



Cyberscope

Audit Report

Swap TC

April 2022

Type BEP20

Network BSC

Address 0x2E1EfFAd54bE5013A6b7DD0a6D26fB21d0e8f7A0

Audited by © cyberscope

Table of Contents

Table of Contents	1
Contract Review	3
Source Files	3
Audit Updates	3
Contract Analysis	4
ST - Stop Transactions	5
Description	5
Recommendation	5
Contract Diagnostics	6
L01 - Public Function could be Declared External	7
Description	7
Recommendation	7
L04 - Conformance to Solidity Naming Conventions	8
Description	8
Recommendation	8
L05 - Unused State Variable	9
Description	9
Recommendation	9
L07 - Missing Events Arithmetic	10
Description	10
Recommendation	10
L08 - Tautology or Contradiction	11
Description	11
Recommendation	11
L09 - Dead Code Elimination	12
Description	12

Recommendation	12
L12 - Using Variables before Declaration	13
Description	13
Recommendation	13
L14 - Uninitialized Variables in Local Scope	14
Description	14
Recommendation	14
L15 - Local Scope Variable Shadowing	15
Description	15
Recommendation	15
Contract Functions	16
Contract Flow	24
Domain Info	25
Summary	26
Disclaimer	27
About Cyberscope	28

Contract Review

Contract Name	BNBDividendPayingERC20Token
Compiler Version	v0.8.11+commit.d7f03943
Optimization	1000 runs
Licence	MIT
Explorer	https://bscscan.com/token/0x2E1EfFAd54bE5013A6b7DD0a6D26fB21d0e8f7A0
Symbol	SWAPTC
Decimals	9
Total Supply	1,000,000,000,000
Domain	swaptc.com

Source Files

Filename	SHA256
contract.sol	7f3f6d216b98924dc40ce78a48e26dac4da8727cd1e8907fd62bede985554d18

Audit Updates

Initial Audit	13th April 2022
Corrected	

Contract Analysis

- The contract supports fees proportional to the weeks that have elapsed.
- It contains a default configuration of weekly fees from the first until the 19th week.
- The weekly basic fee is applied to the sell and transfer transactions.
- The buy transactions have a dedicated fee.
- The buy fees cannot be configured more than 5%.
- The weekly fees cannot be configured more than 30%.

● 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	minor
Location	contract.sol#L1

Description

The contract owner has the authority to stop transactions for all users excluding the owner. The owner may take advantage of it by setting the `gasForProcessing` to a high value. As a result, the callers will be unable to pay the fee for the transfer.

```
uint256 requiredGasValue = gasForProcessing + 400000;  
require(  
    gasleft() >= requiredGasValue,  
    "Insufficient Gas. Try again with gasLimit of at least"  
).appendString((requiredGasValue + 100000).toString())  
);
```

Recommendation

The contract could embody a check for not allowing setting the `_maxTxAmount` less 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.

Contract Diagnostics

● Critical ● Medium ● Minor

Severity	Code	Description
●	L01	Public Function could be Declared External
●	L04	Conformance to Solidity Naming Conventions
●	L05	Unused State Variable
●	L07	Missing Events Arithmetic
●	L08	Tautology or Contradiction
●	L09	Dead Code Elimination
●	L12	Using Variables before Declaration
●	L14	Uninitialized Variables in Local Scope
●	L15	Local Scope Variable Shadowing

L01 - Public Function could be Declared External

Criticality	minor
Location	contract.sol#L36,41,479,483,499,504,508,513,589,694,716,724,851,879,1053,1057,1201,1219,1237,1241,1288,1294

Description

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

```
setAutomatedMarketMakerPair
updateUniswapV2Router
dividendTokenBalanceOf
withdrawableDividendOf
updateGasForProcessing
updateDividendTracker
getNumOfWeeksTokenHeldFor
isExcludedFromFees
process
...
```

Recommendation

Use the external attribute for functions never called from the contract

L04 - Conformance to Solidity Naming Conventions

Criticality

minor

Location

contract.sol#L239,241,259,311,716,720,724,728,669,826,1057,1077

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.

```
_swapTokensAtAmount  
_address  
_account  
magnitude  
_owner  
WETH  
MINIMUM_LIQUIDITY  
PERMIT_TYPEHASH  
DOMAIN_SEPARATOR  
...
```

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#L79

Description

There are segments that contain unused state variables.

```
MAX_INT256
```

Recommendation

Remove unused state variables.

