTokenTransfer	Internal	✓	
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
IERC20Metadata	Interface	IERC20		
	name	External		-
	symbol	External		-
	decimals	External		-
IReflectionTracker	Interface			
	isBoundTo	External		-
	bindTo	External	✓	-
	getBalanceOf	External		-
	setBalanceOf	External	✓	-
	refreshBalanceOf	External	✓	-
	refreshBalance	External	✓	-
	getUniswapV2Router02Address	External		-
	setUniswapV2Router02Address	External	✓	-
	getDefaultReflectionTokenAddress	External		-
	setDefaultReflectionTokenAddress	External	✓	-
	getClaimCooldown	External		-
	setClaimCooldown	External	✓	-
	getMinimumTokenBalanceForReflections	External		-
	setMinimumTokenBalanceForReflections	External	✓	-
	getExcludedReflectionStateOfBNB	External		-

	setExcludedReflectionStateOfBNB	External	✓	-
	getExcludedReflectionTokenStateOf	External		-
	setExcludedReflectionTokenStateOf	External	✓	-
	getExcludedFromReflectionsOf	External		-
	setExcludedFromReflectionsOf	External	✓	-
	getProcessingGas	External		-
	setProcessingGas	External	✓	-
	getReflectionInBNB	External		-
	setReflectionInBNB	External	✓	-
	getReflectionTokenAddress	External		-
	setReflectionTokenAddress	External	✓	-
	getNumberOfHolders	External		-
	getLastProcessedIndex	External		-
	getTotalReflectionsTransferred	External		-
	getWithdrawnReflectionsOf	External		-
	getWithdrawableReflectionsOf	External		-
	getAccountInfoOf	External		-
	getAccountInfoAtIndex	External		-
	transferReflections	External	Payable	-
	transferReflections	External	✓	-
	process	External	✓	-
	processAll	External	✓	-
	processAll	External	✓	-
	processAll	External	✓	-
IReflective	Interface			
	getBalanceOf	External		-
	getTokenPairOtherTokenAddress	External		-
IUniswapV2Factory	Interface			
	feeTo	External		-
	feeToSetter	External		-
	getPair	External		-
	allPairs	External		-
	allPairsLength	External		-

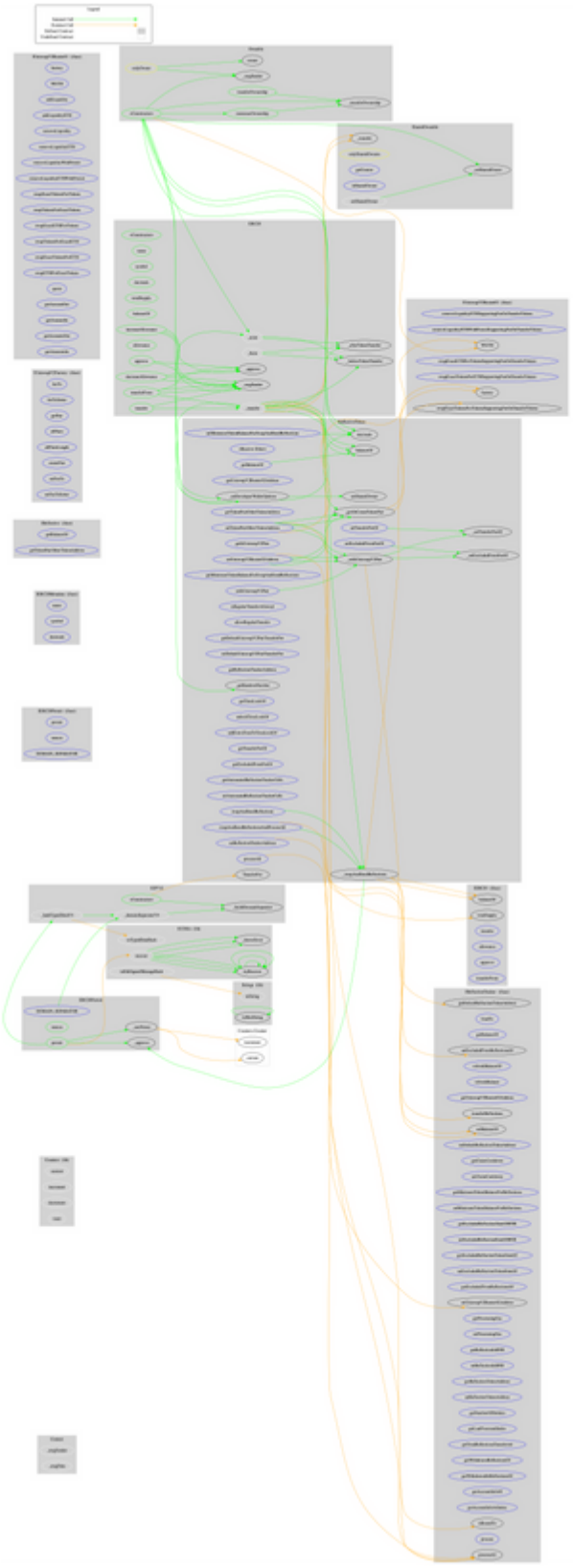
	createPair	External	✓	-
	setFeeTo	External	✓	-
	setFeeToSetter	External	✓	-
IUniswapV2Router01	Interface			
	factory	External		-
	WETH	External		-
	addLiquidity	External	✓	-
	addLiquidityETH	External	Payable	-
	removeLiquidity	External	✓	-
	removeLiquidityETH	External	✓	-
	removeLiquidityWithPermit	External	✓	-
	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	✓	-

