



# Audit Report

## **Superior cars**

January 2022

Type       BEP20

Network    BSC

Address    0xF44DE2b8731cD69d4A727Do0214874aE35559426

Audited by  © coinscope

# Table of Contents

|                                                         |           |
|---------------------------------------------------------|-----------|
| <b>Table of Contents</b>                                | <b>1</b>  |
| <b>Contract Review</b>                                  | <b>3</b>  |
| <b>Audit Updates</b>                                    | <b>3</b>  |
| <b>Contract Analysis</b>                                | <b>4</b>  |
| <b>ELFM - Exceed Limit Fees Manipulation</b>            | <b>5</b>  |
| Description                                             | 5         |
| Recommendation                                          | 5         |
| <b>MT - Mint Tokens</b>                                 | <b>6</b>  |
| Description                                             | 6         |
| Recommendation                                          | 6         |
| <b>BC - Blacklisted Contracts</b>                       | <b>7</b>  |
| Description                                             | 7         |
| Recommendation                                          | 7         |
| <b>Contract Diagnostics</b>                             | <b>8</b>  |
| <b>L01 - Public Function could be Declared External</b> | <b>9</b>  |
| Description                                             | 9         |
| Recommendation                                          | 9         |
| <b>L04 - Conformance to Solidity Naming Conventions</b> | <b>10</b> |
| Description                                             | 10        |
| Recommendation                                          | 10        |
| <b>L09 - Dead Code Elimination</b>                      | <b>11</b> |
| Description                                             | 11        |
| Recommendation                                          | 11        |
| <b>L11 - Unnecessary Boolean equality</b>               | <b>12</b> |
| Description                                             | 12        |
| Recommendation                                          | 12        |

|                           |           |
|---------------------------|-----------|
| <b>Contract Functions</b> | <b>13</b> |
| <b>Contract Flow</b>      | <b>15</b> |
| <b>Domain Info</b>        | <b>16</b> |
| <b>Summary</b>            | <b>17</b> |
| <b>Disclaimer</b>         | <b>18</b> |
| <b>About Coinscope</b>    | <b>19</b> |

## Contract Review

|                         |                                                                                                                                                         |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Contract Name</b>    | CoinToken                                                                                                                                               |
| <b>Compiler Version</b> | v0.4.24+commit.e67f0147                                                                                                                                 |
| <b>Optimization</b>     | 200 runs                                                                                                                                                |
| <b>Licence</b>          | None                                                                                                                                                    |
| <b>Explorer</b>         | <a href="https://bscscan.com/token/0xF44DE2b8731cD69d4A727Da0214874aE35559426">https://bscscan.com/token/0xF44DE2b8731cD69d4A727Da0214874aE35559426</a> |
| <b>Symbol</b>           | SRT                                                                                                                                                     |
| <b>Decimals</b>         | 9                                                                                                                                                       |
| <b>Total Supply</b>     | 10,000,000,000                                                                                                                                          |
| <b>Source</b>           | contract.sol                                                                                                                                            |
| <b>Domain</b>           | superiorcarsgame.com                                                                                                                                    |

## Audit Updates

|                      |                  |
|----------------------|------------------|
| <b>Initial Audit</b> | 4th January 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: red;">●</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: gold;">●</span> | BC   | Contract Owner is not able to blacklist wallets from selling                                                      |

## ELFM - Exceed Limit Fees Manipulation

|                    |                                                                                                                                                                                 |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Criticality</b> | critical                                                                                                                                                                        |
| <b>Location</b>    | <a href="https://bscscan.com/address/0x8983a6f5b70315f9373d39e14de5afeabf835588#code#L285">https://bscscan.com/address/0x8983a6f5b70315f9373d39e14de5afeabf835588#code#L285</a> |

### 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 `updateFee` function with a high percentage value.

```
function updateFee(uint256 _txFee,uint256 _burnFee,address _FeeAddress)
onlyOwner public{
    txFee = _txFee;
    burnFee = _burnFee;
    FeeAddress = _FeeAddress;
}
```

### 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.

## MT - Mint Tokens

|                    |                   |
|--------------------|-------------------|
| <b>Criticality</b> | critical          |
| <b>Location</b>    | contract.sol#L300 |

### 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(address account, uint256 amount) onlyOwner public {  
    totalSupply = totalSupply.add(amount);  
    balances[account] = balances[account].add(amount);  
    emit Mint(address(0), account, amount);  
    emit Transfer(address(0), account, amount);  
}
```

### 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.

## BC - Blacklisted Contracts

|             |                   |
|-------------|-------------------|
| Criticality | medium            |
| Location    | contract.sol#L253 |

### Description

The contract owner has the authority to stop contracts from transactions. The owner may take advantage of it by calling the `blackListAddress` function.

