Cyberscope

Audit Report

Web3Move

June 2022

Table of Contents

Contract Review

Contract Name	Web3Move
Compiler Version	v0.8.7+commit.e28d00a7
Optimization	200 runs
Licence	MIT
Explorer	https://bscscan.com/token/0xf829aA254E6577a4BDB95d5cE61F8A293bf4d3b1
Symbol	W3M
Decimals	18
Total Supply	200,000,000
Domain	web3move.finance

Source Files

Filename	SHA256
BEP20.sol	9fbfcd45afb823a969893c25c91da344039d552cc9216b5569461a36d5ce8610
BEP20Detailed.sol	3a4c8b6fc4293d6d6bab8abf758ce39ca5938c61302f0d5b4cc5e72286dde246
BEPContext.sol	f8cb38984aade219964b1da398a8f6239bb1757065fd4dca760ca8d9b91ba5bb
BEPOwnable.sol	3a822e0d37cd6f1f2c4a47a6468171fcc0c6ede708ef52424ef1ea251584dcf6
IBEP20.sol	5953f0c5ecfc71226a4f934219c72dcbb2ae999aa58131cda84d28fd93a9caa7
SafeMath.sol	8c756491c47588016b20e85f9c12ecb5555a0d5a37737

	b39f8de3b6de5ad98b1
Web3Move.sol	849e6d948a4d649cf0753035b7ddad1e021dd59668d4 dcccbbbbd306ebc590fe

Audit Updates

Initial Audit	6th June 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#L93

Description

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

```
    } else if(liquidityPool[receiver] == true) {
        //It's an LP Pair and it's a sell
        taxAmount = (amount * sellTax) / 100;

        require(lastTrade[sender] < (block.timestamp - tradeCooldown), string("No
consecutive sells allowed. Please wait."));
        lastTrade[sender] = block.timestamp;
```

Recommendation

The contract could embody a check for not allowing setting the `tradeCooldown` lemoress 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.

BC - Blacklisted Contracts

Criticality	medium
Location	contract.sol#L85

Description

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

```
require(!isBlacklist[sender],"User blacklisted");
```

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
●	L11	Unnecessary Boolean equality

L01 - Public Function could be Declared External

Criticality	minor
Location	BEP20.sol#L39,46,58,66,77,94,120,139
	BEP20Detailed.sol#L29,37
	BEPOwnable.sol#L30,56,65
	Web3Move.sol#L108,113

Description

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

```
rescueToken
rescueBNB
transferOwnership
renounceOwnership
owner
symbol
name
decreaseAllowance
increaseAllowance
...
```

Recommendation

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

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	Web3Move.sol#L25,26,27,28,29,30,43,48,53,58,63,77,108

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.

```
_recipient
_status
_address
_transferTax
_buyTax
_sellTax
_marketingPool
_lpAddress
_tradeCooldown
...
```

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	BEP20.sol#L203,242

Description

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

```
_burnFrom
_burn
```

Recommendation

Remove unused functions.

L11 - Unnecessary Boolean equality

Criticality	minor
Location	Web3Move.sol#L83

Description

The comparison to boolean constants is redundant. Boolean constants can be used directly and do not need to be compared to true or false.

```
liquidityPool[receiver] == true
liquidityPool[sender] == true
```

Recommendation

Remove the equality to the boolean constant.

Contract Functions

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
BEP20	Implementation	BEPContext, IBEP20, BEPOwnable		
	totalSupply	Public		-
	balanceOf	Public		-
	transfer	Public	✓	-
	allowance	Public		-
	approve	Public	✓	-
	transferFrom	Public	✓	-
	increaseAllowance	Public	✓	-
	decreaseAllowance	Public	✓	-
	_transfer	Internal	✓	
	_mint	Internal	✓	
	_burn	Internal	✓	
	_approve	Internal	✓	
	_burnFrom	Internal	✓	
BEP20Detailed	Implementation			
	<Constructor>	Public	✓	-
	name	Public		-
	symbol	Public		-
	decimals	Public		-
BEPContext	Implementation			
	<Constructor>	Public	✓	-
	_msgSender	Internal		
	_msgData	Internal		

