Cyberscope

Audit Report

Nowar

June 2022

Type	BEP20
Network	BSC
Address	0x3f8b23753807B83312545b1f6Ff265f13D7Be970
Audited by	© cyberscope

Table of Contents

Contract Review

Contract Name	DxFeeToken
Compiler Version	v0.8.7+commit.e28d00a7
Optimization	200 runs
Licence	MIT
Explorer	https://bscscan.com/token/0x3f8b23753807B83312545b1f6Ff265f13D7Be970
Symbol	Nowar
Decimals	18
Total Supply	1,000,000,000
Domain	nowars.site

Source Files

Filename	**SHA256**
contract.sol	281dbda5194d4ae30c7e91bccc6ce76880e3d3199f675e118f112d6dc5fe6720

Audit Updates

Initial Audit	20th 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

ELFM - Exceed Limit Fees Manipulation

Criticality	medium
Location	contract.sol#L1146,L1151,L1156,L1161

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 `setTaxFeePercent, setLiquidityFeePercent, setDevFeePercent, setSellTaxFeePercent` function to maximum amount. The maximum limit for sell transactions is 40%. The maximum limit for buy transactions is 30%.

```
function setTaxFeePercent(uint256 taxFee) external onlyOwner() {
        require(taxFee >= 0 && taxFee <=maxTaxFee,"taxFee out of range");
       _taxFee = taxFee;
}

function setLiquidityFeePercent(uint256 liquidityFee) external onlyOwner() {
        require(liquidityFee >= 0 && liquidityFee <=maxLiqFee,"liquidityFee out of range");
       _liquidityFee = liquidityFee;
}

function setDevFeePercent(uint256 devFee) external onlyOwner() {
       require(devFee >= 0 && devFee <=maxDevFee,"teamFee out of range");
       _devFee = devFee;
}

function setSellTaxFeePercent(uint256 sellTaxFee) external onlyOwner() {
        require(sellTaxFee >= 0 && sellTaxFee <=maxSellTaxFee,"taxFee out of range");
        _sellTaxFee = sellTaxFee;
}
```

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
●	FSA	Fixed Swap Address
●	L01	Public Function could be Declared External
●	L02	State Variables could be Declared Constant
●	L04	Conformance to Solidity Naming Conventions
●	L07	Missing Events Arithmetic
●	L08	Tautology or Contradiction
●	L09	Dead Code Elimination

FSA - Fixed Swap Address

Criticality	minor
Location	contract.sol#L1003

Description

The swap address is assigned once in the constructor and it can not be changed. The decentralized swaps sometimes create a new swap version or abandon the current. A contract that cannot change the swap address may not be able to catch-up the upgrade.

```
constructor (address tokenOwner,string memory name_, string memory symbol_,uint8 decimal_,
uint256 amountOfTokenWei,uint8[4] memory setFees, uint256[5] memory maxFees, address
devWalletAddress_, address _router, address _basePair) {
        _name = name_;
        _symbol = symbol_;
        _decimals = decimal_;
        _tTotal = amountOfTokenWei;
        _rTotal = (MAX - (MAX % _tTotal));
        router = _router;
```

Recommendation

It could be better to allow the swap address mutation in case of future swap updates.

L01 - Public Function could be Declared External

Criticality	minor
Location	contract.sol#L1082,1102,593,1178,1047,1599,1585,1073,1292,601,1093,1068,1055,1059,1098,1077,1115,1189,1106,1088,1051

Description

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

```
symbol
increaseAllowance
deliver
setSwapAndLiquifyEnabled
reflectionFromToken
approve
isExcludedFromReward
totalSupply
decimals
...
```

Recommendation

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

L02 - State Variables could be Declared Constant

Criticality	minor
Location	contract.sol#L927,953

Description

Constant state variables should be declared constant to save gas.

```
mintedByDxsale
dead
```

Recommendation

Add the constant attribute to state variables that never change.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contract.sol#L1189,946,718,964,1259,1178,967,716,961,958,976,661,1253,1169,714,663,1265,1446,720,681

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.

```
MINIMUM_LIQUIDITY
WHT
ETHAmount
_newAddr
_amount
PERMIT_TYPEHASH
WETH
_addr
DOMAIN_SEPARATOR
...
```

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#L1157,1142,1147,1152,1162

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.

```
_maxTxAmount = _tTotal.mul(maxTxPercent).div(10 ** 2)
_devFee = devFee
_liquidityFee = liquidityFee
_taxFee = taxFee
_sellTaxFee = sellTaxFee
```

Recommendation

Emit an event for critical parameter changes.

