SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT

Customer:	Raku Coin (RAKUC)
Website:	https://www.rakucoin.com
Prepared on:	22/05/2021
Platform:	Ethereum
Language:	Solidity
Audit Type:	Standard

audit@etherauthority.io

Table of contents

THIS IS SECURITY AUDIT REPORT DOCUMENT AND WHICH MAY CONTAIN INFORMATION WHICH IS CONFIDENTIAL. WHICH INCLUDES ANY POTENTIAL VULNERABILITIES AND MALICIOUS CODES WHICH CAN BE USED TO EXPLOIT THE SOFTWARE. THIS MUST BE REFERRED INTERNALLY AND ONLY SHOULD BE MADE AVAILABLE TO PUBLIC AFTER ISSUES ARE RESOLVED.

Email: audit@EtherAuthority.io

Project file

Name	Code Review and Security Analysis Report for Raku Coin (RAKUC) Token Smart Contract
Platform	Ethereum / Solidity
File	RakuCoin.sol
File MD5 hash	5DEE55897778BFB296B66EC1B2498958
Online Contract Code	https://etherscan.io/address/0x714599f7604144a3fe1737c440a70fc0fd6503ea#code

Introduction

We were contracted by the Raku Coin team to perform the Security audit of the Raku Coin Token smart contract code. The audit has been performed using manual analysis as well as using automated software tools. This report presents all the findings regarding the audit performed on 22/05/2021.

The Audit type was Standard Audit. Which means this audit is concluded based on Standard audit scope. This document outlines all the findings as well as an AS-IS overview of the smart contract codes.

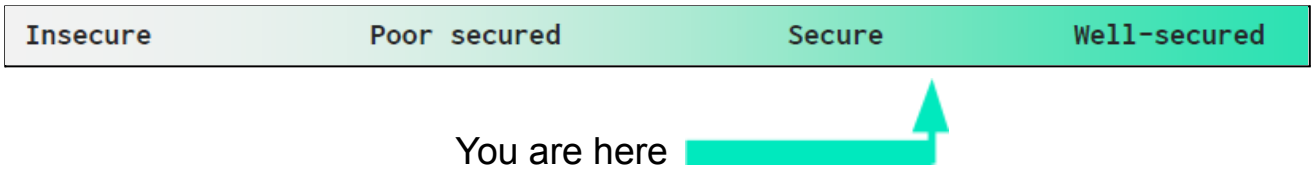
Quick Stats:

Main Category	Subcategory	Result
Contract Programming	Solidity version not specified	Passed
	Solidity version too old	Moderated
	Integer overflow/underflow	Passed
	Function input parameters lack of check	Passed
	Function input parameters check bypass	Passed
	Function access control lacks management	Passed
	Critical operation lacks event log	Moderated
	Human/contract checks bypass	Passed
	Random number generation/use vulnerability	Passed
	Fallback function misuse	Passed
	Race condition	Passed
	Logical vulnerability	Passed
	Other programming issues	Passed
Code Specification	Function visibility not explicitly declared	Passed
	Var. storage location not explicitly declared	Passed
	Use keywords/functions to be deprecated	Passed
	Other code specification issues	Passed
Gas Optimization	Assert() misuse	Passed
	High consumption ‘for/while’ loop	Moderated
	High consumption ‘storage’ storage	Passed
	“Out of Gas” Attack	Passed
Business Risk	The maximum limit for mintage not set	Passed
	“Short Address” Attack	Passed
	“Double Spend” Attack	Passed

Overall Audit Result: PASSED

Executive Summary

According to the **standard** audit assessment, Customer`s solidity smart contract is **Secured**. There are some owner influenced functions which do not make this smart contract 100% decentralized. We suggest to either renounce the ownership (consider lock issue. See the audit findings for more details), or send this to a decentralized governance smart contract.



We used various tools like Mythril, Slither and Remix IDE. At the same time this finding is based on critical analysis of the manual audit.
All issues found during automated analysis were manually reviewed and applicable vulnerabilities are presented in the Audit overview section. General overview is presented in AS-IS section and all identified issues can be found in the Audit overview section.

We found 0 critical, 0 high, 0 medium and 4 low and some very low level issues.

Code Quality

Raku Coin Token smart contract has 1 smart contract. This smart contract also contains Libraries, Smart contract inherits and Interfaces. These are compact and well written contracts.

The libraries in the Raku Coin Token protocol are part of its logical algorithm. A library is a different type of smart contract that contains reusable code. Once deployed on the blockchain (only once), it is assigned a specific address and its properties / methods can be reused many times by other contracts in the Raku Coin Token protocol.

The Raku Coin team has **not** provided scenario and unit test scripts, which would have helped to determine the integrity of the code in an automated way.

Overall, code parts are **not well** commented on smart contracts.

Documentation

We were given Raku Coin token smart contracts code in the form of a Etherscan.io web link. The hash of that code and that web link are mentioned above in the table.

As mentioned above, most code parts are **not well** commented. so it is difficult to quickly understand the programming flow as well as complex code logic. Comments are very helpful in understanding the overall architecture of the protocol.

Another source of information was its official website rakucoin.com which provided rich information about the project architecture and tokenomics.

Use of Dependencies

As per our observation, the libraries are used in this smart contract infrastructure that are based on well known industry standard open source projects. And their core code blocks are written well.

Apart from libraries, its functions are used in external smart contract calls.

AS-IS overview

Raku Coin (RAKUC) is an ERC20 token smart contract, which has additional features like: swap and liquidity, distributing tokens to token holders, etc.

RakuCoin.sol

(1) Interfaces

(a) IERC20

(b) IUniswapV2Factory

(c) IUniswapV2Pair

(d) IUniswapV2Router01

(e) IUniswapV2Router02

(2) Inherited contracts

(a) Context: Context contract.

(b) Ownable: Ownership contract.

(c) IERC20: IERC20 contract.

(3) Usages

(a) using SafeMath for uint256;

(b) using Address for address;

(4) Events

(a) event Transfer(address indexed from, address indexed to, uint256 value);

(b) event Approval(address indexed owner, address indexed spender, uint256 value);

(c) event OwnershipTransferred(address indexed previousOwner, address indexed newOwner);

(d) event PairCreated(address indexed token0, address indexed token1, address pair, uint);

(e) event Approval(address indexed owner, address indexed spender, uint value);

(f) event Transfer(address indexed from, address indexed to, uint value);

(g) event Mint(address indexed sender, uint amount0, uint amount1);

(h) event Burn(address indexed sender, uint amount0, uint amount1, address indexed to);

(i) event Swap(address indexed sender, uint amount0In, uint amount1In, uint amount0Out, uint amount1Out, address indexed to);

(j) event Sync(uint112 reserve0, uint112 reserve1);

(k) event MinTokensBeforeSwapUpdated(uint256 minTokensBeforeSwap);

(l) event SwapAndLiquifyEnabledUpdated(bool enabled);

(m) event SwapAndLiquify(uint256 tokensSwapped,uint256 ethReceived, uint256 tokensIntoLiqudity);

