Cyberscope

Audit Report

ShibaWarp

September 2023

SHA256 56e12e181a792bd7b73df2c4f5f0f4f9e2aebc768fb35a422502e188f0cf7516

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
	GO	Gas Optimization	Unresolved
	RSW	Redundant Storage Writes	Unresolved
	ULTW	Transfers Liquidity to Team Wallet	Unresolved
	OCTD	Transfers Contract's Tokens	Unresolved
	RVD	Redundant Variable Declaration	Unresolved
	RSML	Redundant SafeMath Library	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
	L16	Validate Variable Setters	Unresolved
	L20	Succeeded Transfer Check	Unresolved

Table of Contents

Analysis **1**
Diagnostics **2**
Table of Contents **3**
Review **5**
Audit Updates 5
Source Files 5
Findings Breakdown **6**
ST - Stops Transactions 7
Description 7
Recommendation 7
GO - Gas Optimization 8
Description 8
Recommendation 9
RSW - Redundant Storage Writes 10
Description 10
Recommendation 10
ULTW - Transfers Liquidity to Team Wallet 11
Description 11
Recommendation 11
OCTD - Transfers Contract's Tokens 12
Description 12
Recommendation 12
RVD - Redundant Variable Declaration 13
Description 13
Recommendation 14
RSML - Redundant SafeMath Library 15
Description 15
Recommendation 15
L02 - State Variables could be Declared Constant 16
Description 16
Recommendation 16
L04 - Conformance to Solidity Naming Conventions 17
Description 17
Recommendation 18
L05 - Unused State Variable 19
Description 19
Recommendation 19
L07 - Missing Events Arithmetic 20
Description 20

Recommendation 20
L16 - Validate Variable Setters 21
Description 21
Recommendation 21
L20 - Succeeded Transfer Check 22
Description 22
Recommendation 22
Functions Analysis **23**
Inheritance Graph **31**
Flow Graph **32**
Summary **33**
Disclaimer **34**
About Cyberscope **35**

Review

Contract Name	ShibaWarp
Compiler Version	v0.8.18+commit.87f61d96
Optimization	200 runs
Testing Deploy	https://testnet.bscscan.com/address/0xa78464fe4d934799ef1ae1c1cfe785972cd59485
Network	BSC TESTNET
Symbol	SBWP
Decimals	18
Total Supply	375,000,000

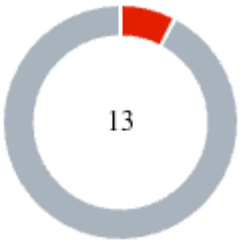
Audit Updates

Initial Audit	10 Sep 2023 https://github.com/cyberscope-io/audits/blob/main/1-sbwp/v1/audit.pdf
Corrected Phase 2	13 Sep 2023

Source Files

Filename	SHA256
ShibaWarp.sol	56e12e181a792bd7b73df2c4f5f0f4f9e2aebc768fb35a422502e188f0cf7516

Findings Breakdown



Critical	1
Medium	0
Minor / Informative	12

Severity	Unresolved	Acknowledged	Resolved	Other
Critical	1	0	0	0
Medium	0	0	0	0
Minor / Informative	12	0	0	0

ST - Stops Transactions

Criticality	Critical
Location	ShibaWarp.sol#L736
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 enabled the owner will not be able to disable them again.

```
if(!_swapEnabled){
    require(_isFeeExempt[sender] || _isFeeExempt[recipient]);
}
```

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.

GO - Gas Optimization

Criticality	Minor / Informative
Location	contracts/ShibaWarp.sol#L801,830
Status	Unresolved

Description

Gas optimization refers to the process of reducing the amount of gas required to execute a transaction. Gas is the unit of measurement used to calculate the fees paid to miners for including a transaction in a block on the blockchain.

In the swap functionality, the contract incorporates a crucial adjustment to the totalFee variable. When its initial value is 0, it is modified to 1. This modification serves a vital purpose: it ensures that the contract can proceed with its operations without encountering division by zero issues, which could disrupt the execution.

