



Smart Contract Audit

FOR

Particles

DATED : 23 September 23'



AUDIT SUMMARY

Project name – Particles

Date: 23 September 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	0
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 conducted on the BSC Test network, and each test has a corresponding transaction attached to it. These tests can be found in the "Functional Tests" section of the report.

3- Slither :

The code has undergone static analysis using Slither.

Testnet version:

The tests were performed using the contract deployed on the BSC Testnet, which can be found at the following address:

<https://testnet.bscscan.com/token/0xd5481c5536c97A066Ae3928D49dDD953b009E47E>



Token Information

Token Address :

0xa7bC4D83c5FcD56D025b5CF870E71817b3cCD679

Name: Particles

Symbol: PRTCLS

Decimals: 9

Network: Binance smart chain

Token Type: BEP20

Owner: 0xAAE811DA55c262468569bA9b56BaFB081c194710

Deployer:

0xAAE811DA55c262468569bA9b56BaFB081c194710

Token Supply: 100,000,000

Checksum:

ab673ab3b0b2ac9b227c0dc8ce447cbbed914f67

Testnet version:

The tests were performed using the contract deployed on the BSC Testnet, which can be found at the following address:

<https://testnet.bscscan.com/token/0xd5481c5536c97A066Ae3928D49dDD953b009E47E>



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

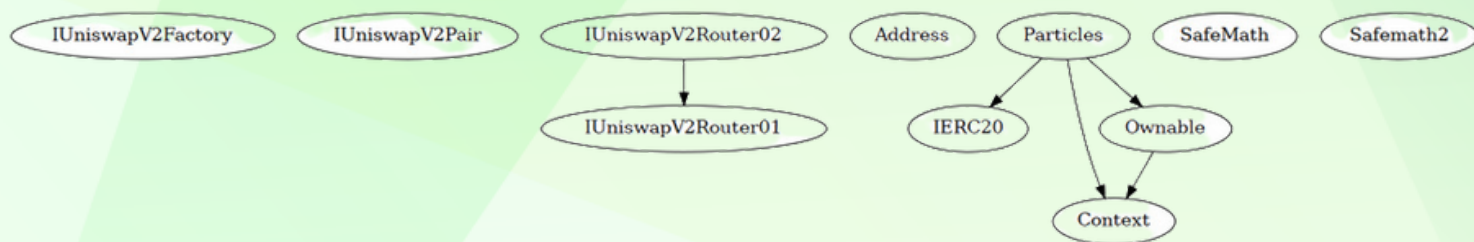
Severity

Found

◆ Critical	0
◆ High-Risk	0
◆ Medium-Risk	0
◆ Low-Risk	0
◆ Gas Optimization / Suggestions	0



INHERITANCE TREE





POINTS TO NOTE

- **Owner is not able to set buy/sell/transfer fees**
 - Owner is not able to blacklist an arbitrary wallet
 - Owner is not able to disable trades
 - Owner is not able to mint new tokens
 - **Owner is able to set maximum buy/sell/transfer amounts**
 - **MaxTx amoun is currently set to 0.0025% of total supply**
-



