



# KISHIELD

Security Audit

**CareCoin Token**

February 28, 2022





# Table of Contents

- 1 Audit Summary**
- 2 Project Overview**
  - 2.1 Token Summary
  - 2.2 Main Contract Assessed
- 3 Smart Contract Vulnerability Checks**
- 4 Contract Ownership**
  - 4.1 Privileged Functions (onlyOwner)
- 5 Important Notes To The Users**
- 6 Statistics**
  - 6.1 Liquidity
  - 6.2 Token Holders
  - 6.3 Liquidity Holders
- 7 Liquidity Ownership**
- 8 Disclaimer**



# Audit Summary

This report has been prepared for CareCoin Token on the Binance Smart Chain network. KISHIELD provides both client-centered and user-centered examination of the smart contracts and their current status when applicable. This report represents the security assessment made to find issues and vulnerabilities on the source code along with the current liquidity and token holder statistics of the protocol.

A comprehensive examination has been performed, utilizing Cross Referencing, Static Analysis, In-House Security Tools, and line-by-line Manual Review.

The auditing process pays special attention to the following considerations:

- Ensuring contract logic meets the specifications and intentions of the client without exposing the user's funds to risk.
- Testing the smart contracts against both common and uncommon attack vectors.
- Inspecting liquidity and holders statistics to inform the current status to both users and client when applicable.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Verifying contract functions that allow trusted and/or untrusted actors to mint, lock, pause, and transfer assets.
- Thorough line-by-line manual review of the entire codebase by industry experts.

# Project Overview

## Token Summary

Parameter	Result
Address	0x442AbdE32b075d4F11124241AAAd16459Ce802fA7
Name	CareCoin
Token Tracker	CareCoin (CARES)
Decimals	9
Supply	60,000,000,000,000,000
Platform	Binance Smart Chain
compiler	v0.8.10+commit.fc410830
Optimization	Yes with 200 runs
LicenseType	Unlicense
Language	Solidity
Codebase	<a href="https://bscscan.com/address/0x442AbdE32b075d4F11124241AAAd16459Ce802fA7">https://bscscan.com/ address/0x442AbdE32b075d4F11124241AAAd16459Ce802fA7</a>
Url	<a href="http://www.projectcarecoin.com">www.projectcarecoin.com</a>

## Main Contract Assessed

Name	Contract	Live
CareCoin	0x442AbdE32b075d4F11124241AAAd16459Ce802fA7	Yes

# Smart Contract Vulnerability Checks

Vulnerability	Automatic Scan	Manual Scan	Result
Unencrypted Private Data On-Chain	Complete	Complete	✓ Low / No Risk
Code With No Effects	Complete	Complete	✓ Low / No Risk
Message call with hardcoded gas amount	Complete	Complete	✓ Low / No Risk
Hash Collisions With Multiple Variable Length Arguments	Complete	Complete	✓ Low / No Risk
Unexpected Ether balance	Complete	Complete	✓ Low / No Risk
Presence of unused variables	Complete	Complete	✓ Low / No Risk
Right-To-Left-Override control character (U+202E)	Complete	Complete	✓ Low / No Risk
Typographical Error	Complete	Complete	✓ Low / No Risk
DoS With Block Gas Limit	Complete	Complete	✓ Low / No Risk
Arbitrary Jump with Function Type Variable	Complete	Complete	✓ Low / No Risk
Insufficient Gas Griefing	Complete	Complete	✓ Low / No Risk
Incorrect Inheritance Order	Complete	Complete	✓ Low / No Risk
Write to Arbitrary Storage Location	Complete	Complete	✓ Low / No Risk
Requirement Violation	Complete	Complete	✓ Low / No Risk
Missing Protection against Signature Replay Attacks	Complete	Complete	✓ Low / No Risk
Weak Sources of Randomness from Chain Attributes	Complete	Complete	✓ Low / No Risk

Vulnerability	Automatic Scan	Manual Scan	Result
Authorization through tx.origin	Complete	Complete	✓ Low / No Risk
Delegatecall to Untrusted Callee	Complete	Complete	✓ Low / No Risk
Use of Deprecated Solidity Functions	Complete	Complete	✓ Low / No Risk
Assert Violation	Complete	Complete	✓ Low / No Risk
Reentrancy	Complete	Complete	✓ Low / No Risk
Unprotected SELFDESTRUCT Instruction	Complete	Complete	✓ Low / No Risk
Unprotected Ether Withdrawal	Complete	Complete	✓ Low / No Risk
Unchecked Call Return Value	Complete	Complete	✓ Low / No Risk
Outdated Compiler Version	Complete	Complete	✓ Low / No Risk
Integer Overflow and Underflow	Complete	Complete	✓ Low / No Risk
Function Default Visibility	Complete	Complete	✓ Low / No Risk

## Contract Ownership

The contract ownership of CareCoin is not currently renounced. The ownership of the contract grants special powers to the protocol creators, making them the sole addresses that can call sensible ownable functions that may alter the state of the protocol.

