Cyberscope

Audit Report

Twittelon BOSS

April 2022

Type	BEP20
Network	BSC
Address	0xf9b0fa7feee99a9c154fbd58a289011320da7f15
Audited by	© cyberscope

Table of Contents

Contract Review

Contract Name	TBOSS
Compiler Version	v0.7.4+commit.3f05b770
Optimization	200 runs
Licence	Unlicense
Explorer	https://bscscan.com/token/0xf9b0fa7feee99a9c154fbd58a289011320da7f15
Symbol	TBOSS
Decimals	18
Total Supply	1,000,000,000,000
Domain	twittelonboss.com

Source Files

Filename	**SHA256**
contract.sol	dcd212f2f4b33ea6fa31f8bcd7b351575929dc6a9a2d2331ca1866cef32a33d2

Audit Updates

Initial Audit	27th 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

OCTD - Owner Contract Tokens Drain

Criticality	minor
Location	contract.sol#L799

Description

The contract owner has the authority to claim all the balance of the contract. The owner may take advantage of it by calling the `withdrawAllTomarketing` function.

```
    function withdrawAllTomarketing() external swapping onlyOwner {

        uint256 amountToSwap = _balances[address(this)];
        require( amountToSwap > 0,"There is no TBOSS token deposited in token
contract");
        address[] memory path = new address[](2);
        path[0] = address(this);
        path[1] = router.WETH();
        router.swapExactTokensForETHSupportingFeeOnTransferTokens(
            amountToSwap,
            0,
            path,
            marketingReceiver,
            block.timestamp
        );
    }
```

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.

ULTW - Unlimited Liquidity to Team Wallet

Criticality	minor
Location	contract.sol#L926, 743

Description

The contract owner has the authority to transfer funds without limit to the team wallet. These funds have been accumulated from fees collected from the contract. The owner may take advantage of it by calling the `setFeeReceivers` function.

```
function setFeeReceivers(
        address _teamReceiver,
        address _marketingReceiver,
        address _burnAddress
    ) external onlyOwner {
        teamReceiver = _teamReceiver;
        marketingReceiver = _marketingReceiver;
        burnAddress = _burnAddress;
    }
```

```
_balances[burnAddress] = _balances[burnAddress].add(
            amount.div(feeDenominator).mul(burnFee)
        );
```

Recommendation

The contract could embody a check for the maximum amount of funds that can be swapped. Since a huge amount may violate the token's price.

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
	MAL	Misused Algorithmic Logic
	CO	Code Optimization
	L01	Public Function could be Declared External
	L02	State Variables could be Declared Constant
	L04	Conformance to Solidity Naming Conventions
	L05	Unused State Variable
	L07	Missing Events Arithmetic
	L09	Dead Code Elimination
	L13	Divide before Multiply Operation

MAL - Misused Algorithmic Logic

Criticality	minor
Location	contract.sol#L739

Description

The algorithmic flow does not follow the required business logic.

```
recipient == pair;
```

Recommendation

The algorithm should be reshaped so it will match to the business logic.

CO - Code Optimization

Criticality	minor
Location	contract.sol#L729

Description

There are code segments that could be optimized. A segment may be optimized so that it becomes a smaller size, consumes less memory, executes more rapidly, or performs fewer operations.

```
function takeFee(
        address sender,
        address recipient,
        uint256 amount
    ) internal  returns (uint256) {
        uint256 _totalFee = totalFee;
        uint256 _marketingFee = marketingFee;
        uint256 _teamFee = teamFee;
        uint256 _DividendFee = DividendFee;

        recipient == pair;

        uint256 feeAmount = amount.div(feeDenominator).mul(_totalFee);

        _balances[burnAddress] = _balances[burnAddress].add(
            amount.div(feeDenominator).mul(burnFee)
        );
        _balances[address(this)] = _balances[address(this)].add(

amount.div(feeDenominator).mul(_marketingFee.add(_DividendFee).add(_teamFee))
        );
        emit Transfer(sender, address(this), feeAmount);
        return amount.sub(feeAmount);
    }
```

Recommendation

Rewrite the code segment without creating and assigning the fees to new variables. Hence, the runtime will be more performant.

