HackSafe

Smart Contract Security Audit Report

Rating

January 2023

Security Status

★★★★½

www.hacksafe.io

Audit Details

Audited project
Rating

Deployer address
0x5419266ea24bebdc8737a07c25b60de100d4c807

Client contacts
Rating

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 Rating to perform an audit of smart contracts:

- https://etherscan.io/token/0xe8663a64a96169ff4d95b4299e7ae9a76b905b31#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 12.01.2023

Token Type	: DEFI
Contract name	: RatingToken
Contract address	: 0xE8663A64A96169ff4d95b4299E7ae9a76b905B31
Total supply	: 10,000,000,000
Token ticker	: Rating
Decimals	: 8
Token Holders	: 6,007
Transactions count	: 22,598
Compiler version	: v0.4.23+commit.124ca40d
Contract deployer address	: 0x5419266ea24bebdc8737a07c25b60de100d4c807
Owner address	: 0x54750a3bB422854e27b3c8AE8e4bfAD039Af8D48

Audit Summary

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

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, 0 medium and 1 low.

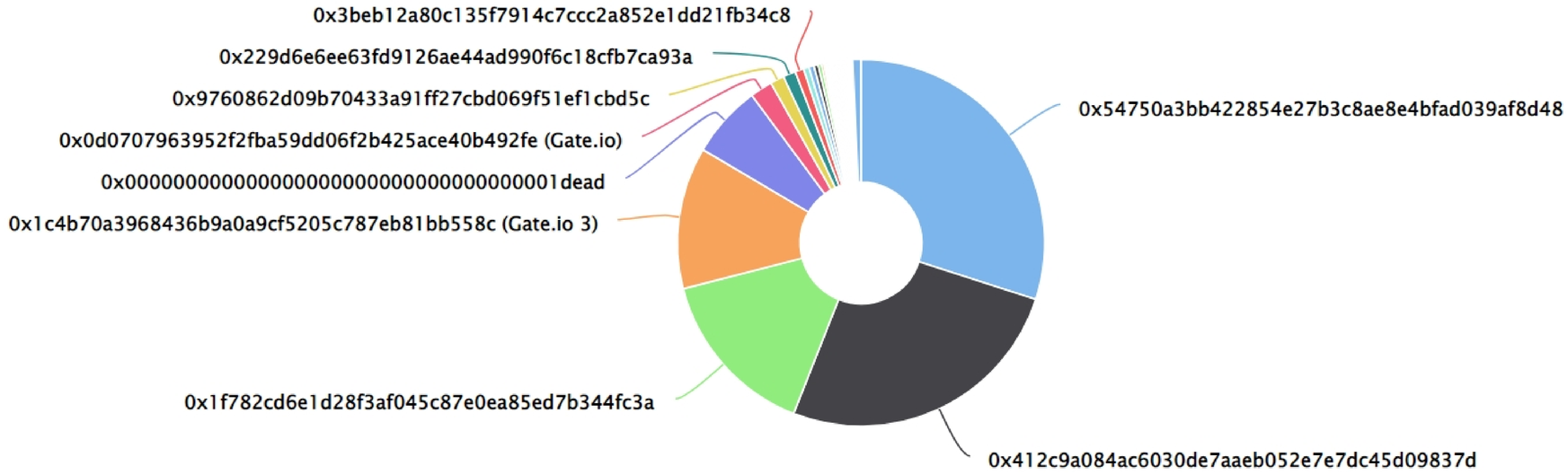
Rating Token Distribution

The top 100 holders collectively own 99.28% (9,927,801,916.64 Tokens) of Rating

Token Total Supply: 10,000,000,000.00 Token | Total Token Holders: 6,007

Rating Top 100 Token Holders

Source: Etherscan.io



Rating Top 20 Token Holders

(A total of 9,927,801,916.64 tokens held by the top 100 accounts from the total supply of 10,000,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0x54750a3bb422854e27b3c8ae8e4bfad039af8d48	3,000,000,000	30.0000%
2	0x412c9a084ac6030de7aaeb052e7e7dc45d09837d	2,599,531,684	25.9953%
3	0x1f782cd6e1d28f3af045c87e0ea85ed7b344fc3a	1,499,000,000	14.9900%
4	Gate.io 3	1,251,100,732.02018862	12.5110%
5	0x000000000000000000000000000000000000dead	637,038,322.91027681	6.3704%
6	Gate.io	198,150,721.06660386	1.9815%
7	0x9760862d09b70433a91ff27cbd069f51ef1cbd5c	121,999,900	1.2200%
8	0x229d6e6ee63fd9126ae44ad990f6c18cfb7ca93a	110,000,000	1.1000%
9	0x3beb12a80c135f7914c7ccc2a852e1dd21fb34c8	75,999,900	0.7600%
10	0x9a471c4a98ddd582d4c4568d75c30446f427222f	50,000,000	0.5000%
11	0x6b3aa5dc7c062ca40e3e01cc92b2a1ac9a0f18f3	44,082,261.41316193	0.4408%
12	0x58bb8b246daa4b03fea3b81b05b39ae37919344a	37,442,320.815	0.3744%
13	0x996eb825654da2dc4c989d6cf46e830fdeb4f7a5	30,000,000	0.3000%
14	0x56c3a1cbebbaed9374884e3214e1beea050de0d4	19,980,000	0.1998%
15	0xa150f5ee5740e4beeab42b816b68eeb329860ed9	15,480,000	0.1548%
16	0x180934262778539bff3b733879c9b9520d0db681	15,428,483.2738	0.1543%