```
function blackListAddress(address listAddress, bool isBlackListed) public  
whenNotPaused onlyOwner returns (bool success) {  
    return super._blackList(listAddress, isBlackListed);  
}
```

### 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                                |
|----------|------|--------------------------------------------|
| ●        | L01  | Public Function could be Declared External |
| ●        | L04  | Conformance to Solidity Naming Conventions |
| ●        | L09  | Dead Code Elimination                      |
| ●        | L11  | Unnecessary Boolean equality               |

## L01 - Public Function could be Declared External

**Criticality**

minor

**Location**

contract.sol#L300,L285,L281 and 6 more

### Description

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

```
mint
updateFee
burn
...
```

### Recommendation

Use the external attribute for functions never called from the contract

## L04 - Conformance to Solidity Naming Conventions

**Criticality**

minor

**Location**

contract.sol#L285,L281,L249 and 27 more

### 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.

```
_FeeAddress  
_burnFee  
_txFee  
...
```

### Recommendation

Follow the Solidity naming convention.

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

## L09 - Dead Code Elimination

**Criticality**

minor

**Location**

contract.sol#L4

### Description

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

```
mul
```

### Recommendation

Remove unused functions.

## L11 - Unnecessary Boolean equality

**Criticality**

minor

**Location**

contract.sol#L161,L128

### Description

The comparison to boolean constants is redundant. Boolean constants can be used directly and do not need to be compared to true or false.