However, it's important to note that this modification exclusively affects the `totalFee` variable. It does not alter the values of individual fee components, such as `rewardDividendBuyFee`, `rewardDividendSellFee`, `shibaBurnBuyFee`, `shibaBurnSellFee`, `buybackBuyFee`, and `buybackSellFee`. Consequently, despite the adjustment to `totalFee`, the individual fee portions remain at zero.

As a consequence, the contract carries out certain code segments redundantly. This redundancy in code execution has the unintended consequence of increasing the overall gas cost associated with these operations.

```
if(totalFee == 0) {
    totalFee = 1;
}

uint256 totalReceived = address(this).balance;

uint256 totalRewardFee = (rewardDividendBuyFee.add(rewardDividendSellFee));

uint256 totalShibaBurnFee = shibaBurnBuyFee.add(shibaBurnSellFee);

uint256 totalBuybackFee = buybackBuyFee.add(buybackSellFee);

uint256 portionToDistributor = totalReceived.mul(totalRewardFee).div(totalFee);

uint256 portionToBuyback = totalReceived.mul(totalBuybackFee).div(totalFee);

uint256 portionToShibaBurn = totalReceived.mul(totalShibaBurnFee).div(totalFee);

uint256 portionToUtility =
totalReceived.sub(portionToBuyback).sub(portionToDistributor).sub(portionToShibaBurn)
;
```

Recommendation

The team is advised to take these segments into consideration and rewrite them so the runtime will be more performant. That way it will improve the efficiency and performance of the source code and reduce the cost of executing it.

RSW - Redundant Storage Writes

Criticality	Minor / Informative
Location	ShibaWarp.sol#L940,1023
Status	Unresolved

Description

There are code segments that could be optimized. A segment may be optimized so that it becomes a smaller size, consumes less memory, executes more rapidly, or performs fewer operations.

The contract modifies the state of certain variables even even when their current state matches the provided argument. As a result, the contract performs redundant storage writes.

```
_swapEnabled = true
_isFeeExempt[_addr] = true
```

Recommendation

The team is advised to take these segments into consideration and rewrite them so the runtime will be more performant. That way it will improve the efficiency and performance of the source code and reduce the cost of executing it.

ULTW - Transfers Liquidity to Team Wallet

Criticality	Minor / Informative
Location	ShibaWarp.sol#L1058
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 `rescueBNB` method.

```
function rescueBNB(uint256 amount) external onlyOwner{
payable(msg.sender).transfer(amount);
}
```

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. Some suggestions are:

- Introduce a time-locker mechanism with a reasonable delay.
- Introduce a multi-sign wallet so that many addresses will confirm the action.
- Introduce a governance model where users will vote about the actions.
- Renouncing the ownership will eliminate the threats but it is non-reversible.

OCTD - Transfers Contract's Tokens

Criticality	Minor / Informative
Location	ShibaWarp.sol#L1050
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 `rescueToken` function.

```
function rescueToken(address tokenAddress, address to) external onlyOwner
returns (bool success) {
    uint256 _contractBalance =
IERC20(tokenAddress).balanceOf(address(this));


    return IERC20(tokenAddress).transfer(to, _contractBalance);
}
```

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 time-locker mechanism with a reasonable delay.
- Introduce a multi-sign wallet so that many addresses will confirm the action.
- Introduce a governance model where users will vote about the actions.
- Renouncing the ownership will eliminate the threats but it is non-reversible.

RVD - Redundant Variable Declaration

Criticality	Minor / Informative
Location	ShibaWarp.sol#L774,817,848,859
Status	Unresolved

Description

There are code segments that could be optimized. A segment may be optimized so that it becomes a smaller size, consumes less memory, executes more rapidly, or performs fewer operations.

