Audit Report

Wizard Pay

December 2021

Type	BEP20
Address	0x8d37cA3285a93e7E2bD50747a57c87EBf738c395
Audited by	© coinscope

Table of Contents

Contract Review

Contract Name	WizardPay
Compiler Version	v0.8.3+commit.8d00100c
Optimization	200 runs
Licence	MIT
Explorer	https://bscscan.com/token/0x8d37cA3285a93e7E2bD50747a57c87EBf738c395
Symbol	WIP
Decimals	18
Total Supply	10,000,000
Source	contract.sol
Domain	wizardpayment.com

Audit Updates

Initial Audit	25th December 2021
Corrected	

Contract Analysis

Critical Medium Pass

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

ST - Stop Transactions

Criticality	medium
Location	https://bscscan.com/address/0x8d37cA3285a93e7E2bD50747a57c87EBf738c395#code#L697

Description

The contract owner has the authority to stop transactions for all users excluding the owner. The owner may take advantage of it by setting the `_maxTxAmount` to zero.

```
if(sender != owner() && recipient != owner())
    require(amount <= _maxTxAmount, "Transfer amount exceeds the maxTxAmount.");
```

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.

OCTD - Owner Contract Tokens Drain

Criticality	high
Location	https://bscscan.com/address/0x8d37cA3285a93e7E2bD50747a57c87EBf738c395#code#L874,L879

Description

The contract owner has the authority to claim all the balance from any contract. The owner may take advantage of it by calling the `transferAnyERC20Tokens` or `TransferETH` function.

```
function transferAnyERC20Tokens(address _tokenAddress, address _to, uint256 _amount) public onlyOwner {
    Token(_tokenAddress).transfer(_to, _amount);
}
```

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.

ELFM - Exceed Limit Fees Manipulation

Criticality	high
Location	https://bscscan.com/address/0x8d37cA3285a93e7E2bD50747a57c87EBf738c395#code#L829,L833,L837,L841,L845

Description

The contract owner has the authority to increase over the allowed limit of 10%. The owner may take advantage of it by calling the `setTaxFee` function with a high percentage value.

```
function setTaxFee(uint256 fee) public onlyOwner {
    _taxFee = fee;
}
```

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.

Contract Diagnostics

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

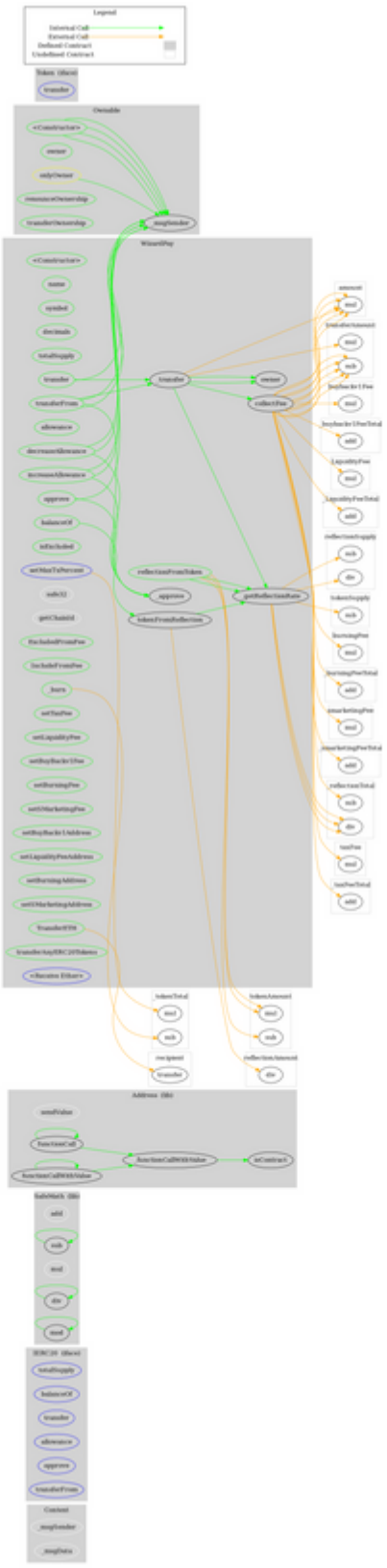
Contract Functions

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
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		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
Token	Interface			
	transfer	External	✓	-
WizardPay	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	✓	-
	isExcluded	Public		-
	reflectionFromToken	Public		-
	tokenFromReflection	Public		-
	_approve	Private	✓	
	_transfer	Private	✓	
	_burn	Public	✓	onlyOwner
	collectFee	Private	✓	

	_getReflectionRate	Private		
	safe32	Internal		
	getChainId	Internal		
	ExcludedFromFee	Public	✓	onlyOwner
	IncludeFromFee	Public	✓	onlyOwner
	setMaxTxPercent	External	✓	onlyOwner
	setTaxFee	Public	✓	onlyOwner
	setLiquidityFee	Public	✓	onlyOwner
	setBuyBackv1Fee	Public	✓	onlyOwner
	setBurningFee	Public	✓	onlyOwner
	setSMarketingFee	Public	✓	onlyOwner
	setBuyBackv1Address	Public	✓	onlyOwner
	setLiquidityFeeAddress	Public	✓	onlyOwner
	setBurningAddress	Public	✓	onlyOwner
	setSMarketingAddress	Public	✓	onlyOwner
	TransferETH	Public	✓	onlyOwner
	transferAnyERC20Tokens	Public	✓	onlyOwner
	<Receive Ether>	External	Payable	-

Contract Flow



Domain Info

Domain Name	wizardpayment.com
Registry Domain ID	2661093772_DOMAIN_COM-VRSN
Creation Date	2021-12-12T04:49:59Z
Updated Date	2021-12-12T04:49:59Z
Registry Expiry Date	2022-12-12T04:49:59Z
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 13 days before the analysis of the audit. It will expire in 12 months.

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

Summary

Wizard Pay is aiming to make quick and cashless transactions. The token 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 indirectly stopping the 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.

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