Cyberscope

Audit Report

Wuacoin

June 2023

Network BSC

Address 0xE489248B132eA8E29788cEd5fB5e68a609cd8C79

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
Medium	MTA	Maximum Token Approval	Unresolved
Minor / Informative	RVD	Redundant Variable Declaration	Unresolved
Minor / Informative	L19	Stable Compiler Version	Unresolved

Table of Contents

Review

Contract Name	WuaoCoin
Compiler Version	v0.8.19+commit.7dd6d404
Optimization	200 runs
Explorer	https://bscscan.com/address/0xe489248b132ea8e29788ced5fb5e68a609cd8c79
Address	0xe489248b132ea8e29788ced5fb5e68a609cd8c79
Network	BSC
Symbol	WUAO
Decimals	18
Total Supply	100,000,000

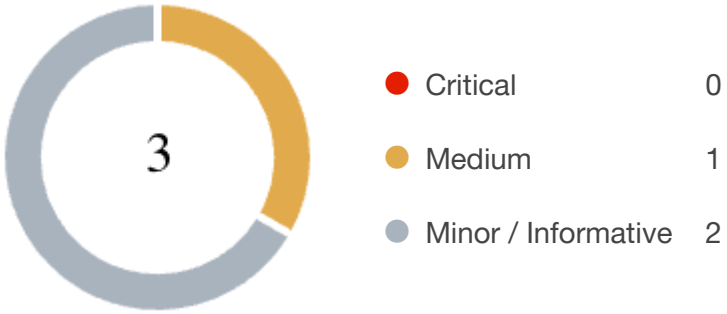
Audit Updates

Initial Audit	01 Jun 2023 https://github.com/cyberscope-io/audits/blob/main/v1/wuao/BSC.pdf
Corrected Phase 2	07 Jun 2023

Source Files

Filename	SHA256
contracts/WUAO_AUDI.sol	c3bcb134fc1ab2c655c6ebc9d8a46b3da17efa641d93562de5d9dc47f7509d12

Findings Breakdown



Severity	Unresolved	Acknowledged	Resolved	Other
Critical	0	0	0	0
Medium	1	0	0	0
Minor / Informative	2	0	0	0

MTA - Maximum Token Approval

Criticality	Medium
Location	contracts/WUAO_AUDI.sol#L48
Status	Unresolved

Description

In the current implementation, the approve method performs a balance check on the user's account before allowing the specified amount to be approved for transfer. While it may seem like a precautionary measure to prevent potential overspending, it is redundant in the context of the approve allowance method. In the contrary, it may produce issues with decentralized applications where the user's balance may be more than the current.

The purpose of the approve method is to grant permission to another address to spend a specific amount of tokens from the user's account. It does not involve an immediate transfer of funds. The balance check within the approve method is unnecessary because the actual transfer will be validated and executed when the approved amount is spent by the authorized address using the transferFrom method.

It is important to note that while the balance check can be removed from the approve method, appropriate balance validations must still be performed during the execution of the transferFrom method to ensure that the approved amount does not exceed the user's available balance. This will safeguard against overspending and maintain the contract's security.

```
function approve(address spender, uint tokens) override public returns (bool
success) {
    require (balances[msg.sender] > tokens,"Sender without balance!");
    allowed[msg.sender][spender] = tokens;
    emit Approval(msg.sender, spender, tokens);
    success = true;
}
```

Recommendation

The approve method should focus solely on updating the allowance for the authorized address without involving balance checks. This ensures that the method's execution is optimized and aligned with its intended purpose.

RVD - Redundant Variable Declaration

Criticality	Minor / Informative
Location	contracts/WUAO_AUDI.sol#L24
Status	Unresolved

Description

There are code segments that could be optimized. A segment may be optimized so that it becomes a smaller size, consumes less memory, executes more rapidly, or performs fewer operations.

The contract declares certain variables that are not used in a meaningful way by the contract. As are result, these variables are redundant.

```
address private immutable manager
```

Recommendation

The team is advised to take these segments into consideration and rewrite them so the runtime will be more performant. That way it will improve the efficiency and performance of the source code and reduce the cost of executing it.

L19 - Stable Compiler Version

Criticality	Minor / Informative
Location	contracts/WUAO_AUDI.sol#L2
Status	Unresolved

Description

The `^` symbol indicates that any version of Solidity that is compatible with the specified version (i.e., any version that is a higher minor or patch version) can be used to compile the contract. The version lock is a mechanism that allows the author to specify a minimum version of the Solidity compiler that must be used to compile the contract code. This is useful because it ensures that the contract will be compiled using a version of the compiler that is known to be compatible with the code.

```
pragma solidity ^0.8.19;
```

