Cyberscope

Audit Report

Seismic

November 2023

Network BSC

Address 0x6602d72a77235bd0666c141989831ad435b1552a

Audited by © cyberscope

Analysis

Critical Medium Minor / Informative Pass

Severity	Code	Description	Status
●	ST	Stops Transactions	Unresolved
●	OTUT	Transfers User's Tokens	Passed
●	ELFM	Exceeds Fees Limit	Passed
●	MT	Mints Tokens	Passed
●	BT	Burns Tokens	Passed
●	BC	Blacklists Addresses	Passed

Diagnostics

Critical Medium Minor / Informative

Severity	Code	Description	Status
●	L04	Conformance to Solidity Naming Conventions	Unresolved

Table of Contents

Review

Contract Name	SCB
Compiler Version	v0.8.17+commit.8df45f5f
Optimization	200 runs
Explorer	https://bscscan.com/address/0x6602d72a77235bd0666c141989831ad435b1552a
Address	0x6602d72a77235bd0666c141989831ad435b1552a
Network	BSC
Symbol	SCB
Decimals	18
Total Supply	10,000,000

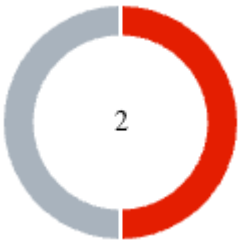
Audit Updates

Initial Audit	16 Mar 2023 https://github.com/cyberscope-io/audits/blob/main/seismic/v1/audit.pdf
Corrected Phase 2	20 Mar 2023 https://github.com/cyberscope-io/audits/tree/main/seismic/v2/audit.pdf
Corrected Phase 3	20 November 2023

Source Files

Filename	SHA256
contracts/Token.sol	e3229a9b1ac6cb20cf88c9058572ea35e1b777dd394253b7517b13e584dce4b4
@openzeppelin/contracts/utils/Context.sol	1458c260d010a08e4c20a4a517882259a23a4baa0b5bd9add9fb6d6a1549814a
@openzeppelin/contracts/utils/math/SafeMath.sol	0dc33698a1661b22981abad8e5c6f5ebca0dfe5ec14916369a2935d888ff257a
@openzeppelin/contracts/token/ERC20/IERC20.sol	94f23e4af51a18c2269b355b8c7cf4db8003d075c9c541019eb8dcf4122864d5
@openzeppelin/contracts/token/ERC20/ERC20.sol	bce14c3fd3b1a668529e375f6b70ffdf9cef8c4e410ae99608be5964d98fa701
@openzeppelin/contracts/token/ERC20/extensions/IERC20Metadata.sol	af5c8a77965cc82c33b7ff844deb9826166689e55dc037a7f2f790d057811990
@openzeppelin/contracts/access/Ownable.sol	9353af89436556f7ba8abb3f37a6677249aa4df6024fbfaa94f79ab2f44f3231

Findings Breakdown



Severity	Unresolved	Acknowledged	Resolved	Other
Critical	1	0	0	0
Medium	0	0	0	0
Minor / Informative	1	0	0	0

ST - Stops Transactions

Criticality	Critical
Location	contracts/token.sol#L313
Status	Unresolved

Description

The buy and sell transactions are initially disabled for all users. The owner can enable the transactions for all users. Once the transactions are enabled the owner will not be able to disable them again.

```
if (isBuy || isSell) {
    require(tradingStatus, "Trading is not enabled yet!");
```

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. Some suggestions are:

- Introduce a multi-sign wallet so that many addresses will confirm the action.
- Introduce a governance model where users will vote about the actions.

L04 - Conformance to Solidity Naming Conventions

Criticality	Minor / Informative
Location	contracts/token.sol#L38,67,102,140,149,158,167,176,186,187,200,201,213,222,233,234,246,266,267,273,406,417,431,450
Status	Unresolved

Description

The Solidity style guide is a set of guidelines for writing clean and consistent Solidity code. Adhering to a style guide can help improve the readability and maintainability of the Solidity code, making it easier for others to understand and work with.