```
require(bool)(tokenBlacklist[msg.sender] == false)
```

### Recommendation

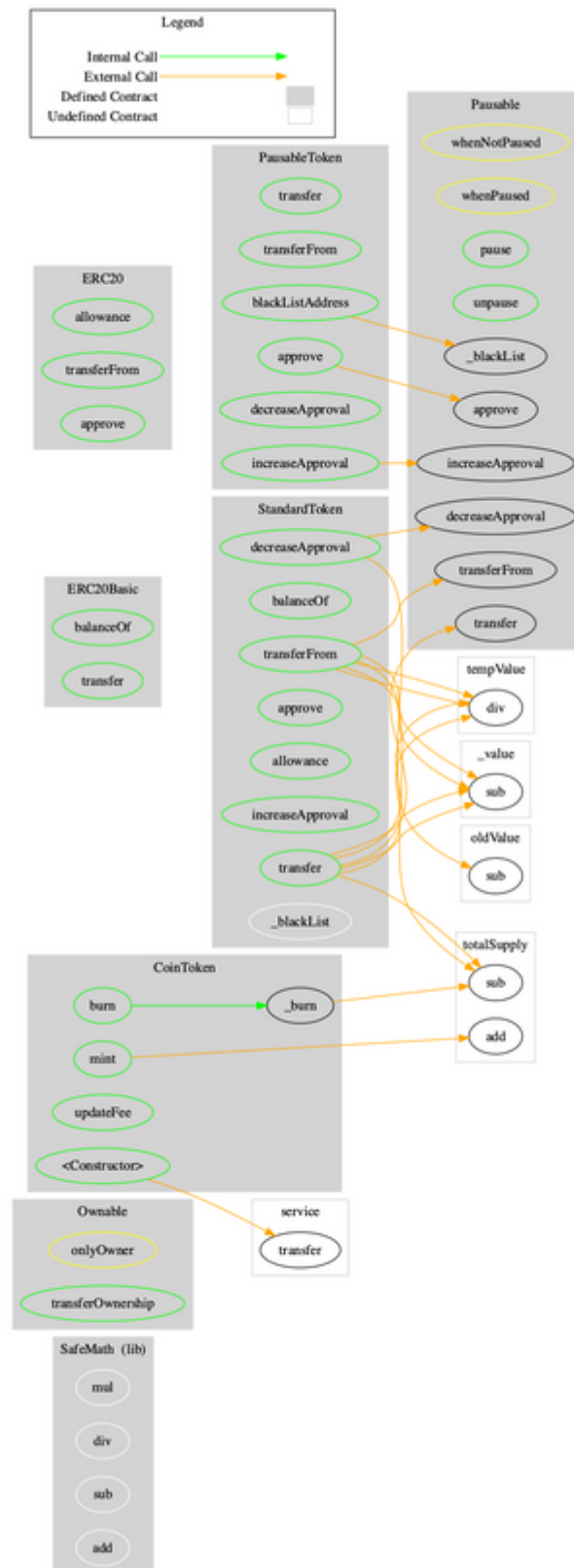
Remove the equality to the boolean constant.

# Contract Functions

| Contract             | Type              | Bases      |            |                            |
|----------------------|-------------------|------------|------------|----------------------------|
|                      | Function Name     | Visibility | Mutability | Modifiers                  |
|                      |                   |            |            |                            |
| <b>SafeMath</b>      | Library           |            |            |                            |
|                      | mul               | Internal   |            |                            |
|                      | div               | Internal   |            |                            |
|                      | sub               | Internal   |            |                            |
|                      | add               | Internal   |            |                            |
|                      |                   |            |            |                            |
| <b>Ownable</b>       | Implementation    |            |            |                            |
|                      | transferOwnership | Public     | ✓          | onlyOwner                  |
|                      |                   |            |            |                            |
| <b>Pausable</b>      | Implementation    | Ownable    |            |                            |
|                      | pause             | Public     | ✓          | onlyOwner<br>whenNotPaused |
|                      | unpause           | Public     | ✓          | onlyOwner<br>whenPaused    |
|                      |                   |            |            |                            |
| <b>ERC20Basic</b>    | Implementation    |            |            |                            |
|                      | balanceOf         | Public     |            | -                          |
|                      | transfer          | Public     | ✓          | -                          |
|                      |                   |            |            |                            |
| <b>ERC20</b>         | Implementation    | ERC20Basic |            |                            |
|                      | allowance         | Public     |            | -                          |
|                      | transferFrom      | Public     | ✓          | -                          |
|                      | approve           | Public     | ✓          | -                          |
|                      |                   |            |            |                            |
| <b>StandardToken</b> | Implementation    | ERC20      |            |                            |
|                      | transfer          | Public     | ✓          | -                          |
|                      | balanceOf         | Public     |            | -                          |

|                      |                  |                            |         |                         |
|----------------------|------------------|----------------------------|---------|-------------------------|
|                      | transferFrom     | Public                     | ✓       | -                       |
|                      | approve          | Public                     | ✓       | -                       |
|                      | allowance        | Public                     |         | -                       |
|                      | increaseApproval | Public                     | ✓       | -                       |
|                      | decreaseApproval | Public                     | ✓       | -                       |
|                      | _blackList       | Internal                   | ✓       |                         |
|                      |                  |                            |         |                         |
| <b>PausableToken</b> | Implementation   | StandardToken,<br>Pausable |         |                         |
|                      | transfer         | Public                     | ✓       | whenNotPaused           |
|                      | transferFrom     | Public                     | ✓       | whenNotPaused           |
|                      | approve          | Public                     | ✓       | whenNotPaused           |
|                      | increaseApproval | Public                     | ✓       | whenNotPaused           |
|                      | decreaseApproval | Public                     | ✓       | whenNotPaused           |
|                      | blackListAddress | Public                     | ✓       | whenNotPaused onlyOwner |
|                      |                  |                            |         |                         |
| <b>CoinToken</b>     | Implementation   | PausableToken              |         |                         |
|                      | <Constructor>    | Public                     | Payable | -                       |
|                      | burn             | Public                     | ✓       | -                       |
|                      | updateFee        | Public                     | ✓       | onlyOwner               |
|                      | _burn            | Internal                   | ✓       |                         |
|                      | mint             | Public                     | ✓       | onlyOwner               |

# Contract Flow



## Domain Info

|                               |                                          |
|-------------------------------|------------------------------------------|
| <b>Domain Name</b>            | superiorcarsgame.com                     |
| <b>Registry Domain ID</b>     | 2662587105_DOMAIN_COM-VRSN               |
| <b>Creation Date</b>          | 2021-12-19T05:01:22Z                     |
| <b>Updated Date</b>           | 2021-12-20T10:09:15Z                     |
| <b>Registry Expiry Date</b>   |                                          |
| <b>Registrar WHOIS Server</b> | whois.registrar.eu                       |
| <b>Registrar URL</b>          | http://www.registrar.eu                  |
| <b>Registrar</b>              | Hosting Concepts B.V. d/b/a Registrar.eu |
| <b>Registrar IANA ID</b>      | 1647                                     |

The domain has been created 16 days before the creation of the audit.

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

## Summary

Superior cars is aiming to create a game with cars. The token has a friendly and growing community. There are some informative comments that do not affect the contract security. The contract analysis reported two major and one medium-level issues. There are some functions that can be abused by the owner, like manipulating fees, blacklisting addresses and minting tokens. The maximum fee percentage that can be set is 25%. 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>