Cyberscope

Audit Report

ShytCoin

November 2023

Network	BSC
Address	0x74cf7da593ba3f07c2843713e299647bec69f691
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
	FAI	Fees Application Inconsistency	Unresolved
	PTRP	Potential Transfer Revert Propagation	Unresolved
	FSA	Fixed Swap Address	Unresolved
	IDI	Immutable Declaration Improvement	Unresolved
	L02	State Variables could be Declared Constant	Unresolved
	L04	Conformance to Solidity Naming Conventions	Unresolved
	L16	Validate Variable Setters	Unresolved
	L19	Stable Compiler Version	Unresolved

Table of Contents

Review

Contract Name	SHYTCOIN
Compiler Version	v0.8.18+commit.87f61d96
Optimization	200 runs
Explorer	https://bscscan.com/address/0x74cf7da593ba3f07c2843713e299647bec69f691
Address	0x74cf7da593ba3f07c2843713e299647bec69f691
Network	BSC
Symbol	SHYTCOIN
Decimals	9
Total Supply	100,000

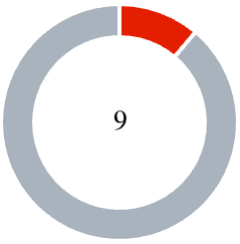
Audit Updates

Initial Audit	18 Nov 2023

Source Files

Filename	SHA256
SHYTCOIN.sol	d9fcc60e9b53094c19f82288fddc597229db939f67a4099c37ee4c979e236036

Findings Breakdown



Critical	1
Medium	0
Minor / Informative	8

Severity	Unresolved	Acknowledged	Resolved	Other
Critical	1	0	0	0
Medium	0	0	0	0
Minor / Informative	8	0	0	0

ST - Stops Transactions

Criticality	Critical
Location	SHYTCOIN.sol#L491
Status	Unresolved

Description

The transactions are initially disabled for all users excluding the authorized addresses. The owner can enable the transactions for all users. Once the transactions are enable the owner will not be able to disable them again.

```
if(!_isExcludedFromFees[from] && !_isExcludedFromFees[to]) {
  require(tradingEnabled, "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.

FAI - Fees Application Inconsistency

Criticality	Minor / Informative
Location	SHYTCOIN.sol#L500
Status	Unresolved

Description

The contract applies sell fees when the recipient is the pair address, buy fees when the sender is the pair address, and zero fees in all the other cases. On the contrary, the contract is taking fees if either the sender or recipient is excluded from fees. This methodology creates an inconsistency since zero fees essentially mean that it should not apply fees.

```
if(to == pair){

    taxes.rfi = selltaxes.rfi;
    taxes.marketing = selltaxes.marketing;

}else if(from == pair){

    taxes.rfi = taxes.rfi;
    taxes.marketing = taxes.marketing;

}else{
    taxes.rfi = 0;
    taxes.marketing = 10;
}

...

bool takeFee = true;
if (swapping || _isExcludedFromFee[from] || _isExcludedFromFee[to])
takeFee = false;
```

Recommendation

The team is advised to comprehensively review and adjust the fee calculation mechanism within the contract. The contract should keep consistency between taking fees and applying zero percentage fees.

PTRP - Potential Transfer Revert Propagation

Criticality	Minor / Informative
Location	SHYTCOIN.sol#L569
Status	Unresolved

Description

The contract sends funds to a `marketingWallet` as part of the transfer flow. This address can either be a wallet address or a contract. If the address belongs to a contract then it may revert from incoming payment. As a result, the error will propagate to the token's contract and revert the transfer.

```
payable(marketingWallet).sendValue(deltaBalance);
```

Recommendation

The contract should tolerate the potential revert from the underlying contracts when the interaction is part of the main transfer flow. This could be achieved by not allowing set contract addresses or by sending the funds in a non-revertable way.

FSA - Fixed Swap Address

Criticality	Minor / Informative
Location	SHYTCOIN.sol#L500
Status	Unresolved

Description

The swap address is assigned once and it can not be changed. It is a common practice in decentralized exchanges to create new swap versions. A contract that cannot change the swap address may not be able to catch up to the upgrade. As a result, the contract will not be able to migrate to a new liquidity pool pair or decentralized exchange.

Furthermore, the contract does not apply taxes in pure token transfers. As a result, if the token is listed in a different pair or decentralized exchange, it will not apply fees, creating an arbitrage from the main pair.