Ownable	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	_transferOwnership	Internal	✓	
ReflectiveToken	Implementation	ERC20Permit, IReflective, SharedOwnable		
	<Constructor>	Public	✓	ERC20Permit ERC20
	<Receive Ether>	External	Payable	-
	getBalanceOf	External		-
	getUniswapV2Router02Address	External		-
	setUniswapV2Router02Address	External	✓	onlySharedOwners
	getTokenPairOtherTokenAddress	External		-
	setTokenPairOtherTokenAddress	External	✓	onlySharedOwners
	getIsUniswapV2Pair	External		-
	setIsUniswapV2Pair	External	✓	onlySharedOwners
	_setIsUniswapV2Pair	Private	✓	
	getMinimumTokenBalanceForSwapAndSendReflections	External		-
	setMinimumTokenBalanceForSwapAndSendReflections	External	✓	onlySharedOwners
	isRegularTransferAllowed	External		-
	allowRegularTransfer	External	✓	onlySharedOwners
	getDefaultUniswapV2PairTransferFee	External		-
	setDefaultUniswapV2PairTransferFee	External	✓	onlySharedOwners
	getReflectionTrackerAddress	External		-
	setReflectionTrackerAddress	External	✓	onlySharedOwners

	getTimeLockOf	External		-
	unlockTimeLockOf	External	✓	onlySharedOwners
	addExtraTimeToTimeLockOf	External	✓	onlySharedOwners
	getTransferFeeOf	External		-
	setTransferFeeOf	External	✓	onlySharedOwners
	getExcludedFromFeeOf	External		-
	setExcludedFromFeeOf	External	✓	onlySharedOwners
	getAutomatedReflectionTrackerCalls	External		-
	setAutomatedReflectionTrackerCalls	External	✓	onlySharedOwners
	swapAndSendReflections	External	✓	onlySharedOwners
	processAll	External	✓	onlySharedOwners
	swapAndSendReflectionsAndProcessAll	External	✓	onlySharedOwners
	_transfer	Internal	✓	
	_getOrCreateTokenPair	Private	✓	
	_setDeveloperWalletOptions	Private	✓	
	_setTransferFeeOf	Private	✓	
	_setExcludedFromFeeOf	Private	✓	
	_swapAndSendReflections	Private	✓	
	_getRandomNumber	Private		
SharedOwnable	Implementation	Ownable		
	<Constructor>	Public	✓	Ownable
	getCreator	External		-
	isSharedOwner	External		-
	setSharedOwner	Internal	✓	onlySharedOwners
	_setSharedOwner	Private	✓	
Strings	Library			
	toString	Internal		

	toHexString	Internal		
	toHexString	Internal		

Contract Flow



Summary

The Smart Contract analysis reported no compiler error or critical issues. The contract Owner can access some admin functions that can not be used in a malicious way to disturb the users' transactions. There is also a limit of max 25% fees.

The contract contains a built-in time lock functionality for the dev wallets. That means that the amount of the dev wallets cannot be transferred until the locked period elapsed.

The contract also contains a reflection distribution mechanism. When the accumulated amount is more than a specific threshold, the contract swaps a pseudo-random percentage of that amount in order to share it as a distribution.

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