STATIC ANALYSIS

```
INFO:Detectors:
Pragma version^0.6.12 (contracts/Token.sol#2) allows old versions
solc-0.6.12 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity
INFO:Detectors:
Low level call in Address.sendValue(address,uint256) (contracts/Token.sol#383-395):
- (success) = recipient.call{value: amount}() (contracts/Token.sol#390)
Low level call in Address._functionCallWithValue(address,bytes,uint256,string) (contracts/Token.sol#480-508):
- (success,returndata) = target.call{value: weiValue}(data) (contracts/Token.sol#489-491)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#low-level-calls
INFO:Detectors:
Function IUniswapV2Pair.DOMAIN_SEPARATOR() (contracts/Token.sol#66) is not in mixedCase
Function IUniswapV2Pair.PERMIT_TYPEHASH() (contracts/Token.sol#68) is not in mixedCase
Function IUniswapV2Pair.MINIMUM_LIQUIDITY() (contracts/Token.sol#99) is not in mixedCase
Function IUniswapV2Router01.WETH() (contracts/Token.sol#141) is not in mixedCase
Parameter Particles.setSwapAndLiquifyEnabled(bool)._enabled (contracts/Token.sol#1264) is not in mixedCase
Variable Particles._maxTxAmount (contracts/Token.sol#992) is not in mixedCase
Variable Particles._maxTxPercent (contracts/Token.sol#993) is not in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions
INFO:Detectors:
Redundant expression "this (contracts/Token.sol#910)" inContext (contracts/Token.sol#904-913)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#redundant-statements
INFO:Detectors:
Variable IUniswapV2Router01.addLiquidity(address,address,uint256,uint256,uint256,uint256,address,uint256).amountADesired (contracts/Token.sol#146) is too similar to IUniswapV2Router01.addLiquidity(address,address,uint256,uint256,uint256,uint256,address,uint256).amountBDesired (contracts/Token.sol#147)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#variable-names-too-similar
INFO:Detectors:
Particles.slitherConstructorVariables() (contracts/Token.sol#976-1291) uses literals with too many digits:
- _totalSupply = 1000000000 * 10 ** 9 (contracts/Token.sol#987)
Particles.slitherConstructorVariables() (contracts/Token.sol#976-1291) uses literals with too many digits:
- _maxTxAmount = 500000 * 10 ** 9 (contracts/Token.sol#992)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#too-many-digits
INFO:Detectors:
Particles._excluded (contracts/Token.sol#985) is never used in Particles (contracts/Token.sol#976-1291)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#unused-state-variable
INFO:Detectors:
Particles._decimals (contracts/Token.sol#990) should be constant
Particles._maxTxPercent (contracts/Token.sol#993) should be constant
Particles._name (contracts/Token.sol#988) should be constant
Particles._symbol (contracts/Token.sol#989) should be constant
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-constant
INFO:Slither:contracts/Token.sol analyzed (11 contracts with 88 detectors), 52 result(s) found
```

Result => A static analysis of contract's source code has been performed using slither,

No major issues were found in the output



CONTRACT ASSESMENT

Contract	Type	Bases			
:-----: :-----: :-----: :-----: :-----:					
└─	**Function Name** **Visibility** **Mutability** **Modifiers**				
IERC20 Interface					
└─	totalSupply	External	!		NO !
└─	balanceOf	External	!		NO !
└─	transfer	External	!	●	NO !
└─	allowance	External	!		NO !
└─	approve	External	!	●	NO !
└─	transferFrom	External	!	●	NO !
SafeMath Library					
└─	mul	Internal	🔒		
└─	div	Internal	🔒		
└─	sub	Internal	🔒		
└─	add	Internal	🔒		
Address Library					
└─	isContract	Internal	🔒		
└─	sendValue	Internal	🔒	●	
└─	functionCall	Internal	🔒	●	
└─	functionCall	Internal	🔒	●	
└─	functionCallWithValue	Internal	🔒	●	
└─	functionCallWithValue	Internal	🔒	●	
└─	_functionCallWithValue	Private	🔒🔑	●	
IUniswapV2Factory Interface					
└─	feeTo	External	!		NO !
└─	feeToSetter	External	!		NO !
└─	getPair	External	!		NO !