L01 - Public Function could be Declared External

Criticality	minor
Location	contract.sol#L497,510,515,541,545,549,913

Description

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

```
getCirculatingSupply
decimals
symbol
name
transferOwnership
renounceOwnership
owner
```

Recommendation

Use the external attribute for functions never called from the contract

L02 - State Variables could be Declared Constant

Criticality	minor
Location	contract.sol#L359,584,575,585,576,582,574,596,577

Description

Constant state variables should be declared constant to save gas.

```
teamFee
swapEnabled
marketingFee
feeDenominator
burnFee
ZERO
DividendFee
DEAD
dividendsPerShareAccuracyFactor
```

Recommendation

Add the constant attribute to state variables that never change.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contract.sol#L141,142,159,179,381,335,344,889,904,927 and 15 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.

```
_totalSupply
DividendReceiver
ZERO
DEAD
DividendFee
Total_Supply
_isFeeExempt
_address
_flag
...
```

Recommendation

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

L05 - Unused State Variable

Criticality	minor
Location	contract.sol#L8,608

Description

There are segments that contain unused state variables.

```
MAX_SUPPLY
MAX_INT256
```

Recommendation

Remove unused state variables.

L07 - Missing Events Arithmetic

Criticality	minor
Location	contract.sol#L381

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.

```
minPeriod = _minPeriod
```

Recommendation

Emit an event for critical parameter changes.

L09 - Dead Code Elimination

Criticality	minor
Location	contract.sol#L36

Description

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

```
abs
```

Recommendation

Remove unused functions.

L13 - Divide before Multiply Operation

Criticality	minor
Location	contract.sol#L729

Description

Performing divisions before multiplications may cause lose of prediction.

```
_balances[address(this)] =
_balances[address(this)].add(amount.div(feeDenominator).mul(_marketingFee.add(
_DividendFee).add(_teamFee)))
_balances[burnAddress] =
_balances[burnAddress].add(amount.div(feeDenominator).mul(burnFee))
feeAmount = amount.div(feeDenominator).mul(_totalFee)
```

Recommendation

The multiplications should be prior to the divisions.

Contract Functions

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
SafeMathInt	Library			
	mul	Internal		
	div	Internal		
	sub	Internal		
	add	Internal		
	abs	Internal		
SafeMath	Library			
	add	Internal		
	sub	Internal		
	sub	Internal		
	mul	Internal		
	div	Internal		
	div	Internal		
	mod	Internal		
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	allowance	External		-
	transfer	External	✓	-
	approve	External	✓	-
	transferFrom	External	✓	-
IPancakeSwapPair	Interface			
	name	External		-
	symbol	External		-
	decimals	External		-

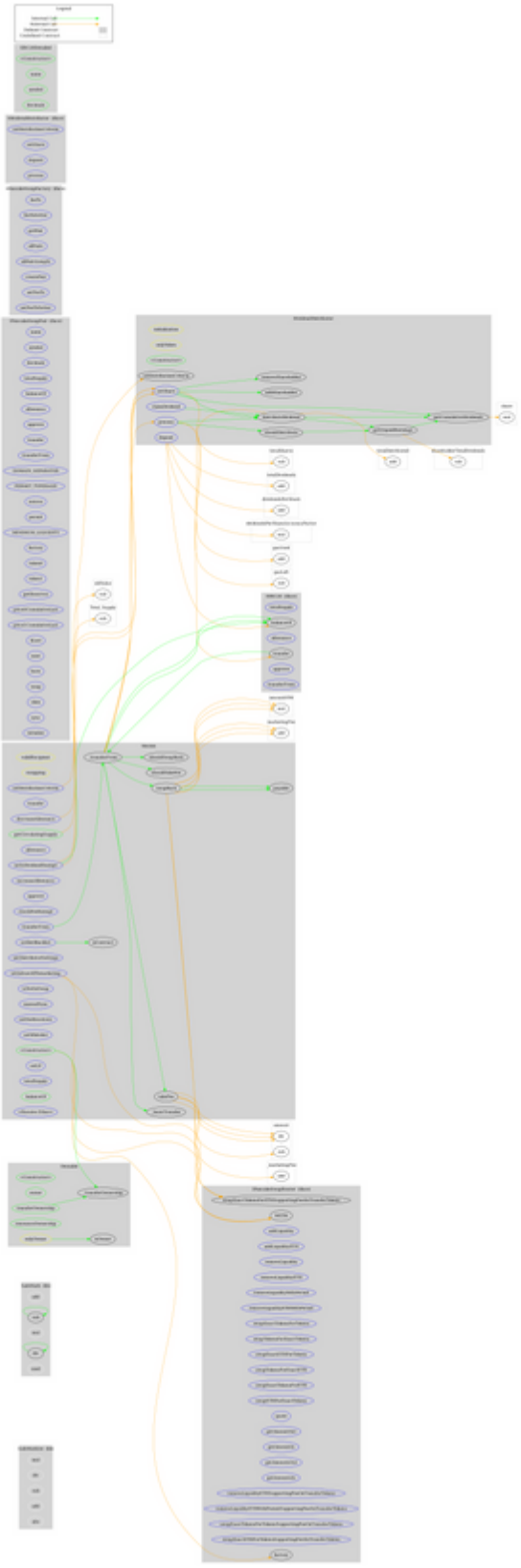
	totalSupply	External		-
	balanceOf	External		-
	allowance	External		-
	approve	External	✓	-
	transfer	External	✓	-
	transferFrom	External	✓	-
	DOMAIN_SEPARATOR	External		-
	PERMIT_TYPEHASH	External		-
	nonces	External		-
	permit	External	✓	-
	MINIMUM_LIQUIDITY	External		-
	factory	External		-
	token0	External		-
	token1	External		-
	getReserves	External		-
	price0CumulativeLast	External		-
	price1CumulativeLast	External		-
	kLast	External		-
	mint	External	✓	-
	burn	External	✓	-
	swap	External	✓	-
	skim	External	✓	-
	sync	External	✓	-
	initialize	External	✓	-
IPancakeSwap Router	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		-
	removeLiquidityETHSupportingFeeOnTransferTokens	External	✓	-
	removeLiquidityETHWithPermitSupportingFeeOnTransferTokens	External	✓	-
	swapExactTokensForTokensSupportingFeeOnTransferTokens	External	✓	-
	swapExactETHForTokensSupportingFeeOnTransferTokens	External	Payable	-
	swapExactTokensForETHSupportingFeeOnTransferTokens	External	✓	-
IPancakeSwapFactory	Interface			
	feeTo	External		-
	feeToSetter	External		-
	getPair	External		-
	allPairs	External		-
	allPairsLength	External		-
	createPair	External	✓	-
	setFeeTo	External	✓	-
	setFeeToSetter	External	✓	-
IDividendDistributor	Interface			
	setDistributionCriteria	External	✓	-
	setShare	External	✓	-

