Cyberscope

Audit Report

SHONEN

April 2022

Type	ERC20
Network	ETH
Address	0x31538c865E4e4Ed6Aa847988dE7AC1c4eeC656D6
Audited by	© cyberscope

Table of Contents

Contract Review

Contract Name	SHONEN
Compiler Version	v0.8.13+commit.abaa5c0e
Optimization	200 runs
Licence	
Explorer	https://bscscan.com/token/0x31538c865E4e4Ed6Aa847988dE7AC1c4eeC656D6
Symbol	SHONEN
Decimals	18
Total Supply	100,000,000,000
Domain	shonen.io

Source Files

Filename	**SHA256**
contract.sol	209103c36d23348f569fcdf7b5ce85a87b9e9d317e5a82f18b983d917c8f7544

Audit Updates

Initial Audit	25th 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

ULTW - Unlimited Liquidity to Team Wallet

Criticality	minor
Location	contract.sol#L766

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 `manualSend()` and `manualSwap()` methods.

```
function manualSend() external onlyOwner {
    uint256 deltaBalance = getContractBalance();
```

```
function manualSwap() external onlyOwner {
    uint256 contractTokenBalance = balanceOf(address(this)).sub(
```

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.

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
	L05	Unused State Variable
	L07	Missing Events Arithmetic
	L09	Dead Code Elimination
	L13	Divide before Multiply Operation

L01 - Public Function could be Declared External

Criticality	minor
Location	contract.sol#L390,394,398,402,410,419,428,437,454,467,489,493,497,501,505,514,564,568,575,579,583

Description

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

```
setSwapAndLiquifyEnabled
removeExchangePair
addExchangePair
setExcludeFromMaxTx
setMinTokenNumberToSell
removeMaxBuyLimit
setAmountLimits
includeInTax
excludeFromTax
...
```

Recommendation

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

L02 - State Variables could be Declared Constant

Criticality	minor
Location	contract.sol#L52,301,299,300,302

Description

Constant state variables should be declared constant to save gas.

```
_tTotal
_symbol
_name
_decimals
_previousOwner
```

Recommendation

Add the constant attribute to state variables that never change.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contract.sol#L107,505,533,534,535,536,549,550,551,552,564,568,575,579,583,589,590,591,592,600,607,611,618,630,663,312,313,314,316,317,318,320,321,322,324,325

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.

```
_buyBackTax
_tempBuyBackTax
_sellDAOTax
_buyDAOTax
_daoTax
_sellDevTax
_buyDevTax
_devTax
_sellMarketingTax
...
```

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#L52

Description

There are segments that contain unused state variables.

```
_previousOwner
```

Recommendation

Remove unused state variables.

L07 - Missing Events Arithmetic

Criticality	minor
Location	contract.sol#L505,532,548,564

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.

```
minTokenNumberToSell = _amount
_buyBackTax = _sBuyBackTax
_buyBackTax = _bBuyBackTax
maxSellTransaction = _maxSellTxAmount
```

Recommendation

Emit an event for critical parameter changes.

L09 - Dead Code Elimination

Criticality	minor
Location	contract.sol#L257,215,222,230,244,188,201

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.

L13 - Divide before Multiply Operation

Criticality	minor
Location	contract.sol#L778,816

Description

Performing divisions before multiplications may cause lose of prediction.

```
devPercent = _devTax.mul(devisor).div(totalPercent)
marketingPercent = _marketingTax.mul(devisor).div(totalPercent)
daoPercent = _daoTax.mul(devisor).div(totalPercent)
buyBackPercent = takeBuyBackTax().mul(devisor).div(totalPercent)
```

Recommendation

The multiplications should be prior to the divisions.