BEPOwnable	Implementation	BEPContext		
	\<Constructor\>	Public	✓	-
	owner	Public		-
	isOwner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	_transferOwnership	Internal	✓	
IBEP20	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		
Web3Move	Implementation	BEP20Detailed, BEP20		
	\<Constructor\>	Public	✓	BEP20Detailed
	setBlacklist	External	✓	onlyOwner
	setCooldownForTrades	External	✓	onlyOwner
	setLiquidityPoolStatus	External	✓	onlyOwner
	setMarketingPool	External	✓	onlyOwner
	setTaxes	External	✓	onlyOwner
	getTaxes	External		-
	setWhitelist	External	✓	onlyOwner
	_transfer	Internal	✓	

	rescueBNB	Public	✓	onlyOwner
	rescueToken	Public	✓	onlyOwner

Contract Flow
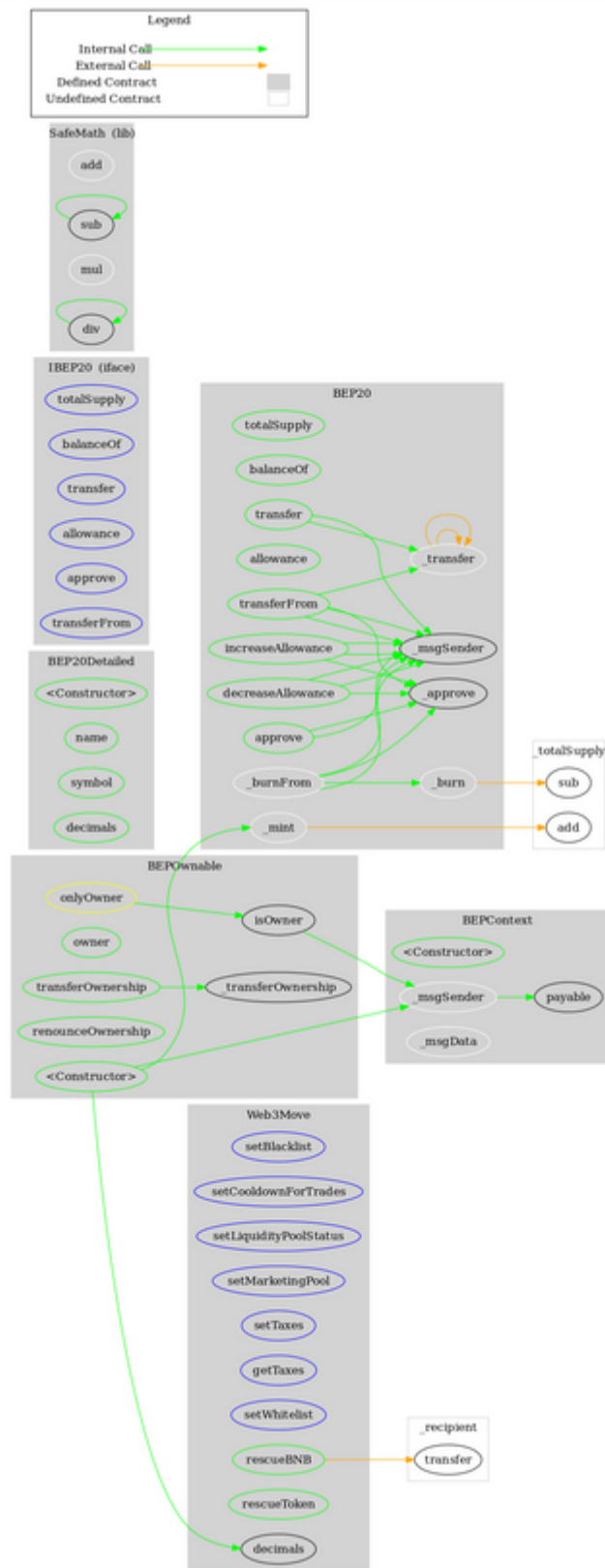
Domain Info

Domain Name	web3move.finance
Registry Domain ID	7ab2e0a7081c49349b9974ce1aa9f019-DONUTS
Creation Date	2022-05-07T11:06:18Z
Updated Date	2022-05-12T11:06:24Z
Registry Expiry Date	2023-05-07T11:06:18Z
Registrar WHOIS Server	whois.godaddy.com/
Registrar URL	http://www.godaddy.com/domains/search.aspx?ci=8990
Registrar	GoDaddy.com, LLC
Registrar IANA ID	146

The domain has been created 30 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

There are some functions that can be abused by the owner like stopping transactions and blacklisting addresses. The contract can be converted into a honeypot and prevent users from selling if the owner abuses the admin functions. 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.

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

About Cyberscope

Coinscope audit and K.Y.C. service has been rebranded to Cyberscope.

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.

Cyberscope and Coinscope are aiming to make crypto discoverable and efficient globally. They provide all the essential tools to assist users draw their own conclusions.

The Cyberscope team

https://www.cyberscope.io