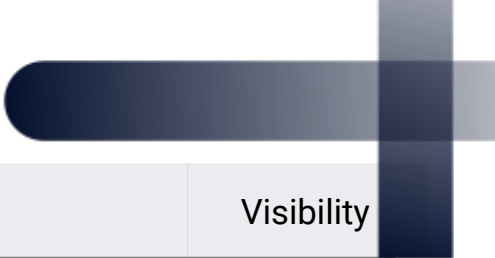
The current owner is the address 0x58E6491D804148FCa789Ef61Ddeb6Eab44073C19 which can be viewed from:  
[HERE](#)

The owner wallet has the power to call the functions displayed on the privileged functions chart below, if the owner wallet is compromised this privileges could be exploited.

We recommend the team to renounce ownership at the right timing if possible, or gradually migrate to a timelock with governing functionalities in respect of transparency and safety considerations.

## Privileged Functions (onlyOwner)

Function Name	Parameters	Visibility
renounceOwnership	none	public
transferOwnership	address newOwner	public
enableTrading	none	external
excludeFromReward	address account	public
includeInReward	address account	external
excludeFromFee	address account	external
setBlackList	address addr, bool value	external
includeInFee	address account	external
setBuyFee	uint16 liq, uint16 market, uint16 tax, uint16 burn, uint16 donation	external
setSellFee	uint16 liq, uint16 market, uint16 tax, uint16 burn, uint16 donation	external
setNumTokensSellToAddToLiquidity	uint256 numTokens	external
updateRouter	address newAddress	external
setMaxWallet	uint256 value	external
setMaxBuyAmount	uint256 value	external
setMaxSellAmount	uint256 value	external



Function Name	Parameters	Visibility
setMarketingWallet	address wallet	external
setDonationWallet	address wallet	external
setSwapAndLiquifyEnabled	bool _enabled	public
claimStuckTokens	address _token	external
swapAndLiquify	none	private



## Important Notes To The Users:

- The team is transparent and trustworthy, All Owners/Devs KYC'd. Company has been NameScanned & KYB'd.
- Team has locked their tokens with Team.Finance
- Lock Trasaction: <https://bscscan.com/tx/0x39b543c65695f81f2132a249abc0939dcbfa6c4687f5cc9e790f577c73495a18>
- The owner cannot stop Trading.
- The owner cannot mint tokens after initial contract deploy.
- The transfer function is implemented correctly.
- The owner can include/exclude addresses from fees and dividends.
- The owner can add and remove wallets form blacklist.
- The owner can change the fees related to buy and sell.
- The owner can change max tx amount.
- No high-risk Exploits/Vulnerabilities Were Found in the Source Code.

## Audit Passed



# Statistics

## Liquidity Info

Parameter	Result
Pair Address	0xa2e2eA2d658245325eA5416207CDC2Fd4f6d2B91
CARES Reserves	0.00 CARES
BNB Reserves	0.00 BNB
Liquidity Value	\$0 USD

## Token (CARES) Holders Info

Parameter	Result
CARES Percentage Burnt	0.00%
CARES Amount Burnt	0 CARES
Top 10 Percentage Own	100.00%
Top 10 Amount Owned	60,000,000,000,000,000 CARES
Top 10 Aprox Value	\$NaN USD

## LP (CARES/BNB) Holders Info

Parameter	Result
CARES/BNB % Burnt	0.00%
CARES/BNB Amount Burnt	0 CARES
Top 10 Percentage Owned	0.00%
Top 10 Amount Owned	0 CARES
Locked Tokens Percentage	0.00%
Locked Tokens Amount	0 CARES

\* All the data displayed above was taken on-chain at block 15641083

\* The tokens on industry-standard burn wallets are not included on the top 10 wallets calculations

## Liquidity Ownership

The token does not have liquidity at the moment of the audit, block 14772401

# KISHIELD



## Disclaimer

KISHIELD has conducted an independent audit to verify the integrity of and highlight any vulnerabilities or errors, intentional or unintentional, that may be present in the codes that were provided for the scope of this audit. This audit report does not constitute agreement, acceptance or advocacy for the Project that was audited, and users relying on this audit report should not consider this as having any merit for financial advice in any shape, form or nature. The contracts audited do not account for any economic developments that may be pursued by the Project in question, and that the veracity of the findings thus presented in this report relate solely to the proficiency, competence, aptitude and discretion of our independent auditors, who make no guarantees nor assurance that the contracts are completely free of exploits, bugs, vulnerabilities or deprecation of technologies.

All information provided in this report does not constitute financial or investment advice, nor should it be used to signal that any persons reading this report should invest their funds without sufficient individual due diligence regardless of the findings presented in this report. Information is provided 'as is', and KISHIELD is under no covenant to the completeness, accuracy or solidity of the contracts audited. In no event will KISHIELD or its partners, employees, agents or parties related to the provision of this audit report be liable to any parties for, or lack thereof, decisions and/or actions with regards to the information provided in this audit report.

The assessment services provided by KISHIELD is subject to dependencies and 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.