Contract Functions

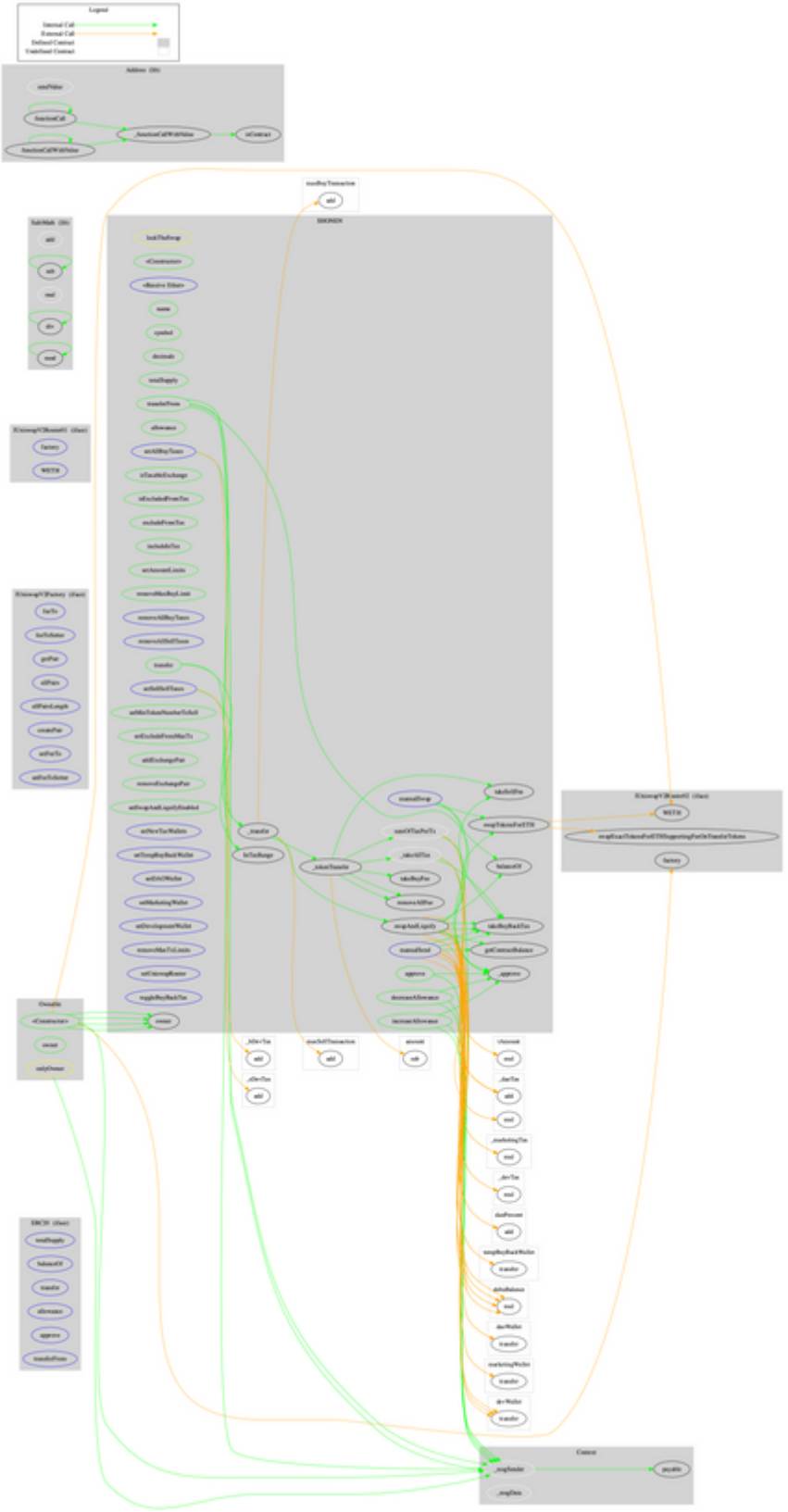
Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
ERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
Ownable	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
IUniswapV2Factory	Interface			
	feeTo	External		-
	feeToSetter	External		-
	getPair	External		-
	allPairs	External		-
	allPairsLength	External		-
	createPair	External	✓	-
	setFeeTo	External	✓	-
	setFeeToSetter	External	✓	-
IUniswapV2Router01	Interface			

	factory	External		-
	WETH	External		-
IUniswapV2Router02	Interface	IUniswapV2Router01		
	swapExactTokensForETHSupportingFeeOnTransferTokens	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	✓	
SHONEN	Implementation	Context, ERC20, Ownable		
	<Constructor>	Public	✓	-
	<Receive Ether>	External	Payable	-
	name	Public		-
	symbol	Public		-
	decimals	Public		-
	totalSupply	Public		-
	balanceOf	Public		-

	transfer	Public	✓	-
	allowance	Public		-
	approve	Public	✓	-
	transferFrom	Public	✓	-
	increaseAllowance	Public	✓	-
	decreaseAllowance	Public	✓	-
	getContractBalance	Public		-
	isTaxableExchange	Public		-
	isExcludedFromTax	Public		-
	excludeFromTax	Public	✓	onlyOwner
	includeInTax	Public	✓	onlyOwner
	setAmountLimits	Public	✓	onlyOwner
	removeMaxBuyLimit	Public	✓	onlyOwner
	removeAllBuyTaxes	External	✓	onlyOwner
	removeAllSellTaxes	External	✓	onlyOwner
	setAllBuyTaxes	External	✓	onlyOwner
	setSellSellTaxes	External	✓	onlyOwner
	setMinTokenNumberToSell	Public	✓	onlyOwner
	setExcludeFromMaxTx	Public	✓	onlyOwner
	addExchangePair	Public	✓	onlyOwner
	removeExchangePair	Public	✓	onlyOwner
	setSwapAndLiquifyEnabled	Public	✓	onlyOwner
	setNewTaxWallets	External	✓	onlyOwner
	setTempBuyBackWallet	External	✓	onlyOwner
	setDAOWallet	External	✓	onlyOwner
	setMarketingWallet	External	✓	onlyOwner
	setDevelopmentWallet	External	✓	onlyOwner
	removeMaxTxLimits	External	✓	onlyOwner
	setUniswapRouter	External	✓	onlyOwner
	toggleBuyBackTax	External	✓	onlyOwner
	takeBuyBackTax	Internal		
	sumOfTaxPerTx	Internal		
	_takeAllTax	Internal	✓	
	InTaxRange	Private		
	removeAllFee	Private	✓	

	takeBuyFee	Private	✓	
	takeSellFee	Private	✓	
	_approve	Private	✓	
	_transfer	Private	✓	
	_tokenTransfer	Private	✓	
	manualSwap	External	✓	onlyOwner
	manualSend	External	✓	onlyOwner
	swapAndLiquify	Private	✓	
	swapTokensForETH	Internal	✓	lockTheSwap

Contract Flow



Domain Info

Domain Name	shonen.io
Registry Domain ID	c4cf9c4869a04bb9a1c263ceca6c088d-DONUTS
Creation Date	2022-02-08T14:44:06Z
Updated Date	2022-04-20T12:43:07Z
Registry Expiry Date	2023-02-08T14:44:06Z
Registrar WHOIS Server	whois.namecheap.com
Registrar URL	https://www.namecheap.com/
Registrar	NameCheap, Inc.
Registrar IANA ID	1068

The domain has been created 3 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

SHONEN 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 transfer the contract's accumulated funds to the dev's wallet. Other than that, 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 16% 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