The followings are a few key points from the Solidity style guide:

1. Use camelCase for function and variable names, with the first letter in lowercase (e.g., myVariable, updateCounter).
2. Use PascalCase for contract, struct, and enum names, with the first letter in uppercase (e.g., MyContract, UserStruct, ErrorEnum).
3. Use uppercase for constant variables and enums (e.g., MAX_VALUE, ERROR_CODE).
4. Use indentation to improve readability and structure.
5. Use spaces between operators and after commas.
6. Use comments to explain the purpose and behavior of the code.
7. Keep lines short (around 120 characters) to improve readability.

```
function WETH() external pure returns (address);
uint256 private constant _totalSupply = 1e7 * 1e18
address public TreasuryWallet = 0x74Adf47aD22a9C95EE58A6D956FA58924D697E0F
address _newTreasury
uint256 _mb
uint256 _ms
uint256 _mt
uint256 _mx
uint256 _lpTax
uint256 _TreasuryTax
uint256 _sc
uint256 _db
uint256 _newAmount
address _wallet
...
```

Recommendation

By following the Solidity naming convention guidelines, the codebase increased the readability, maintainability, and makes it easier to work with.
Find more information on the Solidity documentation
https://docs.soliditylang.org/en/v0.8.17/style-guide.html#naming-convention.

Functions Analysis

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
DexFactory	Interface			
	createPair	External	✓	-
DexRouter	Interface			
	factory	External		-
	WETH	External		-
	addLiquidityETH	External	Payable	-
	swapExactTokensForETHSupportingFeeOnTransferTokens	External	✓	-
SCB	Implementation	ERC20, Ownable		
		Public	✓	ERC20
	enableTrading	External	✓	onlyOwner
	setTreasuryWallet	External	✓	onlyOwner
	setMaxBuy	External	✓	onlyOwner
	setMaxSell	External	✓	onlyOwner
	setMaxTx	External	✓	onlyOwner
	setMaxWallet	External	✓	onlyOwner
	setBuyTaxes	External	✓	onlyOwner

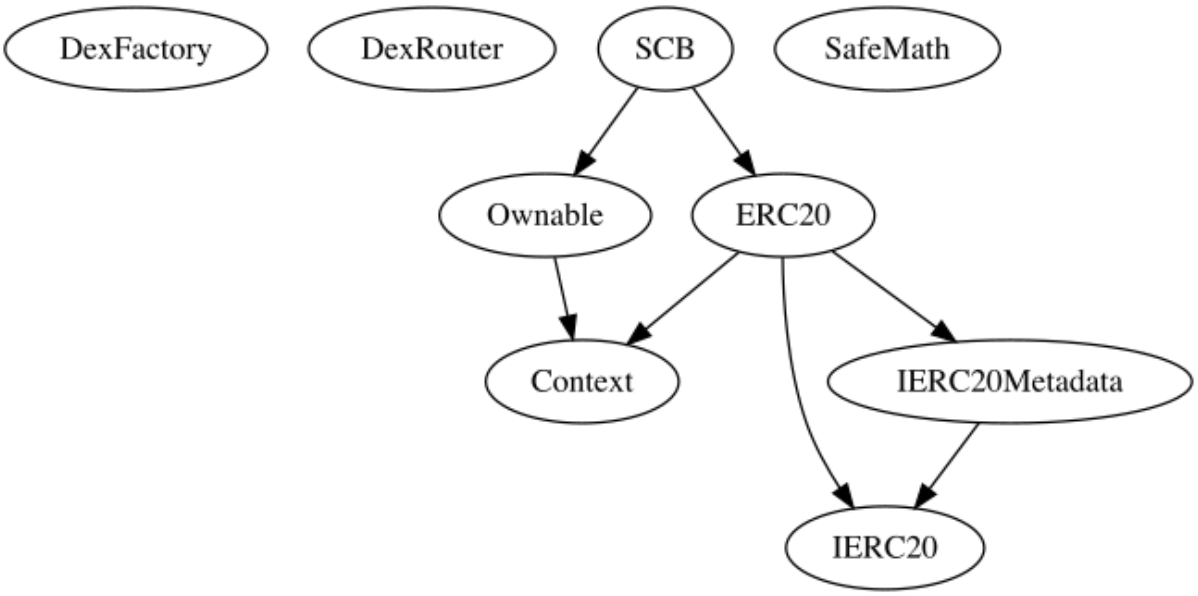
	setSellTaxes	External	✓	onlyOwner
	setSellCooldown	External	✓	onlyOwner
	setDeadBlocks	External	✓	onlyOwner
	setTransferFees	External	✓	onlyOwner
	setSwapTokensAtAmount	External	✓	onlyOwner
	toggleSellCooldown	External	✓	onlyOwner
	toggleSwapping	External	✓	onlyOwner
	setWhitelistStatus	External	✓	onlyOwner
	checkWhitelist	External		-
	_takeTax	Internal	✓	
	_transfer	Internal	✓	
	internalSwap	Internal	✓	
	swapAndLiquify	Internal	✓	
	swapToETH	Internal	✓	
	addLiquidity	Private	✓	
	withdrawStuckETH	External	✓	onlyOwner
	withdrawStuckTokens	External	✓	onlyOwner
		External	Payable	-
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		

