CRACKEN

Smart Contract Security Audit

Project: CCA

Oct 17, 2023

Contract Address

0x5631470C672F81A33d707758f9E63bD1Ad19Dc63

Table of Contents

Disclaimer

The contents of this report reflect only the CRACKEN TECH audit team's understanding of the current progress and status of the security of the code audited, to verify the integrity of the code provided for the scope of this audit. You agree that your access and/or use, including but not limited to any associated services, products, protocols, platforms, content, and materials, will be at your sole risk. Given the size of the project, the findings detailed here are not to be considered exhaustive, and further testing and audit are recommended after the issues covered are fixed. We do not warrant, endorse, guarantee, or assume responsibility for any product or service advertised or offered by a third party through the product, any open source or third-party software, code, libraries, materials, or information linked to, called by, referenced by or accessible through the report, its content, and the related services and products, any hyperlinked websites, any websites or mobile applications appearing on any advertising, and we will not be a party to or in any way be responsible for monitoring any transaction between you and any third-party providers of products or services.

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.

The review does not address the compiler layer, any other areas beyond the programming language, or other programming aspects that could present security risks. If the audited source files are smart contract files, risks or issues introduced by using data feeds from off-chain sources are not extended by this review either.

Audit Review

The source code of the CCA was audited in order to acquire a clear impression of how the project was implemented. The Cracken Tech audit team conducted in-depth research, analysis, and scrutiny, resulting in a series of observations. A detailed list of each issue found, and vulnerabilities in the source code will be included in the audit report. The problems and potential solutions are given in this report, we will identify common sources for such problems and comments for improvement.

The auditing process will follow a routine as special considerations by Cracken:

- Review of the specifications, sources, and instructions provided to Cracken to make sure the contract logic meets the intentions of the client without exposing the user's funds to risk.
- Manual review of the entire code base by our experts, which is the process of reading source code line-by-line in an attempt to identify potential vulnerabilities.
- Specification comparison is the process of checking whether the code does what the specifications, sources, and instructions provided to Cracken describe.
- Test coverage analysis determines whether the test cases are covering the code and how much code is exercised when we run the test cases.
- Symbolic execution is analyzing a program to determine what inputs cause each part of a program to execute.
- Reviewing the code base to improve maintainability, security, and control based on the established industry and academic practices.

Project Review

Token Summary

Parameter	Result
Token Name	**CCA**
Token Symbol	CCA
Token Decimal	18
Total Supply	10,121.482804
Platform	BSC
Buy Tax Fee	4%
Sell Tax Fee	4%
Contract Creation Date	Oct 14, 2023
Liquidity Status	51.59K
Liquidity Lockup Time	Locked for 364 days (2024.10.15)
Compiler Version	v0.8.6+commit.11564f7e
Optimization	No with 200 runs
Contract Address	0x5631470C672F81A33d707758f9E63bD1Ad19Dc63
Deployer Address	0x4f6A8B88f4681070c66374Db6B9E580e74dA3c81
Owner Address	0x000000000000000000000000000000000000dEaD

Source Code

CRACKEN was commissioned by CCA to perform an audit based on the following smart contract:
https://bscscan.com/token/0x5631470c672f81a33d707758f9e63bd1ad19dc63#code

Smart Contract Vulnerability Checks

Vulnerability	Auto-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 Grieving	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
Authorization through tx. origin	Complete	Complete	Low / No Risk
Delegate call to Untrusted Callee	Complete	Complete	Low / No Risk

Vulnerability	Auto-Scan	Manual-Scan	Result
Use of Deprecated Solidity Functions	Complete	Complete	Low / No Risk
Assert Violation	Complete	Complete	Low / No Risk
Reentrancy	Complete	Complete	Low / No Risk
Unprotected SELF-DESTRUCT Instruction	Complete	Complete	Low / No Risk
Unprotected Ether Withdrawal	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

Manual Code Review

Classification of Issues

Severity	Description
High-Risk	A vulnerability that affects the desired outcome when using a contract, or provides the opportunity to use a contract in an unintended way.
Medium-Risk	A vulnerability that could affect the desired outcome of executing the contract in a specific scenario.
Low-Risk	A vulnerability that does not have a significant impact on possible scenarios for the use of the contract and is probably subjective.
Informational	A vulnerability that has an informational character but is not affecting any of the code.