17	0x785fa5d856e23b3ceb434cb458e989a04feac354	15,325,334.45165736	0.1533%
18	0xb99334a0673a1f09c7069f8706e210af24180352	15,047,433.394242	0.1505%
19	0x609556e9cb546622dd60174a07855186c51f8810	13,000,000	0.1300%
20	0x277abeade282a1e0177342517f908ccc3f447890	11,818,678.946068	0.1182%

Rating Token Distribution

Rating Contract Overview

Contract functions details

+ERC20Basic
  -[Pub] balanceOf
  -[Pub] transfer

+ERC20 (ERC20Basic)
  -[Pub] allowance
  -[Pub] transferFrom #
  -[Pub] approve #

+[Lib] SafeMath
  -[Int] mul
  -[Int] div
  -[Int] sub
  -[Int] add

+BasicToken (ERC20Basic)
  -[Pub] transfer #
  -[Pub] balanceOf

+StandardToken (ERC20, BasicToken)
  -[Pub] transferFrom #
  -[Pub] approve #
  -[Pub] allowance
  -[Pub] increaseApproval #
  -[Pub] decreaseApproval #

+Ownable (Context)
  -[Pub] Ownable
  -[Pub] transferOwnership #
    -modifiers: onlyOwner

+Pausable (Ownable)
  -[Pub] pause #
    -modifiers: onlyOwner

+PausableToken (StandardToken, Pausable)
  -[Pub] transfer #
    -modifiers: whenNotPaused
  -[Pub] transferFrom #
    -modifiers: whenNotPaused
  -[Pub] approve #
    -modifiers: whenNotPaused

Contract functions details

-[Pub] approve #
  -modifiers: whenNotPaused
-[Pub] increaseApproval #
  -modifiers: whenNotPaused
-[Pub] decreaseApproval #
  -modifiers: whenNotPaused

+RatingToken (PausableToken)
  -RatingToken #
  -transfer #
    -modifiers: validDestination
  -transferFrom #
    -modifiers: validDestination
  -burn #
  -burnFrom #
  -emergencyERC20Drain #
    -modifiers: onlyOwner
  -changeAdmin #
    -modifiers: onlyOwner

($) = payable function
= non-constant function

Issues Checking Status

No.	Title	Status
1.	Compiler error	Passed
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.	Too old version	Low issue

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 issue found.
- **Low Severity Issues**
  One low severity issue found.

1. Old compiler version

Description

- Contract has been deployed using too old solidity version.

Recommendation

- It is advisable to deploy contract using any of the latest version of solidity.

Centralization

Owner privileges :

- Rating Contract:
    - owner can transfer ownership.
    - owner can pause.
    - owner can transfer tokens to owner address.
    - owner can change admin.

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:

- changeadmin
- emergencyerc20drain
- transferownership
- pause

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.