



# Audit Report

## **VRALLES**

February 2022

Type	BEP20
Network	BSC
Address	0x1fb67E24D354DcF3646262102B3F9dCCc5a464b2
Audited by	© coinscope

# Table of Contents

<b>Table of Contents</b>	<b>1</b>
<b>Contract Review</b>	<b>2</b>
<b>Audit Updates</b>	<b>2</b>
<b>Contract Analysis</b>	<b>3</b>
<b>MT - Mint Tokens</b>	<b>4</b>
<b>Description</b>	<b>4</b>
<b>Recommendation</b>	<b>4</b>
<b>Contract Diagnostics</b>	<b>5</b>
<b>L01 - Public Function could be Declared External</b>	<b>6</b>
<b>Description</b>	<b>6</b>
<b>Recommendation</b>	<b>6</b>
<b>L09 - Dead Code Elimination</b>	<b>7</b>
<b>Description</b>	<b>7</b>
<b>Recommendation</b>	<b>7</b>
<b>Contract Functions</b>	<b>8</b>
<b>Contract Flow</b>	<b>10</b>
<b>Domain Info</b>	<b>11</b>
<b>Summary</b>	<b>12</b>
<b>Disclaimer</b>	<b>13</b>
<b>About Coinscope</b>	<b>14</b>

## Contract Review

<b>Contract Name</b>	BEP20Token
<b>Compiler Version</b>	v0.5.16+commit.9c3226ce
<b>Optimization</b>	200 runs
<b>Licence</b>	None
<b>Explorer</b>	<a href="https://bscscan.com/token/0x1fb67E24D354DcF3646262102B3F9dCCc5a464b2">https://bscscan.com/token/0x1fb67E24D354DcF3646262102B3F9dCCc5a464b2</a>
<b>Symbol</b>	VRL
<b>Decimals</b>	18
<b>Total Supply</b>	250,000,000
<b>Source</b>	contract.sol
<b>Domain</b>	vralles.com

## Audit Updates

<b>Initial Audit</b>	24th February 2022
<b>Corrected</b>	

# Contract Analysis

● Critical
 ● Medium
 ● Minor
 ● Pass

Severity	Code	Description
<span style="color: blue;">●</span>	ST	Contract Owner is not able to stop or pause transactions
<span style="color: blue;">●</span>	OCTD	Contract Owner is not able to transfer tokens from specific address
<span style="color: blue;">●</span>	OTUT	Owner Transfer User's Tokens
<span style="color: blue;">●</span>	ELFM	Contract Owner is not able to increase fees more than a reasonable percent (25%)
<span style="color: blue;">●</span>	ULTW	Contract Owner is not able to increase the amount of liquidity taken by dev wallet more than a reasonable percent
<span style="color: red;">●</span>	MT	Contract Owner is not able to mint new tokens
<span style="color: blue;">●</span>	BT	Contract Owner is not able to burn tokens from specific wallet
<span style="color: blue;">●</span>	BC	Contract Owner is not able to blacklist wallets from selling

## MT - Mint Tokens

<b>Criticality</b>	critical
<b>Location</b>	contract.sol#L497

### Description

The contract owner has the authority to mint tokens. The owner may take advantage of it by calling the `mint` function. As a result the contract tokens will be highly inflated.

```
function mint(uint256 amount) public onlyOwner returns (bool) {  
    _mint(_msgSender(), amount);  
    return true;  
}
```

### Recommendation

The owner should carefully manage the credentials of the owner's account. We advised considering an extra-strong security mechanism that the actions may be quarantined by many users instead of one. The owner could also renounce the contract ownership for a period of time or pass the access to the zero address.

# Contract Diagnostics

● Critical    ● Medium    ● Minor

Severity	Code	Description
●	L01	Public Function could be Declared External
●	L09	Dead Code Elimination

## L01 - Public Function could be Declared External

<b>Criticality</b>	minor
<b>Location</b>	contract.sol#L316,325,465,484,497

### Description

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

```
mint
decreaseAllowance
increaseAllowance
transferOwnership
renounceOwnership
```

### Recommendation

Use the external attribute for functions never called from the contract

## L09 - Dead Code Elimination

<b>Criticality</b>	minor
<b>Location</b>	contract.sol#L553,588,113,212,227,247,262,187,158

### Description

Functions that are not used in the contract, and make the code's size bigger.

```
sub
mul
mod
div
_msgData
_burnFrom
_burn
```

### Recommendation

Remove unused functions.



# Contract Functions

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
<b>IBEP20</b>	Interface			
	totalSupply	External		-
	decimals	External		-
	symbol	External		-
	name	External		-
	getOwner	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
<b>Context</b>	Implementation			
	<Constructor>	Internal	✓	
	_msgSender	Internal		
	_msgData	Internal		
<b>SafeMath</b>	Library			
	add	Internal		
	sub	Internal		
	sub	Internal		
	mul	Internal		
	div	Internal		
	div	Internal		
	mod	Internal		
	mod	Internal		
<b>Ownable</b>	Implementation	Context		
	<Constructor>	Internal	✓	

	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	_transferOwnership	Internal	✓	
<b>BEP20Token</b>	Implementation	Context, IBEP20, Ownable		
	<Constructor>	Public	✓	-
	getOwner	External		-
	decimals	External		-
	symbol	External		-
	name	External		-
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
	increaseAllowance	Public	✓	-
	decreaseAllowance	Public	✓	-
	mint	Public	✓	onlyOwner
	_transfer	Internal	✓	
	_mint	Internal	✓	
	_burn	Internal	✓	
	_approve	Internal	✓	
	_burnFrom	Internal	✓	

# Contract Flow



## Domain Info

<b>Domain Name</b>	vralles.com
<b>Registry Domain ID</b>	2669403027_DOMAIN_COM-VRSN
<b>Creation Date</b>	2022-01-19T14:20:08Z
<b>Updated Date</b>	2022-01-31T10:17:29Z
<b>Registry Expiry Date</b>	
<b>Registrar WHOIS Server</b>	whois.aerotek.com.tr
<b>Registrar URL</b>	
<b>Registrar</b>	Aerotek Bilisim Sanayi ve Ticaret AS
<b>Registrar IANA ID</b>	1534

The domain has been created about 1 month before the creation of the audit.

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

## Summary

The Smart Contract analysis reported one critical issue. The contract Owner has the ability to mint tokens. If this functionality is abused, the contract tokens would be highly inflated. 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.

Coinscope 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 Coinscope 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 Coinscope 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 Coinscope team disclaims any liability for the resulting losses.

## About Coinscope

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.

Coinscope is aiming to make crypto discoverable and efficient globally. It provides all the essential tools to assist users draw their own conclusions.



The Coinscope.co team

<https://www.coinscope.co>