



Smart Contract Audit

FOR
AiWallet
DATED : 19 FEB 23'



AUDIT SUMMARY

Project name – AiWallet Token

Date: 19 February, 2023

Scope of Audit- Audit Ace was consulted to conduct the smart contract audit of the solidity source codes.

Audit Status: **Passed**

Issues Found

Status	Critical	High	Medium	Low	Suggestion
Open	0	0	0	0	2
Acknowledged	0	0	0	0	0
Resolved	0	0	0	0	0

USED TOOLS

Tools:

1- Manual Review:

a line by line code review has been performed by audit ace team.

2- BSC Test network:

All tests were done on BSC Test network, each test has its transaction has attached to it. You can check this tests in “functionality tests” section of the report.

3- Slither : Static Analysis



TESTNET LINKS

All tests were done using this contract, BSC Testnet (main token is on ethereum chain):

<https://testnet.bscscan.com/token/0xCde3990f4E476f7e7F23e8A083Ead4aCe9082877>

Token Address: :

0xc5A927AD2d1a92Dc5f9662Ce03F7140a8B738B19

Checksum:

50e721e49c013f00c62cf59f2163542a9d8df02464ef
eb615d31051b0fddc326

Deployer:

0xd6DF4789a95fC2080d8f8E989D0602374E1Eaa89

Owner:

0xd6DF4789a95fC2080d8f8E989D0602374E1Eaa89



TOKEN OVERVIEW

Fees:

Buy Fees: up to 10%

Sell Fees: up to 10%

Transfer Fees: up to 10%

Fees Privilege: owner

Ownership : Owned

Minting: No mint function

Max Tx Amount/ Max Wallet Amount:NO

Blacklist: No

Other Privileges: none



AUDIT METHODOLOGY

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

- Review of the specifications, sources, and instructions provided to Auditace 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 codebase 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 Auditace 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 analysing a program to determine what inputs cause each part of a program to execute.
 - Reviewing the codebase to improve maintainability, security, and control based on the established industry and academic practices.
-

VULNERABILITY CHECKLIST

- | | |
|--|---|
|  Return values of low-level calls |  Gasless Send |
|  Private modifier |  Using block.timestamp |
|  Multiple Sends |  Re-entrancy |
|  Using Suicide |  Tautology or contradiction |
|  Gas Limitand Loops |  Timestamp Dependence |
|  Address hardcoded |  Revert/require functions |
|  Exception Disorder |  Use of tx.origin |
|  Using inline assembly |  Integer overflow/underflow |
|  Divide before multiply |  Dangerous strict equalities |
|  Missing Zero Address Validation |  Using SHA3 |
|  Compiler version not fixed |  Using throw |
-



CLASSIFICATION OF RISK

Severity

Description

◆ Critical

These vulnerabilities could be exploited easily and can lead to asset loss, data loss, asset, or data manipulation. They should be fixed right away.

◆ 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.

◆ Gas Optimization /Suggestion

A vulnerability that has an informational character but is not affecting any of the code.

