Cyberscope

Audit Report

Tortuga

October 2022

Type	ERC20
Network	ETH
Address	0x62886752DDd3D27288dB6C886D9c72F1BE763615
Audited by	© cyberscope

Table of Contents

Contract Review

Contract Name	TOKEN
Compiler Version	v0.8.16+commit.07a7930e
Optimization	200 runs
Licence	Unlicense
Explorer	https://etherscan.io/token/0x62886752DDd3D27288dB6C886D9c72F1BE763615
Symbol	TOR
Decimals	9
Total Supply	1,000,000,000,000,000
Domain	tortugatoken.io

Source Files

Filename	**SHA256**
contract.sol	a05ebebd8197b9f4b8064813968a99a07d3ec4870b40c7191c6c338a05c18bf2

Audit Updates

Initial Audit	25th October 2022 https://github.com/cyberscope-io/audits/blob/main/1-tor/v1/audit.pdf
Corrected	31st October 2022

Contract Analysis

🔴 Critical 🟡 Medium ⚪ Minor / Informative 🔵 Pass

Severity	Code	Description	Status
🔵	ST	Stops Transactions	Passed
⚪	OCTD	Transfers Contract's Tokens	Unresolved
🔵	OTUT	Transfers User's Tokens	Passed
🔵	ELFM	Exceeds Fees Limit	Passed
⚪	ULTW	Transfers Liquidity to Team Wallet	Unresolved
🔵	MT	Mints Tokens	Passed
🔵	BT	Burns Tokens	Passed
🟡	BC	Blacklists Addresses	Unresolved

OCTD - Transfers Contract's Tokens

Criticality	minor / informative
Location	contract.sol#L973
Status	Unresolved

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 withdrawStuckedTokens function.

```
 function withdrawStuckedTokens(address tokenAddress, uint256 tokens) external onlyOwner
returns (bool success){
        return IERC20(tokenAddress).transfer(msg.sender, tokens);
   }
```

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 - Transfers Liquidity to Team Wallet

Criticality	minor / informative
Location	contract.sol#L966
Status	Unresolved

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 method1 and method2 methods.

```
function withdrawStuckedFunds(uint256 amount) external onlyOwner {
        // This is the current recommended method to use.
        (bool sent, ) = _owner.call{value: amount}("");
        require(sent, "Failed to send ETH");
}
```

Recommendation

The contract could embody a check for the maximum amount of funds that can be swapped. Since a huge amount may volatile 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.

BC - Blacklists Addresses

Criticality	medium
Location	contract.sol#L886
Status	Unresolved

Description

The contract owner has the authority to stop addresses from transactions. The owner may take advantage of it by calling the addToBlackList function.

```
function addToBlackList(address account) external onlyOwner {
 require(account != owner(),"Owner address can not blacklisted");
 _isBlacklisted[account] = true;
 }
```

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 / Informative

Severity	Code	Description	Status
●	STC	Succeeded Transfer Check	Unresolved
●	BLC	Business Logic Concern	Unresolved
●	MC	Missing Check	Unresolved
●	L02	State Variables could be Declared Constant	Unresolved
●	L04	Conformance to Solidity Naming Conventions	Unresolved
●	L05	Unused State Variable	Unresolved
●	L07	Missing Events Arithmetic	Unresolved
●	L09	Dead Code Elimination	Unresolved
●	L13	Divide before Multiply Operation	Unresolved

STC - Succeeded Transfer Check

Criticality	minor / informative
Location	contract.sol#L973
Status	Unresolved

Description

According to the ERC20 specification, the transfer methods should be checked if the result is successful. Otherwise, the contract may wrongly assume that the transfer has been established.

```
function withdrawStuckedTokens(address tokenAddress, uint256 tokens) external onlyOwner
returns (bool success){
        return IERC20(tokenAddress).transfer(msg.sender, tokens);
    }
```

Recommendation

The contract should check if the result of the transfer methods is successful.

BLC - Business Logic Concern

Criticality	minor / informative
Location	contract.sol#L1250
Status	Unresolved

Description

In Solidity, all integer division rounds down to the nearest integer. The contract distributes the funds proportional to the receipients. These calculations may produce unexpected left-over funds to the contract.

```
uint256 ethForMarketing = ethBalance * marketingTokens / (totalTokensToSwap);
uint256 ethForCharity = ethBalance * charityTokens / (totalTokensToSwap);
(success,) = address(_marketingWalletAddress).call{value: ethForMarketing}("");
(success,) = address(_CharityWalletAddress).call{value: ethForCharity}("");
```

Recommendation

In the last ratio, the contract could subtract the sum of the rest ratios from the totalTokensToSwap. Hence, it will be guaranteed that the calculations will not produce leftover amounts.