(5) Functions

Sl.	Functions	Type	Observation	Conclusion
1	name	read	Passed	No Issue
2	symbol	read	Passed	No Issue
3	decimals	read	Passed	No Issue
4	totalSupply	read	Passed	No Issue
5	balanceOf	read	Passed	No Issue
6	transfer	write	Passed	No Issue
7	allowance	read	Passed	No Issue
8	approve	write	Passed	No Issue
9	transferFrom	write	Passed	No Issue
10	increaseAllowance	write	Passed	No Issue
11	decreaseAllowance	write	Passed	No Issue
12	isExcluded	read	Passed	No Issue
13	totalFees	write	Passed	No Issue

14	deliver	write	Passed	No Issue
15	reflectionFromToken	read	Passed	No Issue
16	tokenFromReflection	read	Passed	No Issue
17	excludeAccount	write	access by only owner	No Issue
18	includeAccount	write	Infinite loop possibility	**Refer Audit Findings**
19	_transferBothExcluded	write	Passed	No Issue
20	setExcludeFromFee	write	access by only owner	No Issue
21	_reflectFee	write	Passed	No Issue
22	_getValues	read	Passed	No Issue
23	_getTValues	read	Passed	No Issue
24	_getRValues	write	Passed	No Issue
25	_getRate	read	Passed	No Issue
26	_getCurrentSupply	read	Infinite loop possibility	**Refer Audit Findings**
27	removeAllFee	write	Passed	No Issue
28	restoreAllFee	write	Passed	No Issue
29	isExcludedFromFee	read	Passed	No Issue
30	_approve	write	Passed	No Issue
31	_transfer	write	Passed	No Issue
32	swapTokensForEth	write	Passed	No Issue
33	_tokenTransfer	write	Passed	No Issue
34	_transferStandard	write	Passed	No Issue
35	_transferFromExcluded	write	Passed	No Issue
36	_msgSender	read	Passed	No Issue
37	_msgData	read	Passed	No Issue
38	owner	read	Passed	No Issue
39	renounceOwnership	write	Passed	No Issue
40	transferOwnership	write	Passed	No Issue
41	geUnlockTime	read	Passed	No Issue
42	lock / unlock	write	Ownership issue	**Refer Audit Findings**
44	_transferToExcluded	write	Passed	No Issue

Severity Definitions

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to tokens loss etc.
High	High-level vulnerabilities are difficult to exploit; however, they also have significant impact on smart contract execution, e.g. public access to crucial functions
Medium	Medium-level vulnerabilities are important to fix; however, they can't lead to tokens lose
Low	Low-level vulnerabilities are mostly related to outdated, unused etc. code snippets, that can't have significant impact on execution
Lowest / Code Style / Best Practice	Lowest-level vulnerabilities, code style violations and info statements can't affect smart contract execution and can be ignored.

Audit Findings

Critical

No critical severity vulnerabilities were found.

High

No High severity vulnerabilities were found.

Medium

No Medium severity vulnerabilities were found.

Low

(1) Infinite loop possibility

```
function includeAccount(address account) external onlyOwner() {
    require(_isExcluded[account], "Account is already excluded");
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (_excluded[i] == account) {
            _excluded[i] = _excluded[_excluded.length - 1];
            _tOwned[account] = 0;
            _isExcluded[account] = false;
            _excluded.pop();
            break;
        }
    }
}
```

If there are many excluded wallets, then this logic will fail. Because it might hit the block's gas limit. If there are very limited exceptions, then this will work, but will cost more gas.

Solution: Just use a mapping that will map wallet to bool and make excluded wallets to be true. Alternatively, please exclude limited wallets only.

(2) Possible to gain ownership after renouncing the contract ownership. Owner can renounce ownership and make a contract without the owner but here is a catch. Owner can misuse it by performing the following operations:
1) Owner calls the lock function in contract to set the current owner as _previousOwner.
2) Owner calls unlock to unlock contract and set _owner = _previousOwner.
3) Owner called renounceOwnership to leave the contract without the owner.
4) Owner calls unlock to regain ownership.

Solution: We advise updating/removing lock and unlock functions in the contract or call renounceOwnership function first before calling lock/unlock functions.

(3) Missing Events: Following state changing functions should emit an event.

- setExcludeFromFee
- excludeAccount
- _setMaxTxAmount
- _setTaxFee
- _setMarketingPoolFee
- _setMarketingPoolWallet

(4) Variable could be declared as constant

```
string private _name = 'Raku Coin';
string private _symbol = 'RAKUC';
uint8 private _decimals = 18;
```

Never changing state variables should be declared as constants. Such as:

- _name
- _symbol
- _decimals
- _tTotal

Very Low / Discussion / Best practices:

(1) Solidity version

```
pragma solidity ^0.6.12;
```

Use the latest solidity version while contract deployment to prevent any compiler version level bugs.

Solution: This issue is acknowledged.

(2) Approve of ERC20 standard: This can be used to front run. From the client side, only use this function to change the allowed amount to 0 or from 0 (wait till transaction is mined and approved). This should be done from the client side.

(3) All functions which are not called internally, must be declared as external. It is more efficient as sometimes it saves some gas.
https://ethereum.stackexchange.com/questions/19380/external-vs-public-best-practices

Centralization

This smart contract has some functions which can be executed by Admin (Owner) only. If the admin wallet private key would be compromised, then it puts this smart contract in the hands of an attacker. Following are Admin functions:

- Owner has permission to change the owner address.
- Owner can lock the contract. This has "**back doors**" to regain the ownership after renouncing. See the audit finding section.
- Owner can **send all the contract's Ether to the marketing wallet**. This gives the owner privilege to take all the Ether out of smart contract.
- Owner can enable swap, set tax fee, marketing pool fee, change marketing pool wallet, set max transaction amount, etc.
- Owner can include/exclude any wallet from reward and fees.

Conclusion

We were given a contract code. And we have used all possible tests based on given objects as files. We observed some issues in the smart contract and those are fixed/acknowledged in the smart contract. **So it is good to go for the production.**

Since possible test cases can be unlimited for such extensive smart contract protocol, we provide no such guarantee of future outcomes. We have used all the latest static tools and manual observations to cover maximum possible test cases to scan everything.

Smart contracts within the scope were manually reviewed and analyzed with static analysis tools. Smart Contract's high level description of functionality was presented in As-is overview section of the report.

Audit report contains all found security vulnerabilities and other issues in the reviewed code.

Security state of the reviewed contract, based on standard audit procedure scope, is "**Secured**". We suggest to renounce the ownership or send it to a decentralized governance smart contract to make this contract "well secured".

Our Methodology

We like to work with a transparent process and make our reviews a collaborative effort. The goals of our security audits are to improve the quality of systems we review and aim for sufficient remediation to help protect users. The following is the methodology we use in our security audit process.

Manual Code Review:

In manually reviewing all of the code, we look for any potential issues with code logic, error handling, protocol and header parsing, cryptographic errors, and random number generators. We also watch for areas where more defensive programming could reduce the risk of future mistakes and speed up future audits. Although our primary focus is on the in-scope code, we examine dependency code and behavior when it is relevant to a particular line of investigation.