Findings

Severity

Found

◆ Critical

0

◆ High-Risk

0

◆ Medium-Risk

0

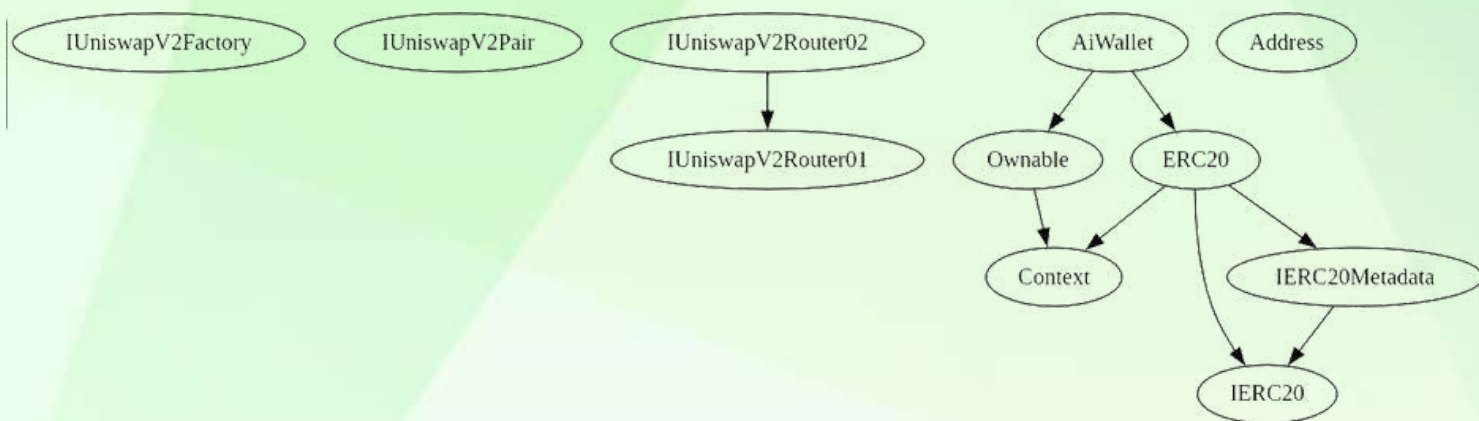
◆ Low-Risk

0

◆ Gas Optimization / Suggestions

2

INHERITANCE TREE





POINTS TO NOTE

- Owner is not able to set buy/sell/transfer taxes over 10%
 - Owner is not able to blacklist an arbitrary wallet
 - Owner is not able to set max buy/sell/transfer amounts
 - Owner is not able to disable trades
 - Owner is not able to mint new tokens
-

CONTRACT ASSESMENT

Contract	Type	Bases			
:-----: :-----: :-----: :-----: :-----:					
L	**Function Name**	**Visibility**	**Mutability**	**Modifiers**	
IUniswapV2Factory Interface					
L	feeTo	External !	NO !		
L	feeToSetter	External !	NO !		
L	getPair	External !	NO !		
L	allPairs	External !	NO !		
L	allPairsLength	External !	NO !		
L	createPair	External !	● NO !		
L	setFeeTo	External !	● NO !		
L	setFeeToSetter	External !	● NO !		
IUniswapV2Pair Interface					
L	name	External !	NO !		
L	symbol	External !	NO !		
L	decimals	External !	NO !		
L	totalSupply	External !	NO !		
L	balanceOf	External !	NO !		
L	allowance	External !	NO !		
L	approve	External !	● NO !		
L	transfer	External !	● NO !		
L	transferFrom	External !	● NO !		
L	DOMAIN_SEPARATOR	External !	NO !		
L	PERMIT_TYPEHASH	External !	NO !		
L	nonces	External !	NO !		
L	permit	External !	● NO !		
L	MINIMUM_LIQUIDITY	External !	NO !		
L	factory	External !	NO !		
L	token0	External !	NO !		
L	token1	External !	NO !		
L	getReserves	External !	NO !		
L	price0CumulativeLast	External !	NO !		
L	price1CumulativeLast	External !	NO !		
L	kLast	External !	NO !		
L	mint	External !	● NO !		
L	burn	External !	● NO !		
L	swap	External !	● NO !		
L	skim	External !	● NO !		
L	sync	External !	● NO !		
L	initialize	External !	● NO !		



