HackSafe

Smart Contract Security Audit Report

Moon Rocket Coin

December 2022

Security Status

★★★★☆

www.hacksafe.io

Audit Details

Audited project
Moon Rocket Coin

Deployer address
0xc6f0bb2775b1fea7c0ec7fa71fff1a0ceaea237a

Client contacts
Moon Rocket Coin Team

Blockchain
Binance smart chain

Website
Not provieded

Disclaimer

This is a limited report on our findings based on our analysis, in accordance with good industry practice as at 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.

DISCLAIMER: By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. 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 TechRate and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (HackSafe) owe no duty of care towards you or any other person, nor does HackSafe make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and HackSafe hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, HackSafe hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against HackSafe, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report.

The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed.

Procedure

Step 1 - In-Depth Manual Review

Manual line-by-line code reviews to ensure the logic behind each function is sound and safe from various attack vectors. This is the most important and lengthy portion of the audit process (as automated tools often cannot find the nuances that lead to exploits such as flash loan attacks).

Step 2 - Automated Testing

Simulation of a variety of interactions with your Smart Contract on a test blockchain leveraging a combination of automated test tools and manual testing to determine if any security vulnerabilities exist.

Step 3 – Leadership Review

The engineers assigned to the audit will schedule meetings with our leadership team to review the contracts, any comments or findings, and ask questions to further apply adversarial thinking to discuss less common attack vectors.

Step 4 - Resolution of Issues

Consulting with the team to provide our recommendations to ensure the code's security and optimize its gas efficiency, if possible. We assist project team's in resolving any outstanding issues or implementing our recommendations.

Step 5 - Published Audit Report

Boiling down results and findings into an easy-to-read report tailored to the project. Our audit reports highlight resolved issues and any risks that exist to the project or its users, along with any remaining suggested remediation measures. Diagrams are included at the end of each report to help users understand the interactions which occur within the project.

Background

HackSafe was commissioned by Moon Rocket Coin perform an audit of smart contracts:

- https://bscscan.com/token/0x9299C132c34E691edea58102d276A61a0a622dBD#code

The purpose of the audit was to achieve the following:

- Ensure that the smart contract functions as intended.
- Identify potential security issues with the smart contract.

The information in this report should be understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Contract Details

Token contract details for 08.12.2022

Token Type	: DEFI
Contract name	: MoonRocketCoin
Contract address	: 0x9299C132c34E691edea58102d276A61a0a622dBD
Total supply	: 100,000,000
Token ticker	: MRC
Decimals	: 18
Token Holders	: 843
Transactions count	: 7,499
Compiler version	: v0.8.7+commit.e28d00a7
Contract deployer address	: 0xc6f0bb2775b1fea7c0ec7fa71fff1a0ceaea237a
Owner address	: 0xd8ee50587a326d8022ebef6460c960f3645354a4

Audit Summary

According to the standard audit assessment, Customer`s solidity smart contracts are **“Secure”.** This token contract does contain owner control, which do not make it fully decentralized as owner does have control over smart contract.

Insecure	Poor secured	Secure	Well-secured

You are here 

We used various tools like Slither, Mythril 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 issues checking status.

We found 0 critical, 0 high, 1 medium and 1 low.