Vulnerability Analysis:

Our audit techniques included manual code analysis, user interface interaction, and whitebox penetration testing. We look at the project's web site to get a high level understanding of what functionality the software under review provides. We then meet with the developers to gain an appreciation of their vision of the software. We install and use the relevant software, exploring the user interactions and roles. While we do this, we brainstorm threat models and attack surfaces. We read design documentation, review other audit results, search for similar projects, examine source code dependencies, skim open issue tickets, and generally investigate details other than the implementation.

Documenting Results:

We follow a conservative, transparent process for analyzing potential security vulnerabilities and seeing them through successful remediation. Whenever a potential issue is discovered, we immediately create an Issue entry for it in this document, even though we have not yet verified the feasibility and impact of the issue. This process is conservative because we document our suspicions early even if they are later shown to not represent exploitable vulnerabilities. We generally follow a process of first documenting the suspicion with unresolved questions, then confirming the issue through code analysis, live experimentation, or automated tests. Code analysis is the most tentative, and we strive to provide test code, log captures, or screenshots demonstrating our confirmation. After this we analyze the feasibility of an attack in a live system.

Suggested Solutions:

We search for immediate mitigations that live deployments can take, and finally we suggest the requirements for remediation engineering for future releases. The mitigation and remediation recommendations should be scrutinized by the developers and deployment engineers, and successful mitigation and remediation is an ongoing collaborative process after we deliver our report, and before the details are made public.

Disclaimers

EtherAuthority.io Disclaimer

EtherAuthority team has analyzed this smart contract in accordance with the best industry practices at the date of this report, in relation to: cybersecurity vulnerabilities and issues in smart contract source code, the details of which are disclosed in this report, (Source Code); the Source Code compilation, deployment and functionality (performing the intended functions).

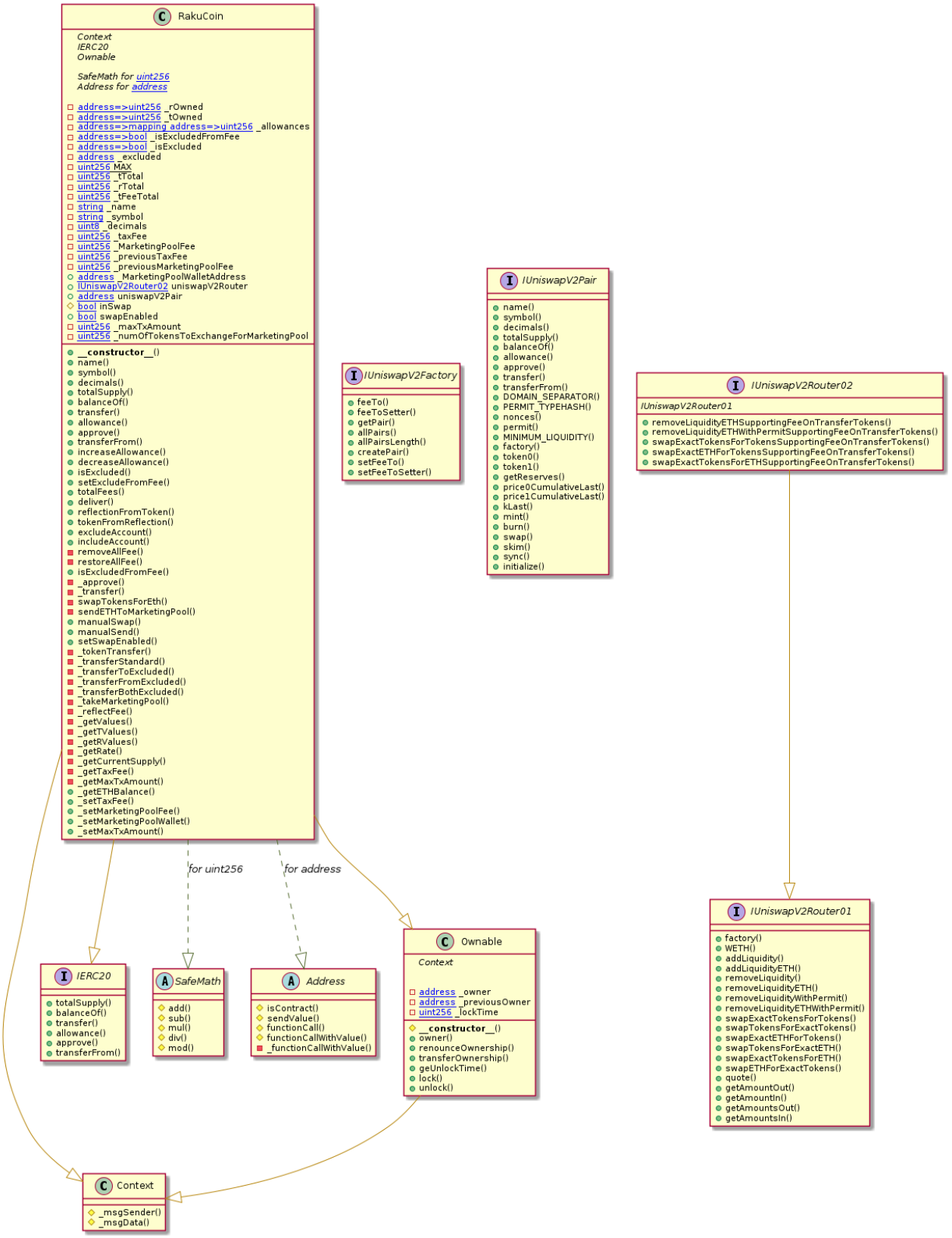
Due to the fact that the total number of test cases are unlimited, the audit makes no statements or warranties on security of the code. It also cannot be considered as a sufficient assessment regarding the utility and safety of the code, bugfree status or any other statements of the contract. While we have done our best in conducting the analysis and producing this report, it is important to note that you should not rely on this report only. We also suggest conducting a bug bounty program to confirm the high level of security of this smart contract.

Technical Disclaimer

Smart contracts are deployed and executed on the blockchain platform. The platform, its programming language, and other software related to the smart contract can have their own vulnerabilities that can lead to hacks. Thus, the audit can’t guarantee explicit security of the audited smart contracts.