MC - Missing Check

Criticality	minor / informative
Location	contract.sol#L930,934
Status	Unresolved

Description

The contract is processing variables that have not been properly sanitized and checked that they form the proper shape. These variables may produce vulnerability issues.

The contract does not sanitize the address properly.

```
function setMarketingWalletAddress(address _addr) external onlyOwner {
    _marketingWalletAddress = _addr;
}

function setCharityWalletAddress(address _addr) external onlyOwner {
    _CharityWalletAddress = _addr;
}
```

Recommendation

The contract should properly check the variables according to the required specifications. It is recommended to embody a check for not allowing addresses to be set to zero.

L01 - Public Function could be Declared External

Criticality	minor / informative
Location	contract.sol#L194,199,682,686,694,703,712,721,730,747,760,776,780,784,796,824,870,874,878,1158
Status	Unresolved

Description

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

```
renounceOwnership
transferOwnership
name
symbol
totalSupply
transfer
allowance
approve
transferFrom
...
```

Recommendation

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

L03 - Redundant Statements

Criticality	minor / informative
Location	contract.sol#L151
Status	Unresolved

Description

The contract contains statements that are not used and have no effect. As a result, those segments increase the code size of the contract unnecessarily.

```
Context
```

Recommendation

Remove the redundant statements in order to decrease the code size.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor / informative
Location	contract.sol#L173,227,296,298,329,375,631,930,934,957,1119,1123,1131,588,591,592,593,602,616,617,618,619
Status	Unresolved

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.

```
_owner
_users
_trueFalse
DOMAIN_SEPARATOR
PERMIT_TYPEHASH
MINIMUM_LIQUIDITY
WETH
swapEnabledUpdated
_addr
...
```

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 / informative
Location	contract.sol#L892,911,938,943
Status	Unresolved

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.

```
_sellTaxFee = tFee
_buyTaxFee = tFee
_maxTxAmount = maxTxAmount * 10 ** decimals()
numTokensSellToSendFees = amount * 10 ** _decimals
```

Recommendation

Emit an event for critical parameter changes.

L09 - Dead Code Elimination

Criticality	minor / informative
Location	contract.sol#L163
Status	Unresolved

Description

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

```
isContract
```

Recommendation

Remove unused functions.

L13 - Divide before Multiply Operation

Criticality	minor / informative
Location	contract.sol#L1234
Status	Unresolved

Description

Performing divisions before multiplications may cause lose of prediction.

```
marketingTokens = contractBalance.mul(_marketingFee).div(100)
charityTokens = contractBalance.mul(_charityFee).div(100)
```

Recommendation

The multiplications should be prior to the divisions.

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		

Ownable	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
LockToken	Implementation	Ownable		
	<Constructor>	Public	✓	-
	openTrade	External	✓	onlyOwner
	includeToWhiteList	External	✓	onlyOwner
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		-