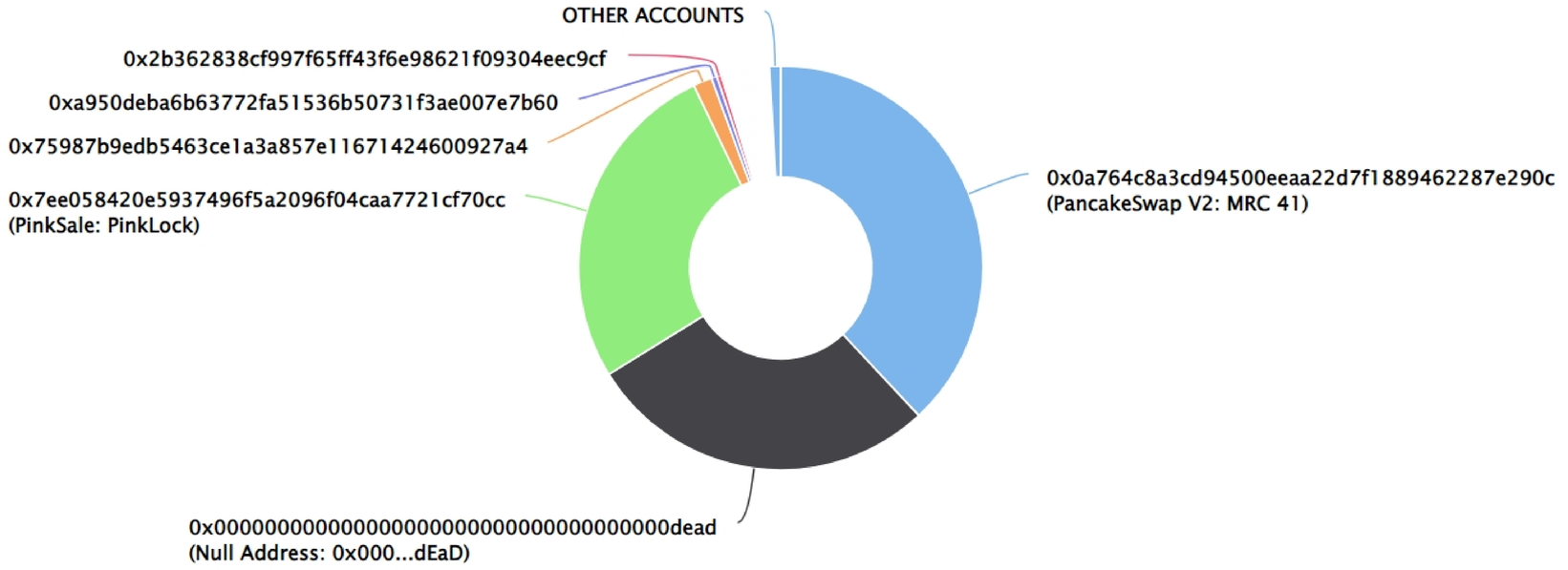
Moon Rocket Coin Token Distribution

The top 100 holders collectively own 99.12% (99,124,495.14 Tokens) of Moon Rocket Coin

Token Total Supply: 100,000,000.00 Token | Total Token Holders: 843

Moon Rocket Coin Top 100 Token Holders

Source: BscScan.com



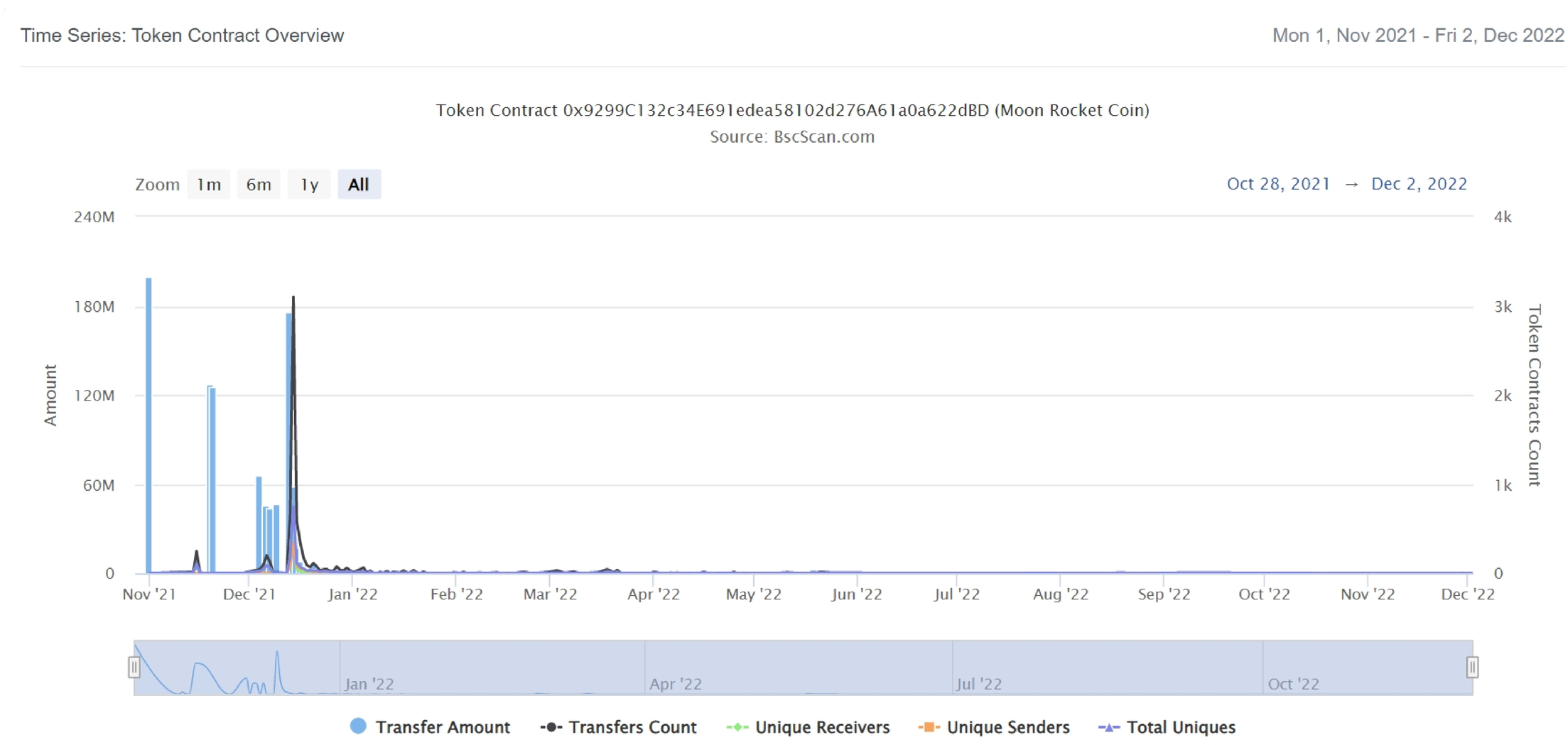
Moon Rocket Coin Token Top 20 Token Holders

