Cyberscope

A TAC Security Company

Audit Report

CRTAI

June 2025

Network	BSC
Address	0x6F87e50ff96aB9231E79dF1F816a00ed2bb0890C
Audited by	© cyberscope

Analysis

🔴 Critical 🟠 Medium ⚪ Minor / Informative ● Pass

Severity	Code	Description	Status
●	ST	Stops Transactions	Passed
●	OTUT	Transfers User's Tokens	Passed
●	ELFM	Exceeds Fees Limit	Passed
●	MT	Mints Tokens	Passed
●	BT	Burns Tokens	Passed
●	BC	Blacklists Addresses	Passed

Diagnostics

● Critical ● Medium ● Minor / Informative

Severity	Code	Description	Status
●	RFD	Redundant Function Definitions	Unresolved
●	UDO	Unnecessary Decimals Override	Unresolved

Table of Contents

Risk Classification

The criticality of findings in Cyberscope's smart contract audits is determined by evaluating multiple variables. The two primary variables are:

1. **Likelihood of Exploitation**: This considers how easily an attack can be executed, including the economic feasibility for an attacker.
2. **Impact of Exploitation**: This assesses the potential consequences of an attack, particularly in terms of the loss of funds or disruption to the contract's functionality.

Based on these variables, findings are categorized into the following severity levels:

1. **Critical**: Indicates a vulnerability that is both highly likely to be exploited and can result in significant fund loss or severe disruption. Immediate action is required to address these issues.
2. **Medium**: Refers to vulnerabilities that are either less likely to be exploited or would have a moderate impact if exploited. These issues should be addressed in due course to ensure overall contract security.
3. **Minor**: Involves vulnerabilities that are unlikely to be exploited and would have a minor impact. These findings should still be considered for resolution to maintain best practices in security.
4. **Informative**: Points out potential improvements or informational notes that do not pose an immediate risk. Addressing these can enhance the overall quality and robustness of the contract.

Severity	Likelihood / Impact of Exploitation
● Critical	Highly Likely / High Impact
● Medium	Less Likely / High Impact or Highly Likely/ Lower Impact
● Minor / Informative	Unlikely / Low to no Impact

Review

Contract Name	CRTAI
Compiler Version	v0.8.20+commit.a1b79de6
Optimization	200 runs
Explorer	https://bscscan.com/address/0x6f87e50ff96ab9231e79df1f816a00ed2bb0890c
Address	0x6f87e50ff96ab9231e79df1f816a00ed2bb0890c
Network	BSC
Symbol	CRTAI
Decimals	18
Total Supply	1,000,000,000
Badge Eligibility	Yes

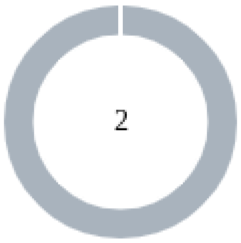
Audit Updates

Initial Audit	20 Jun 2025

Source Files

Filename	SHA256
contracts/CRTAI.sol	b23e503f166091395b9816dd3eb1c6c093d4364c9d3caa6e086cacfee5e10cfd

Findings Breakdown



●	Critical	0
●	Medium	0
●	Minor / Informative	2

Severity		Unresolved	Acknowledged	Resolved	Other
●	Critical	0	0	0	0
●	Medium	0	0	0	0
●	Minor / Informative	2	0	0	0

RFD - Redundant Function Definitions

Criticality	Minor / Informative
Location	contracts/CRTAI.sol#L48,56
Status	Unresolved

Description

The contract includes two functions that do not contribute meaningfully to the intended logic or functionality of the system. The `isMintable()` function is declared and returns a constant `false` value, while the contract does not implement or support any minting mechanisms, rendering the function misleading and unnecessary. Additionally, the `renounceOwnership()` function is explicitly redeclared without any additional logic, despite being fully available through inheritance from the `Ownable` contract. These redundant declarations may increase contract size and complexity without providing functional value.

```
    function isMintable() public pure returns (bool) {
         return false;
    }

     function renounceOwnership() public override onlyOwner {
         super.renounceOwnership();
    }
```

Recommendation

It is recommended to remove both the `isMintable()` and the redeclared `renounceOwnership()` functions to optimise the contract's size and clarity. Removing unused or duplicate functions improves maintainability, reduces potential confusion for integrators and auditors, and may slightly reduce deployment and execution costs.