CONTRACT ASSESMENT

|||||

| ****IUniswapV2Router01**** | Interface | |||

| | factory | External ! | | NO ! |

| | WETH | External ! | | NO ! |

| | addLiquidity | External ! | ● | NO ! |

| | addLiquidityETH | External ! | 🟢 | NO ! |

| | removeLiquidity | External ! | ● | NO ! |

| | removeLiquidityETH | External ! | ● | NO ! |

| | removeLiquidityWithPermit | External ! | ● | NO ! |

| | removeLiquidityETHWithPermit | External ! | ● | NO ! |

| | swapExactTokensForTokens | External ! | ● | NO ! |

| | swapTokensForExactTokens | External ! | ● | NO ! |

| | swapExactETHForTokens | External ! | 🟢 | NO ! |

| | swapTokensForExactETH | External ! | ● | NO ! |

| | swapExactTokensForETH | External ! | ● | NO ! |

| | swapETHForExactTokens | External ! | 🟢 | NO ! |

| | quote | External ! | | NO ! |

| | getAmountOut | External ! | | NO ! |

| | getAmountIn | External ! | | NO ! |

| | getAmountsOut | External ! | | NO ! |

| | getAmountsIn | External ! | | NO ! |

|||||

| ****IUniswapV2Router02**** | Interface | IUniswapV2Router01 |||

| | removeLiquidityETHSupportingFeeOnTransferTokens | External ! | ● | NO ! |

| | removeLiquidityETHWithPermitSupportingFeeOnTransferTokens | External ! | ● | NO ! |

|

| | swapExactTokensForTokensSupportingFeeOnTransferTokens | External ! | ● | NO ! |