(A total of 99,124,495.14 tokens held by the top 100 accounts from the total supply of 100,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	PancakeSwap V2: MRC 41	38,029,391.41224715198630979	38.0294%
2	Null Address: 0x000...dEaD	28,155,823.311587893315443667	28.1558%
3	PinkSale: PinkLock	26,758,579.450688508721757559	26.7586%
4	0x75987b9edb5463ce1a3a857e11671424600927a4	1,493,018.496427530011981556	1.4930%
5	0xa950deba6b63772fa51536b50731f3ae007e7b60	450,370.618869086122010188	0.4504%
6	0x2b362838cf997f65ff43f6e98621f09304eec9cf	365,557.160667870334948191	0.3656%
7	0x80e33ce32271e00e2e0e43110c092aea50024c3a	170,824.212412627306900943	0.1708%
8	0x12a8b474f0b27da91fdb724b90e72cf8d808ba67	166,528.093508774415621801	0.1665%
9	0xf7c9a1651751f26df1a378585c6abcccd994b839	157,876.811832957146671695	0.1579%
10	0xc2a20684a72d861c932c159717607327e9b65817	130,690.214156855723261804	0.1307%
11	0xff1ce534723c951472dbc9774b0242cb6d279172	130,286.374256603400099893	0.1303%
12	0x155adbd9fbe1896a357dc59e866623cac00c828e	125,000	0.1250%
13	0xfc9fe01649989d6d4cdbbda7b7d07e4ce7e6b6b7	121,234.705739905160716376	0.1212%
14	0x39f0457ac343b1aa6f3b9df136cd2a71b5911940	113,109.904534954851171174	0.1131%
15	0x4f7dc03db99e3a41135fc947fabc62b86cfb096c	104,697.136659866850439967	0.1047%
16	0x29966ed528e86ac69398fb78e07c6461c1617a68	104,326.92	0.1043%
17	0x1d3eb4517b5d4756b1230e6f579439029a6a36c6	101,599.749675575735541361	0.1016%
18	0x8adfb0084dfe2f8c38d0d33658d8542520c92928	93,648.801663314605762411	0.0936%
19	0xf77b4a22dd6a5a0a12e7ad2fc157f7597dd9de8e	91,151.83259852376753477	0.0912%
20	0xf446c3f2e005b29a4fb38ad81e58f71360512322	88,427.644393231331668929	0.0884%