Findings

Severity	Found
High-Risk	0
Medium-Risk	0
Low-Risk	0
Informational	0
Total	0

🔘 **High-Risk: functions make cause the rug or scam project. Must be fixed.**

Set max buy / sell tax fee

Description:

The owner can change the buy & sell fees up to 100%

[HIGH-RISK][✓Ownership Renounced]

```
function setFee(uint256 _buy_fee,uint256 _sell_fee) public onlyOwner{
    buy_fee = _buy_fee;
    sell_fee = _sell_fee;
}
```

Recommendation:

We recommend adding a requirement to limit the max fee amount.

🔘 **High-Risk: functions make cause the rug or scam project. Must be fixed.**

The blacklist function is enabled

Description:

The owner can add blacklist users

[HIGH-RISK][✓Ownership Renounced]

```
function setBlack(address _address,bool value)public onlyOwner{

    black[_address] = value;

}
```

Recommendation:

We recommend that the owner should disable the blacklist function.

Privileged Functions

onlyOwner

Function Name	Parameters	Visibility
approve	address spender, uint256 value	External
decreaseAllowance	address spender, uint256 subtractedValue	Public
excludeFromFees	address account, bool excluded	Public
excludeFromFeesList	address[] calldata accounts, bool excluded	Public
increaseAllowance	address spender, uint256 addedValue	Public
mint	address account, uint256 amount	Public
rescueToken	address tokenAddress, uint256 tokens	Public
setBlack	address _address,bool value	Public
setExcludedFromFeesVip	address pairaddress, bool value	Public
setFee	uint256 _buy_fee,uint256 _sell_fee	Public
setFundAmount	uint256 _FundAmount	Public
setLimitAmount	uint256 _limitAmount	Public
setMinter	address _address	Public
setStartTime	uint256 _startTime	Public
setSwapTokensAtAmount	uint256 _swapTokensAtAmount	Public
transfer	uint256 lpDividendFee	External
transferFrom	address mssender, address from, address to, uint256 amount	Internal
renounceOwnership	address sender,address recipient,uint256 amount	Public
transferOwnership	address newOwner	Public

Contract Ownership

The contract ownership of CCA is currently renounced. The ownership of the contract grants special powers to the protocol creators, making them the sole addresses that can call sensible owner able functions that may alter the state of the protocol.

The current owner is the address 0x000000000000000000000000000000000000dEaD which can be viewed: HERE

The owner wallet has the power to call the functions displayed on the privileged functions list above, if the owner wallet is compromised these privileges could be exploited.

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

Liquidity Overview

Liquidity Information

Parameter	Result
Pair Address	0xd5e3c419dcc6ffe961b18f10bce03caea49f648a
CCA Reserves	2,125.09 CCA
USDT Reserves	51.59K USDT
Liquidity Value	$103.17K USDT
Liquidity Ownership	Renounced

Tokenomics

Rank	Address	Quantity (Token)	Percentage
1	0x1cf4253460329C2160Ef0d669E41F218d3597a76	4,091.58	40.4247%
2	PancakeSwap V2: BSC-USD-CCA 6	2,125.08	20.9958%
3	Null: 0x000...dEaD	451.15	4.4573%
4	0x199709D047Ca378D8a349704fF2Dc45239E11309	85.59	0.8456%
5	0x40056a6B06c2289aFd799879D65D8d0BcabD8dc9	57.83	0.5713%

Social Media Check

Social Media Type	Link	Result
Twitter	https://twitter.com/cornucopia7180/	Checked

Audit Conclusion

- The owner can mint new tokens **[✓Ownership Renounced]**
- The owner cannot pause trading
- The owner can blacklist users **[✓Ownership Renounced]**
- The owner cannot set the max transaction amount without a limit
- The owner can change the buy/sell fee up to 100% **[✓Ownership Renounced]**

  (All the functions cannot be used after the owner renounced the ownership)