Techrate1 Techrate

TechRate

AUDIT COMPANY

Restore

Smart Contract Security Audit

TechRate

Audit Details

Audited project

Restore

Deployer address

0x6753795d67eD0b2b65B57FC45C7Ac0F53b55f4FE

Client contacts:

Restore team

Blockchain

Ethereum

Project website:

https://restoretoken.net

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) (TechRate) owe no duty of care towards you or any other person, nor does TechRate 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 TechRate 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, TechRate hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against TechRate, 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.

Background

TechRate was commissioned by Restore to perform an audit of smart contracts:

https://etherscan.io/address/0x6753795d67ed0b2b65b57fc45c7ac0f53b55f4fe#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.

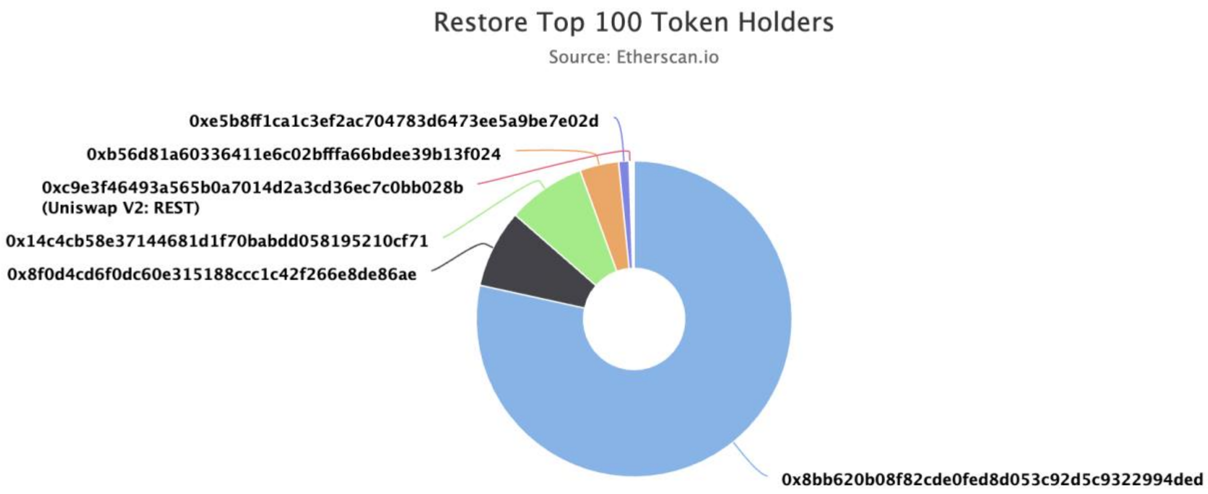
The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Contract Details

Token contract details for 18.06.2021

Contract name	RESTToken
Contract address	0x6753795d67eD0b2b65B57FC45C7Ac0F53b55f4FE
Total supply	500,000,000
Token ticker	REST
Decimals	18
Token holders	274
Transactions count	457
Top 100 holders dominance	99.99%
Contract deployer address	0xd59817ca4cd39ca254170e0f475d8d513ca6d601