```
address _pair =
IFactory(_router.factory()).createPair(address(this),
_router.WETH());

router = _router;
pair = _pair;

...

if(to == pair){

    taxes.rfi = selltaxes.rfi;
    taxes.marketing = selltaxes.marketing;

}else if(from == pair){

    taxes.rfi = taxes.rfi;
    taxes.marketing = taxes.marketing;

}else{
    taxes.rfi = 0;
    taxes.marketing = 10;
}
```

Recommendation

The team is advised to add the ability to add multiple the pair addresses in order to cover potential liquidity pools. It would be better to support multiple pair addresses so the token will be able to have the same behavior in all the decentralized liquidity pairs.

IDI - Immutable Declaration Improvement

Criticality	Minor / Informative
Location	SHYTCOIN.sol#L218,219
Status	Unresolved

Description

The contract declares state variables that their value is initialized once in the constructor and are not modified afterwards. The `immutable` is a special declaration for this kind of state variables that saves gas when it is defined.

```
router
pair
```

Recommendation

By declaring a variable as immutable, the Solidity compiler is able to make certain optimizations. This can reduce the amount of storage and computation required by the contract, and make it more gas-efficient.

L02 - State Variables could be Declared Constant

Criticality	Minor / Informative
Location	SHYTCOIN.sol#L167,170,172,173
Status	Unresolved

Description

State variables can be declared as constant using the constant keyword. This means that the value of the state variable cannot be changed after it has been set. Additionally, the constant variables decrease gas consumption of the corresponding transaction.

```
kensAtAmount = 10000000000;

    address publi
ddress public marketingWallet = 0x701A4f34A4d06

E0DAd68CAF2dcB2b8e;

    string private constant _name = "ShytCoin";

tring private constant _symbol = "SHYTCOIN";

    struct BuyTaxes {
```

Recommendation

Constant state variables can be useful when the contract wants to ensure that the value of a state variable cannot be changed by any function in the contract. This can be useful for storing values that are important to the contract's behavior, such as the contract's address or the maximum number of times a certain function can be called. The team is advised to add the constant keyword to state variables that never change.

L04 - Conformance to Solidity Naming Conventions

Criticality	Minor / Informative
Location	SHYTCOIN.sol#L111,164,175,176,198,237,246
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.

```
Desired,
        uint256 amountTokenMin,


decimals;
    uint256 private _rTot

56 rfi;
        uint256 marketing;
    }


    struct SellTaxes {
        uint256 rfi

...
```

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.

L16 - Validate Variable Setters

Criticality	Minor / Informative
Location	SHYTCOIN.sol#L219
Status	Unresolved

Description

The contract performs operations on variables that have been configured on user-supplied input. These variables are missing of proper check for the case where a value is zero. This can lead to problems when the contract is executed, as certain actions may not be properly handled when the value is zero.

```
_isExclu
```

Recommendation

By adding the proper check, the contract will not allow the variables to be configured with zero value. This will ensure that the contract can handle all possible input values and avoid unexpected behavior or errors. Hence, it can help to prevent the contract from being exploited or operating unexpectedly.

L19 - Stable Compiler Version

Criticality	Minor / Informative
Location	SHYTCOIN.sol#L35
Status	Unresolved

Description

The `^` symbol indicates that any version of Solidity that is compatible with the specified version (i.e., any version that is a higher minor or patch version) can be used to compile the contract. The version lock is a mechanism that allows the author to specify a minimum version of the Solidity compiler that must be used to compile the contract code. This is useful because it ensures that the contract will be compiled using a version of the compiler that is known to be compatible with the code.