Moon Rocket Coin Token Distribution

Moon Rocket Coin Contract Overview



Contract functions details

+[Int] IERC20
    -[Ext] totalSupply
    -[Ext] balanceOf
    -[Ext] transfer
    -[Ext] allowance
    -[Ext] approve
    -[Ext] transferFrom

+[Lib] SafeMath
    -[Int] tryAdd
    -[Int] trySub
    -[Int] tryMul
    -[Int] tryDiv
    -[Int] tryMod
    -[Int] add
    -[Int] sub
    -[Int] mul
    -[Int] div
    -[Int] mod
    -[Int] sub
    -[Int] div
    -[Int] mod

+Context
    -[Int] _msgSender
    -[Int] _msgData

+[Lib] Address
    -[Int] isContract
    -[Int] sendValue
    -[Int] functionCall
    -[Int] functionCall
    -[Int] functionCallWithValue
    -[Int] functionCallWithValue
    -[Int] functionStaticCall
    -[Int] functionStaticCall
    -[Int] functionDelegateCall
    -[Int] functionDelegateCall
    -[Pvt] _verifyCallResult

Contract functions details

+Ownable (Context)
    -[Pub] <Constructor> #
    -[Pub] owner
    -[Pub] renounceOwnership #
     - modifiers: onlyOwner
    -[Pub] transferOwnership #
     - modifiers: onlyOwner
    -[Pvt] _setOwner #

+[Int] IFactory
    -[Ext] createPair #
    -[Ext] getPair

+[Int] IRouter
    -[Ext] factory
    -[Ext] WETH
    -[Ext] addLiquidityETH ($)
    -[Ext] swapExactETHForTokensSupportingFeeOnTransferTokens ($)
    -[Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #

+ MoonRocketCoin (Context, IERC20, Ownable)
    -[Pub] <constructor>#
    -[Pub] name
    -[Pub] symbol
    -[Pub] decimals
    -[Pub] totalSupply
    -[Pub] balanceOf
    -[Pub] transfer #
    -[Pub] allowance
    -[Pub] approve #
    -[Pub] transferFrom #
    -[Pub] increaseAllowance #
    -[Pub] decreaseAllowance #
    -[Pub] isExcludedFromReward
    -[Pub] deliver #
    -[Pub] reflectionFromToken
    -[Ext] startTrading #
     - modifiers: onlyOwner
    -[Pub] tokenFromReflection

Contract functions details

-[Pub] excludeFromReward #
  - modifiers: onlyOwner
-[Ext] includeInReward #
  - modifiers: onlyOwner
-[Pub] excludeFromFee #
  - modifiers: onlyOwner
-[Pub] includeInFee #
  - modifiers: onlyOwner
-[Pub] isExcludedFromFee
-[Ext] setFeeRates #
  - modifiers: onlyOwner
-[Ext] setSellFeeRates #
  - modifiers: onlyOwner
-[Pvt] _reflectRfi #
-[Pvt] _takeDevelopment #
-[Pvt] _takeCharity #
-[Pvt] _takeBuyback #
-[Pvt] _takeLiquidity #
-[Pvt] _getValues
-[Prv] _getTValues
-[Prv] _getRValues
-[Prv] _getRate
-[Prv] _getCurrentSupply
-[Prv] _approve #
-[Prv] _transfer #
-[Prv] _tokenTransfer #
-[Prv] buyBackTokens #
  - modifiers: lockTheSwap
-[Prv] swapETHForTokens #
-[Prv] swapAndLiquify #
  - modifiers: lockTheSwap
-[Prv] addLiquidity #
-[Prv] swapTokensForBNB #
-[Ext] updateDevelopmentWallet #
  - modifiers: onlyOwner
-[Ext] setMaxBuyAndSellAmount #
  - modifiers: onlyOwner
-[Ext] setMaxWalletTokend #

Contract functions details

```
    - modifiers: onlyOwner
-[Ext] updateSwapTokensAtAmount #
  - modifiers: onlyOwner
-[Ext] updateSwapEnabled #
  - modifiers: onlyOwner
-[Ext] updateBuybackEnabled #
  - modifiers: onlyOwner
-[Ext] setAntibot #
  - modifiers: onlyOwner
-[Ext] setBuybackUpperLimit #
  - modifiers: onlyOwner
-[Pub] isBot
-[Ext] setRouterAddress #
  - modifiers: onlyOwner
-[Ext] <Fallback> ($)

($) = payable function
# = non-constant function
```