L07 - Missing Events Arithmetic

Criticality

minor

Location

contract.sol#L1077

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.

```
swapTokensAtAmount = _swapTokensAtAmount
```

Recommendation

Emit an event for critical parameter changes.

L08 - Tautology or Contradiction

Criticality

minor

Location

contract.sol#L1081,1090

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)((total >= 0) && (total <= 300),Invalid total week fee.)  
require(bool,string)((total >= 0) && (total <= 50),Invalid total buy fee.)
```

Recommendation

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

L09 - Dead Code Elimination

Criticality

minor

Location

contract.sol#L733,105,208

Description

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

```
toString  
abs  
_transfer
```

Recommendation

Remove unused functions.

L12 - Using Variables before Declaration

Criticality

minor

Location

contract.sol#L1191

Description

The contract is using a variable before the declaration. This is usually happening either if it has not been declared yet or the variable has been declared in a different scope.

```
lastProcessedIndex  
iterations  
claims
```

Recommendation

The variables should be declared before any usage of them.

L14 - Uninitialized Variables in Local Scope

Criticality

minor

Location

contract.sol#L1191

Description

There are variables that are defined in the local scope and are not initialized.

```
lastProcessedIndex  
claims  
iterations
```

Recommendation

All the local scoped variables should be initialized.

L15 - Local Scope Variable Shadowing

Criticality

minor

Location

contract.sol#L678,786,982,983

Description

There are variables that are defined in the local scope containing the same name from an upper scope.

