Baby Doge Coin

Smart Contract Audit Report

SYSFIXED

22 May 2021

TABLE OF CONTENTS

AUDITED DETAILS

Audited Project

Project name	Token ticker	Blockchain
Baby Doge Coin	BabyDoge	Binance Smart Chain

Addresses

Contract address	0xc748673057861a797275cd8a068abb95a902e8de
Contract deployer address	0xf103d2AbA493749a402B7dE11cF31f5844062B74

Project Website

https://babydoge.com/

Codebase

https://bscscan.com/address/0xc748673057861a797275cd8a068abb95a902e8de#code

SUMMARY

Launched in June 2021, Baby Doge Coin one of the fastest growing community in crypto memes. Baby Doge is on a mission to bring crypto to the average person while also helping save dogs in need. Baby Doge is built on binance smart chain with extremely fast 5 second block times and cheaper gas fees than ethereum. Baby Doge Coin has learned a few tricks and lessons from his meme father, Doge. A new crypto birthed by fans of the Doge Meme online community. Baby Doge seeks to impress his father by showing his new improved transaction speeds & adorableness. He is Hyper-deflationary with static reflections, so more baby doge coins are being automatically added to your wallet each transaction.

Contract Summary

Documentation Quality

Baby Doge Coin provides a very good documentation with standard of solidity base code.

- The technical description is provided clearly and structured and also dont have any high risk issue.

Code Quality

The Overall quality of the basecode is standard.

- Standard solidity basecode and rules are already followed by Baby Doge Coin with the discovery of several low issues.

Test Coverage

Test coverage of the project is 100% (Through Codebase)

Audit Findings Summary

- SWC-100 SWC-108 | Explicitly define visibility for all state variables on lines 708.
- SWC-101 | It is recommended to use vetted safe math libraries for arithmetic operations consistently on lines 104, 136, 159, 160, 195, 231, 450, 732, 732, 733, 733, 738, 738, 739, 739, 858, 860, 896, 896, 900, 900, 945, 969, 975 and 860.
- SWC-103 | Pragma statements can be allowed to float when a contract is intended on lines 5.
- SWC-110 SWC-123 | It is recommended to use of revert(), assert(), and require() in Solidity, and the new REVERT opcode in the EVM on lines 859, 860, 860, 946, 946, 947, 948, 1078 and 1079.

CONCLUSION

We have audited the Baby Doge Coin project released on May 2021 to discover issues and identify potential security vulnerabilities in Baby Doge Coin Project. This process is used to find technical issues and security loopholes which might be found in the smart contract.

The security audit report provides satisfactory results with low-risk issues.

The Baby Doge Coin smart contract code issues do not pose a considerable risk. The writing of the contract is close to the standard of writing contracts in general. The low-risk issues found are some arithmetic operation issues, a floating pragma is set, a state variable visibility is not set, and out-of-bounds array access which the index access expression can cause an exception in case of the use of an invalid array index value.

AUDIT RESULT

Article	Category	Description	Result
Default Visibility	SWC-100 SWC-108	Functions and state variables visibility should be set explicitly. Visibility levels should be specified consciously.	ISSUE FOUND
Integer Overflow and Underflow	SWC-101	If unchecked math is used, all math operations should be safe from overflows and underflows.	ISSUE FOUND
Outdated Compiler Version	SWC-102	It is recommended to use a recent version of the Solidity compiler.	PASS
Floating Pragma	SWC-103	Contracts should be deployed with the same compiler version and flags that they have been tested thoroughly.	ISSUE FOUND
Unchecked Call Return Value	SWC-104	The return value of a message call should be checked.	PASS
Unprotected Ether Withdrawal	SWC-105	Due to missing or insufficient access controls, malicious parties can withdraw from the contract.	PASS
SELFDESTRUCT Instruction	SWC-106	The contract should not be self-destructible while it has funds belonging to users.	PASS
Reentrancy	SWC-107	Check effect interaction pattern should be followed if the code performs recursive call.	PASS
Uninitialized Storage Pointer	SWC-109	Uninitialized local storage variables can point to unexpected storage locations in the contract.	PASS
Assert Violation	SWC-110 SWC-123	Properly functioning code should never reach a failing assert statement.	ISSUE FOUND
Deprecated Solidity Functions	SWC-111	Deprecated built-in functions should never be used.	PASS
Delegate call to Untrusted Callee	SWC-112	Delegatecalls should only be allowed to trusted addresses.	PASS

