



Smart Contract Security Audit Report

RR/MAYC

June 2022

Security Status



www.hacksafe.io



Audit Details



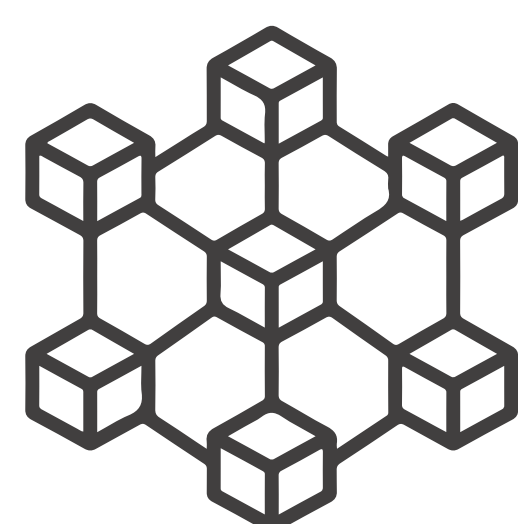
Audited project
RR/MAYC



Deployer address
0x80cFd0322554Eb3cb263FD29559828440F957582



Client contacts
RR/MAYC team



Blockchain
Ethereum



Website
Not provided

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 RR/MAYC token to perform an audit of smart contracts:

- <https://etherscan.io/address/0x0406243ca557c259712be750773177bc714e49f6#code>

The purpose of the audit was to achieve the

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

The information in this report should be understood to 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.

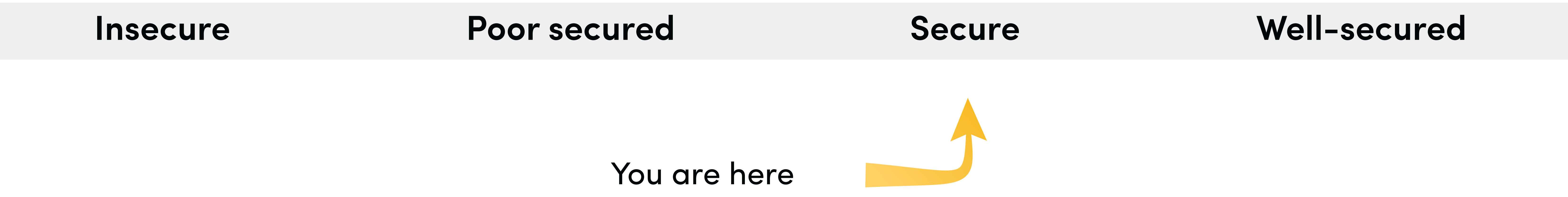
Contract Details

Token contract details for 22.06.2022

Token Type	: ERC721
Contract name	: RRMAYC
Contract address	: 0x0406243Ca557c259712be750773177bc714e49f6
Compiler version	: v0.8.7+commit.e28d00a7
Max Total supply	: 5,555
Token Ticker	: RR/MAYC
Token Holders	: 2,240
Top 100 token holder's dominance	: 42.32%
Transactions count	: 13,147
Contract deployer address	: 0x80cFd0322554Eb3cb263FD29559828440F957582
Owner address	: 0x80cFd0322554Eb3cb263FD29559828440F957582

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.



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, 0 medium and 1 low and some very low-level issues. These issues are not critical ones.