```
_totalSupply  
_decimals  
_symbol  
_name
```

Recommendation

The local variables should have different names from the upper scoped variables.

Contract Functions

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
Ownable	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
IERC20Metadata	Interface	IERC20		
	name	External		-
	symbol	External		-
	decimals	External		-
SafeMathInt	Library			
	mul	Internal		
	div	Internal		
	sub	Internal		
	add	Internal		

	abs	Internal		
	toUint256Safe	Internal		
SafeMathUint	Library			
	toInt256Safe	Internal		
SafeMath	Library			
	add	Internal		
	sub	Internal		
	sub	Internal		
	mul	Internal		
	div	Internal		
	div	Internal		
	mod	Internal		
	mod	Internal		
StringTools	Library			
	appendString	Internal		
	appendString	Internal		
	appendString	Internal		
	toString	Internal		
	toString	Internal		
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	✓	-
IUniswapV2Factory	Interface			
	feeTo	External		-
	feeToSetter	External		-
	getPair	External		-
	allPairs	External		-
	allPairsLength	External		-
	createPair	External	✓	-
	setFeeTo	External	✓	-
	setFeeToSetter	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	✓	-
ERC20	Implementation	Context, IERC20, IERC20Metadata		
	<Constructor>	Public	✓	-
	name	Public		-
	symbol	Public		-
	decimals	Public		-
	totalSupply	Public		-
	balanceOf	Public		-
	transfer	Public	✓	-

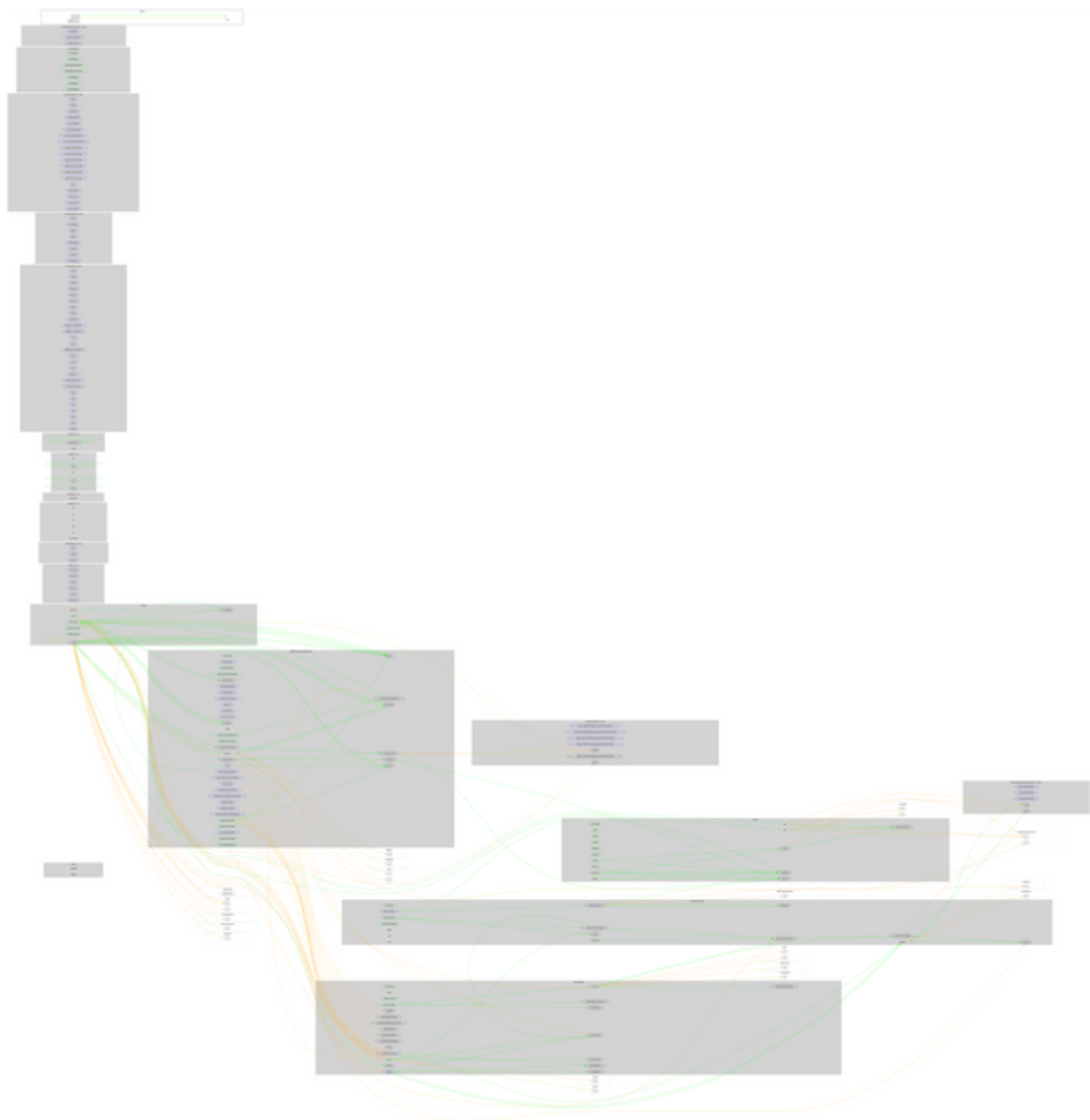
	allowance	Public		-
	approve	Public	✓	-
	transferFrom	Public	✓	-
	_transfer	Internal	✓	
	_mint	Internal	✓	
	_burn	Internal	✓	
	_approve	Internal	✓	
	_beforeTokenTransfer	Internal	✓	
IterableMapping	Implementation			
	<Constructor>	Public	✓	-
	iterableMapGet	Public		-
	iterableMapGetIndexOfKey	Public		-
	iterableMapGetKeyAtIndex	Public		-
	iterableMapSize	Public		-
	iterableMapSet	Public	✓	-
	iterableMapRemove	Public	✓	-
DividendPayingTokenOptionalInterface	Interface			
	withdrawableDividendOf	External		-
	withdrawnDividendOf	External		-
	accumulativeDividendOf	External		-
DividendPayingTokenInterface	Interface			
	dividendOf	External		-
	distributeDividends	External	Payable	-
	withdrawDividend	External	✓	-
DividendPayingToken	Implementation	ERC20, DividendPayingTokenInterface, DividendPayingTokenOp		

		tionallInterfa ce		
	<Constructor>	Public	✓	ERC20
	<Receive Ether>	External	Payable	-
	distributeDividends	Public	Payable	-
	withdrawDividend	Public	✓	-
	_withdrawDividendOfUser	Internal	✓	
	dividendOf	Public		-
	withdrawableDividendOf	Public		-
	withdrawnDividendOf	Public		-
	accumulativeDividendOf	Public		-
	_transfer	Internal	✓	