The contract declares certain variables that are not used in a meaningful way by the contract. As a result, these variables are redundant.

```
uint256 _totalFee = totalBuyFee;
uint256 _rewardDividendFee = rewardDividendBuyFee;
uint256 _shibaBurnFee = shibaBurnBuyFee;
uint256 _buybackFee = buybackBuyFee;
uint256 _utilityFee = utilityBuyFee;

if (recipient == pair) {
    _totalFee = totalSellFee;
    _rewardDividendFee = rewardDividendSellFee;
    _shibaBurnFee = shibaBurnSellFee;
    _buybackFee = buybackSellFee;
    _utilityFee = utilitySellFee;
}

bool swapTokensForETHSuccess = false
bool swapETHForTokensSuccess = false

bool distributorDepositSuccess = false;
try distributor.deposit{value: portionToDistributor}() {
    distributorDepositSuccess = true;
} catch {}
```

Recommendation

The team is advised to take these segments into consideration and rewrite them so the runtime will be more performant. That way it will improve the efficiency and performance of the source code and reduce the cost of executing it.

RSML - Redundant SafeMath Library

Criticality	Minor / Informative
Location	contracts/ShibaWarp.sol
Status	Unresolved

Description

SafeMath is a popular Solidity library that provides a set of functions for performing common arithmetic operations in a way that is resistant to integer overflows and underflows.

Starting with Solidity versions that are greater than or equal to 0.8.0, the arithmetic operations revert to underflow and overflow. As a result, the native functionality of the Solidity operations replaces the SafeMath library. Hence, the usage of the SafeMath library adds complexity, overhead and increases gas consumption unnecessarily.

```
library SafeMath {...}
```

Recommendation

The team is advised to remove the SafeMath library. Since the version of the contract is greater than `0.8.0` then the pure Solidity arithmetic operations produce the same result.

If the previous functionality is required, then the contract could exploit the `unchecked { ... }` statement.

Read more about the breaking change on https://docs.soliditylang.org/en/v0.8.16/080-breaking-changes.html#solidity-v0-8-0-breaking-changes.

L02 - State Variables could be Declared Constant

Criticality	Minor / Informative
Location	contracts/ShibaWarp.sol#L337,610
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.

```
IERC20 SHIBA = IERC20(0x95aD61b0a150d79219dCF64E1E6Cc01f0B64C4cE)
address public selllessSwap
```

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	contracts/ShibaWarp.sol#L135,136,153,171,329,337,378,383,387,582,601,602,613,625,638,958,966,971,980,987,1000,1013,1014,1022,1026,1039
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 DOMAIN_SEPARATOR() external view returns (bytes32);
function PERMIT_TYPEHASH() external pure returns (bytes32);
function MINIMUM_LIQUIDITY() external pure returns (uint);
function WETH() external pure returns (address);
address public _token
IERC20 SHIBA = IERC20(0x95aD61b0a150d79219dCF64E1E6Cc01f0B64C4cE)
uint256 _minDistribution
uint256 _minPeriod
address _selllessSwap
uint256 _minSharesRequired
mapping(address => bool) _isFeeExempt
uint256 public _swapEnabledTime
uint256 public immutable _totalSupply = 375000000 * 10**DECIMALS
address payable public immutable DividendReceiver

...
```

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.

L05 - Unused State Variable

Criticality	Minor / Informative
Location	contracts/ShibaWarp.sol#L7
Status	Unresolved

Description

An unused state variable is a state variable that is declared in the contract, but is never used in any of the contract's functions. This can happen if the state variable was originally intended to be used, but was later removed or never used.

Unused state variables can create clutter in the contract and make it more difficult to understand and maintain. They can also increase the size of the contract and the cost of deploying and interacting with it.

```
int256 private constant MAX_INT256 = ~(int256(1) << 255)
```

Recommendation

To avoid creating unused state variables, it's important to carefully consider the state variables that are needed for the contract's functionality, and to remove any that are no longer needed. This can help improve the clarity and efficiency of the contract.

L07 - Missing Events Arithmetic

Criticality	Minor / Informative
Location	contracts/ShibaWarp.sol#L379,402
Status	Unresolved

Description

Events are a way to record and log information about changes or actions that occur within a contract. They are often used to notify external parties or clients about events that have occurred within the contract, such as the transfer of tokens or the completion of a task.

It's important to carefully design and implement the events in a contract, and to ensure that all required events are included. It's also a good idea to test the contract to ensure that all events are being properly triggered and logged.