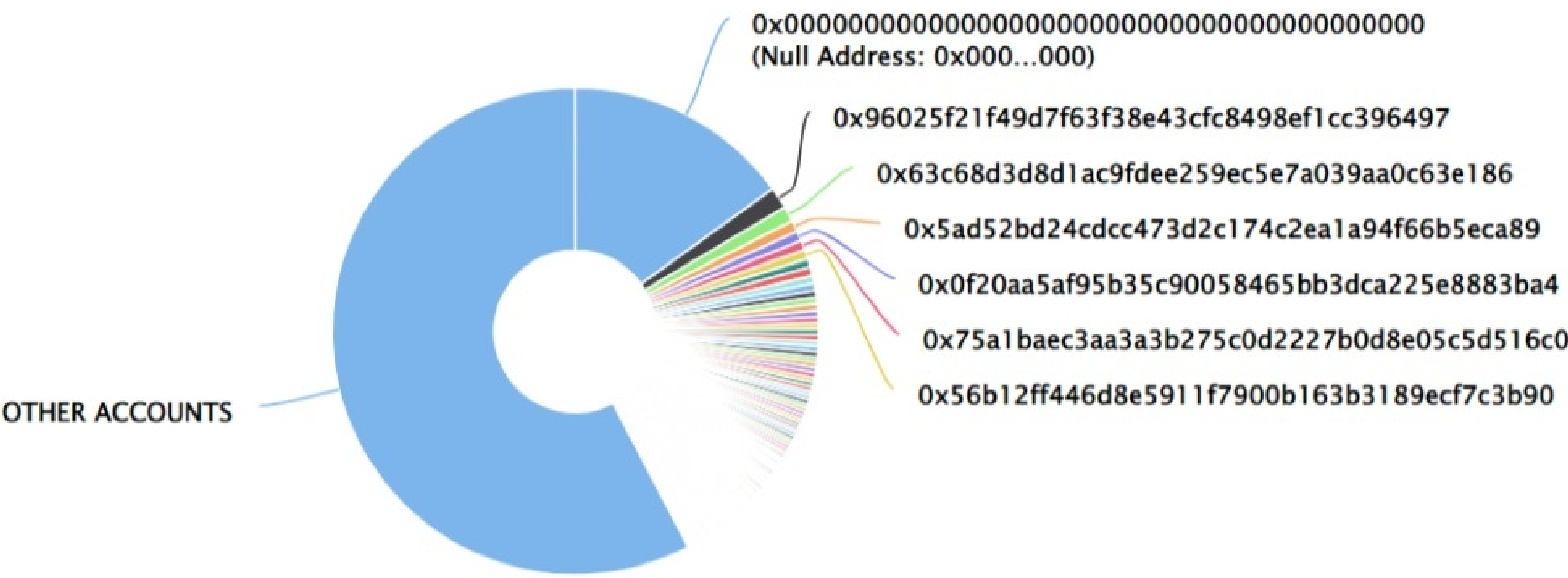
RR/MAYC Distribution

💡 The top 100 holders collectively own 42.32% (2,351.00 Tokens) of RR/MAYC

💡 Token Total Supply: 5,555.00 Token | Total Token Holders: 2,239

RR/MAYC Top 100 Token Holders

Source: Etherscan.io



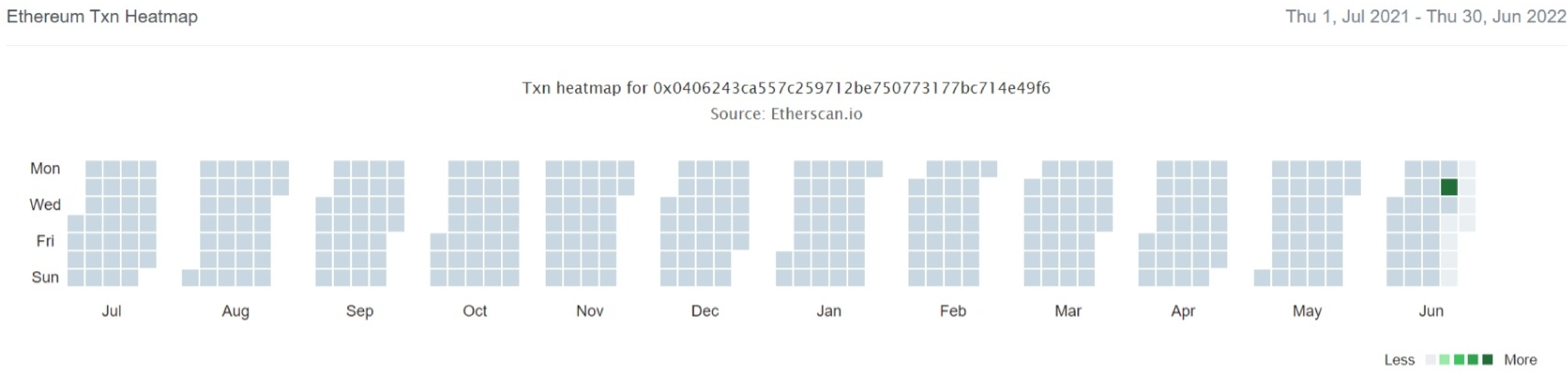
RR/MAYC Top 20 Token Holders

(A total of 2,351.00 tokens held by the top 100 accounts from the total supply of 5,555.00 token)

Rank	Address	Quantity (Token)	Percentage
1	Null Address: 0x000...000	837	15.0675%
2	(<) azrx.eth	80	1.4401%
3	(<) 1980925.eth	56	1.0081%
4	0x5ad52bd24cdcc473d2c174c2ea1a94f66b5eca89	43	0.7741%
5	0x0f20aa5af95b35c90058465bb3dca225e8883ba4	36	0.6481%
6	0x75a1baec3aa3a3b275c0d2227b0d8e05c5d516c0	35	0.6301%
7	0x56b12ff446d8e5911f7900b163b3189ecf7c3b90	35	0.6301%
8	(<) lavajava.eth	32	0.5761%
9	0xdf17f86923266b4ed9b78e5c26da55b98cdee854	31	0.5581%
10	(<) guguzx.eth	29	0.5221%
11	0x7eed45f23bec843e4437cadd35f2c03117d4a17b	26	0.4680%
12	0xdbee45ad97ab3f2779043f93a0ff29f89adaf144	25	0.4500%
13	(<) thatjpeg.eth	24	0.4320%
14	0x47b20272ebee4233aad387dd88aa80ddaf55032b	24	0.4320%
15	(<) thelotto.eth	24	0.4320%
16	(<) dachui.eth	23	0.4140%
17	0xfa25e9dc5a105202483d1b9dfef79627a95e4999	21	0.3780%
18	0x2d923d4846b958b19662c1b3d2c686b4b8b2aadf	21	0.3780%
19	0x342fd6acca1de5fdef53740ce1e0062b8112fa03	21	0.3780%
20	0x45889f54899cf22660a98e2a493d22a158cb626c	20	0.3600%

