Cyberscope

Audit Report
Walletika

January 2024

Network	BSC
Address	0x9eE10d2E9571AecfE5a604aF7fE71B96eBa84b7b
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
●	OCTD	Transfers Contract's Tokens	Acknowledged
●	L02	State Variables could be Declared Constant	Acknowledged

Table of Contents

Review

Contract Name	WalletikaToken
Compiler Version	v0.6.12+commit.27d51765
Optimization	200 runs
Explorer	https://bscscan.com/address/0x9ee10d2e9571aecfe5a604af7fe71b96eba84b7b
Address	0x9ee10d2e9571aecfe5a604af7fe71b96eba84b7b
Network	BSC
Symbol	WLTK
Decimals	18
Total Supply	100,000,000
Badge Eligibility	Yes

Audit Updates

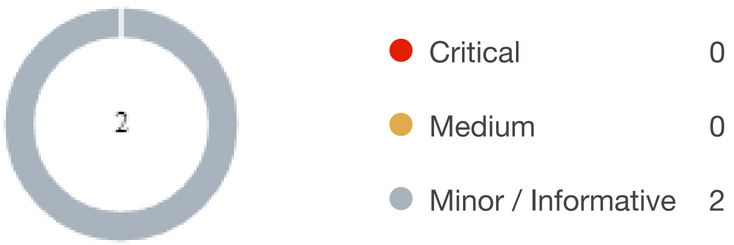
Initial Audit	29 Dec 2023
Acknowledged Phase	10 Jan 2024

Source Files

Filename	SHA256
WalletikaToken.sol	1ea5c17ee425ec7489f2389c8885425f307de915d3f9a4fffdd2dcd1d95d5e66

SafeMath.sol	2434d0a668584602239efef65445bf680fe0e2cc07510e30f4fc15f53a34630b
Ownable.sol	6f3cd49341a2d77dd19cdccc4544df17af1c7de335e93a988600ae41f2eca088
IBEP20.sol	a35a3fa2d4a42413a0d5d04712e43b301bd3fc40721261e2f0571ef57f93d8c1
Context.sol	a246695d446d1b5fe3413757b13fd66ef9b72d21316f7efc27d0930506443a48
BEP20.sol	90e5a76179f67688aff64f63311a11636c8546dc26fa2706a761df94c0eb9955
Address.sol	35b53645660016443e38835b9a0e2f7f92b3dbd6684aba9784b4155af673ce53

Findings Breakdown



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

OCTD - Transfers Contract's Tokens

Criticality	Minor / Informative
Location	WalletikaToken.sol#L33
Status	Acknowledged

Description

The contract owner has the authority to claim all the balance of the contract. The owner may take advantage of it by calling the `recoverToken` function.

```
function recoverToken(address tokenAddress, uint256 amount)
external onlyOwner returns (bool) {
  return IBEP20(tokenAddress).transfer(owner(), amount);
}
```

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.

Temporary Solutions:

These measurements do not decrease the severity of the finding

- Introduce a time-locker mechanism with a reasonable delay.
- Introduce a multi-signature wallet so that many addresses will confirm the action.
- Introduce a governance model where users will vote about the actions.

Permanent Solution:

- Renouncing the ownership, which will eliminate the threats but it is non-reversible.

Team Update

The team has acknowledged that this is not a security issue and states: *This function is required to handle the transfer of tokens that have been accidentally sent to the contract address. It allows for the return of these tokens back to their original sender.*

L02 - State Variables could be Declared Constant

Criticality	Minor / Informative
Location	WalletikaToken.sol#L8
Status	Acknowledged

Description

State variables can be declared as constant using the constant keyword. This means that the value of the state variable cannot be changed after it has been set. Additionally, the constant variables decrease gas consumption of the corresponding transaction.

```
uint256 private _maxSupply = 100000000e18
```