DoS (Denial of Service)	SWC-113 SWC-128	Execution of the code should never be blocked by a specific contract state unless required.	PASS
Race Conditions	SWC-114	Race Conditions and Transactions Order Dependency should not be possible.	PASS
Authorization through tx.origin	SWC-115	tx.origin should not be used for authorization.	PASS
Block values as a proxy for time	SWC-116	Block numbers should not be used for time calculations.	PASS
Signature Unique ID	SWC-117 SWC-121 SWC-122	Signed messages should always have a unique id. A transaction hash should not be used as a unique id.	PASS
Incorrect Constructor Name	SWC-118	Constructors are special functions that are called only once during the contract creation.	PASS
Shadowing State Variable	SWC-119	State variables should not be shadowed.	PASS
Weak Sources of Randomness	SWC-120	Random values should never be generated from Chain Attributes or be predictable.	PASS
Write to Arbitrary Storage Location	SWC-124	The contract is responsible for ensuring that only authorized user or contract accounts may write to sensitive storage locations.	PASS
Incorrect Inheritance Order	SWC-125	When inheriting multiple contracts, especially if they have identical functions, a developer should carefully specify inheritance in the correct order. The rule of thumb is to inherit contracts from more /general/ to more /specific/.	PASS
Insufficient Gas Griefing	SWC-126	Insufficient gas griefing attacks can be performed on contracts which accept data and use it in a sub-call on another contract.	PASS
Arbitrary Jump Function	SWC-127	As Solidity doesnt support pointer arithmetics, it is impossible to change such variable to an arbitrary value.	PASS

Typographical Error	SWC-129	A typographical error can occur for example when the intent of a defined operation is to sum a number to a variable.	PASS
Override control character	SWC-130	Malicious actors can use the Right-To-Left-Override unicode character to force RTL text rendering and confuse users as to the real intent of a contract.	PASS
Unused variables	SWC-131 SWC-135	Unused variables are allowed in Solidity and they do not pose a direct security issue.	PASS
Unexpected Ether balance	SWC-132	Contracts can behave erroneously when they strictly assume a specific Ether balance.	PASS
Hash Collisions Variable	SWC-133	Using abi.encodePacked() with multiple variable length arguments can, in certain situations, lead to a hash collision.	PASS
Hardcoded gas amount	SWC-134	The transfer() and send() functions forward a fixed amount of 2300 gas.	PASS
Unencrypted Private Data	SWC-136	It is a common misconception that private type variables cannot be read.	PASS

SMART CONTRACT ANALYSIS

Started	Friday May 21 2021 07:21:59 GMT+0000 (Coordinated Universal Time)
Finished	Saturday May 22 2021 11:07:21 GMT+0000 (Coordinated Universal Time)
Mode	Standard
Main Source File	CoinToken.sol

Detected Issues

ID	Title	Severity	Status
SWC-101	ARITHMETIC OPERATION "+" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "-" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "*" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "/" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "/" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "%" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "+" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "*" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "**" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "-" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "%" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "*" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "**" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "*" DISCOVERED	low	acknowledged

SWC-101	ARITHMETIC OPERATION "**" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "++" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "-" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "*" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "**" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "*" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "**" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "++" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "**" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "**" DISCOVERED	low	acknowledged
SWC-101	COMPILER-REWRITABLE "<UINT> - 1" DISCOVERED	low	acknowledged

