Cyberscope

Audit Report

Vacuum

November 2022

SHA256	00dcdf3d8bee8bb483f0cbe2f6ec6d05acf430b44df1d61e8dce3bf2e68a355b
Audited by	© cyberscope

Table of Contents

Contract Review

Contract Name	Vacuum
Compiler Version	v0.8.15+commit.e14f2714
Optimization	200 runs
Explorer	https://testnet.bscscan.com/token/0x472265b6743A2e4D01F95B5B4859571b22623A02
Symbol	VC
Decimals	9
Total Supply	2,997,924,580
Domain	vacuum.ltd

Source Files

Filename	**SHA256**
contract.sol	00dcdf3d8bee8bb483f0cbe2f6ec6d05acf430b44df1d61e8dce3bf2e68a355b

Audit Updates

Initial Audit	7th November 2022 https://github.com/cyberscope-io/audits/blob/main/1-vc/v1/audit.pdf
Corrected Phase 1	23rd November 2022 https://github.com/cyberscope-io/audits/blob/main/1-vc/v2/audit.pdf
Corrected Phase 2	25th November 2022

Contract Analysis

🔴 Critical 🟠 Medium ⚪ Minor / Informative 🔵 Pass

Severity	Code	Description	Status
🟠	ST	Stops Transactions	Unresolved
🔵	OCTD	Transfers Contract's Tokens	Passed
🔵	OTUT	Transfers User's Tokens	Passed
🔴	ELFM	Exceeds Fees Limit	Unresolved
🔵	ULTW	Transfers Liquidity to Team Wallet	Passed
🔵	MT	Mints Tokens	Passed
🔵	BT	Burns Tokens	Passed
🔴	BC	Blacklists Addresses	Unresolved

ST - Stops Transactions

Criticality	medium
Location	contract.sol#L443,444,448,450,454,460
Status	Unresolved

Description

The contract owner has the authority to stop the transactions for all users excluding the owner. The owner may take advantage of it by setting the maxBuyLimit to zero.

```
require(amount <= maxBuyLimit, "You are exceeding maxBuyLimit");
```

The contract owner has the authority to stop the transactions for all users excluding the owner. The owner may take advantage of it by setting the maxSellLimit to zero.

```
require(amount <= maxSellLimit, "You are exceeding maxSellLimit");
```

The contract owner has the authority to stop the transactions for all users excluding the owner. The owner may take advantage of it by setting the maxWalletLimit to zero.

```
require(balanceOf(to) + amount <= maxWalletLimit, "You are exceeding
maxWalletLimit");
```

The contract owner has the authority to stop the transactions for all users excluding the owner. The owner may take advantage of it by setting the coolDownTime to a high number.

```
require(timePassed >= coolDownTime, "Cooldown enabled");
```

This line of code can lead to an overflow and stop the transaction. An example that may lead to such case can be: **balanceOf(from)**: 2, **amount**: 1. Doing the math operation will result in a negative number, but overflow in solidity.

```
if(balanceOf(from) - amount <= 10 *  10**decimals()) amount -= (10 *
10**decimals() + amount - balanceOf(from));
```

Recommendation

The contract could embody a check for not allowing setting the _whaleLimit 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.

ELFM - Exceeds Fees Limit

Criticality	critical
Location	contract.sol#L335,340
Status	Unresolved

Description

The contract owner has the authority to increase over the allowed limit of 25%. The owner may take advantage of it by calling the setTaxes and setSellTaxes functions with a high percentage value.

```
function setTaxes(uint256 _rfi, uint256 _marketing, uint256 _liquidity) public
onlyOwner {
    taxes = Taxes(_rfi,_marketing,_liquidity);
    emit FeesChanged();
}
....
function setSellTaxes(uint256 _rfi, uint256 _marketing, uint256 _liquidity)
public onlyOwner {
    sellTaxes = Taxes(_rfi,_marketing,_liquidity);
    emit FeesChanged();
}
```

Recommendation

The contract could embody a check for the maximum acceptable value.

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.

BC - Blacklists Addresses

Criticality	critical
Location	contract.sol#L836
Status	Unresolved

Description

The contract owner has the authority to stop up to 20 addresses from transactions. The owner may take advantage of it by calling the `updateIsBlacklisted` or `bulkIsBlacklisted` function.

```
require(!_isBlacklisted[from] && !_isBlacklisted[to], "You are a bot");
```

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. That risk can be prevented by temporarily locking the contract or renouncing ownership.