	deposit	External	Payable	-
	process	External	✓	-
DividendDistributor	Implementation	IDividendDistributor		
	<Constructor>	Public	✓	-
	setDistributionCriteria	External	✓	onlyToken
	setShare	External	✓	onlyToken
	deposit	External	Payable	onlyToken
	process	External	✓	onlyToken
	shouldDistribute	Internal		
	distributeDividend	Internal	✓	
	claimDividend	External	✓	-
	getUnpaidEarnings	Public		-
	getCumulativeDividends	Internal		
	addShareholder	Internal	✓	
	removeShareholder	Internal	✓	
Ownable	Implementation			
	<Constructor>	Public	✓	-
	owner	Public		-
	isOwner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	_transferOwnership	Internal	✓	
ERC20Detailed	Implementation	IERC20		
	<Constructor>	Public	✓	-
	name	Public		-
	symbol	Public		-
	decimals	Public		-
TBOSS	Implementation	ERC20Detailed, Ownable		

	<Constructor>	Public	✓	ERC20Detailed Ownable
	transfer	External	✓	validRecipient
	transferFrom	External	✓	validRecipient
	_basicTransfer	Internal	✓	
	_transferFrom	Internal	✓	
	takeFee	Internal	✓	
	swapBack	Internal	✓	swapping
	withdrawAllTomarketing	External	✓	swapping onlyOwner
	shouldTakeFee	Internal		
	shouldSwapBack	Internal		
	allowance	External		-
	decreaseAllowance	External	✓	-
	increaseAllowance	External	✓	-
	approve	External	✓	-
	checkFeeExempt	External		-
	setIsDividendExempt	External	✓	onlyOwner
	setDistributionCriteria	External	✓	onlyOwner
	setDistributorSettings	External	✓	onlyOwner
	getCirculatingSupply	Public		-
	isNotInSwap	External		-
	manualSync	External	✓	-
	setFeeReceivers	External	✓	onlyOwner
	setWhitelist	External	✓	onlyOwner
	setBotBlacklist	External	✓	onlyOwner
	setLP	External	✓	onlyOwner
	totalSupply	External		-
	balanceOf	Public		-
	isContract	Internal		
	<Receive Ether>	External	Payable	-

Contract Flow



Domain Info

Domain Name	twittelonboss.com
Registry Domain ID	2690807761_DOMAIN_COM-VRSN
Creation Date	2022-04-21T00:23:10.00Z
Updated Date	0001-01-01T00:00:00.00Z
Registry Expiry Date	2023-04-21T00:23:10.00Z
Registrar WHOIS Server	whois.namecheap.com
Registrar URL	http://www.namecheap.com
Registrar	NAMECHEAP INC
Registrar IANA ID	1068

The domain has been created 7 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

Twittelon BOSS is an interesting project that has a friendly and growing community. The Smart Contract analysis reported no compiler error or critical issues. The contract Owner can access some admin functions that can not be used in a malicious way to disturb the users' transactions. The fees are fixed to 7%.

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