| | swapExactETHForTokensSupportingFeeOnTransferTokens | External ! | 🟢 | NO ! |

| | swapExactTokensForETHSupportingFeeOnTransferTokens | External ! | ● | NO ! |

|||||

| ****IERC20**** | Interface | |||

| | totalSupply | External ! | | NO ! |

| | balanceOf | External ! | | NO ! |

| | transfer | External ! | ● | NO ! |

| | allowance | External ! | | NO ! |

| | approve | External ! | ● | NO ! |

| | transferFrom | External ! | ● | NO ! |

|||||

| ****IERC20Metadata**** | Interface | IERC20 |||

| | name | External ! | | NO ! |

| | symbol | External ! | | NO ! |


| | decimals | External ! | | NO ! |



CONTRACT ASSESMENT



|||||



| ****Address**** | Library | |||



| | isContract | Internal  | |

| | sendValue | Internal  |  | |

| | functionCall | Internal  |  | |



| | functionCall | Internal  |  | |

| | functionCallWithValue | Internal  |  | |


| | functionCallWithValue | Internal  |  | |

| | functionStaticCall | Internal  | |

| | functionStaticCall | Internal  | |

| | functionDelegateCall | Internal  |  | |

| | functionDelegateCall | Internal  |  | |


| | verifyCallResultFromTarget | Internal  | |

| | verifyCallResult | Internal  | |

| | _revert | Private  | |

|||||

| ****Context**** | Implementation | |||

| | _msgSender | Internal  | |

| | _msgData | Internal  | |

|||||

| ****Ownable**** | Implementation | Context |||

| | <Constructor> | Public  |  | NO  |

| | owner | Public  | | NO  |

| | renounceOwnership | Public  |  | onlyOwner |

| | transferOwnership | Public  |  | onlyOwner |

|||||

| ****ERC20**** | Implementation | Context, IERC20, IERC20Metadata |||

| | <Constructor> | Public  |  | NO  |

| | name | Public  | | NO  |

| | symbol | Public  | | NO  |

| | decimals | Public  | | NO  |

| | totalSupply | Public  | | NO  |

| | balanceOf | Public  | | NO  |

| | transfer | Public  |  | NO  |

| | allowance | Public  | | NO  |

| | approve | Public  |  | NO  |

| | transferFrom | Public  |  | NO  |

| | increaseAllowance | Public  |  | NO  |

| | decreaseAllowance | Public  |  | NO  |

| | _transfer | Internal  |  | |

| | _mint | Internal  |  | |

| | _burn | Internal  |  | |

CONTRACT ASSESMENT

```

|  | _approve | Internal | 🔒 | ● | |
|  | _beforeTokenTransfer | Internal | 🔒 | ● | |
|  | _afterTokenTransfer | Internal | 🔒 | ● | |
|||||
| **AiWallet** | Implementation | ERC20, Ownable |||
|  | <Constructor> | Public | ! | ● | ERC20 |
|  | <Receive Ether> | External | ! | 💰 | NO ! |
|  | claimStuckTokens | External | ! | ● | onlyOwner |
|  | excludeFromFees | External | ! | ● | onlyOwner |
|  | isExcludedFromFees | Public | ! | | NO ! |
|  | updateBuyFees | External | ! | ● | onlyOwner |
|  | updateSellFees | External | ! | ● | onlyOwner |
|  | updateWalletToWalletTransferFee | External | ! | ● | onlyOwner |
|  | changeMarketingWallet | External | ! | ● | onlyOwner |
|  | _transfer | Internal | 🔒 | ● | |
|  | setSwapEnabled | External | ! | ● | onlyOwner |
|  | setSwapTokensAtAmount | External | ! | ● | onlyOwner |
|  | swapAndSendFee | Private | 🔒 | ● | |

```

| Symbol | Meaning |

|:-----:|-----|

| ● | Function can modify state |

| 💰 | Function is payable |



STATIC ANALYSIS

A static analysis of contract's source code has been performed using slither. No major issues were found in the output

```
Address.revert(bytes,string) (contracts/Token.sol#329-341) is never used and should be removed
Address.functionCall(address,bytes) (contracts/Token.sol#242-244) is never used and should be removed
Address.functionCall(address,bytes,string) (contracts/Token.sol#246-252) is never used and should be removed
Address.functionCallWithValue(address,bytes,uint256) (contracts/Token.sol#254-260) is never used and should be removed
Address.functionCallWithValue(address,bytes,uint256,string) (contracts/Token.sol#262-271) is never used and should be removed
Address.functionDelegateCall(address,bytes) (contracts/Token.sol#286-288) is never used and should be removed
Address.functionDelegateCall(address,bytes,string) (contracts/Token.sol#290-297) is never used and should be removed
Address.functionStaticCall(address,bytes) (contracts/Token.sol#273-275) is never used and should be removed
Address.functionStaticCall(address,bytes,string) (contracts/Token.sol#277-284) is never used and should be removed
Address.isContract(address) (contracts/Token.sol#231-233) is never used and should be removed
Address.verifyCallResult(bool,bytes,string) (contracts/Token.sol#317-327) is never used and should be removed
Address.verifyCallResultFromTarget(address,bool,bytes,string) (contracts/Token.sol#299-315) is never used and should be removed
Context.msgData() (contracts/Token.sol#349-352) is never used and should be removed
ERC20_burn(address,uint256) (contracts/Token.sol#503-510) is never used and should be removed
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code

Pragma version0.8.17 (contracts/Token.sol#7) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.16
solc-0.8.17 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity

Low level call in Address.sendValue(address,uint256) (contracts/Token.sol#235-240):
- (success) = recipient.call(value: amount)() (contracts/Token.sol#230)
Low level call in Address.functionCallWithValue(address,bytes,uint256,string) (contracts/Token.sol#262-271):
- (success, returndata) = target.call(value: value)(data) (contracts/Token.sol#260)
Low level call in Address.functionStaticCall(address,bytes,string) (contracts/Token.sol#277-284):
- (success, returndata) = target.staticcall(data) (contracts/Token.sol#282)
Low level call in Address.functionDelegateCall(address,bytes,string) (contracts/Token.sol#290-297):
- (success, returndata) = target.delegatecall(data) (contracts/Token.sol#295)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#low-level-calls

Function IUniswapV2Pair.DOMAIN_SEPARATOR() (contracts/Token.sol#37) is not in mixedCase
Function IUniswapV2Pair.PERMIT_TYPEHASH() (contracts/Token.sol#38) is not in mixedCase
Function IUniswapV2Pair.MINIMUM_LIQUIDITY() (contracts/Token.sol#55) is not in mixedCase
Function IUniswapV2Router01.WETH() (contracts/Token.sol#75) is not in mixedCase
Parameter AIWallet.updateBuyFees(uint256).feeOnBuy (contracts/Token.sol#646) is not in mixedCase
Parameter AIWallet.updateSellFees(uint256).feeOnSell (contracts/Token.sol#654) is not in mixedCase
Parameter AIWallet.updateWalletToWalletTransferFee(uint256).walletToWalletTransferFee (contracts/Token.sol#662) is not in mixedCase
Parameter AIWallet.changeMarketingWallet(address).marketingWallet (contracts/Token.sol#669) is not in mixedCase
Parameter AIWallet.setSwapEnabled(bool).enabled (contracts/Token.sol#726) is not in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions

Redundant expression "this (contracts/Token.sol#350)" inContext (contracts/Token.sol#344-353)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#redundant-statements

Variable IUniswapV2Router01.addLiquidity(address,address,uint256,uint256,uint256,uint256,address,uint256).amountADesired (contracts/Token.sol#60) is too similar to IUniswapV2Router01.addLiquidity(address,address,uint256,uint256,uint256,uint256,address,uint256).amountBDesired (contracts/Token.sol#61)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#variable-names-too-similar

AIWallet.maxFee (contracts/Token.sol#556) should be immutable
AIWallet.uniswapV2Pair (contracts/Token.sol#549) should be immutable
AIWallet.uniswapV2Router (contracts/Token.sol#548) should be immutable
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-immutable
```