Issues Checking Status

No.	Title	Status
1.	Unlocked Compiler Version	Low issue
2.	Missing Input Validation	Passed
3.	Race conditions and Reentrancy. Cross-function race conditions.	Passed
4.	Possible delays in data delivery	Passed
5.	Oracle calls.	Passed
6.	Timestamp dependence.	Passed
7.	Integer Overflow and Underflow	Passed
8.	DoS with Revert.	Passed
9.	DoS with block gas limit.	Medium Issue
10.	Methods execution permissions.	Passed
11.	Economy model of the contract.	Passed
12.	Private use data leaks.	Passed
13.	Malicious Event log.	Passed
14.	Scoping and Declarations.	Passed
15.	Uninitialized storage pointers.	Passed
16.	Arithmetic accuracy.	Passed
17.	Design Logic.	Passed
18.	Safe Open Zeppelin contracts implementation and usage.	Passed
19.	Incorrect Naming State Variable	Passed
20.	Too old version	Passed

Severity Definitions

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to assets loss or data manipulations.
High	High-level vulnerabilities are difficult to exploit; however, they also have a 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 assets loss or data manipulations.
Low	Low-level vulnerabilities are mostly related to outdated, unused, etc. code snippets that can't have a significant impact on execution.

Security Issues

Critical Severity Issues

No critical severity issue found.

High Severity Issues

No high severity issue found.

Medium Severity Issues

One medium severity issue found.

1. Out of gas limit

- **Description**

  The function includeInReward() uses the loop to find and remove addresses from the _excluded list. Function will be aborted with OUT_OF_GAS exception if there will be a long excluded addresses list.

  The function _getCurrentSupply also uses the loop for evaluating total supply. It also could be aborted with OUT_OF_GAS exception if there will be a long excluded addresseses list.

- **Recommendation**

  Use EnumerableSet instead of array or do not use long arrays.

Low Severity Issues

One low severity issue found.

1. Unlocked Compiler Version.

- **Description**

  The contract utilizes an unlocked compiler version. An unlocked compiler version in the contract's source code permits the user to compile it at or above a particular version. This, in turn, leads to differences in the generated bytecode between compilations due to differing compiler version numbers. This can lead to ambiguity when debugging as compiler-specific bugs may occur in the codebase that would be difficult to identify over a span of multiple compiler versions rather than a specific one.

- **Recommendation**

  It is advisable that the compiler version is alternatively locked at the lowest version possible so that the contract can be compiled. For example, for version ^0.8.0 the contract should contain the following line:

  pragma solidity 0.8.7;

Centralization

Owner privileges :

- Moon Rocket Coin Contract:
    - Owner can start trading.
    - Owner can change fee rates.
    - Owner can exclude from the fee.
    - Owner can change development wallet address.
    - Owner can change maxBuyAmount and maxSellAmount.
    - Owner can change _maxWalletToken.
    - Owner can change swapTokensAtAmount.
    - Owner can enable/disable swapEnabled and buyBackEnabled.
    - Owner can include in _isBot array.
    - Owner can change buyBackUpperLimit.
    - Owner can change router address.
    - Owner can lock and unlock. By the way, using these functions the owner could retake privileges even after the ownership was renounced.

This smart contract has some functions which can be executed by the admin (Owner) only. If the admin wallet private key would be compromised, then it would create trouble, as smart contract ownership has not been renounced.Following are Admin functions:

- renounceOwnership
- transferOwnership
- startTrading
- excludeFromReward
- includeInReward
- excludeFromFee
- includeinFee
- setfeeRaTes
- seTsellFeeRates
- updateDevelopmentWallet
- setMaxBuyAndsellAmount
- setMaxWalletTokend
- updateSwapTokensAtAmount
- updateSwapEnabled
- updateBuybackEnabled
- setAntibot
- setBuybackUpperLimit
- setRouterAddress

Conclusion

Smart contract contains low and medium severity issues! The further transfer and operations with the fund raised are not related to this particular contract.

HackSafe note: Please check the disclaimer above and note, the audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is provided for the only contract mentioned in the report and does not include any other potential contracts deployed by Owner.