	_mint	Internal	✓	
	_burn	Internal	✓	
	_setBalance	Internal	✓	
DividendTracker	Implementation	DividendPay ingToken, IterableMap ping, Ownable		
	<Constructor>	Public	✓	DividendPayin gToken
	_transfer	Internal		
	withdrawDividend	Public		-
	excludeFromDividends	External	✓	onlyOwner
	updateClaimWait	External	✓	onlyOwner
	getLastProcessedIndex	External		-
	getNumberOfTokenHolders	External		-
	getAccount	Public		-
	getAccountAtIndex	Public		-
	canAutoClaim	Private		
	setBalance	External	✓	onlyOwner
	process	Public	✓	-
	processAccount	Public	✓	onlyOwner

BNB Dividend Paying ERC20 Token	Implementation	ERC20, Ownable		
	<Constructor>	Public	✓	ERC20
	<Receive Ether>	External	Payable	-
	isExcludedFromFees	Public		-
	getNumOfWeeksTokenHeldFor	Public		-
	excludeFromFees	Public	✓	onlyOwner
	setIsSwappingEnabled	External	✓	onlyOwner
	setTradingEnabled	External	✓	onlyOwner
	setSwapTokensAtAmount	External	✓	onlyOwner
	setBuyFees	External	✓	onlyOwner
	setWeeklyFees	External	✓	onlyOwner
	recoverLostCoins	External	✓	onlyOwner
	subTransfer	Internal	✓	
	_transfer	Internal	✓	
	updateDividendTracker	Public	✓	onlyOwner
	updateGasForProcessing	Public	✓	onlyOwner
	updateClaimWait	External	✓	onlyOwner
	getClaimWait	External		-
	getTotalDividendsDistributed	External		-
	withdrawableDividendOf	Public		-
	dividendTokenBalanceOf	Public		-
	getAccountDividendsInfo	External		-
	getAccountDividendsInfoAtIndex	External		-
	processDividendTracker	External	✓	-
	claim	External	✓	-
	getLastProcessedIndex	External		-
	getNumberOfDividendTokenHolders	External		-
	getMinimumTokenBalanceForDividends	External		-
	swapAndSendDividends	Private	✓	
	updateUniswapV2Router	Public	✓	onlyOwner
	setAutomatedMarketMakerPair	Public	✓	onlyOwner
	_setAutomatedMarketMakerPair	Private	✓	
	swapAndLiquify	Private	✓	

	swapTokensForEth	Private	✓	
	addLiquidity	Private	✓	

Contract Flow



Domain Info

Domain Name	swaptc.com
Registry Domain ID	2672230778_DOMAIN_COM-VRSN
Creation Date	2022-01-31T22:36:29Z
Updated Date	2022-01-31T22:53:31Z
Registry Expiry Date	2023-01-31T22:36:29Z
Registrar WHOIS Server	whois.1api.net
Registrar URL	http://www.1api.net
Registrar	1API GmbH
Registrar IANA ID	1387

The domain has been created 2 months before the creation of the audit. It will expire in 10 months.

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

Summary

Swap TC 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 has the ability to stop the transactions for everybody. 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.

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>