SWC-103	A FLOATING PRAGMA IS SET.	low	acknowledged
SWC-108	STATE VARIABLE VISIBILITY IS NOT SET.	low	acknowledged
SWC-110	OUT OF BOUNDS ARRAY ACCESS	low	acknowledged
SWC-110	OUT OF BOUNDS ARRAY ACCESS	low	acknowledged
SWC-110	OUT OF BOUNDS ARRAY ACCESS	low	acknowledged
SWC-110	OUT OF BOUNDS ARRAY ACCESS	low	acknowledged
SWC-110	OUT OF BOUNDS ARRAY ACCESS	low	acknowledged
SWC-110	OUT OF BOUNDS ARRAY ACCESS	low	acknowledged
SWC-110	OUT OF BOUNDS ARRAY ACCESS	low	acknowledged
SWC-110	OUT OF BOUNDS ARRAY ACCESS	low	acknowledged
SWC-110	OUT OF BOUNDS ARRAY ACCESS	low	acknowledged

SWC-101 | ARITHMETIC OPERATION "+" DISCOVERED

LINE 104

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CoinToken.sol

Locations

```
103   function add(uint256 a, uint256 b) internal pure returns (uint256) {
104   uint256 c = a + b;
105   require(c >= a, "SafeMath: addition overflow");
106
107   return c;
108
```

SWC-101 | ARITHMETIC OPERATION "-" DISCOVERED

LINE 136

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CoinToken.sol

Locations

```
135   require(b <= a, errorMessage);
136   uint256 c = a - b;
137
138   return c;
139   }
140
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 159

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CoinToken.sol

Locations

```
158
159   uint256 c = a * b;
160   require(c / a == b, "SafeMath: multiplication overflow");
161
162   return c;
163
```

SWC-101 | ARITHMETIC OPERATION "/" DISCOVERED

LINE 160

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CoinToken.sol

Locations

```
159   uint256 c = a * b;
160   require(c / a == b, "SafeMath: multiplication overflow");
161
162   return c;
163   }
164
```

SWC-101 | ARITHMETIC OPERATION "/" DISCOVERED

LINE 195

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CoinToken.sol

Locations

```
194   require(b > 0, errorMessage);
195   uint256 c = a / b;
196   // assert(a == b * c + a % b); // There is no case in which this doesn't hold
197
198   return c;
199
```

SWC-101 | ARITHMETIC OPERATION "%" DISCOVERED

LINE 231

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CoinToken.sol

Locations

```
230   require(b != 0, errorMessage);
231   return a % b;
232   }
233   }
234
235
```

SWC-101 | ARITHMETIC OPERATION "+" DISCOVERED

LINE 450

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CoinToken.sol

Locations

```
449   _owner = address(0);
450   _lockTime = now + time;
451   emit OwnershipTransferred(_owner, address(0));
452   }
453
454
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 732

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CoinToken.sol

Locations

```
731   _decimals = _DECIMALS;
732   _tTotal = _supply * 10 ** _decimals;
733   _rTotal = (MAX - (MAX % _tTotal));
734   _taxFee = _txFee;
735   _liquidityFee = _lpFee;
736
```

SWC-101 | ARITHMETIC OPERATION "**" DISCOVERED

LINE 732

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CoinToken.sol

Locations

```
731   _decimals = _DECIMALS;
732   _tTotal = _supply * 10 ** _decimals;
733   _rTotal = (MAX - (MAX % _tTotal));
734   _taxFee = _txFee;
735   _liquidityFee = _lpFee;
736
```

SWC-101 | ARITHMETIC OPERATION "-" DISCOVERED

LINE 733

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CoinToken.sol

Locations

```
732   _tTotal = _supply * 10 ** _decimals;
733   _rTotal = (MAX - (MAX % _tTotal));
734   _taxFee = _txFee;
735   _liquidityFee = _lpFee;
736   _previousTaxFee = _txFee;
737
```