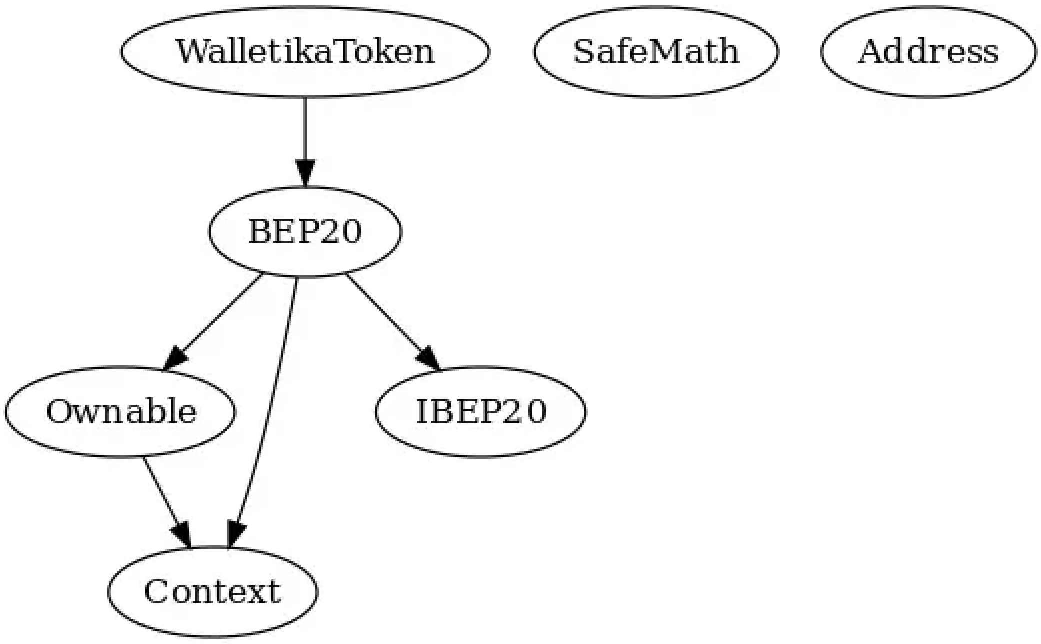
Recommendation

Constant state variables can be useful when the contract wants to ensure that the value of a state variable cannot be changed by any function in the contract. This can be useful for storing values that are important to the contract's behavior, such as the contract's address or the maximum number of times a certain function can be called. The team is advised to add the constant keyword to state variables that never change.

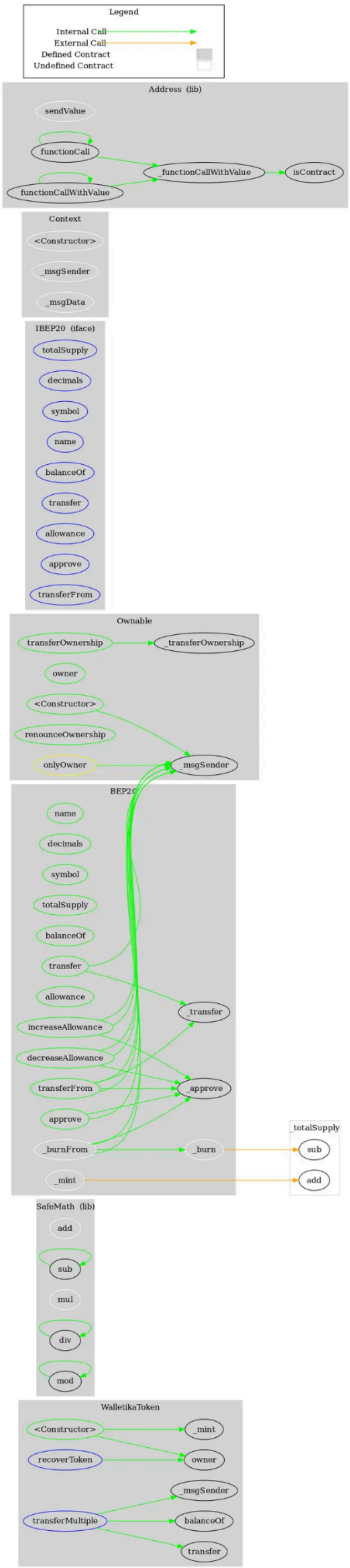
Functions Analysis

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
WalletikaToken	Implementation	BEP20		
		Public	✓	-
	transferMultiple	External	✓	-
	recoverToken	External	✓	onlyOwner

Inheritance Graph



Flow Graph


Legend
Internal Call
External Call
Defined Contract
Undefined Contract
Address (lib)
sendValue
functionCall
functionCallWithValue
_functionCallWithValue
isContract
Context
<Constructor>
_msgSender
_msgData
IBEP20 (iface)
totalSupply
decimals
symbol
name
balanceOf
transfer
allowance
approve
transferFrom
Ownable
transferOwnership
_transferOwnership
owner
<Constructor>
renounceOwnership
onlyOwner
_msgSender
BEP20
name
decimals
symbol
totalSupply
balanceOf
transfer
allowance
increaseAllowance
decreaseAllowance
transferFrom
approve
_burnFrom
_mint
_transfer
_approve
_burn
_totalSupply
sub
add
SafeMath (lib)
add
sub
mul
div
mod
WalletikaToken
<Constructor>
recoverToken
transferMultiple
_mint
owner
_msgSender
balanceOf
transfer

Summary

Walletika contract implements a token mechanism. This audit investigates security issues, business logic concerns and potential improvements. Walletika is an interesting project that has a friendly and growing community. The Smart Contract analysis reported no compiler error 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 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