FUNCTIONAL TESTING

Functionality Tests

Router (PCS V2):

0xD99D1c33F9fC3444f8101754aBC46c52416550D1

increased fees to max limit

1- Adding liquidity (passed):

<https://testnet.bscscan.com/tx/0x1aec1d149b665a869efa526b7f1f4cde1d981f3c09450707b429f4360238409f>

2- Buying (marketing tax= 10% max) (passed):

<https://testnet.bscscan.com/tx/0x4973dc9e0d19a44378be4016e95f947bf5164dedb6b7163de8bf3b3373525da1>

3- Selling (marketing tax = 10% max) (passed):

<https://testnet.bscscan.com/tx/0xd46aefc3e79e21ed3689605f602cddb44c361dfcea9e2e8100d3d5129404f685>

4- Transferring (marketing tax = 10% max) (passed):

<https://testnet.bscscan.com/tx/0x20d057098e54b2d5848a449be62c9e3419f4cc271a7ea44c881f106ef2808c64>

5- Internal swap (passed):

this wallet received BNB from contract (internal swap)

marketing wallet:

<https://testnet.bscscan.com/address/0xd6df4789a95fc2080d8f8e989d0602374e1eaa89#internaltx>



MANUAL TESTING

Gas optimizations:

- Declare this variables as constant: `_nymbol` - `_symbol`

Suggestions:

- use indexed keyword to declare events





MANUAL TESTING

Critical Risk Findings:

NO RISKS WERE FOUND IN THE CONTRACT



Social Media Overview

**Here are the Social Media Accounts of
AiWallet**



https://t.me/aiwallet_chat



https://twitter.com/aiwallet_world



<https://aiwallet.world/>



DISCLAIMER

All the content provided in this document is for general information only and should not be used as financial advice or a reason to buy any investment. Team provides no guarantees against the sale of team tokens or the removal of liquidity by the project audited in this document. Always Do your own research and protect yourselves from being scammed. The Auditace team has audited this project for general information and only expresses their opinion based on similar projects and checks from popular diagnostic tools. Under no circumstances did Auditace receive a payment to manipulate those results or change the awarding badge that we will be adding in our website. Always Do your own research and protect yourselves from scams. This document should not be presented as a reason to buy or not buy any particular token. The Auditace team disclaims any liability for the resulting losses.



ABOUT AUDITACE

We specialize in providing thorough and reliable audits for Web3 projects. With a team of experienced professionals, we use cutting-edge technology and rigorous methodologies to evaluate the security and integrity of blockchain systems. We are committed to helping our clients ensure the safety and transparency of their digital assets and transactions.



<https://auditace.tech/>



https://t.me/Audit_Ace



https://twitter.com/auditace_



<https://github.com/Audit-Ace>