```
address account) externa
```

Recommendation

The team is advised to lock the pragma to ensure the stability of the codebase. The locked pragma version ensures that the contract will not be deployed with an unexpected version. An unexpected version may produce vulnerabilities and undiscovered bugs. The compiler should be configured to the lowest version that provides all the required functionality for the codebase. As a result, the project will be compiled in a well-tested LTS (Long Term Support) environment.

Functions Analysis

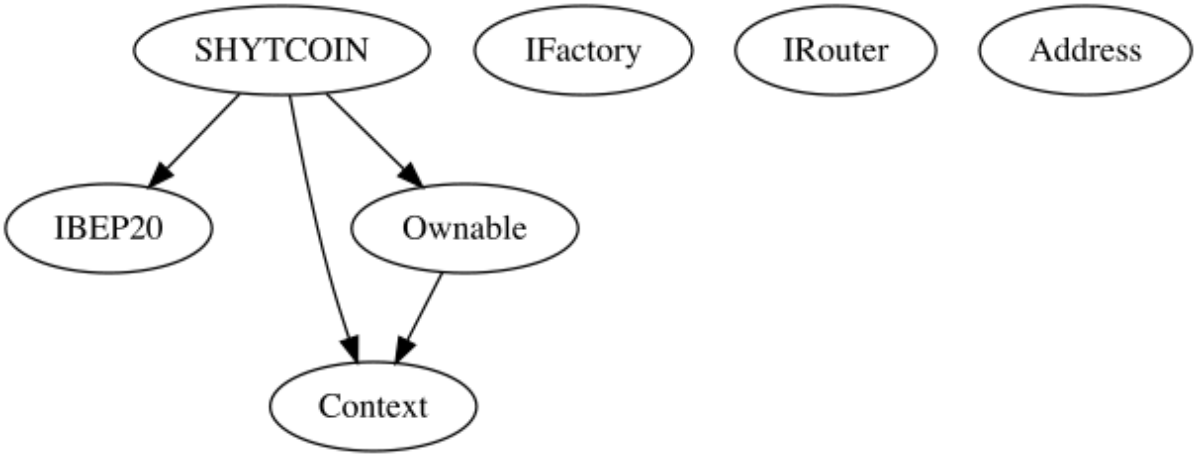
Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
IBEP20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
Ownable	Implementation	Context		
		Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	_setOwner	Private	✓	

IFactory	Interface			
	createPair	External	✓	-
IRouter	Interface			
	factory	External		-
	WETH	External		-
	addLiquidityETH	External	Payable	-
	swapExactTokensForETHSupportingFeeOnTransferTokens	External	✓	-
Address	Library			
	sendValue	Internal	✓	
SHYTCOIN	Implementation	Context, IBEP20, Ownable		
		Public	✓	-
	enableTrading	External	✓	onlyOwner
	updateBTax	External	✓	onlyOwner
	updateSTax	External	✓	onlyOwner
	name	Public		-
	symbol	Public		-
	decimals	Public		-
	totalSupply	Public		-
	balanceOf	Public		-
	allowance	Public		-

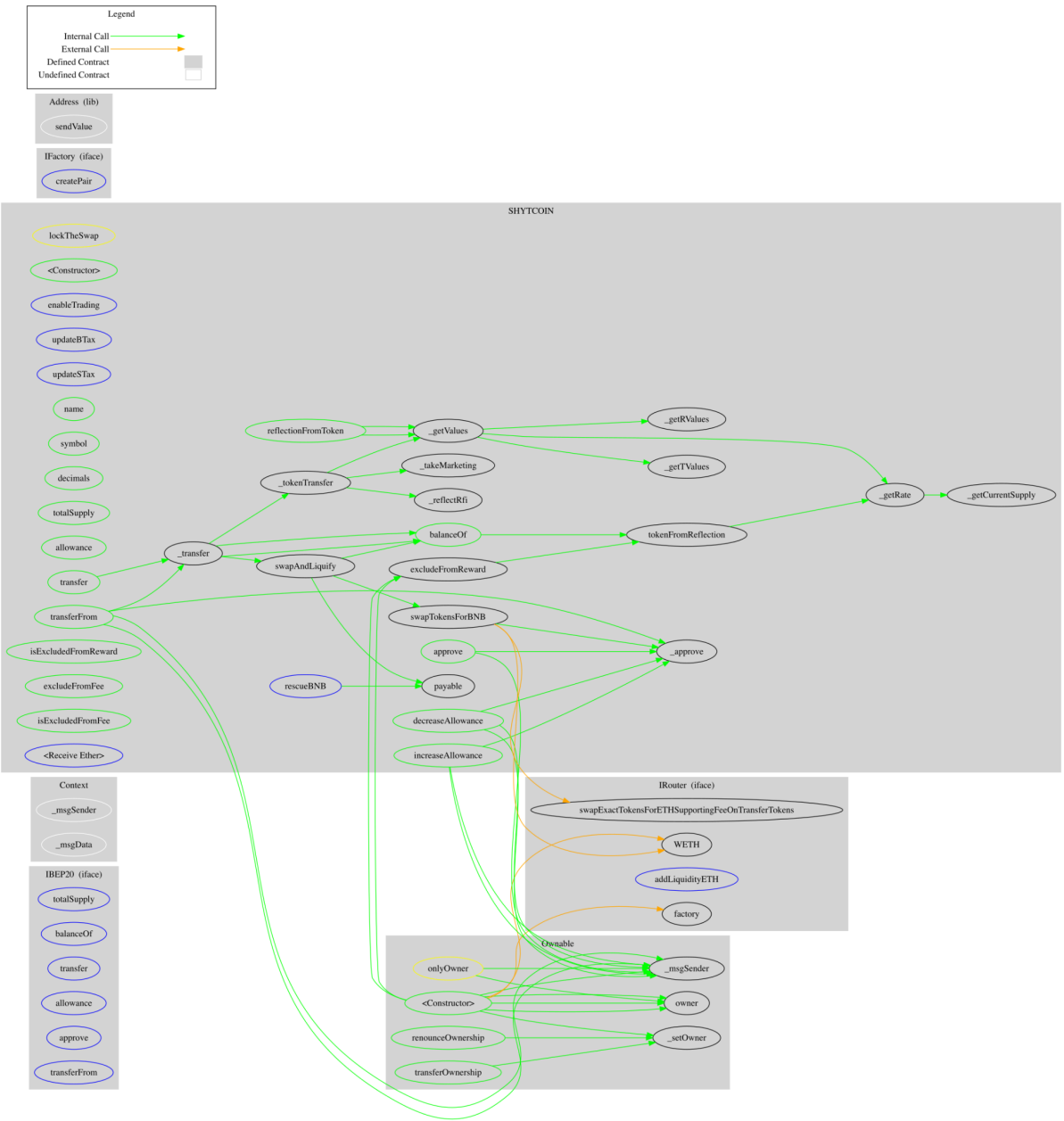
	approve	Public	✓	-
	transferFrom	Public	✓	-
	increaseAllowance	Public	✓	-
	decreaseAllowance	Public	✓	-
	transfer	Public	✓	-
	isExcludedFromReward	Public		-
	reflectionFromToken	Public		-
	tokenFromReflection	Public		-
	excludeFromReward	Public	✓	onlyOwner
	excludeFromFee	Public	✓	onlyOwner
	isExcludedFromFee	Public		-
	_reflectRfi	Private	✓	
	_takeMarketing	Private	✓	
	_getValues	Private		