RR/MAYC Distribution

Ethereum Txn Heatmap



Contract functions details

+ [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

+ [Lib] Counters

- [Int] current
- [Int] increment
- [Int] decrement
- [Int] reset

+ ReentrancyGuard

- <constructor>

+ [Int] IERC20

- [Ext] totalSupply
- [Ext] balanceOf
- [Ext] transfer
- [Ext] allowance
- [Ext] approve
- [Ext] transferFrom

+ [Lib] Strings

- [Int] toString
- [Int] toHexString
- [Int] toHexString

+Context

- [Int] _msgSender
- [Int] _msgData

Contract functions details

+ Ownable (Context)

- <constructor>
- [Pub] owner
- [Pub] renounceOwnership #
-modifiers: onlyOwner
- [Pub] transferOwnership #
-modifiers: onlyOwner
- [Int] _transferOwnership #

+ [Lib] Address

- [Int] isContract
- [Int] sendValue
- [Int] functionCall
- [Int] functionCall
- [Int] functionCallWithValue
- [Int] functionCallWithValue
- [Int] functionStaticCall
- [Int] functionStaticCall
- [Int] functionDelegateCall
- [Int] functionDelegateCall
- [Int] verifyCallResult

+ [Int] IERC721Receiver

- [Ext] onERC721Received

+ [Int] IERC165

- [Ext] supportsInterface

+ [Int] IERC2981 (IERC165)

- [Ext] royaltyInfo

+ ERC165 (IERC165)

- [Pub] supportsInterface

+ [Int] IERC721 (IERC165)

- [Ext] balanceOf
- [Ext] ownerOf
- [Ext] safeTransferFrom #
- [Ext] transferFrom #
- [Ext] approve #
- [Ext] getApproved #

Contract functions details

-[Ext] setApprovalForAll #

-[Ext] isApprovedForAll #

-[Ext] safeTransferFrom #

+ [Int] IERC721Enumerable (IERC721)

-[Ext] totalSupply

-[Ext] tokenOfOwnerByIndex

-[Ext] tokenByIndex

+ [Int] IERC721Metadata (IERC721)

-[Ext] name

-[Ext] symbol

-[Ext] tokenURI

+ ERC721A(Context,
ERC165,
IERC721,
IERC721Metadata,
IERC721Enumerable)

-<constructor> #

-[Pub] totalSupply

-[Pub] tokenByIndex

-[Pub] tokenOfOwnerByIndex

-[Pub] supportsInterface

-[Pub] balanceOf

-[Int] _numberMinted

-[Int] ownershipOf

-[Pub] ownerOf

-[Pub] name

-[Pub] symbol

-[Pub] tokenURI

-[Int] _baseURI

-[Pub] approve

-[Pub] getApproved #

-[Pub] setApprovalForAll #

-[Pub] isApprovedForAll #

-[Pub] transferFrom #

-[Pub] safeTransferFrom #

-[Pub] safeTransferFrom #

Contract functions details

- [Int] _exists
- [Int] _safeMint
- [Int] _safeMint
- [Pvt] _transfer #
- [Pvt] _approve #
- [Int] _setOwnersExplicit #
- [Pvt] _checkOnERC721Received #
- [Int] _beforeTokenTransfers
- [Int] _afterTokenTransfers

+ RRMAYC (ERC721A, IERC2981, Ownable, ReentrancyGuard)

- <constructor >
- [Ext] mint \$
 - modifiers: nonReentrant, isCorrectPayment, publicSaleActive, canMintNFTs, maxMintsPerTX
- [Ext] setIsOpenSeaProxyActive #
 - modifiers: onlyOwner,
- [Ext] setIsPublicSaleActive #
 - modifiers: onlyOwner
- [Ext] setNumFreeMints #
 - modifiers: onlyOwner
- [Pub] withdraw \$
 - modifiers: onlyOwner
- [Pub] withdrawTokens #
 - modifiers: onlyOwner
- [Pvt] nextTokenId #
- [Pub] supportsInterface
- [Pub] isApprovedForAll
- [Pub] tokenURI
- [Ext] royaltyInfo

+ OwnableDelegateProxy

+ ProxyRegistry

(\$) = 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.	Passed
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.	Compiler version too old	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

No medium severity issues found.

✔ 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 0.8.0;
```


Centralization

Owner Privileges

- REN Contract:
 - Owner can transfer ownership.
 - Owner can renounce ownership
 - Owner can set bool variable if opensea ever shuts down or is compromised.
 - Owner can set bool variable if public sale is active or not.
 - Owner can set free mints number
 - Owner can withdraw tokens and contract native balance.

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. Following are Admin functions:

- Renounceownership
- Transferownership
- Setisopenseaproxyactive
- Setispublicsaleactive
- Setnumfreemints
- Withdraw
- Withdrawtokens

Conclusion

Smart contract contains low 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.