L08 - Tautology or Contradiction

Criticality	minor
Location	contract.sol#L1147,1142,1152,1157

Description

Detects expressions that are tautologies or contradictions. For instance, an uint variable will always be greater than or equal to zero.

```
require(bool,string)(sellTaxFee >= 0 && sellTaxFee <= maxSellTaxFee,taxFee out of range)
require(bool,string)(devFee >= 0 && devFee <= maxDevFee,teamFee out of range)
require(bool,string)(taxFee >= 0 && taxFee <= maxTaxFee,taxFee out of range)
require(bool,string)(liquidityFee >= 0 && liquidityFee <= maxLiqFee,liquidityFee out of range)
```

Recommendation

Fix the incorrect comparison by changing the value type or the comparison.

L09 - Dead Code Elimination

Criticality	minor
Location	contract.sol#L524,383,437,507,497,451,470,359,418,480,408

Description

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

```
functionCall
functionStaticCall
isContract
functionCallWithValue
functionDelegateCall
sendValue
verifyCallResult
...
```

Recommendation

Remove unused functions.

Contract Functions

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
SafeMath	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		
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
Address	Library			
	isContract	Internal		

	sendValue	Internal	✓	
	functionCall	Internal	✓	
	functionCall	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionStaticCall	Internal		
	functionStaticCall	Internal		
	functionDelegateCall	Internal	✓	
	functionDelegateCall	Internal	✓	
	verifyCallResult	Internal		
Ownable	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	_transferOwnership	Internal	✓	
UniSwapFactory	Interface			
	feeTo	External		-
	feeToSetter	External		-
	getPair	External		-
	allPairs	External		-
	allPairsLength	External		-
	createPair	External	✓	-
	setFeeTo	External	✓	-
	setFeeToSetter	External	✓	-
IIUniSwapPair	Interface			
	name	External		-
	symbol	External		-
	decimals	External		-
	totalSupply	External		-
	balanceOf	External		-
	allowance	External		-

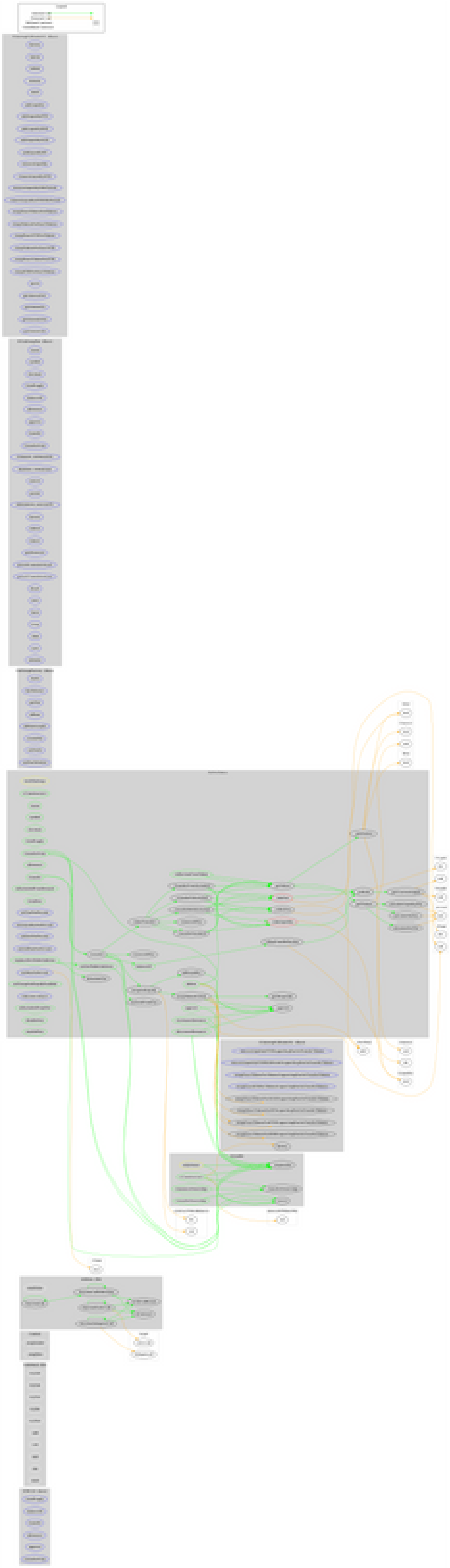
	approve	External	✓	-
	transfer	External	✓	-
	transferFrom	External	✓	-
	DOMAIN_SEPARATOR	External		-
	PERMIT_TYPEHASH	External		-
	nonces	External		-
	permit	External	✓	-
	MINIMUM_LIQUIDITY	External		-
	factory	External		-
	token0	External		-
	token1	External		-
	getReserves	External		-
	price0CumulativeLast	External		-
	price1CumulativeLast	External		-
	kLast	External		-
	mint	External	✓	-
	burn	External	✓	-
	swap	External	✓	-
	skim	External	✓	-
	sync	External	✓	-
	initialize	External	✓	-
IUniswapV2Router01	Interface			
	factory	External		-
	WETH	External		-
	WBNB	External		-
	WAVAX	External		-
	WHT	External		-
	addLiquidity	External	✓	-
	addLiquidityETH	External	Payable	-
	addLiquidityBNB	External	Payable	-
	addLiquidityAVAX	External	Payable	-
	addLiquidityHT	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	✓	-
	swapExactTokensForBNBSupportingFeeOnTransferTokens	External	✓	-
	swapExactTokensForAVAXSupportingFeeOnTransferTokens	External	✓	-
	swapExactTokensForHTSupportingFeeOnTransferTokens	External	✓	-
DxFeeToken	Implementation	Context, IERC20, Ownable		
	<Constructor>	Public	✓	-
	getWrapAddr	Public		-
	name	Public		-