SWC-101 | ARITHMETIC OPERATION "%" DISCOVERED

LINE 733

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CoinToken.sol

Locations

```
732   _tTotal = _supply * 10 ** _decimals;
733   _rTotal = (MAX - (MAX % _tTotal));
734   _taxFee = _txFee;
735   _liquidityFee = _lpFee;
736   _previousTaxFee = _txFee;
737
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 738

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CoinToken.sol

Locations

```
737   _previousLiquidityFee = _lpFee;
738   _maxTxAmount = _MAXAMOUNT * 10 ** _decimals;
739   numTokensSellToAddToLiquidity = SELLMAXAMOUNT * 10 ** _decimals;
740
741
742
```

SWC-101 | ARITHMETIC OPERATION "**" DISCOVERED

LINE 738

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CoinToken.sol

Locations

```
737   _previousLiquidityFee = _lpFee;
738   _maxTxAmount = _MAXAMOUNT * 10 ** _decimals;
739   numTokensSellToAddToLiquidity = SELLMAXAMOUNT * 10 ** _decimals;
740
741
742
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 739

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CoinToken.sol

Locations

```
738   _maxTxAmount = _MAXAMOUNT * 10 ** _decimals;
739   numTokensSellToAddToLiquidity = SELLMAXAMOUNT * 10 ** _decimals;
740
741
742   _rOwned[tokenOwner] = _rTotal;
743
```

SWC-101 | ARITHMETIC OPERATION "**" DISCOVERED

LINE 739

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CoinToken.sol

Locations

```
738   _maxTxAmount = _MAXAMOUNT * 10 ** _decimals;
739   numTokensSellToAddToLiquidity = SELLMAXAMOUNT * 10 ** _decimals;
740
741
742   _rOwned[tokenOwner] = _rTotal;
743
```

SWC-101 | ARITHMETIC OPERATION "++" DISCOVERED

LINE 858

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CoinToken.sol

Locations

```
857   require(_isExcluded[account], "Account is already excluded");
858   for (uint256 i = 0; i < _excluded.length; i++) {
859   if (_excluded[i] == account) {
860   _excluded[i] = _excluded[_excluded.length - 1];
861   _tOwned[account] = 0;
862
```

SWC-101 | ARITHMETIC OPERATION "-" DISCOVERED

LINE 860

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CoinToken.sol

Locations

```
859   if (_excluded[i] == account) {
860   _excluded[i] = _excluded[_excluded.length - 1];
861   _tOwned[account] = 0;
862   _isExcluded[account] = false;
863   _excluded.pop();
864
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 896

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CoinToken.sol

Locations

```
895   function setNumTokensSellToAddToLiquidity(uint256 swapNumber) public onlyOwner {
896   numTokensSellToAddToLiquidity = swapNumber * 10 ** _decimals;
897   }
898
899   function setMaxTxPercent(uint256 maxTxPercent) public onlyOwner {
900
```

SWC-101 | ARITHMETIC OPERATION "**" DISCOVERED

LINE 896

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CoinToken.sol

Locations

```
895   function setNumTokensSellToAddToLiquidity(uint256 swapNumber) public onlyOwner {
896   numTokensSellToAddToLiquidity = swapNumber * 10 ** _decimals;
897   }
898
899   function setMaxTxPercent(uint256 maxTxPercent) public onlyOwner {
900
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 900

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CoinToken.sol

Locations

```
899   function setMaxTxPercent(uint256 maxTxPercent) public onlyOwner {
900   _maxTxAmount = maxTxPercent  * 10 ** _decimals;
901   }
902
903   function setSwapAndLiquifyEnabled(bool _enabled) public onlyOwner {
904
```