REST Token Distribution

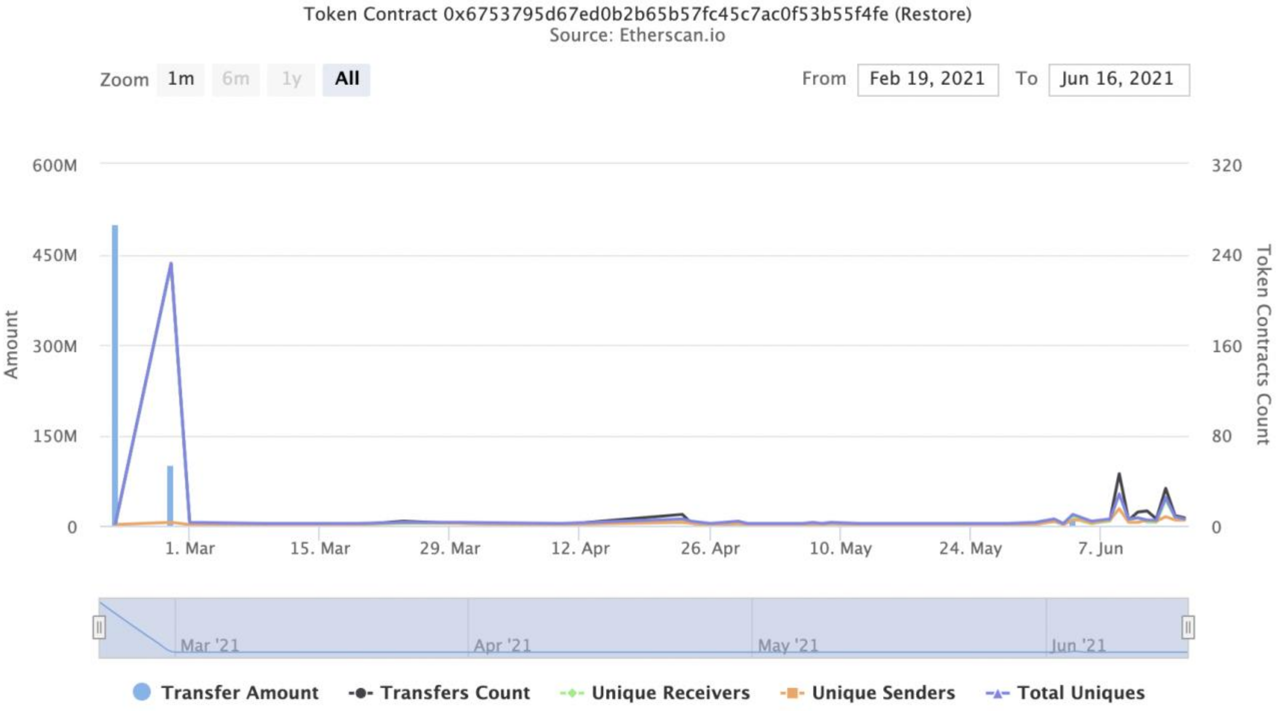


Restore Top 100 Token Holders

Source: Etherscan.io

(A total of 499,938,091.00 tokens held by the top 100 accounts from the total supply of 500,000,000.00 token)