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		
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-

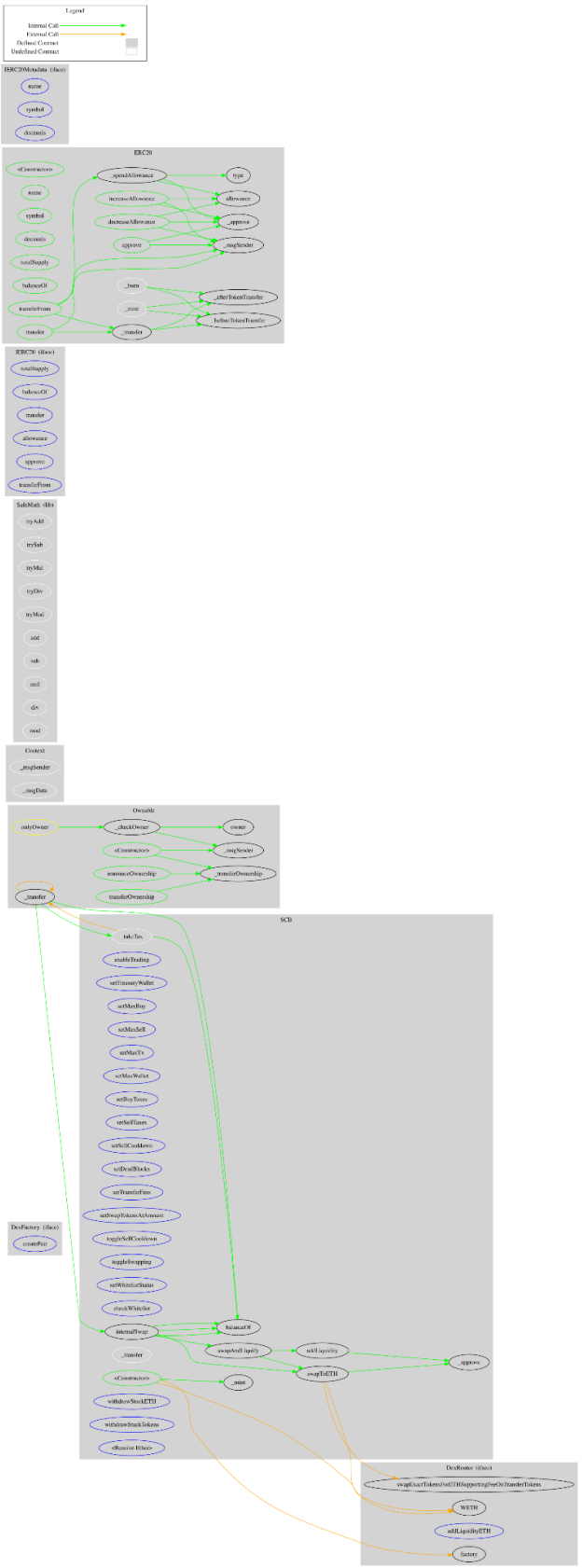
ERC20	Implementation	Context, IERC20, IERC20Metadata		
		Public	✓	-
	name	Public		-
	symbol	Public		-
	decimals	Public		-
	totalSupply	Public		-
	balanceOf	Public		-
	transfer	Public	✓	-
	allowance	Public		-
	approve	Public	✓	-
	transferFrom	Public	✓	-
	increaseAllowance	Public	✓	-
	decreaseAllowance	Public	✓	-
	_transfer	Internal	✓	
	_mint	Internal	✓	
	_burn	Internal	✓	
	_approve	Internal	✓	
	_spendAllowance	Internal	✓	
	_beforeTokenTransfer	Internal	✓	
	_afterTokenTransfer	Internal	✓	
IERC20Metadata	Interface	IERC20		