UDO - Unnecessary Decimals Override

Criticality	Minor / Informative
Location	contracts/CRTAI.sol#L33
Status	Unresolved

Description

The contract is currently implementing an override of the decimals function, which simply returns the value 18. This override is redundant since the extending token contract already specifies 18 decimals as its standard. In the context of ERC-20 tokens, 18 decimals is a common default, and overriding this function to return the same value adds unnecessary complexity to the contract. This redundancy does not contribute to the functionality of the contract and could potentially lead to confusion about the necessity of this override.

```
function decimals() public view virtual override returns
(uint8) {
    return 18;
}
```

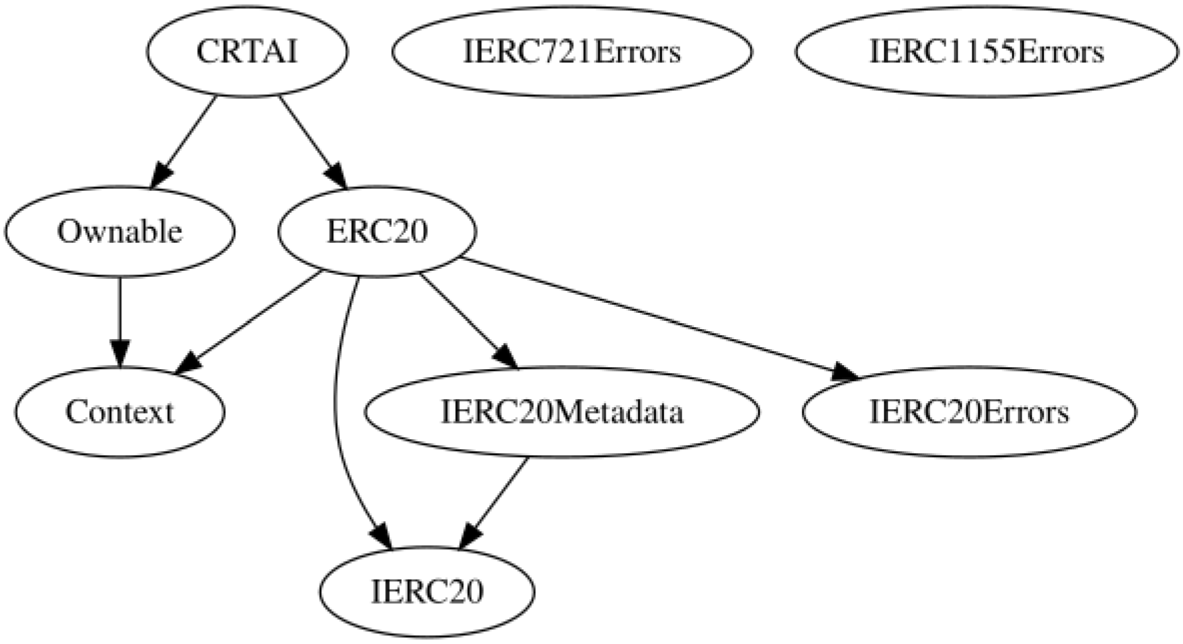
Recommendation

Since the inherited ERC-20 contract already defines the decimals number, maintaining an overriding function that merely repeats this value does not contribute to the contract's effectiveness. As a result, it is recommended to remove the redundant `decimals` function from the contract. Removing this function will simplify the contract, making it more straightforward to maintain without impacting its operational capabilities.