SWC-101 | ARITHMETIC OPERATION "**" DISCOVERED

LINE 900

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CoinToken.sol

Locations

```
899   function setMaxTxPercent(uint256 maxTxPercent) public onlyOwner {
900   _maxTxAmount = maxTxPercent  * 10 ** _decimals;
901   }
902
903   function setSwapAndLiquifyEnabled(bool _enabled) public onlyOwner {
904
```

SWC-101 | ARITHMETIC OPERATION "++" DISCOVERED

LINE 945

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CoinToken.sol

Locations

```
944   uint256 tSupply = _tTotal;
945   for (uint256 i = 0; i < _excluded.length; i++) {
946   if (_rOwned[_excluded[i]] > rSupply || _tOwned[_excluded[i]] > tSupply) return
(_rTotal, _tTotal);
947   rSupply = rSupply.sub(_rOwned[_excluded[i]]);
948   tSupply = tSupply.sub(_tOwned[_excluded[i]]);
949
```

SWC-101 | ARITHMETIC OPERATION "**" DISCOVERED

LINE 969

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CoinToken.sol

Locations

```
968   return _amount.mul(_taxFee).div(
969   10**2
970   );
971   }
972
973
```

SWC-101 | ARITHMETIC OPERATION "**" DISCOVERED

LINE 975

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CoinToken.sol

Locations

```
974   return _amount.mul(_liquidityFee).div(
975   10**2
976   );
977   }
978
979
```

SWC-101 | COMPILER-REWRITABLE "<UINT> - 1" DISCOVERED

LINE 860

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- CoinToken.sol

Locations

```
859   if (_excluded[i] == account) {
860   _excluded[i] = _excluded[_excluded.length - 1];
861   _tOwned[account] = 0;
862   _isExcluded[account] = false;
863   _excluded.pop();
864
```

SWC-103 | A FLOATING PRAGMA IS SET.

LINE 5

low SEVERITY

The current pragma Solidity directive is ""^0.6.12"". It is recommended to specify a fixed compiler version to ensure that the bytecode produced does not vary between builds. This is especially important if you rely on bytecode-level verification of the code.

Source File

- CoinToken.sol

Locations

```
4
5   pragma solidity ^0.6.12;
6   // SPDX-License-Identifier: Unlicensed
7   interface IERC20 {
8
9
```

SWC-108 | STATE VARIABLE VISIBILITY IS NOT SET.

LINE 708

low SEVERITY

It is best practice to set the visibility of state variables explicitly. The default visibility for "inSwapAndLiquify" is internal. Other possible visibility settings are public and private.

Source File

- CoinToken.sol

Locations

```
707
708   bool inSwapAndLiquify;
709   bool public swapAndLiquifyEnabled = true;
710
711   uint256 public _maxTxAmount;
712
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 859

low SEVERITY

The index access expression can cause an exception in case of use of invalid array index value.

Source File

- CoinToken.sol

Locations

```
858   for (uint256 i = 0; i < _excluded.length; i++) {
859   if (_excluded[i] == account) {
860   _excluded[i] = _excluded[_excluded.length - 1];
861   _tOwned[account] = 0;
862   _isExcluded[account] = false;
863
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 860

low SEVERITY

The index access expression can cause an exception in case of use of invalid array index value.

Source File

- CoinToken.sol

Locations

```
859   if (_excluded[i] == account) {
860   _excluded[i] = _excluded[_excluded.length - 1];
861   _tOwned[account] = 0;
862   _isExcluded[account] = false;
863   _excluded.pop();
864
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 860

low SEVERITY

The index access expression can cause an exception in case of use of invalid array index value.

Source File

- CoinToken.sol

Locations

```
859   if (_excluded[i] == account) {
860   _excluded[i] = _excluded[_excluded.length - 1];
861   _tOwned[account] = 0;
862   _isExcluded[account] = false;
863   _excluded.pop();
864
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 946

low SEVERITY

The index access expression can cause an exception in case of use of invalid array index value.