```
minPeriod = _minPeriod
totalShares = totalShares.sub(shares[shareholder].amount).add(amount)
```

Recommendation

By including all required events in the contract and thoroughly testing the contract's functionality, the contract ensures that it performs as intended and does not have any missing events that could cause issues with its arithmetic.

L16 - Validate Variable Setters

Criticality	Minor / Informative
Location	contracts/ShibaWarp.sol#L384,1016,1017
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.

```
selllessSwap = _selllessSwap
utilityReceiver = payable(_utilityReceiver)
buybackReceiver = payable(_buybackReceiver)
```

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.

L20 - Succeeded Transfer Check

Criticality	Minor / Informative
Location	contracts/ShibaWarp.sol#L462
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.

```
SHIBA.transfer(shareholder, amount)
```

Recommendation

The contract should check if the result of the transfer methods is successful. The team is advised to check the SafeERC20 library from the Openzeppelin library.

Functions Analysis

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
SafeMathInt	Library			
	mul	Internal		
	div	Internal		
	sub	Internal		
	add	Internal		
SafeMath	Library			
	add	Internal		
	sub	Internal		
	sub	Internal		
	mul	Internal		
	div	Internal		
	div	Internal		
	mod	Internal		
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-

	allowance	External		-
	transfer	External	✓	-
	approve	External	✓	-
	transferFrom	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	✓	-
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	IUniswapV2 Router01		
	removeLiquidityETHSupportingFeeOnTransferTokens	External	✓	-
	removeLiquidityETHWithPermitSupportingFeeOnTransferTokens	External	✓	-
	swapExactTokensForTokensSupportingFeeOnTransferTokens	External	✓	-
	swapExactETHForTokensSupportingFeeOnTransferTokens	External	Payable	-
	swapExactTokensForETHSupportingFeeOnTransferTokens	External	✓	-
IUniswapV2Factory	Interface			
	getPair	External		-
	allPairs	External		-
	allPairsLength	External		-
	feeTo	External		-
	feeToSetter	External		-
	createPair	External	✓	-

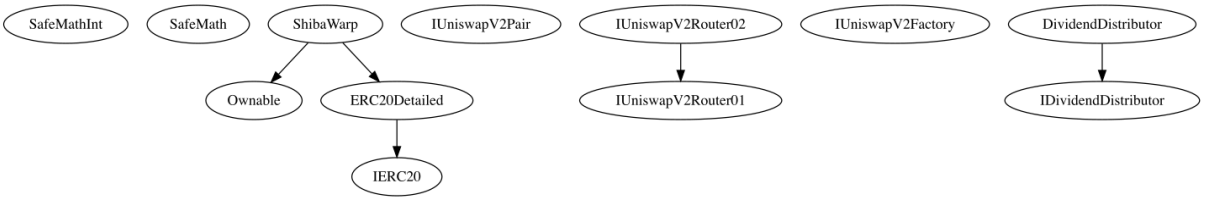
IDividendDistributor	Interface			
	setDistributionCriteria	External	✓	-
	setShare	External	✓	-
	deposit	External	Payable	-