	symbol	Public		-
	decimals	Public		-
	totalSupply	Public		-
	balanceOf	Public		-
	transfer	Public	✓	-
	allowance	Public		-
	approve	Public	✓	-
	transferFrom	Public	✓	-
	increaseAllowance	Public	✓	-
	decreaseAllowance	Public	✓	-
	isExcludedFromReward	Public		-
	totalFees	Public		-
	deliver	Public	✓	-
	reflectionFromToken	Public		-
	tokenFromReflection	Public		-
	excludeFromFee	Public	✓	onlyOwner
	includeInFee	Public	✓	onlyOwner
	setTaxFeePercent	External	✓	onlyOwner
	setLiquidityFeePercent	External	✓	onlyOwner
	setDevFeePercent	External	✓	onlyOwner
	setSellTaxFeePercent	External	✓	onlyOwner
	setMaxTxPercent	External	✓	onlyOwner
	setDevWalletAddress	Public	✓	onlyOwner
	replaceDevWalletAddress	Public	✓	onlyOwner
	setSwapAndLiquifyEnabled	Public	✓	onlyOwner
	<Receive Ether>	External	Payable	-
	_getValues	Private		
	_getTValues	Private		
	_getRValues	Private		
	_getRate	Private		
	_getCurrentSupply	Private		
	_takeLiquidity	Private	✓	
	_takeDev	Private	✓	
	calculateTaxFee	Private		
	calculateLiquidityFee	Private		

	calculateDevFee	Private		
	removeAllFee	Private	✓	
	restoreAllFee	Private	✓	
	isExcludedFromFee	Public		-
	_approve	Private	✓	
	_transfer	Private	✓	
	swapAndLiquify	Private	✓	lockTheSwap
	swapTokensForEth	Private	✓	
	addLiquidity	Private	✓	
	_tokenTransfer	Private	✓	
	_transferStandard	Private	✓	
	_transferToExcluded	Private	✓	
	_transferFromExcluded	Private	✓	
	_transferBothExcluded	Private	✓	
	_reflectFee	Private	✓	
	disableFees	Public	✓	onlyOwner
	enableFees	Public	✓	onlyOwner

Contract Flow



Domain Info

Domain Name	nowars.site
Registry Domain ID	D302588140-CNIC
Creation Date	2022-06-11T19:00:27+00:00
Updated Date	2022-06-16T19:02:08+00:00
Registry Expiry Date	2023-06-11T23:59:59+00:00
Registrar WHOIS Server	whois.gabia.com
Registrar URL	
Registrar	Gabia, Inc.
Registrar IANA ID	244

The domain has been created 8 days before the creation of the audit. It will expire in 12 months.

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

Summary

The Smart Contract analysis reported one medium severity issue. The contract owner has the authority to manipulate the fees. 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 30% fees for buy transactions and 40% for sell 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.

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