Appendix

Code Flow Diagram - Raku Coin Token



Slither Results Log

RakuCoin.sendETHToMarketingPool(uint256) (RakuCoin.sol#915-918) sends eth to arbitrary user
Dangerous calls:
- _MarketingPoolWalletAddress.transfer(amount) (RakuCoin.sol#916)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#functions-that-sendether-to-arbitrary-destinations
INFO:Detectors:
Reentrancy in RakuCoin._transfer(address,address,uint256) (RakuCoin.sol#853-895):
External calls:
- swapTokensForEth(contractTokenBalance) (RakuCoin.sol#877)
- uniswapV2Router.swapExactTokensForETHSupportingFeeOnTransferTokens(tokenAmount,0,path,
address(this),block.timestamp) (RakuCoin.sol#906-912)
External calls sending eth:
- sendETHToMarketingPool(address(this).balance) (RakuCoin.sol#881)
- _MarketingPoolWalletAddress.transfer(amount) (RakuCoin.sol#916)
State variables written after the call(s):
- _tokenTransfer(sender,recipient,amount,takeFee) (RakuCoin.sol#894)
- _rOwned[address(this)] = _rOwned[address(this)].add(rMarketingPool) (RakuCoin.sol#999)
- _rOwned[sender] = _rOwned[sender].sub(rAmount) (RakuCoin.sol#967)
- _rOwned[sender] = _rOwned[sender].sub(rAmount) (RakuCoin.sol#958)
- _rOwned[sender] = _rOwned[sender].sub(rAmount) (RakuCoin.sol#978)
- _rOwned[sender] = _rOwned[sender].sub(rAmount) (RakuCoin.sol#988)
- _rOwned[recipient] = _rOwned[recipient].add(rTransferAmount) (RakuCoin.sol#959)
- _rOwned[recipient] = _rOwned[recipient].add(rTransferAmount) (RakuCoin.sol#979)
- _rOwned[recipient] = _rOwned[recipient].add(rTransferAmount) (RakuCoin.sol#969)
- _rOwned[recipient] = _rOwned[recipient].add(rTransferAmount) (RakuCoin.sol#990)
- _tokenTransfer(sender,recipient,amount,takeFee) (RakuCoin.sol#894)
- _rTotal = _rTotal.sub(rFee) (RakuCoin.sol#1005)
- _tokenTransfer(sender,recipient,amount,takeFee) (RakuCoin.sol#894)
- _tOwned[address(this)] = _tOwned[address(this)].add(tMarketingPool) (RakuCoin.sol#1001)
- _tOwned[sender] = _tOwned[sender].sub(tAmount) (RakuCoin.sol#987)
- _tOwned[sender] = _tOwned[sender].sub(tAmount) (RakuCoin.sol#977)
- _tOwned[recipient] = _tOwned[recipient].add(tTransferAmount) (RakuCoin.sol#968)
- _tOwned[recipient] = _tOwned[recipient].add(tTransferAmount) (RakuCoin.sol#989)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancyvulnerabilities
INFO:Detectors:

RakuCoin._setTaxFee(uint256) (RakuCoin.sol#1062-1065) contains a tautology or contradiction:
- require(bool,string)(taxFee >= 0 && taxFee <= 10,taxFee should be in 0 - 10) (RakuCoin.sol#1063)
RakuCoin._setMarketingPoolFee(uint256) (RakuCoin.sol#1067-1070) contains a tautology or
contradiction:
- require(bool,string)(MarketingPoolFee >= 0 && MarketingPoolFee <= 11,MarketingPoolFee should be in 0 - 11) (RakuCoin.sol#1068)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#tautology-orcontradiction
INFO:Detectors:
RakuCoin.allowance(address,address).owner (RakuCoin.sol#740) shadows:
- Ownable.owner() (RakuCoin.sol#387-389) (function)
RakuCoin._approve(address,address,uint256).owner (RakuCoin.sol#845) shadows:
- Ownable.owner() (RakuCoin.sol#387-389) (function)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#local-variable-shadowing
INFO:Detectors:
RakuCoin.constructor(address).MarketingPoolWalletAddress (RakuCoin.sol#695) lacks a zerocheck
on :
- _MarketingPoolWalletAddress = MarketingPoolWalletAddress (RakuCoin.sol#696)
RakuCoin._setMarketingPoolWallet(address).MarketingPoolWalletAddress (RakuCoin.sol#1072)
lacks a zero-check on :
- _MarketingPoolWalletAddress = MarketingPoolWalletAddress (RakuCoin.sol#1073)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#missing-zero-addressvalidation
INFO:Detectors:
Reentrancy in RakuCoin._transfer(address,address,uint256) (RakuCoin.sol#853-895):
External calls:
- swapTokensForEth(contractTokenBalance) (RakuCoin.sol#877)
- uniswapV2Router.swapExactTokensForETHSupportingFeeOnTransferTokens(tokenAmount,0,path,
address(this),block.timestamp) (RakuCoin.sol#906-912)
External calls sending eth:
- sendETHToMarketingPool(address(this).balance) (RakuCoin.sol#881)
- _MarketingPoolWalletAddress.transfer(amount) (RakuCoin.sol#916)
State variables written after the call(s):
- _tokenTransfer(sender,recipient,amount,takeFee) (RakuCoin.sol#894)
- _MarketingPoolFee = _previousMarketingPoolFee (RakuCoin.sol#838)
- _MarketingPoolFee = 0 (RakuCoin.sol#833)
- _tokenTransfer(sender,recipient,amount,takeFee) (RakuCoin.sol#894)
- _previousMarketingPoolFee = _MarketingPoolFee (RakuCoin.sol#830)
- _tokenTransfer(sender,recipient,amount,takeFee) (RakuCoin.sol#894)
- _previousTaxFee = _taxFee (RakuCoin.sol#829)
- _tokenTransfer(sender,recipient,amount,takeFee) (RakuCoin.sol#894)
- _tFeeTotal = _tFeeTotal.add(tFee) (RakuCoin.sol#1006)
- _tokenTransfer(sender,recipient,amount,takeFee) (RakuCoin.sol#894)

- _taxFee = _previousTaxFee (RakuCoin.sol#837)
- _taxFee = 0 (RakuCoin.sol#832)
Reentrancy in RakuCoin.constructor(address) (RakuCoin.sol#695-712):
External calls:
- uniswapV2Pair =
IUniswapV2Factory(_uniswapV2Router.factory()).createPair(address(this),_uniswapV2Ro
uter.WE
TH()) (RakuCoin.sol#701-702)
State variables written after the call(s):
- _isExcludedFromFee[owner()] = true (RakuCoin.sol#708)
- _isExcludedFromFee[address(this)] = true (RakuCoin.sol#709)
- uniswapV2Router = _uniswapV2Router (RakuCoin.sol#705)
Reentrancy in RakuCoin.transferFrom(address,address,uint256) (RakuCoin.sol#749-753):
External calls:
- _transfer(sender,recipient,amount) (RakuCoin.sol#750)
-
uniswapV2Router.swapExactTokensForETHSupportingFeeOnTransferTokens(tokenAmou
nt,0,path,
address(this),block.timestamp) (RakuCoin.sol#906-912)
External calls sending eth:
- _transfer(sender,recipient,amount) (RakuCoin.sol#750)
- _MarketingPoolWalletAddress.transfer(amount) (RakuCoin.sol#916)
State variables written after the call(s):
-
_approve(sender,_msgSender(),_allowances[sender][_msgSender()].sub(amount,ERC20:
transfer amount exceeds allowance)) (RakuCoin.sol#751)
- _allowances[owner][spender] = amount (RakuCoin.sol#849)
Reference:
https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancyvulnerabilities-
2
INFO:Detectors:
Reentrancy in RakuCoin._transfer(address,address,uint256) (RakuCoin.sol#853-895):
External calls:
- swapTokensForEth(contractTokenBalance) (RakuCoin.sol#877)
-
uniswapV2Router.swapExactTokensForETHSupportingFeeOnTransferTokens(tokenAmou
nt,0,path,
address(this),block.timestamp) (RakuCoin.sol#906-912)
External calls sending eth:
- sendETHToMarketingPool(address(this).balance) (RakuCoin.sol#881)
- _MarketingPoolWalletAddress.transfer(amount) (RakuCoin.sol#916)
Event emitted after the call(s):
- Transfer(sender,recipient,tTransferAmount) (RakuCoin.sol#962)
- _tokenTransfer(sender,recipient,amount,takeFee) (RakuCoin.sol#894)
- Transfer(sender,recipient,tTransferAmount) (RakuCoin.sol#972)
- _tokenTransfer(sender,recipient,amount,takeFee) (RakuCoin.sol#894)
- Transfer(sender,recipient,tTransferAmount) (RakuCoin.sol#982)
- _tokenTransfer(sender,recipient,amount,takeFee) (RakuCoin.sol#894)
- Transfer(sender,recipient,tTransferAmount) (RakuCoin.sol#993)
- _tokenTransfer(sender,recipient,amount,takeFee) (RakuCoin.sol#894)
Reentrancy in RakuCoin.constructor(address) (RakuCoin.sol#695-712):
External calls:
- uniswapV2Pair =
IUniswapV2Factory(_uniswapV2Router.factory()).createPair(address(this),_uniswapV2Ro