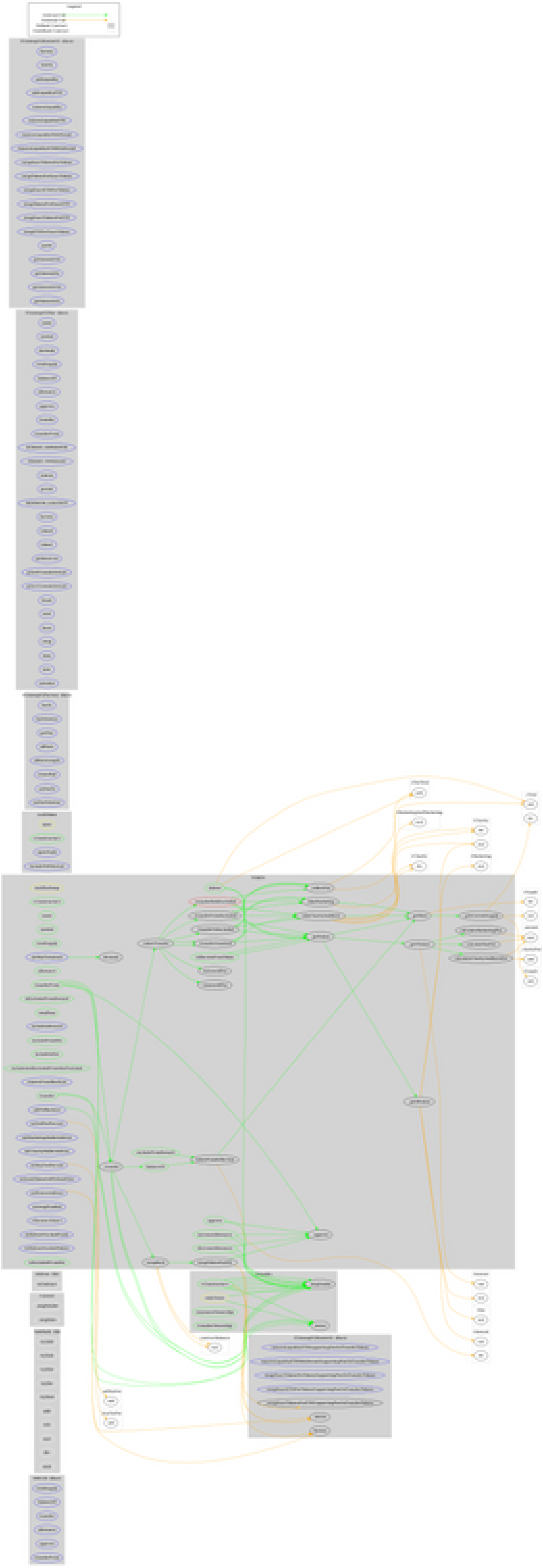
	PERMIT_TYPEHASH	External		-
	nonces	External		-
	permit	External	✓	-
	MINIMUM_LIQUIDITY	External		-
	factory	External		-
	token0	External		-
	token1	External		-
	getReserves	External		-
	price0CumulativeLast	External		-
	price1CumulativeLast	External		-
	kLast	External		-
	mint	External	✓	-
	burn	External	✓	-
	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	✓	-
TOKEN	Implementation	Context, IERC20, Ownable, LockToken		
	<Constructor>	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		-
	excludeFromReward	Public	✓	onlyOwner
	includeInReward	External	✓	onlyOwner
	_transferBothExcluded	Private	✓	
	excludeFromFee	Public	✓	onlyOwner
	includeInFee	Public	✓	onlyOwner
	includeAndExcludedFromMaxTnxLimit	Public	✓	onlyOwner
	removeFromBlackList	External	✓	onlyOwner
	addToBlackList	External	✓	onlyOwner
	setSellFeePercent	External	✓	onlyOwner
	setBuyFeePercent	External	✓	onlyOwner
	setMarketingWalletAddress	External	✓	onlyOwner
	setCharityWalletAddress	External	✓	onlyOwner
	setMaxTxAmount	External	✓	onlyOwner
	setnumTokensSellToSendFees	External	✓	onlyOwner
	setRouterAddress	External	✓	onlyOwner
	setswapEnabled	External	✓	onlyOwner
	<Receive Ether>	External	Payable	-
	withdrawStuckedFunds	External	✓	onlyOwner
	withdrawStuckedTokens	External	✓	onlyOwner
	_reflectFee	Private	✓	
	_getValues	Private		
	_getTValues	Private		
	_getRValues	Private		
	_getRate	Private		
	_getCurrentSupply	Private		
	_takeMarketing	Private	✓	
	_takeCharityAndBurn	Private	✓	
	calculateTaxFee	Private		
	calculateCharityAndBurnFee	Private		
	calculateMarketingFee	Private		
	removeAllFee	Private	✓	
	restoreAllFee	Private	✓	
	isExcludedFromFee	Public		-

	_approve	Private	✓	
	_transfer	Private	✓	open
	swapBack	Private	✓	lockTheSwap
	swapTokensForEth	Private	✓	
	_tokenTransfer	Private	✓	
	_transferStandard	Private	✓	
	_transferToExcluded	Private	✓	
	_transferFromExcluded	Private	✓	

Contract Flow



Domain Info

Domain Name	tortugatoken.io
Registry Domain ID	fa1386166a584bfd99b5b42c22a1e4de-DONUTS
Creation Date	2022-09-12T08:52:43Z
Updated Date	2022-09-19T02:24:24Z
Registry Expiry Date	2023-09-12T08:52:43Z
Registrar WHOIS Server	whois.tldregistrarsolutions.com
Registrar URL	http://www.tldregistrarsolutions.com
Registrar	TLD Registrar Solutions Ltd.
Registrar IANA ID	1564

The domain was created about 1 month 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 transferring contract tokens, transferring funds to the team's wallet, and blacklisting addresses. 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