	name	External		-
	symbol	External		-
	decimals	External		-
Ownable	Implementation	Context		
		Public	✓	-
	owner	Public		-
	_checkOwner	Internal		
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	_transferOwnership	Internal	✓	

Inheritance Graph



Flow Graph


Legend
Internal Call
External Call
Defined Contract
Undefined Contract
IERC20Metadata (iface)
name
symbol
decimals
ERC20
<Constructor>
name
symbol
decimals
totalSupply
balanceOf
transferFrom
transfer
_spendAllowance
increaseAllowance
decreaseAllowance
approve
type
allowance
_approve
_msgSender
_burn
_mint
_transfer
_afterTokenTransfer
_beforeTokenTransfer
IERC20 (iface)
totalSupply
balanceOf
transfer
allowance
approve
transferFrom
SafeMath (lib)
tryAdd
trySub
tryMul
tryDiv
tryMod
add
sub
mul
div
mod
Context
_msgSender
_msgData
Ownable
onlyOwner
_checkOwner
owner
<Constructor>
renounceOwnership
transferOwnership
_msgSender
_transferOwnership
_transfer
SCB
takeTax
enableTrading
setTreasuryWallet
setMaxBuy
setMaxSell
setMaxTx
setMaxWallet
setBuyTaxes
setSellTaxes
setSellCooldown
setDeadBlocks
setTransferFees
setSwapTokensAtAmount
toggleSellCooldown
toggleSwapping
setWhitelistStatus
checkWhitelist
internalSwap
_transfer
<Constructor>
withdrawStuckETH
withdrawStuckTokens
<Receive Ether>
balanceOf
swapAndLiquify
swapToETH
addLiquidity
_approve
_mint
DexFactory (iface)
createPair
DexRouter (iface)
swapExactTokensForETHSupportingFeeOnTransferTokens
WETH
addLiquidityETH
factory

Summary

Seismic contract implements a token mechanism. This audit investigates security issues, business logic concerns, and potential improvements. Seismic is an interesting project that has a friendly and growing community. The Smart Contract analysis reported no compiler errors 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. There is also a limit of max 22% buy/sell fees and 11% transfer fees.

Disclaimer

The information provided in this report does not constitute investment, financial or trading advice and you should not treat any of the document's content as such. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes nor may copies be delivered to any other person other than the Company without Cyberscope's prior written consent. This report is not nor should be considered an "endorsement" or "disapproval" of any particular project or team. This report is not nor should be regarded as an indication of the economics or value of any "product" or "asset" created by any team or project that contracts Cyberscope to perform a security assessment. This document does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors' business, business model or legal compliance. This report should not be used in any way to make decisions around investment or involvement with any particular project. This report represents an extensive assessment process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk Cyberscope's position is that each company and individual are responsible for their own due diligence and continuous security Cyberscope's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies and in no way claims any guarantee of security or functionality of the technology we agree to analyze. The assessment services provided by Cyberscope are subject to dependencies and are under continuing development. You agree that your access and/or use including but not limited to any services reports and materials will be at your sole risk on an as-is where-is and as-available basis Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives false negatives and other unpredictable results. The services may access and depend upon multiple layers of third parties.

About Cyberscope

Cyberscope is a blockchain cybersecurity company that was founded with the vision to make web3.0 a safer place for investors and developers. Since its launch, it has worked with thousands of projects and is estimated to have secured tens of millions of investors' funds.

Cyberscope is one of the leading smart contract audit firms in the crypto space and has built a high-profile network of clients and partners.

The Cyberscope team

https://www.cyberscope.io