uter.WE
TH()) (RakuCoin.sol#701-702)
Event emitted after the call(s):
- Transfer(address(0),_msgSender(),_tTotal) (RakuCoin.sol#711)
Reentrancy in RakuCoin.transferFrom(address,address,uint256) (RakuCoin.sol#749-753):
External calls:
- _transfer(sender,recipient,amount) (RakuCoin.sol#750)
-
uniswapV2Router.swapExactTokensForETHSupportingFeeOnTransferTokens(tokenAmou
nt,0,path,
address(this),block.timestamp) (RakuCoin.sol#906-912)
External calls sending eth:
- _transfer(sender,recipient,amount) (RakuCoin.sol#750)
- _MarketingPoolWalletAddress.transfer(amount) (RakuCoin.sol#916)
Event emitted after the call(s):
- Approval(owner,spender,amount) (RakuCoin.sol#850)
- _approve(sender,_msgSender(),_allowances[sender]
[_msgSender()].sub(amount,ERC20: transfer amount exceeds allowance))
(RakuCoin.sol#751)
Reference:
https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancyvulnerabilities-
3
INFO:Detectors:
Ownable.unlock() (RakuCoin.sol#434-439) uses timestamp for comparisons
Dangerous comparisons:
- require(bool,string)(now > _lockTime,Contract is locked until 7 days) (RakuCoin.sol#436)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#block-timestamp
INFO:Detectors:
Address.isContract(address) (RakuCoin.sol#251-260) uses assembly
- INLINE ASM (RakuCoin.sol#258)
Address._functionCallWithValue(address,bytes,uint256,string) (RakuCoin.sol#344-365)
uses
assembly
- INLINE ASM (RakuCoin.sol#357-360)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#assembly-usage
INFO:Detectors:
Address._functionCallWithValue(address,bytes,uint256,string) (RakuCoin.sol#344-365) is
never
used and should be removed
Address.functionCall(address,bytes) (RakuCoin.sol#304-306) is never used and should be
removed
Address.functionCall(address,bytes,string) (RakuCoin.sol#314-316) is never used and
should be
removed
Address.functionCallWithValue(address,bytes,uint256) (RakuCoin.sol#329-331) is never
used and
should be removed
Address.functionCallWithValue(address,bytes,uint256,string) (RakuCoin.sol#339-342) is
never
used and should be removed
Address.isContract(address) (RakuCoin.sol#251-260) is never used and should be
removed
Address.sendValue(address,uint256) (RakuCoin.sol#278-284) is never used and should
be removed

Context._msgData() (RakuCoin.sol#13-16) is never used and should be removed
RakuCoin._getMaxTxAmount() (RakuCoin.sol#1054-1056) is never used and should be removed
RakuCoin._getTaxFee() (RakuCoin.sol#1050-1052) is never used and should be removed
SafeMath.mod(uint256,uint256) (RakuCoin.sol#211-213) is never used and should be removed
SafeMath.mod(uint256,uint256,string) (RakuCoin.sol#227-230) is never used and should be
removed
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code
INFO:Detectors:
RakuCoin._rTotal (RakuCoin.sol#660) is set pre-construction with a non-constant function or state
variable:
- (MAX - (MAX % _tTotal))
RakuCoin._previousTaxFee (RakuCoin.sol#671) is set pre-construction with a non-constant
function or state variable:
- _taxFee
RakuCoin._previousMarketingPoolFee (RakuCoin.sol#672) is set pre-construction with a nonconstant
function or state variable:
- _MarketingPoolFee
Reference:
https://github.com/crytic/slither/wiki/Detector-Documentation#function-initializingstate-variables
INFO:Detectors:
Low level call in Address.sendValue(address,uint256) (RakuCoin.sol#278-284):
- (success) = recipient.call{value: amount}() (RakuCoin.sol#282)
Low level call in Address._functionCallWithValue(address,bytes,uint256,string) (RakuCoin.sol#344-365):
- (success,returndata) = target.call{value: weiValue}(data) (RakuCoin.sol#348)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#low-level-calls
INFO:Detectors:
Function IUniswapV2Pair.DOMAIN_SEPARATOR() (RakuCoin.sol#473) is not in mixedCase
Function IUniswapV2Pair.PERMIT_TYPEHASH() (RakuCoin.sol#474) is not in mixedCase
Function IUniswapV2Pair.MINIMUM_LIQUIDITY() (RakuCoin.sol#491) is not in mixedCase
Function IUniswapV2Router01.WETH() (RakuCoin.sol#511) is not in mixedCase
Function RakuCoin._getETHBalance() (RakuCoin.sol#1058-1060) is not in mixedCase
Function RakuCoin._setTaxFee(uint256) (RakuCoin.sol#1062-1065) is not in mixedCase
Function RakuCoin._setMarketingPoolFee(uint256) (RakuCoin.sol#1067-1070) is not in mixedCase
Parameter RakuCoin._setMarketingPoolFee(uint256).MarketingPoolFee (RakuCoin.sol#1067) is
not in mixedCase
Function RakuCoin._setMarketingPoolWallet(address) (RakuCoin.sol#1072-1074) is not in mixedCase
Parameter RakuCoin._setMarketingPoolWallet(address).MarketingPoolWalletAddress (RakuCoin.sol#1072) is not in mixedCase
Function RakuCoin._setMaxTxAmount(uint256) (RakuCoin.sol#1076-1079) is not in mixedCase
Variable RakuCoin._MarketingPoolFee (RakuCoin.sol#670) is not in mixedCase