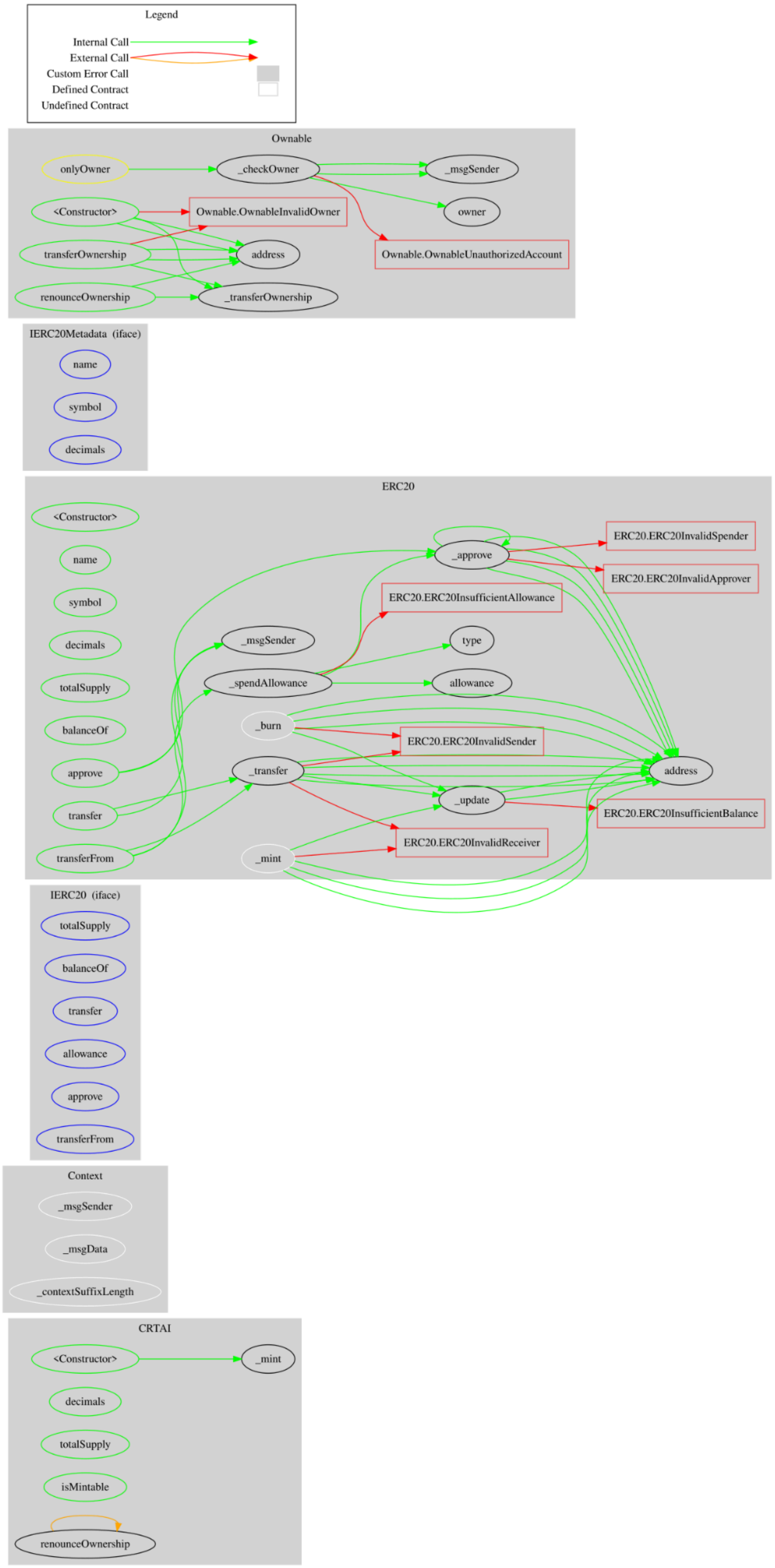
Functions Analysis

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
CRTAI	Implementation	ERC20, Ownable		
		Public	✓	ERC20 Ownable
	decimals	Public		-
	totalSupply	Public		-
	isMintable	Public		-
	renounceOwnership	Public	✓	onlyOwner

Inheritance Graph



Flow Graph


Legend
Internal Call
External Call
Custom Error Call
Defined Contract
Undefined Contract
Ownable
onlyOwner
_checkOwner
_msgSender
<Constructor>
Ownable.OwnableInvalidOwner
owner
transferOwnership
address
Ownable.OwnableUnauthorizedAccount
renounceOwnership
_transferOwnership
IERC20Metadata (iface)
name
symbol
decimals
ERC20
<Constructor>
name
symbol
decimals
totalSupply
balanceOf
approve
transfer
transferFrom
_approve
ERC20.ERC20InvalidSpender
ERC20.ERC20InvalidApprover
ERC20.ERC20InsufficientAllowance
_msgSender
type
_spendAllowance
allowance
_burn
ERC20.ERC20InvalidSender
_transfer
address
_update
ERC20.ERC20InsufficientBalance
_mint
ERC20.ERC20InvalidReceiver
IERC20 (iface)
totalSupply
balanceOf
transfer
allowance
approve
transferFrom
Context
_msgSender
_msgData
_contextSuffixLength
CRTAI
<Constructor>
_mint
decimals
totalSupply
isMintable
renounceOwnership

Summary

CRTAI contract implements a token mechanism. This audit investigates security issues, business logic concerns, and potential improvements. CRTAI is an interesting project that has a friendly and growing community. The Smart Contract analysis reported no compiler errors or critical issues. The contract Owner can access some admin functions that can not be used in a malicious way to disturb the users' transactions.

Disclaimer

The information provided in this report does not constitute investment, financial or trading advice and you should not treat any of the document's content as such. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes nor may copies be delivered to any other person other than the Company without Cyberscope’s prior written consent. This report is not nor should be considered an “endorsement” or “disapproval” of any particular project or team. This report is not nor should be regarded as an indication of the economics or value of any “product” or “asset” created by any team or project that contracts Cyberscope to perform a security assessment. This document does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors' business, business model or legal compliance. This report should not be used in any way to make decisions around investment or involvement with any particular project. This report represents an extensive assessment process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk Cyberscope’s position is that each company and individual are responsible for their own due diligence and continuous security Cyberscope’s goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies and in no way claims any guarantee of security or functionality of the technology we agree to analyze. The assessment services provided by Cyberscope are subject to dependencies and are 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.

About Cyberscope

Cyberscope is a TAC blockchain cybersecurity company that was founded with the vision to make web3.0 a safer place for investors and developers. Since its launch, it has worked with thousands of projects and is estimated to have secured tens of millions of investors' funds.

Cyberscope is one of the leading smart contract audit firms in the crypto space and has built a high-profile network of clients and partners.

A *TAC Security* Company

The Cyberscope team

cyberscope.io