



# Audit Report

## **Road of Iron**

December 2021

Type       BEP20

Address     0x258a307ea90619df58ef2140ec845629bf1769a0

Audited by  © coinscope

# Table of Contents

<b>Table of Contents</b>	<b>1</b>
<b>Contract Review</b>	<b>2</b>
<b>Audit Updates</b>	<b>2</b>
<b>Contract Analysis</b>	<b>3</b>
<b>ULTW - Unlimited Liquidity to Team Wallet</b>	<b>3</b>
<b>Description</b>	<b>4</b>
<b>Recommendation</b>	<b>4</b>
<b>Contract Diagnostics</b>	<b>5</b>
<b>Contract Functions</b>	<b>6</b>
<b>Contract Flow</b>	<b>11</b>
<b>Domain Info</b>	<b>12</b>
<b>Summary</b>	<b>13</b>
<b>Disclaimer</b>	<b>14</b>
<b>About Coinscope</b>	<b>15</b>

## Contract Review

<b>Contract Name</b>	Iron
<b>Compiler Version</b>	v0.8.7+commit.e28d00a7
<b>Optimization</b>	200 runs
<b>Licence</b>	MIT
<b>Explorer</b>	<a href="https://bscscan.com/token/0x258A307EA90619Df58eF2140eC845629bF1769a0">https://bscscan.com/token/0x258A307EA90619Df58eF2140eC845629bF1769a0</a>
<b>Symbol</b>	IRON
<b>Decimals</b>	9
<b>Total Supply</b>	1,000,000,000,000,000
<b>Source</b>	Iron.sol, misc.sol
<b>Domain</b>	roadofiron.com

## Audit Updates

<b>Initial Audit</b>	20th December 2021
<b>Corrected</b>	

# Contract Analysis

● Critical
 ● Medium
 ● Pass

Severity	Code	Description
<span style="color: blue;">●</span>	MT	Contract Owner is not able to mint new tokens
<span style="color: blue;">●</span>	BT	Contract Owner is not able to burn tokens from specific wallet
<span style="color: blue;">●</span>	ELFM	Contract Owner is not able to increase fees more than a reasonable percent (25%)
<span style="color: blue;">●</span>	ST	Contract Owner is not able to pause transactions for everyone else except him
<span style="color: blue;">●</span>	OCTD	Contract Owner is not able to transfer tokens from specific address
<span style="color: red;">●</span>	ULTW	Contract Owner is not able to increase the amount of liquidity taken by dev wallet more than a reasonable percent
<span style="color: blue;">●</span>	BC	Contract Owner is not able to blacklist wallets from selling

## ULTW - Unlimited Liquidity to Team Wallet

<b>Criticality</b>	critical
<b>Location</b>	<a href="https://bscscan.com/address/0x258a307ea90619df58ef2140ec845629bf1769a0#code#F1#L213">https://bscscan.com/address/0x258a307ea90619df58ef2140ec845629bf1769a0#code#F1#L213</a>

### Description

The contract always sends half of the liquidity to the `0xf8778e43B838725ba539c2fdcc9229f251D6Cbe7` address. These funds have been swiped from the swap & liquify feature.

```
addLiquidity(otherHalf, newBalance);
swapTokensForEth(division);
uint256 balanceToSend = address(this).balance;
payable(_dw).transfer(balanceToSend);
```

### Recommendation

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

If the contract is not going to be redeployed, we advise the team to disable the `swapAndLiquifyEnabled` or decrease the liquidity fee dramatically.

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

Pass	Name
✓	Integer Underflow
✓	Parity Multisig Bug
✓	Callstack Depth Attack
✓	Transaction-Ordering Dependency
✓	Timestamp Dependency
✓	Re-Entrancy

# Contract Functions

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
<b>Iron</b>	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	✓	-
	excludeFromFee	Public	✓	onlyOwner
	includeInFee	Public	✓	onlyOwner
	setSwapAndLiquifyEnabled	Public	✓	onlyOwner
	<Receive Ether>	External	Payable	-
	isExcludedFromFee	Public		-
	_approve	Private	✓	
	_transfer	Private	✓	
	swapAndLiquify	Private	✓	lockTheSwap
	swapTokensForEth	Private	✓	
	addLiquidity	Private	✓	
	_addLiquidityFee	Private	✓	
	_tokenTransfer	Private	✓	
	_transferStandard	Private	✓	
	_transferExcluded	Private	✓	

	_getValues	Private		
	calculateLiquidityFee	Private		
<b>IERC20</b>	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
<b>SafeMath</b>	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		
<b>Context</b>	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
<b>Address</b>	Library			
	isContract	Internal		
	sendValue	Internal	✓	
	functionCall	Internal	✓	
	functionCall	Internal	✓	