Variable RakuCoin._MarketingPoolWalletAddress (RakuCoin.sol#674) is not in mixedCase
Reference:
https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-soliditynaming-
conventions
INFO:Detectors:
Redundant expression "this (RakuCoin.sol#14)" inContext (RakuCoin.sol#8-17)
Reference:
https://github.com/crytic/slither/wiki/Detector-Documentation#redundant-statements
INFO:Detectors:
Reentrancy in RakuCoin._transfer(address,address,uint256) (RakuCoin.sol#853-895):
External calls:
- sendETHToMarketingPool(address(this).balance) (RakuCoin.sol#881)
- _MarketingPoolWalletAddress.transfer(amount) (RakuCoin.sol#916)
State variables written after the call(s):
- _tokenTransfer(sender,recipient,amount,takeFee) (RakuCoin.sol#894)
- _MarketingPoolFee = _previousMarketingPoolFee (RakuCoin.sol#838)
- _MarketingPoolFee = 0 (RakuCoin.sol#833)
- _tokenTransfer(sender,recipient,amount,takeFee) (RakuCoin.sol#894)
- _previousMarketingPoolFee = _MarketingPoolFee (RakuCoin.sol#830)
- _tokenTransfer(sender,recipient,amount,takeFee) (RakuCoin.sol#894)
- _previousTaxFee = _taxFee (RakuCoin.sol#829)
- _tokenTransfer(sender,recipient,amount,takeFee) (RakuCoin.sol#894)
- _rOwned[address(this)] = _rOwned[address(this)].add(rMarketingPool)
(RakuCoin.sol#999)
- _rOwned[sender] = _rOwned[sender].sub(rAmount) (RakuCoin.sol#967)
- _rOwned[sender] = _rOwned[sender].sub(rAmount) (RakuCoin.sol#958)
- _rOwned[sender] = _rOwned[sender].sub(rAmount) (RakuCoin.sol#978)
- _rOwned[sender] = _rOwned[sender].sub(rAmount) (RakuCoin.sol#988)
- _rOwned[recipient] = _rOwned[recipient].add(rTransferAmount)
(RakuCoin.sol#959)
- _rOwned[recipient] = _rOwned[recipient].add(rTransferAmount)
(RakuCoin.sol#979)
- _rOwned[recipient] = _rOwned[recipient].add(rTransferAmount)
(RakuCoin.sol#969)
- _rOwned[recipient] = _rOwned[recipient].add(rTransferAmount)
(RakuCoin.sol#990)
- _tokenTransfer(sender,recipient,amount,takeFee) (RakuCoin.sol#894)
- _rTotal = _rTotal.sub(rFee) (RakuCoin.sol#1005)
- _tokenTransfer(sender,recipient,amount,takeFee) (RakuCoin.sol#894)
- _tFeeTotal = _tFeeTotal.add(tFee) (RakuCoin.sol#1006)
- _tokenTransfer(sender,recipient,amount,takeFee) (RakuCoin.sol#894)
- _tOwned[address(this)] = _tOwned[address(this)].add(tMarketingPool)
(RakuCoin.sol#1001)
- _tOwned[sender] = _tOwned[sender].sub(tAmount) (RakuCoin.sol#987)
- _tOwned[sender] = _tOwned[sender].sub(tAmount) (RakuCoin.sol#977)
- _tOwned[recipient] = _tOwned[recipient].add(tTransferAmount)
(RakuCoin.sol#968)
- _tOwned[recipient] = _tOwned[recipient].add(tTransferAmount)
(RakuCoin.sol#989)
- _tokenTransfer(sender,recipient,amount,takeFee) (RakuCoin.sol#894)
- _taxFee = _previousTaxFee (RakuCoin.sol#837)
- _taxFee = 0 (RakuCoin.sol#832)
Event emitted after the call(s):

- Transfer(sender,recipient,tTransferAmount) (RakuCoin.sol#962)
- _tokenTransfer(sender,recipient,amount,takeFee) (RakuCoin.sol#894)
- Transfer(sender,recipient,tTransferAmount) (RakuCoin.sol#982)
- _tokenTransfer(sender,recipient,amount,takeFee) (RakuCoin.sol#894)
- Transfer(sender,recipient,tTransferAmount) (RakuCoin.sol#972)
- _tokenTransfer(sender,recipient,amount,takeFee) (RakuCoin.sol#894)
- Transfer(sender,recipient,tTransferAmount) (RakuCoin.sol#993)
- _tokenTransfer(sender,recipient,amount,takeFee) (RakuCoin.sol#894)
Reentrancy in RakuCoin.transferFrom(address,address,uint256) (RakuCoin.sol#749-753):
External calls:
- _transfer(sender,recipient,amount) (RakuCoin.sol#750)
- _MarketingPoolWalletAddress.transfer(amount) (RakuCoin.sol#916)
State variables written after the call(s):
-
_approve(sender,_msgSender(),_allowances[sender][_msgSender()].sub(amount,ERC20:
transfer amount exceeds allowance)) (RakuCoin.sol#751)
- _allowances[owner][spender] = amount (RakuCoin.sol#849)
Event emitted after the call(s):
- Approval(owner,spender,amount) (RakuCoin.sol#850)
- _approve(sender,_msgSender(),_allowances[sender]
[_msgSender()].sub(amount,ERC20: transfer amount exceeds allowance))
(RakuCoin.sol#751)
Reference:
https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancyvulnerabilities-
4
INFO:Detectors:
Variable
IUniswapV2Router01.addLiquidity(address,address,uint256,uint256,uint256,uint256,addre
ss,uint25
6).amountADesired (RakuCoin.sol#516) is too similar to
IUniswapV2Router01.addLiquidity(address,address,uint256,uint256,uint256,uint256,addre
ss,uint25
6).amountBDesired (RakuCoin.sol#517)
Variable RakuCoin._takeMarketingPool(uint256).rMarketingPool (RakuCoin.sol#998) is
too
similar to RakuCoin._transferFromExcluded(address,address,uint256).tMarketingPool
(RakuCoin.sol#976)
Variable RakuCoin._takeMarketingPool(uint256).rMarketingPool (RakuCoin.sol#998) is
too
similar to RakuCoin._getTValues(uint256,uint256,uint256).tMarketingPool
(RakuCoin.sol#1021)
Variable RakuCoin._takeMarketingPool(uint256).rMarketingPool (RakuCoin.sol#998) is
too
similar to RakuCoin._transferToExcluded(address,address,uint256).tMarketingPool
(RakuCoin.sol#966)
Variable RakuCoin._takeMarketingPool(uint256).rMarketingPool (RakuCoin.sol#998) is
too
similar to RakuCoin._transferStandard(address,address,uint256).tMarketingPool
(RakuCoin.sol#957)
Variable RakuCoin._takeMarketingPool(uint256).rMarketingPool (RakuCoin.sol#998) is
too
similar to RakuCoin._takeMarketingPool(uint256).tMarketingPool (RakuCoin.sol#996)
Variable RakuCoin._takeMarketingPool(uint256).rMarketingPool (RakuCoin.sol#998) is
too