	_getTValues	Private		
	_getRValues	Private		
	_getRate	Private		
	_getCurrentSupply	Private		
	_approve	Private	✓	
	_transfer	Private	✓	
	_tokenTransfer	Private	✓	
	swapAndLiquify	Private	✓	lockTheSwap
	swapTokensForBNB	Private	✓	

	rescueBNB	External	✓	onlyOwner
		External	Payable	-

Inheritance Graph



Flow Graph


Legend
Internal Call
External Call
Defined Contract
Undefined Contract
Address (lib)
sendValue
IFactory (iface)
createPair
SHYTCOIN
lockTheSwap
<Constructor>
enableTrading
updateBTax
updateSTax
name
symbol
decimals
totalSupply
allowance
transfer
transferFrom
isExcludedFromReward
excludeFromFee
isExcludedFromFee
<Receive Ether>
reflectionFromToken
_getValues
_getRValues
_getTValues
_takeMarketing
_tokenTransfer
_reflectRfi
_getRate
_getCurrentSupply
balanceOf
tokenFromReflection
_transfer
swapAndLiquify
excludeFromReward
swapTokensForBNB
approve
_approve
rescueBNB
payable
decreaseAllowance
increaseAllowance
Context
_msgSender
_msgData
IBEP20 (iface)
totalSupply
balanceOf
transfer
allowance
approve
transferFrom
IRouter (iface)
swapExactTokensForETHSupportingFeeOnTransferTokens
WETH
addLiquidityETH
factory
Ownable
onlyOwner
_msgSender
<Constructor>
owner
renounceOwnership
_setOwner
transferOwnership

Summary

ShytCoin contract implements a token mechanism. This audit investigates security issues, business logic concerns and potential improvements. There are some functions that can be abused by the owner like stop transactions. A multi-wallet signing pattern will provide security against potential hacks. Temporarily locking the contract or renouncing ownership will eliminate all the contract threats. There is also a limit of max 20% fees in sales and 15% in buys.

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