Cyberscope

Audit Report

TribalWars

April 2022

Type	BEP20
Network	BSC
Address	0x687398E537AF9Cef19D21aFdDcc28Fd2e63d4F5b
Audited by	© cyberscope

Table of Contents

Contract Review

Contract Name	TribalWars
Compiler Version	v0.8.4+commit.c7e474f2
Optimization	200 runs
Licence	MIT
Explorer	https://bscscan.com/token/0x687398E537AF9Cef19D21aFdDcc28Fd2e63d4F5b
Symbol	TW
Decimals	9
Total Supply	1,000,000,000
Domain	tribalwars.world

Source Files

Filename	SHA256
contract.sol	b84463abe56bf6312048a528fce62ce4c96b10ddd2c176adab9c71ec23682144

Audit Updates

Initial Audit	6th April 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

ELFM - Exceed Limit Fees Manipulation

Criticality	critical
Location	contract.sol#L521

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 setBuyTaxes function with a high percentage value.

```
function setBuyTaxes(uint256 marketMakerFeeNew, uint256 marketingFeeNew,
uint256 lpFeeNew, uint256 stakeFeeNew) external onlyOwner() {
        _marketMakerFee = marketMakerFeeNew;
        _marketingFee = marketingFeeNew;
        _lpFee = lpFeeNew;
        _stakeFee = stakeFeeNew;
        _totalTax =
_marketMakerFee.add(_marketingFee).add(_lpFee).add(_stakeFee);
    }
```

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

● 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
●	L07	Missing Events Arithmetic
●	L09	Dead Code Elimination

L01 - Public Function could be Declared External

Criticality	minor
Location	contract.sol#L159,164,170,462,466,470,474,482,486,491 and 10 more

Description

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

```
transferFrom
transfer
changeRouterVersion
getCirculatingSupply
setSwapAndLiquifyByLimitOnly
setSwapAndLiquifyEnabled
setIsExcludedFromFee
setMarketPairStatus
approve
...
```

Recommendation

Use the external attribute for functions never called from the contract

L02 - State Variables could be Declared Constant

Criticality	minor
Location	contract.sol#L383,381,382

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#L207,208,224,243,545,391,397,398,399,400 and 1 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.

```
_totalTax
_stakeFee
_lpFee
_marketingFee
_marketMakerFee
_balances
_enabled
WETH
MINIMUM_LIQUIDITY
...
```

Recommendation

Follow the Solidity naming convention.
https://docs.soliditylang.org/en/v0.4.25/style-guide.html#naming-conventions

L07 - Missing Events Arithmetic

Criticality	minor
Location	contract.sol#L521,529

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.

```
minimumTokensBeforeSwap = newLimit
_marketMakerFee = marketMakerFeeNew
```

Recommendation

Emit an event for critical parameter changes.

L09 - Dead Code Elimination

Criticality	minor
Location	contract.sol#L119,102,106,110,114,83,94

Description

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

```
sendValue
isContract
functionCallWithValue
functionCall
_functionCallWithValue
```

Recommendation

Remove unused functions.

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		-
	waiveOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	getTime	Public		-
IUniswapV2Factory	Interface			
	feeTo	External		-
	feeToSetter	External		-
	getPair	External		-
	allPairs	External		-
	allPairsLength	External		-
	createPair	External	✓	-
	setFeeTo	External	✓	-
	setFeeToSetter	External	✓	-
IUniswapV2Pair	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		-
	burn	External	✓	-
	swap	External	✓	-
	skim	External	✓	-
	sync	External	✓	-
	initialize	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	✓	-	
TribalWars	Implementation	Context, IERC20, Ownable			
	<Constructor>	Public	✓	-	
	name	Public		-	
	symbol	Public		-	
	decimals	Public		-	
	totalSupply	Public		-	
	balanceOf	Public		-	
	allowance	Public		-	
	increaseAllowance	Public	✓	-	
	decreaseAllowance	Public	✓	-	
	minimumTokensBeforeSwapAmount	Public		-	
	approve	Public	✓	-	
	_approve	Private	✓		
	setMarketPairStatus	Public	✓	onlyOwner	
	setIsExcludedFromFee	Public	✓	onlyOwner	
	setBuyTaxes	External	✓	onlyOwner	
	setNumTokensBeforeSwap	External	✓	onlyOwner	
	setMarketingWalletAddress	External	✓	onlyOwner	
	setMarketMakerWalletAddress	External	✓	onlyOwner	
	setStakeWalletAddress	External	✓	onlyOwner	
	setSwapAndLiquifyEnabled	Public	✓	onlyOwner	
	setSwapAndLiquifyByLimitOnly	Public	✓	onlyOwner	

	getCirculatingSupply	Public		-
	transferToAddressETH	Private	✓	
	changeRouterVersion	Public	✓	onlyOwner
	<Receive Ether>	External	Payable	-
	transfer	Public	✓	-
	transferFrom	Public	✓	-
	_transfer	Private	✓	
	_basicTransfer	Internal	✓	
	swapAndLiquify	Private	✓	lockTheSwap
	swapTokensForEth	Private	✓	
	addLiquidity	Private	✓	
	takeFee	Internal	✓	

Contract Flow

Domain Info

Domain Name	tribalwars.world
Registry Domain ID	2b327270ce9d42f787b4f1de25134a41-DONUTS
Creation Date	2022-03-14T07:29:41Z
Updated Date	2022-03-19T07:30:13Z
Registry Expiry Date	2023-03-14T07:29:41Z
Registrar WHOIS Server	whois.namecheap.com
Registrar URL	https://www.namecheap.com/
Registrar	NameCheap, Inc.
Registrar IANA ID	1068

The domain has been created 23 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

TribalWars is an interesting project that has a friendly and growing community. The Smart Contract analysis reported one critical issue. The contract Owner can manipulate fees up to 100%. 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 provides all the essential tools to assist users draw their own conclusions.

The Cyberscope team

https://www.cyberscope.io