similar to RakuCoin._getValues(uint256).tMarketingPool (RakuCoin.sol#1013)
Variable RakuCoin._takeMarketingPool(uint256).rMarketingPool (RakuCoin.sol#998) is too
similar to RakuCoin._transferBothExcluded(address,address,uint256).tMarketingPool (RakuCoin.sol#986)
Variable RakuCoin._transferBothExcluded(address,address,uint256).rTransferAmount (RakuCoin.sol#986) is too similar to
RakuCoin._transferFromExcluded(address,address,uint256).tTransferAmount (RakuCoin.sol#976)
Variable RakuCoin._transferBothExcluded(address,address,uint256).rTransferAmount (RakuCoin.sol#986) is too similar to RakuCoin._getValues(uint256).tTransferAmount (RakuCoin.sol#1013)
Variable RakuCoin._transferFromExcluded(address,address,uint256).rTransferAmount (RakuCoin.sol#976) is too similar to RakuCoin._getValues(uint256).tTransferAmount (RakuCoin.sol#1013)
Variable RakuCoin.reflectionFromToken(uint256,bool).rTransferAmount (RakuCoin.sol#792) is
too similar to RakuCoin._transferBothExcluded(address,address,uint256).tTransferAmount (RakuCoin.sol#986)
Variable RakuCoin._getRValues(uint256,uint256,uint256).rTransferAmount (RakuCoin.sol#1029)
is too similar to RakuCoin._getTValues(uint256,uint256,uint256).tTransferAmount (RakuCoin.sol#1022)
Variable RakuCoin._transferBothExcluded(address,address,uint256).rTransferAmount (RakuCoin.sol#986) is too similar to
RakuCoin._transferBothExcluded(address,address,uint256).tTransferAmount (RakuCoin.sol#986)
Variable RakuCoin._getRValues(uint256,uint256,uint256).rTransferAmount (RakuCoin.sol#1029)
is too similar to
RakuCoin._transferFromExcluded(address,address,uint256).tTransferAmount (RakuCoin.sol#976)
Variable RakuCoin._transferToExcluded(address,address,uint256).rTransferAmount (RakuCoin.sol#966) is too similar to RakuCoin._getValues(uint256).tTransferAmount (RakuCoin.sol#1013)
Variable RakuCoin._transferToExcluded(address,address,uint256).rTransferAmount (RakuCoin.sol#966) is too similar to
RakuCoin._transferFromExcluded(address,address,uint256).tTransferAmount (RakuCoin.sol#976)
Variable RakuCoin._transferFromExcluded(address,address,uint256).rTransferAmount (RakuCoin.sol#976) is too similar to
RakuCoin._transferFromExcluded(address,address,uint256).tTransferAmount (RakuCoin.sol#976)
Variable RakuCoin._transferBothExcluded(address,address,uint256).rTransferAmount (RakuCoin.sol#986) is too similar to
RakuCoin._getTValues(uint256,uint256,uint256).tTransferAmount (RakuCoin.sol#1022)
Variable RakuCoin._transferStandard(address,address,uint256).rTransferAmount (RakuCoin.sol#957) is too similar to RakuCoin._getValues(uint256).tTransferAmount (RakuCoin.sol#1013)
Variable RakuCoin._getRValues(uint256,uint256,uint256).rTransferAmount (RakuCoin.sol#1029)
is too similar to RakuCoin._getValues(uint256).tTransferAmount (RakuCoin.sol#1013)
Variable RakuCoin.reflectionFromToken(uint256,bool).rTransferAmount (RakuCoin.sol#792) is

too similar to RakuCoin._transferStandard(address,address,uint256).tTransferAmount (RakuCoin.sol#957)
Variable RakuCoin._getRValues(uint256,uint256,uint256).rTransferAmount (RakuCoin.sol#1029)
is too similar to RakuCoin._transferToExcluded(address,address,uint256).tTransferAmount (RakuCoin.sol#966)
Variable RakuCoin._transferBothExcluded(address,address,uint256).rTransferAmount (RakuCoin.sol#986) is too similar to RakuCoin._transferToExcluded(address,address,uint256).tTransferAmount (RakuCoin.sol#966)
Variable RakuCoin._transferToExcluded(address,address,uint256).rTransferAmount (RakuCoin.sol#966) is too similar to RakuCoin._transferToExcluded(address,address,uint256).tTransferAmount (RakuCoin.sol#966)
Variable RakuCoin.reflectionFromToken(uint256,bool).rTransferAmount (RakuCoin.sol#792) is
too similar to RakuCoin._transferToExcluded(address,address,uint256).tTransferAmount (RakuCoin.sol#966)
Variable RakuCoin._getRValues(uint256,uint256,uint256).rTransferAmount (RakuCoin.sol#1029)
is too similar to RakuCoin._transferStandard(address,address,uint256).tTransferAmount (RakuCoin.sol#957)
Variable RakuCoin.reflectionFromToken(uint256,bool).rTransferAmount (RakuCoin.sol#792) is
too similar to RakuCoin._getValues(uint256).tTransferAmount (RakuCoin.sol#1013)
Variable RakuCoin._transferFromExcluded(address,address,uint256).rTransferAmount (RakuCoin.sol#976) is too similar to RakuCoin._transferStandard(address,address,uint256).tTransferAmount (RakuCoin.sol#957)
Variable RakuCoin._transferStandard(address,address,uint256).rTransferAmount (RakuCoin.sol#957) is too similar to RakuCoin._transferStandard(address,address,uint256).tTransferAmount (RakuCoin.sol#957)
Variable RakuCoin._transferBothExcluded(address,address,uint256).rTransferAmount (RakuCoin.sol#986) is too similar to RakuCoin._transferStandard(address,address,uint256).tTransferAmount (RakuCoin.sol#957)
Variable RakuCoin.reflectionFromToken(uint256,bool).rTransferAmount (RakuCoin.sol#792) is
too similar to RakuCoin._transferFromExcluded(address,address,uint256).tTransferAmount (RakuCoin.sol#976)
Variable RakuCoin._transferToExcluded(address,address,uint256).rTransferAmount (RakuCoin.sol#966) is too similar to RakuCoin._transferStandard(address,address,uint256).tTransferAmount (RakuCoin.sol#957)
Variable RakuCoin._getRValues(uint256,uint256,uint256).rTransferAmount (RakuCoin.sol#1029)
is too similar to RakuCoin._transferBothExcluded(address,address,uint256).tTransferAmount (RakuCoin.sol#986)
Variable RakuCoin.reflectionFromToken(uint256,bool).rTransferAmount (RakuCoin.sol#792) is
too similar to RakuCoin._getTValues(uint256,uint256,uint256).tTransferAmount

