



Cyberscope

# Audit Report

## **Vartifact**

August 2022

Type           BEP20

Network       BSC

Address       0xf367e69498450466878cc95ba5276ab1a91eeab3

Audited by   © cyberscope

# Table of Contents

<b>Table of Contents</b>	<b>1</b>
<b>Contract Review</b>	<b>2</b>
<b>Source Files</b>	<b>2</b>
<b>Audit Updates</b>	<b>2</b>
<b>Contract Analysis</b>	<b>3</b>
<b>OCTD - Owner Contract Tokens Drain</b>	<b>4</b>
Description	4
Recommendation	4
<b>Contract Diagnostics</b>	<b>5</b>
<b>STC - Succeeded Transfer Check</b>	<b>6</b>
Description	6
Recommendation	6
<b>L01 - Public Function could be Declared External</b>	<b>7</b>
Description	7
Recommendation	7
<b>L04 - Conformance to Solidity Naming Conventions</b>	<b>8</b>
Description	8
Recommendation	8
<b>Contract Functions</b>	<b>9</b>
<b>Contract Flow</b>	<b>11</b>
<b>Domain Info</b>	<b>12</b>
<b>Summary</b>	<b>13</b>
<b>Disclaimer</b>	<b>14</b>
<b>About Cyberscope</b>	<b>15</b>

## Contract Review

<b>Contract Name</b>	VartifactContract
<b>Compiler Version</b>	v0.4.26+commit.4563c3fc
<b>Optimization</b>	200 runs
<b>Licence</b>	MIT
<b>Explorer</b>	<a href="https://bscscan.com/token/0xf367e69498450466878cC95BA5276aB1A91EEab3">https://bscscan.com/token/0xf367e69498450466878cC95BA5276aB1A91EEab3</a>
<b>Symbol</b>	VARTI
<b>Decimals</b>	18
<b>Total Supply</b>	1,000,000,000
<b>Domain</b>	<a href="https://vartifact.io">https://vartifact.io</a>

## Source Files

<b>Filename</b>	<b>SHA256</b>
<b>contract.sol</b>	88581d64df32cfdef311b1a475e875f339769842955a31f8a52c47609599fa7d

## Audit Updates

<b>Initial Audit</b>	17th August 2022
<b>Corrected</b>	

# 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

## OCTD - Owner Contract Tokens Drain

<b>Criticality</b>	minor
<b>Location</b>	contract.sol#L204

### 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 `transferAnyERC20Token` function.

```
function transferAnyERC20Token(address tokenAddress, uint tokens) public onlyOwner returns (bool success) {  
    return ERC20Interface(tokenAddress).transfer(owner, tokens);  
}
```

### 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

Severity	Code	Description
●	STC	Succeeded Transfer Check
●	L01	Public Function could be Declared External
●	L04	Conformance to Solidity Naming Conventions

## STC - Succeeded Transfer Check

**Criticality**

minor

**Location**

contract.sol#L205

### 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.

```
function transferAnyERC20Token(address tokenAddress, uint tokens) public onlyOwner returns (bool success) {  
    return ERC20Interface(tokenAddress).transfer(owner, tokens);  
}
```

### Recommendation

The contract should check if the result of the transfer methods is successful.

## L01 - Public Function could be Declared External

**Criticality**

minor

**Location**

contract.sol#L48,33,32,73,192,21,34,70,181,36,37,35,200,17

### Description

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

```
safeMul
transferAnyERC20Token
transfer
transferFrom
approve
approveAndCall
transferOwnership
allowance
safeDiv
...
```

### Recommendation

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



## L04 - Conformance to Solidity Naming Conventions

**Criticality**

minor

**Location**

contract.sol#L70,90

### 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.

```
_totalSupply  
_newOwner
```

### Recommendation

Follow the Solidity naming convention.

<https://docs.soliditylang.org/en/v0.4.25/style-guide.html#naming-conventions>.

# Contract Functions

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
<b>SafeMath</b>	Implementation			
	safeAdd	Public		-
	safeSub	Public		-
	safeMul	Public		-
	safeDiv	Public		-
<b>ERC20Interface</b>	Implementation			
	totalSupply	Public		-
	balanceOf	Public		-
	allowance	Public		-
	transfer	Public	✓	-
	approve	Public	✓	-
	transferFrom	Public	✓	-
<b>ApproveAndCallFallback</b>	Implementation			
	receiveApproval	Public	✓	-
<b>Owned</b>	Implementation			
	<Constructor>	Public	✓	-
	transferOwnership	Public	✓	onlyOwner
	acceptOwnership	Public	✓	-
<b>VartifactContract</b>	Implementation	ERC20Interface, Owned, SafeMath		
	<Constructor>	Public	✓	-
	totalSupply	Public		-

	balanceOf	Public		-
	transfer	Public	✓	-
	approve	Public	✓	-
	transferFrom	Public	✓	-
	allowance	Public		-
	approveAndCall	Public	✓	-
	<Fallback>	Public	Payable	-
	transferAnyERC20Token	Public	✓	onlyOwner

# Contract Flow



## Domain Info

<b>Domain Name</b>	vartifact.io
<b>Registry Domain ID</b>	365e0bb3b87f4ea0a3e76b6e4e7d7841-DONUTS
<b>Creation Date</b>	2021-11-21T17:12:46Z
<b>Updated Date</b>	2022-07-11T19:29:13Z
<b>Registry Expiry Date</b>	2022-11-21T17:12:46Z
<b>Registrar WHOIS Server</b>	whois.ionos.com
<b>Registrar URL</b>	<a href="https://www.ionos.com">https://www.ionos.com</a>
<b>Registrar</b>	IONOS SE
<b>Registrar IANA ID</b>	83

The domain was created 3 months before the creation of the audit.

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

## Summary

Vartifact is an interesting project that has a friendly and growing community. The Smart Contract analysis reported one minor severity issue. 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.

## 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>