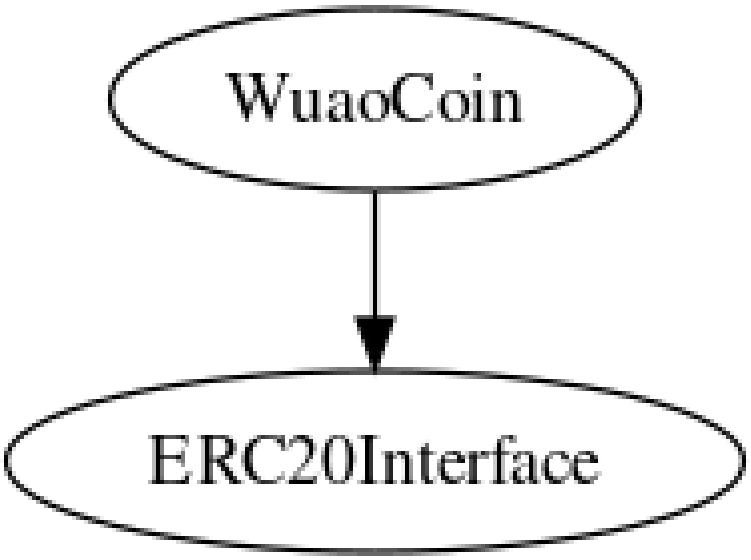
Recommendation

The team is advised to lock the pragma to ensure the stability of the codebase. The locked pragma version ensures that the contract will not be deployed with an unexpected version. An unexpected version may produce vulnerabilities and undiscovered bugs. The compiler should be configured to the lowest version that provides all the required functionality for the codebase. As a result, the project will be compiled in a well-tested LTS (Long Term Support) environment.

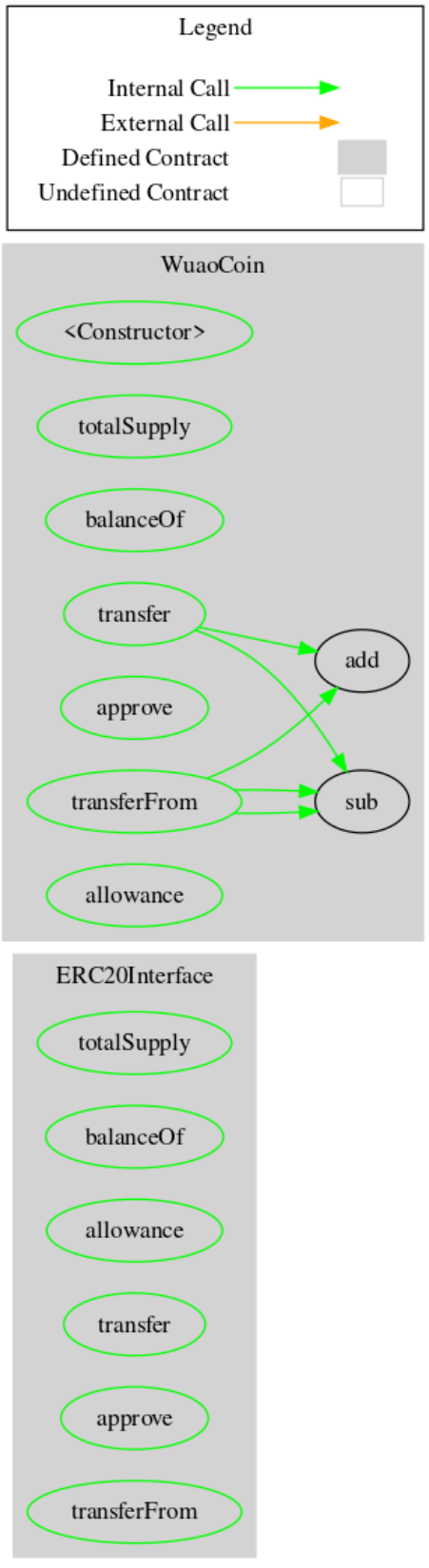
Functions Analysis

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
ERC20Interface	Implementation			
	totalSupply	Public		-
	balanceOf	Public		-
	allowance	Public		-
	transfer	Public	✓	-
	approve	Public	✓	-
	transferFrom	Public	✓	-
WuaoCoin	Implementation	ERC20Interface		
		Public	✓	-
	totalSupply	Public		-
	balanceOf	Public		-
	transfer	Public	✓	-
	approve	Public	✓	-
	transferFrom	Public	✓	-
	allowance	Public		-
	add	Internal		
	sub	Internal		

Inheritance Graph



Flow Graph


Legend
Internal Call
External Call
Defined Contract
Undefined Contract
WuaoCoin
<Constructor>
totalSupply
balanceOf
transfer
approve
transferFrom
allowance
add
sub
ERC20Interface
totalSupply
balanceOf
allowance
transfer
approve
transferFrom

Summary

Wuacoin contract implements a token mechanism. This audit investigates security issues, business logic concerns, and potential improvements. Wuacoin is an interesting project that has a friendly and growing community. The Smart Contract may face some issues because of the approval threshold. 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 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.

The Cyberscope team

https://www.cyberscope.io