(RakuCoin.sol#1022)
Variable RakuCoin._transferToExcluded(address,address,uint256).rTransferAmount (RakuCoin.sol#966) is too similar to RakuCoin._getTValues(uint256,uint256,uint256).tTransferAmount (RakuCoin.sol#1022)
Variable RakuCoin._transferToExcluded(address,address,uint256).rTransferAmount (RakuCoin.sol#966) is too similar to RakuCoin._transferBothExcluded(address,address,uint256).tTransferAmount (RakuCoin.sol#986)
Variable RakuCoin._transferFromExcluded(address,address,uint256).rTransferAmount (RakuCoin.sol#976) is too similar to RakuCoin._getTValues(uint256,uint256,uint256).tTransferAmount (RakuCoin.sol#1022)
Variable RakuCoin._getValues(uint256).rTransferAmount (RakuCoin.sol#1015) is too similar to RakuCoin._getTValues(uint256,uint256,uint256).tTransferAmount (RakuCoin.sol#1022)
Variable RakuCoin._transferStandard(address,address,uint256).rTransferAmount (RakuCoin.sol#957) is too similar to RakuCoin._transferBothExcluded(address,address,uint256).tTransferAmount (RakuCoin.sol#986)
Variable RakuCoin._transferStandard(address,address,uint256).rTransferAmount (RakuCoin.sol#957) is too similar to RakuCoin._getTValues(uint256,uint256,uint256).tTransferAmount (RakuCoin.sol#1022)
Variable RakuCoin._getValues(uint256).rTransferAmount (RakuCoin.sol#1015) is too similar to RakuCoin._transferToExcluded(address,address,uint256).tTransferAmount (RakuCoin.sol#966)
Variable RakuCoin._transferStandard(address,address,uint256).rTransferAmount (RakuCoin.sol#957) is too similar to RakuCoin._transferFromExcluded(address,address,uint256).tTransferAmount (RakuCoin.sol#976)
Variable RakuCoin._getValues(uint256).rTransferAmount (RakuCoin.sol#1015) is too similar to RakuCoin._transferBothExcluded(address,address,uint256).tTransferAmount (RakuCoin.sol#986)
Variable RakuCoin._getValues(uint256).rTransferAmount (RakuCoin.sol#1015) is too similar to RakuCoin._transferStandard(address,address,uint256).tTransferAmount (RakuCoin.sol#957)
Variable RakuCoin._transferFromExcluded(address,address,uint256).rTransferAmount (RakuCoin.sol#976) is too similar to RakuCoin._transferBothExcluded(address,address,uint256).tTransferAmount (RakuCoin.sol#986)
Variable RakuCoin._transferStandard(address,address,uint256).rTransferAmount (RakuCoin.sol#957) is too similar to RakuCoin._transferToExcluded(address,address,uint256).tTransferAmount (RakuCoin.sol#966)
Variable RakuCoin._getValues(uint256).rTransferAmount (RakuCoin.sol#1015) is too similar to RakuCoin._transferFromExcluded(address,address,uint256).tTransferAmount (RakuCoin.sol#976)
Variable RakuCoin._getValues(uint256).rTransferAmount (RakuCoin.sol#1015) is too similar to RakuCoin._getValues(uint256).tTransferAmount (RakuCoin.sol#1013)
Variable RakuCoin._transferFromExcluded(address,address,uint256).rTransferAmount (RakuCoin.sol#976) is too similar to

RakuCoin._transferToExcluded(address,address,uint256).tTransferAmount
(RakuCoin.sol#966)
Reference:
https://github.com/crytic/slither/wiki/Detector-Documentation#variable-names-are-toosimila
r
INFO:Detectors:
RakuCoin._setMaxTxAmount(uint256) (RakuCoin.sol#1076-1079) uses literals with too
many
digits:
- require(bool,string)(maxTxAmount >= 1000000000000000000000000000,maxTxAmount
should be greater than 1000000000000000000000000000) (RakuCoin.sol#1077)
RakuCoin.slitherConstructorVariables() (RakuCoin.sol#645-1080) uses literals with too
many
digits:
- _tTotal = 1000000000000 * 10 ** 18 (RakuCoin.sol#659)
RakuCoin.slitherConstructorVariables() (RakuCoin.sol#645-1080) uses literals with too
many
digits:
- _maxTxAmount = 1000000000000 * 10 ** 18 (RakuCoin.sol#682)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#too-many-digits
INFO:Detectors:
RakuCoin._decimals (RakuCoin.sol#665) should be constant
RakuCoin._name (RakuCoin.sol#663) should be constant
RakuCoin._numOfTokensToExchangeForMarketingPool (RakuCoin.sol#684) should be
constant
RakuCoin._symbol (RakuCoin.sol#664) should be constant
RakuCoin._tTotal (RakuCoin.sol#659) should be constant
Reference:
https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-thatcould-
be-declared-constant
INFO:Detectors:
renounceOwnership() should be declared external:
- Ownable.renounceOwnership() (RakuCoin.sol#406-409)
transferOwnership(address) should be declared external:
- Ownable.transferOwnership(address) (RakuCoin.sol#415-419)
geUnlockTime() should be declared external:
- Ownable.geUnlockTime() (RakuCoin.sol#421-423)
lock(uint256) should be declared external:
- Ownable.lock(uint256) (RakuCoin.sol#426-431)
unlock() should be declared external:
- Ownable.unlock() (RakuCoin.sol#434-439)
name() should be declared external:
- RakuCoin.name() (RakuCoin.sol#714-716)
symbol() should be declared external:
- RakuCoin.symbol() (RakuCoin.sol#718-720)
decimals() should be declared external:
- RakuCoin.decimals() (RakuCoin.sol#722-724)
totalSupply() should be declared external:
- RakuCoin.totalSupply() (RakuCoin.sol#726-728)
transfer(address,uint256) should be declared external:
- RakuCoin.transfer(address,uint256) (RakuCoin.sol#735-738)
allowance(address,address) should be declared external:
- RakuCoin.allowance(address,address) (RakuCoin.sol#740-742)
approve(address,uint256) should be declared external:

- RakuCoin.approve(address,uint256) (RakuCoin.sol#744-747)
transferFrom(address,address,uint256) should be declared external:
- RakuCoin.transferFrom(address,address,uint256) (RakuCoin.sol#749-753)
increaseAllowance(address,uint256) should be declared external:
- RakuCoin.increaseAllowance(address,uint256) (RakuCoin.sol#755-758)
decreaseAllowance(address,uint256) should be declared external:
- RakuCoin.decreaseAllowance(address,uint256) (RakuCoin.sol#760-763)
isExcluded(address) should be declared external:
- RakuCoin.isExcluded(address) (RakuCoin.sol#765-767)
totalFees() should be declared external:
- RakuCoin.totalFees() (RakuCoin.sol#773-775)
deliver(uint256) should be declared external:
- RakuCoin.deliver(uint256) (RakuCoin.sol#777-784)
reflectionFromToken(uint256,bool) should be declared external:
- RakuCoin.reflectionFromToken(uint256,bool) (RakuCoin.sol#786-795)
isExcludedFromFee(address) should be declared external:
- RakuCoin.isExcludedFromFee(address) (RakuCoin.sol#841-843)
_getETHBalance() should be declared external:
- RakuCoin._getETHBalance() (RakuCoin.sol#1058-1060)
Reference:
https://github.com/crytic/slither/wiki/Detector-Documentation#public-function-thatcould-be-declared-external
INFO:Slither:RakuCoin.sol analyzed (10 contracts with 75 detectors), 129 result(s) found
INFO:Slither:Use https://crytic.io/ to get access to additional detectors and Github integration
root@mnb-ThinkPad-T410:/home/mnb/slitherContracts#

Email: audit@EtherAuthority.io