Contract Diagnostics

● Critical ● Medium ● Minor / Informative

Severity	Code	Description	Status
●	PVC	Price Volatility Concern	Unresolved
●	L02	State Variables could be Declared Constant	Unresolved
●	L04	Conformance to Solidity Naming Conventions	Unresolved
●	L07	Missing Events Arithmetic	Unresolved
●	L13	Divide before Multiply Operation	Unresolved

PVC - Price Volatility Concern

Criticality	minor / informative
Location	contract.sol#L574
Status	Unresolved

Description

The swapTokensAtAmount could produce a dramatically price volatility. If the variable set to a high number, then the contract will sell a huge amount of tokens in a single transaction.

```
function updateSwapTokensAtAmount(uint256 amount) external onlyOwner{
    swapTokensAtAmount = amount * 10**_decimals;
}
```

Recommendation

The contract could ensure that it will not sell more than a reasonable amount of tokens once. A suggested implementation could check that the maximum amount should be less than a fixed percentage of the total supply.

L02 - State Variables could be Declared Constant

Criticality	minor / informative
Location	contract.sol#L139
Status	Unresolved

Description

Constant state variables should be declared constant to save gas.

```
_tTotal
```

Recommendation

Add the constant attribute to state variables that never change.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor / informative
Location	contract.sol#L335,340,618,149,578,78,169,136,150
Status	Unresolved

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.

```
_liquidity
_amount
_to
_name
_rfi
_marketing
_enabled
WETH
valuesFromGetValues
...
```

Recommendation

Follow the Solidity naming convention.
https://docs.soliditylang.org/en/v0.8.17/style-guide.html#naming-conventions.

L07 - Missing Events Arithmetic

Criticality	minor / informative
Location	contract.sol#L602,574,597,569
Status	Unresolved

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.

```
maxWalletLimit = amount * 10 ** decimals()
swapTokensAtAmount = amount * 10 ** _decimals
maxBuyLimit = maxBuy * 10 ** decimals()
coolDownTime = time * 1
```

Recommendation

Emit an event for critical parameter changes.

L13 - Divide before Multiply Operation

Criticality	minor / informative
Location	contract.sol#L502
Status	Unresolved

Description

Performing divisions before multiplications may cause lose of prediction.

```
unitBalance = deltaBalance / (denominator - temp.liquidity)
```

Recommendation

The multiplications should be prior to the divisions.