	process	External	✓	-
	setMinimumSharesRequired	External	✓	-
	setSelllessSwapAddress	External	✓	-
DividendDistributor	Implementation	IDividendDistributor		
		Public	✓	-
		External	Payable	-
	setDistributionCriteria	External	✓	onlyToken
	setSelllessSwapAddress	External	✓	onlyToken
	setMinimumSharesRequired	External	✓	onlyToken
	setShare	External	✓	onlyToken
	deposit	External	Payable	-
	process	External	✓	onlyToken
	shouldDistribute	Internal		
	distributeDividend	Internal	✓	
	claimDividend	External	✓	-
	getSelllessSwap	External		-
	getUnpaidEarnings	Public		-

	getCumulativeDividends	Internal		
	addShareholder	Internal	✓	
	removeShareholder	Internal	✓	
Ownable	Implementation			
		Public	✓	-
	owner	External		-
	isOwner	Public		-
	renounceOwnership	External	✓	onlyOwner
	transferOwnership	External	✓	onlyOwner
	_transferOwnership	Internal	✓	
ERC20Detailed	Implementation	IERC20		
		Public	✓	-
	name	External		-
	symbol	External		-
	decimals	External		-
ShibaWarp	Implementation	ERC20Detailed, Ownable		
		Public	✓	ERC20Detailed Ownable
	transfer	External	✓	-
	transferFrom	External	✓	-
	_basicTransfer	Internal	✓	

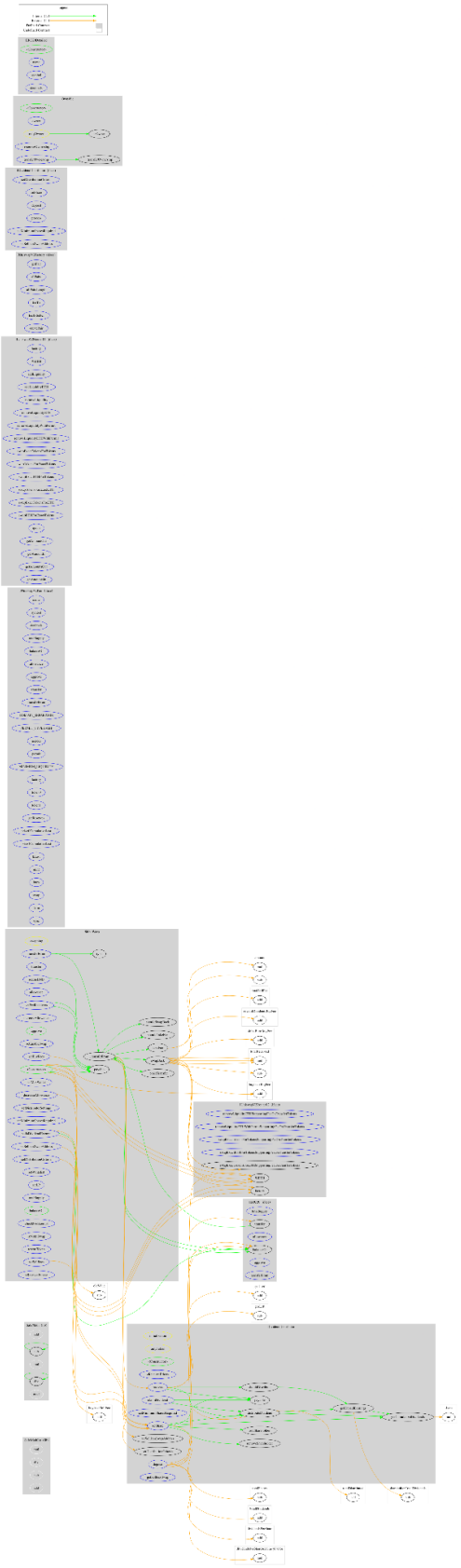
	_transferFrom	Internal	✓	
	takeFee	Internal	✓	
	swapBack	Public	✓	swapping
	shouldTakeFee	Internal		
	shouldSwapBack	Internal		
	allowance	External		-
	decreaseAllowance	External	✓	-
	increaseAllowance	External	✓	-
	approve	Public	✓	-
	setEnableSwap	External	✓	onlyOwner
	setIsDividendExempt	External	✓	onlyOwner
	setSelllessSwapAddress	External	✓	onlyOwner
	setMaxWallet	External	✓	onlyOwner
	setDistributionCriteria	External	✓	onlyOwner
	setDistributorSettings	External	✓	onlyOwner
	setMinimumSharesRequired	External	✓	onlyOwner
	setBuyFees	External	✓	onlyOwner
	setSellFees	External	✓	onlyOwner
	setFeeReceivers	External	✓	onlyOwner
	setWhitelist	External	✓	onlyOwner
	setLP	External	✓	onlyOwner
	totalSupply	External		-
	balanceOf	Public		-

	checkFeeExempt	External		-
	isNotInSwap	External		-
	rescueToken	External	✓	onlyOwner
	rescueBNB	External	✓	onlyOwner
		External	Payable	-

Inheritance Graph



Flow Graph



Summary

ShibaWarp 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 stopping transactions. A multi-wallet signing pattern will provide security against potential hacks. There is also a limit of max 25% 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