CONTRACT ASSESMENT

```
|  | allPairs | External  | | |NO  | |
|  | allPairsLength | External  | | |NO  | |
|  | createPair | External  | | ●|NO  | |
|  | setFeeTo | External  | | ●|NO  | |
|  | setFeeToSetter | External  | | ●|NO  | |
|||||
| **IUniswapV2Pair** | Interface | |||
|  | name | External  | | |NO  | |
|  | symbol | External  | | |NO  | |
|  | decimals | External  | | |NO  | |
|  | totalSupply | External  | | |NO  | |
|  | balanceOf | External  | | |NO  | |
|  | allowance | External  | | |NO  | |
|  | approve | External  | | ●|NO  | |
|  | transfer | External  | | ●|NO  | |
|  | transferFrom | External  | | ●|NO  | |
|  | DOMAIN_SEPARATOR | External  | | |NO  | |
|  | PERMIT_TYPEHASH | External  | | |NO  | |
|  | nonces | External  | | |NO  | |
|  | permit | External  | | ●|NO  | |
|  | MINIMUM_LIQUIDITY | External  | | |NO  | |
|  | factory | External  | | |NO  | |
|  | token0 | External  | | |NO  | |
|  | token1 | External  | | |NO  | |
|  | getReserves | External  | | |NO  | |
|  | price0CumulativeLast | External  | | |NO  | |
|  | price1CumulativeLast | External  | | |NO  | |
|  | kLast | External  | | |NO  | |
|  | mint | External  | | ●|NO  | |
|  | burn | External  | | ●|NO  | |
|  | swap | External  | | ●|NO  | |
|  | skim | External  | | ●|NO  | |
|  | sync | External  | | ●|NO  | |
|  | initialize | External  | | ●|NO  | |
|||||
| **IUniswapV2Router01** | Interface | |||
|  | factory | External  | | |NO  | |
|  | WETH | External  | | |NO  | |
|  | addLiquidity | External  | | ●|NO  | |
```



CONTRACT ASSESMENT

```
|  | 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 ! |
|||||
| **Context** | Implementation | |||
|  | _msgSender | Internal 🔒 | | |
|  | _msgData | Internal 🔒 | | |
|||||
| **Ownable** | Implementation | Context |||
|  | <Constructor> | Public ! | 🔴 | NO ! |
|  | owner | Public ! | | NO ! |
|  | renounceOwnership | Public ! | 🔴 | onlyOwner |
|  | transferOwnership | Public ! | 🔴 | onlyOwner |
|  | getUnlockTime | Public ! | | NO ! |
```



CONTRACT ASSESMENT

```
|  | lock | Public ! |  | onlyOwner |
|  | unlock | Public ! |  | NO ! |
|||||
| **Particles** | Implementation | Context, IERC20, Ownable |||
|  | <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 ! |
|  | isExcludedFromFee | Public ! |  | NO ! |
|  | excludeFromFee | External ! |  | onlyOwner |
|  | includeInFee | External ! |  | onlyOwner |
|  | _approve | Private  |  |  |
|  | _transfer | Private  |  |  |
|  | isExcludedFromMaxTx | Public ! |  | NO ! |
|  | excludeFromMaxTx | External ! |  | onlyOwner |
|  | includeInMaxTx | External ! |  | onlyOwner |
|  | swapAndLiquify | Private  |  | lockTheSwap |
|  | swapTokensForEth | Private  |  |  |
|  | addLiquidity | Private  |  |  |
|  | _tokenTransfer | Private  |  |  |
|  | _transferStandard | Private  |  |  |
|  | setMaxTxPercent | External ! |  | onlyOwner |
|  | isExcludedFromMaxTxPercent | Public ! |  | NO ! |
|  | setSwapAndLiquifyEnabled | Public ! |  | onlyOwner |
|  | withdrawETH | External ! |  | onlyOwner |
|  | withdrawERC20 | External ! |  | onlyOwner |
|  | deposit | External ! |  | NO ! |
```




CONTRACT ASSESMENT

Legend

| Symbol| Meaning |

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

|  | Function can modify state |

|  | Function is payable |



FUNCTIONAL TESTING

1- Adding liquidity (**passed**):

<https://testnet.bscscan.com/tx/0xdf8b726cf1da46a90b7af65d7536643de1070532d5fc6ac73a2e4abfaafd1ad1>

2- Buying (0% tax) (**passed**):

<https://testnet.bscscan.com/tx/0x0bd25eb2eedfc58ec06db874c03b5581f6c7043b6f5d65d9bcc4450794b1c97a>

3- Selling (0% tax) (**passed**):

<https://testnet.bscscan.com/tx/0x6ac23b380935f9802611b25a1fcd144465d963afcefa4fbaddf6277989100250>

4- Transferring (0% tax) (**passed**):

<https://testnet.bscscan.com/tx/0xcb15532ec01a0eea7b47874bba647f330d158e743659b8d6cf30408584d24805>



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 specializes 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>