Source File

- CoinToken.sol

Locations

```
945   for (uint256 i = 0; i < _excluded.length; i++) {
946   if (_rOwned[_excluded[i]] > rSupply || _tOwned[_excluded[i]] > tSupply) return
(_rTotal, _tTotal);
947   rSupply = rSupply.sub(_rOwned[_excluded[i]]);
948   tSupply = tSupply.sub(_tOwned[_excluded[i]]);
949   }
950
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 946

low SEVERITY

The index access expression can cause an exception in case of use of invalid array index value.

Source File

- CoinToken.sol

Locations

```
945   for (uint256 i = 0; i < _excluded.length; i++) {
946   if (_rOwned[_excluded[i]] > rSupply || _tOwned[_excluded[i]] > tSupply) return
(_rTotal, _tTotal);
947   rSupply = rSupply.sub(_rOwned[_excluded[i]]);
948   tSupply = tSupply.sub(_tOwned[_excluded[i]]);
949   }
950
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 947

low SEVERITY

The index access expression can cause an exception in case of use of invalid array index value.

Source File

- CoinToken.sol

Locations

```
946   if (_rOwned[_excluded[i]] > rSupply || _tOwned[_excluded[i]] > tSupply) return
(_rTotal, _tTotal);
947   rSupply = rSupply.sub(_rOwned[_excluded[i]]);
948   tSupply = tSupply.sub(_tOwned[_excluded[i]]);
949   }
950   if (rSupply < _rTotal.div(_tTotal)) return (_rTotal, _tTotal);
951
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 948

low SEVERITY

The index access expression can cause an exception in case of use of invalid array index value.

Source File

- CoinToken.sol

Locations

```
947   rSupply = rSupply.sub(_rOwned[_excluded[i]]);
948   tSupply = tSupply.sub(_tOwned[_excluded[i]]);
949   }
950   if (rSupply < _rTotal.div(_tTotal)) return (_rTotal, _tTotal);
951   return (rSupply, tSupply);
952
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 1078

low SEVERITY

The index access expression can cause an exception in case of use of invalid array index value.

Source File

- CoinToken.sol

Locations

```
1077   address[] memory path = new address[](2);
1078   path[0] = address(this);
1079   path[1] = uniswapV2Router.WETH();
1080
1081   _approve(address(this), address(uniswapV2Router), tokenAmount);
1082
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 1079

low SEVERITY

The index access expression can cause an exception in case of use of invalid array index value.

Source File

- CoinToken.sol

Locations

```
1078   path[0] = address(this);
1079   path[1] = uniswapV2Router.WETH();
1080
1081   _approve(address(this), address(uniswapV2Router), tokenAmount);
1082
1083
```

DISCLAIMER

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Services Agreement, or the scope of services, and terms and conditions provided to you ("Customer" or the "Company") in connection with the Agreement. This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement. 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 Sysfixed's prior written consent in each instance.

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 considered, an indication of the economics or value of any "product" or "asset" created by any team or project that contracts Sysfixed to perform a security assessment. This report 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 is a limited report on our findings based on our analysis, in accordance with good industry practice as of the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the below disclaimer below – please make sure to read it in full.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing 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.

This report is provided for information purposes only and on a non-reliance basis and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and Sysfixed and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers, and other representatives) (Sysfixed) owe no duty of care.

ABOUT US

Sysfixed is a blockchain security certification organization established in 2021 with the objective to provide smart contract security services and verify their correctness in blockchain-based protocols. Sysfixed automatically scans for security vulnerabilities in Ethereum and other EVM-based blockchain smart contracts. Sysfixed a comprehensive range of analysis techniques—including static analysis, dynamic analysis, and symbolic execution—can accurately detect security vulnerabilities to provide an in-depth analysis report. With a vibrant ecosystem of world-class integration partners that amplify developer productivity, Sysfixed can be utilized in all phases of your project's lifecycle. Our team of security experts is dedicated to the research and improvement of our tools and techniques used to fortify your code.