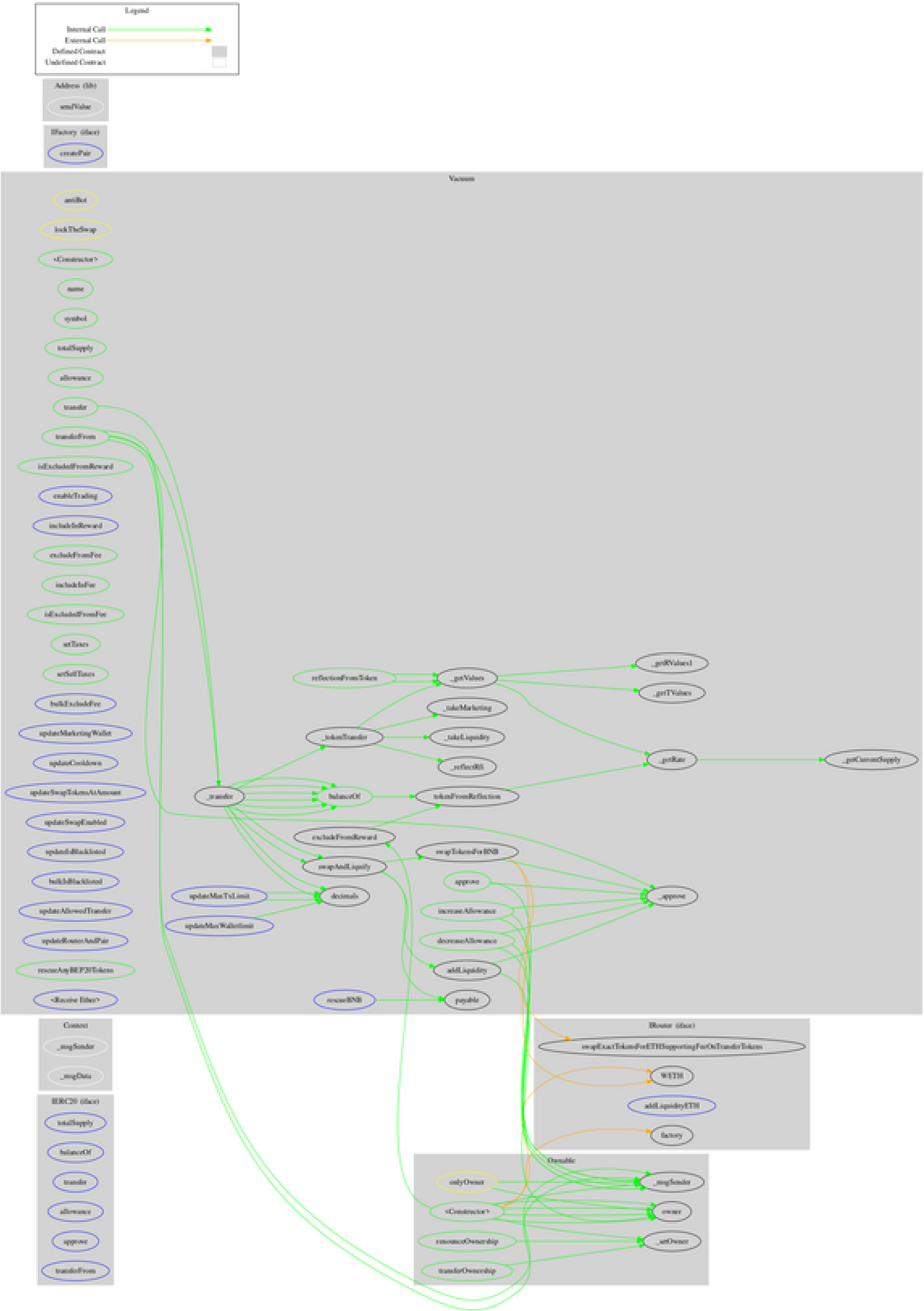
Contract Functions

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
IERC20	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		-
	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	✓	
Vacuum	Implementation	Context, IERC20, Ownable		
	<Constructor>	Public	✓	-
	name	Public		-
	symbol	Public		-
	decimals	Public		-
	totalSupply	Public		-
	balanceOf	Public		-
	allowance	Public		-
	approve	Public	✓	antiBot
	transferFrom	Public	✓	antiBot
	increaseAllowance	Public	✓	antiBot
	decreaseAllowance	Public	✓	antiBot
	transfer	Public	✓	antiBot
	isExcludedFromReward	Public		-
	reflectionFromToken	Public		-
	enableTrading	External	✓	onlyOwner
	tokenFromReflection	Public		-
	excludeFromReward	Public	✓	onlyOwner
	includeInReward	External	✓	onlyOwner
	excludeFromFee	Public	✓	onlyOwner
	includeInFee	Public	✓	onlyOwner
	isExcludedFromFee	Public		-
	setTaxes	Public	✓	onlyOwner
	setSellTaxes	Public	✓	onlyOwner
	_reflectRfi	Private	✓	
	_takeLiquidity	Private	✓	
	_takeMarketing	Private	✓	
	_getValues	Private		
	_getTValues	Private		
	_getRValues1	Private		
	_getRate	Private		

	_getCurrentSupply	Private		
	_approve	Private	✓	
	_transfer	Private	✓	
	_tokenTransfer	Private	✓	
	swapAndLiquify	Private	✓	lockTheSwap
	addLiquidity	Private	✓	
	swapTokensForBNB	Private	✓	
	bulkExcludeFee	External	✓	onlyOwner
	updateMarketingWallet	External	✓	onlyOwner
	updateCooldown	External	✓	onlyOwner
	updateSwapTokensAtAmount	External	✓	onlyOwner
	updateSwapEnabled	External	✓	onlyOwner
	updateIsBlacklisted	External	✓	onlyOwner
	bulkIsBlacklisted	External	✓	onlyOwner
	updateAllowedTransfer	External	✓	onlyOwner
	updateMaxTxLimit	External	✓	onlyOwner
	updateMaxWalletlimit	External	✓	onlyOwner
	updateRouterAndPair	External	✓	onlyOwner
	rescueBNB	External	✓	onlyOwner
	rescueAnyBEP20Tokens	Public	✓	onlyOwner
	<Receive Ether>	External	Payable	-

Contract Flow



Domain Info

Domain Name	vacuum.ltd
Registry Domain ID	953ba04742b4447ca62fb390dcaa9482-DONUTS
Creation Date	2022-08-12T09:22:39Z
Updated Date	2022-08-17T09:22:40Z
Registry Expiry Date	2023-08-12T09:22:39Z
Registrar WHOIS Server	whois.godaddy.com/
Registrar URL	http://www.godaddy.com/domains/search.aspx?ci=8990
Registrar	GoDaddy.com, LLC
Registrar IANA ID	146

The domain was created 4 months before the creation of the audit. It will expire in 9 months.

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

Summary

There are some functions that can be abused by the owner like stopping transactions, manipulating fees and massively blacklisting addresses. A multi-wallet signing pattern will provide security against potential hacks. Temporarily locking the contract or renouncing ownership will eliminate all the contract threats.

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 provide all the essential tools to assist users draw their own conclusions.

The Cyberscope team

https://www.cyberscope.io