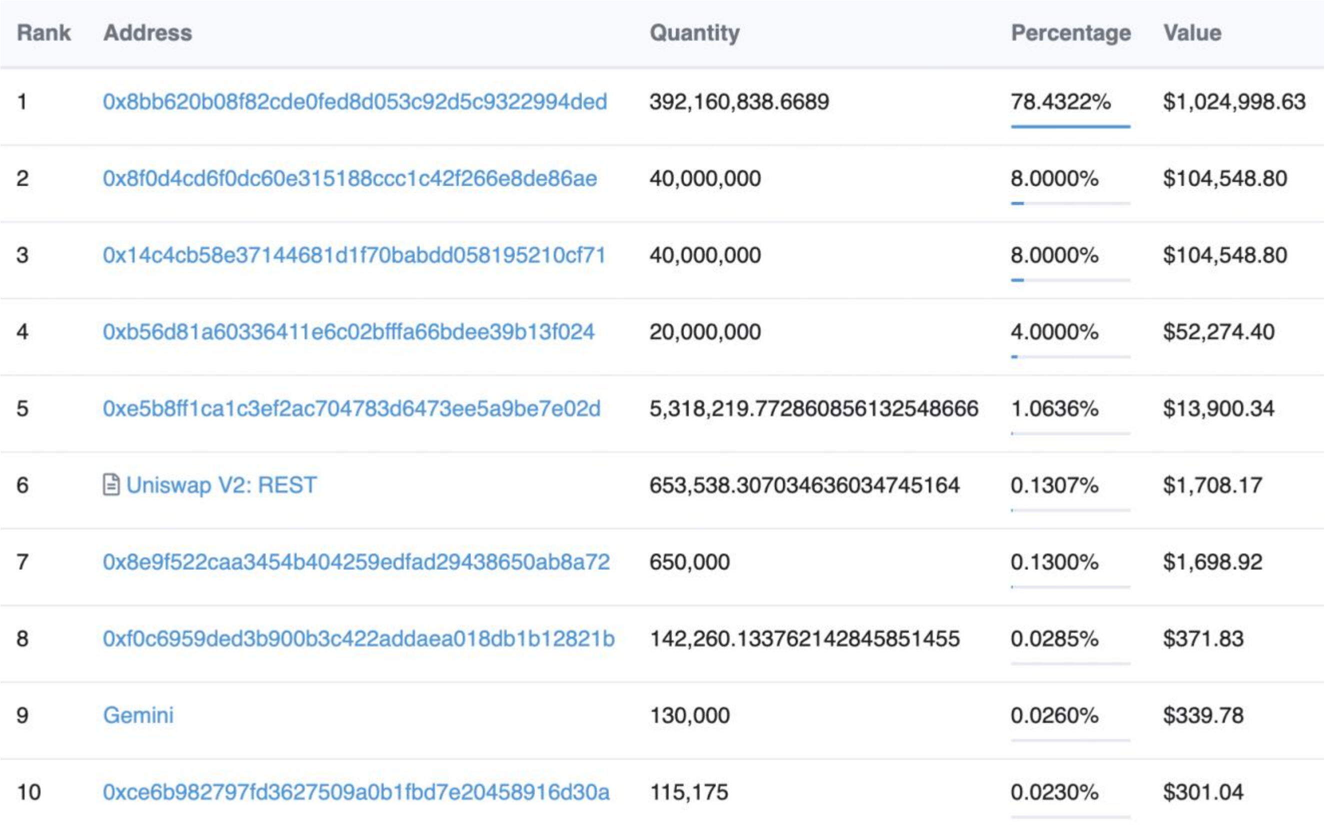
RESTToken Contract Interaction Details



Token Contract 0x6753795d67ed0b2b65b57fc45c7ac0f53b55f4fe (Restore)

Source: Etherscan.io

RESTToken Top 10 Token Holders



Rank	Address	Quantity	Percentage	Value
1	0x8bb620b08f82cde0fed8d053c92d5c9322994ded	392,160,838.6689	78.4322%	$1,024,998.63
2	0x8f0d4cd6f0dc60e315188ccc1c42f266e8de86ae	40,000,000	8.0000%	$104,548.80
3	0x14c4cb58e37144681d1f70babdd058195210cf71	40,000,000	8.0000%	$104,548.80
4	0xb56d81a60336411e6c02bfffa66bdee39b13f024	20,000,000	4.0000%	$52,274.40
5	0xe5b8ff1ca1c3ef2ac704783d6473ee5a9be7e02d	5,318,219.772860856132548666	1.0636%	$13,900.34
6	Uniswap V2: REST	653,538.307034636034745164	0.1307%	$1,708.17
7	0x8e9f522caa3454b404259edfad29438650ab8a72	650,000	0.1300%	$1,698.92
8	0xf0c6959ded3b900b3c422addaea018db1b12821b	142,260.133762142845851455	0.0285%	$371.83
9	Gemini	130,000	0.0260%	$339.78
10	0xce6b982797fd3627509a0b1fbd7e20458916d30a	115,175	0.0230%	$301.04

Contract functions details

+ SafeMath
  - [Pub] safeAdd
  - [Pub] safeSub
  - [Pub] safeMul
  - [Pub] safeDiv

+ ERC20Interface
  - [Pub] totalSupply
  - [Pub] balanceOf
  - [Pub] allowance
  - [Pub] transfer #
  - [Pub] approve #
  - [Pub] transferFrom #

+ ApproveAndCallFallBack
  - [Pub] receiveApproval #

+ RESTToken (ERC20Interface, SafeMath)
  - [Pub] <Constructor> #
  - [Pub] totalSupply
  - [Pub] balanceOf
  - [Pub] transfer #
  - [Pub] approve #
  - [Pub] transferFrom #
  - [Pub] allowance
  - [Pub] approveAndCall #
  - [Pub] <Fallback> ($)

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

Issues Checking Status

	Issue description	Checking status
1.	Compiler errors.	Passed
2.	Race conditions and Reentrancy. Cross-function race conditions.	Passed
3.	Possible delays in data delivery.	Passed
4.	Oracle calls.	Passed
5.	Front running.	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.	Low issue
12.	The impact of the exchange rate on the logic.	Passed
13.	Private user data leaks.	Passed
14.	Malicious Event log.	Passed
15.	Scoping and Declarations.	Passed
16.	Uninitialized storage pointers.	Passed
17.	Arithmetic accuracy.	Passed
18.	Design Logic.	Passed
19.	Cross-function race conditions.	Passed
20.	Safe Open Zeppelin contracts implementation and usage.	Passed
21.	Fallback function security.	Passed

Security Issues

✓ High Severity Issues

No high severity issues found.

✓ Medium Severity Issues

No medium severity issues found.

✓ Low Severity Issues

1. Burning method

Issue:

- The function transfer() can send tokens to zero address.

Recommendation:

Add require(to != address(0)); into transfer() function.
Create burn() function that will subtract tokens from msg.sender balance and from _totalSupply variable.

Conclusion

Smart contracts contain low severity issue!

TechRate 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.