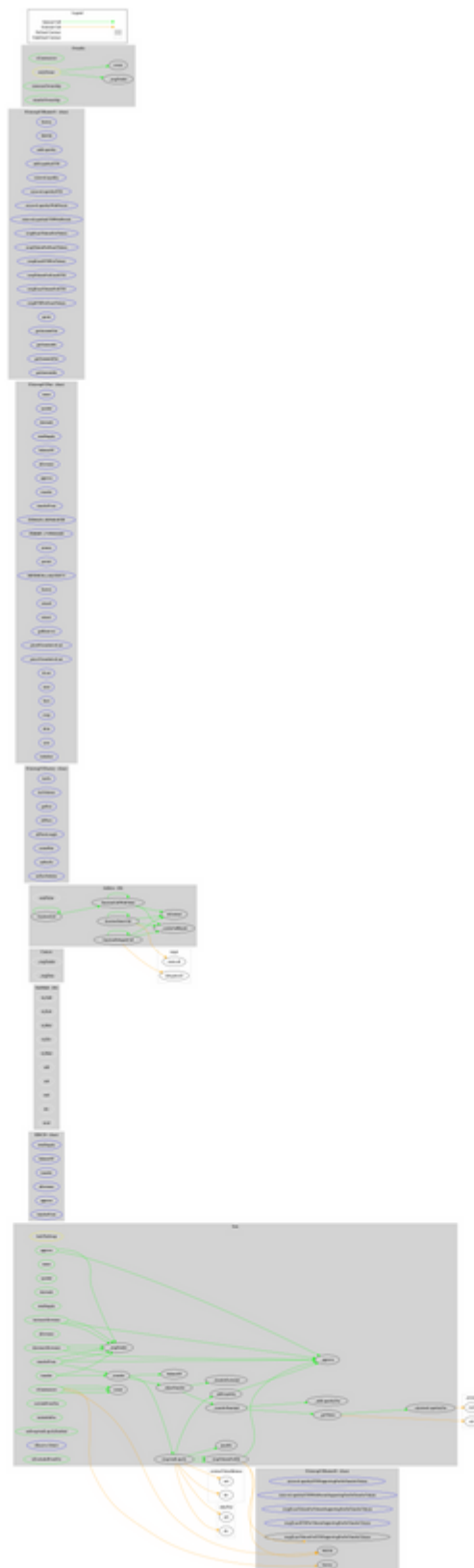


	functionCallWithValue	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionStaticCall	Internal		
	functionStaticCall	Internal		
	functionDelegateCall	Internal	✓	
	functionDelegateCall	Internal	✓	
	_verifyCallResult	Private		
<b>IUniswapV2Factory</b>	Interface			
	feeTo	External		-
	feeToSetter	External		-
	getPair	External		-
	allPairs	External		-
	allPairsLength	External		-
	createPair	External	✓	-
	setFeeTo	External	✓	-
	setFeeToSetter	External	✓	-
<b>IUniswapV2Pair</b>	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		-
	mint	External	✓	-
	burn	External	✓	-
	swap	External	✓	-
	skim	External	✓	-
	sync	External	✓	-
	initialize	External	✓	-
<b>IUniswapV2Router01</b>	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		-

<b>IUniswapV2Router02</b>	Interface	IUniswapV2Router01		
	removeLiquidityETHSupportingFeeOnTransferTokens	External	✓	-
	removeLiquidityETHWithPermitSupportingFeeOnTransferTokens	External	✓	-
	swapExactTokensForTokensSupportingFeeOnTransferTokens	External	✓	-
	swapExactETHForTokensSupportingFeeOnTransferTokens	External	Payable	-
	swapExactTokensForETHSupportingFeeOnTransferTokens	External	✓	-
<b>Ownable</b>	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner

# Contract Flow



## Domain Info

<b>Domain Name</b>	ROADOFIRON.COM
<b>Registry Domain ID</b>	2660490810_DOMAIN_COM-VRSN
<b>Creation Date</b>	2021-12-09T10:13:46Z
<b>Updated Date</b>	2021-12-09T11:57:48Z
<b>Registry Expiry Date</b>	2022-12-09T10:13:46Z
<b>Registrar WHOIS Server</b>	whois.reg.com
<b>Registrar URL</b>	<a href="https://www.reg.com">https://www.reg.com</a>
<b>Registrar</b>	Registrar of domain names REG.RU LLC
<b>Registrar IANA ID</b>	1606

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

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

## Summary

Road of Iron is aiming to create an onchain pixel art PVP/PVE RPG strategy on BSC with multiple ways of Play-to-Earn. The token has a friendly and growing community. The contract analysis did not report any major issue except the funds transfer. This issue can be produced indirectly by following specific steps. 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>