TechRate
April, 2022

TECH
RATE

SMART CONTRACTS SECURITY AUDIT REPORT

Techrate_audits Techrate Techrate1

Audit Details

Audited project

VIRAL

Deployer address

0x8091b75c7591162fcfba1e8b0c54ba0a17c84eff

Client contacts:

VIRAL team

Blockchain

Ethereum

Project website:

https://theviralcrypto.co

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 VIRAL to perform an audit of smart contracts:

https://etherscan.io/address/0x9D37F31A4e8c6af7f64F1cE6241D24F5cACd391C#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.

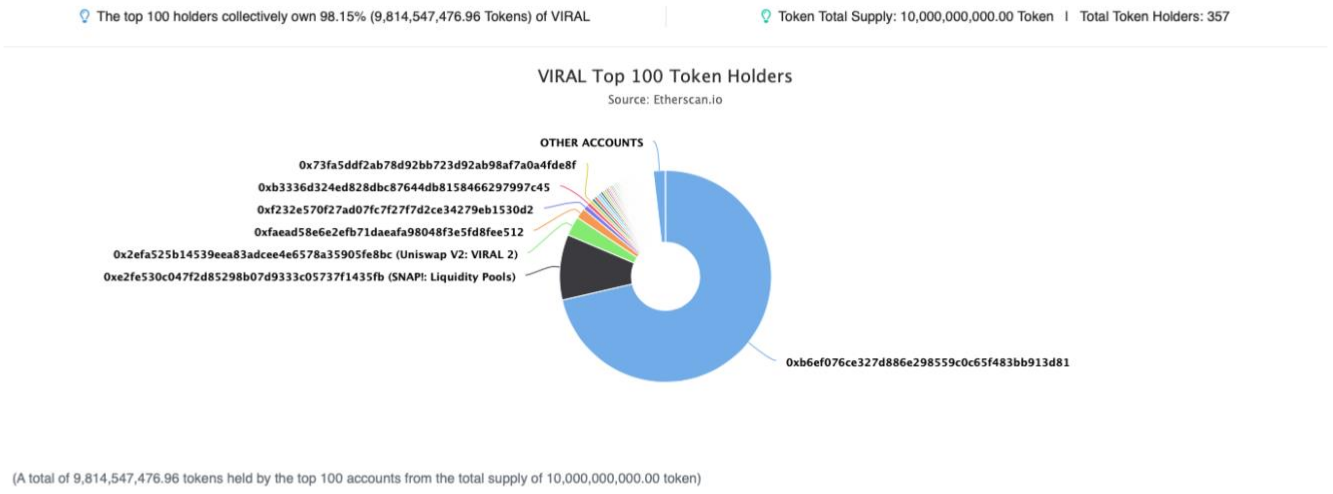
The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Contracts Details

Token contract details for 25.04.2022

Contract name	VIRAL
Contract address	0x9D37F31A4e8c6af7f64F1cE6241D24F5cACd391C
Total supply	10,000,000,000
Token ticker	VIRAL
Decimals	18
Token holders	357
Transactions count	3,983
Top 100 holders dominance	98.15%
Total sell fees	15
Total buy fees	2
Treasury wallet	0x73fa5ddf2ab78d92bb723d92ab98af7a0a4fde8f
pair	0x2efa525b14539eea83adcee4e6578a35905fe8bc
Contract deployer address	0x8091b75c7591162fcfba1e8b0c54ba0a17c84eff
Owner address	0x8091b75c7591162fcfba1e8b0c54ba0a17c84eff

VIRAL Token Distribution



The top 100 holders collectively own 98.15% (9,814,547,476.96 Tokens) of VIRAL

Token Total Supply: 10,000,000,000.00 Token | Total Token Holders: 357

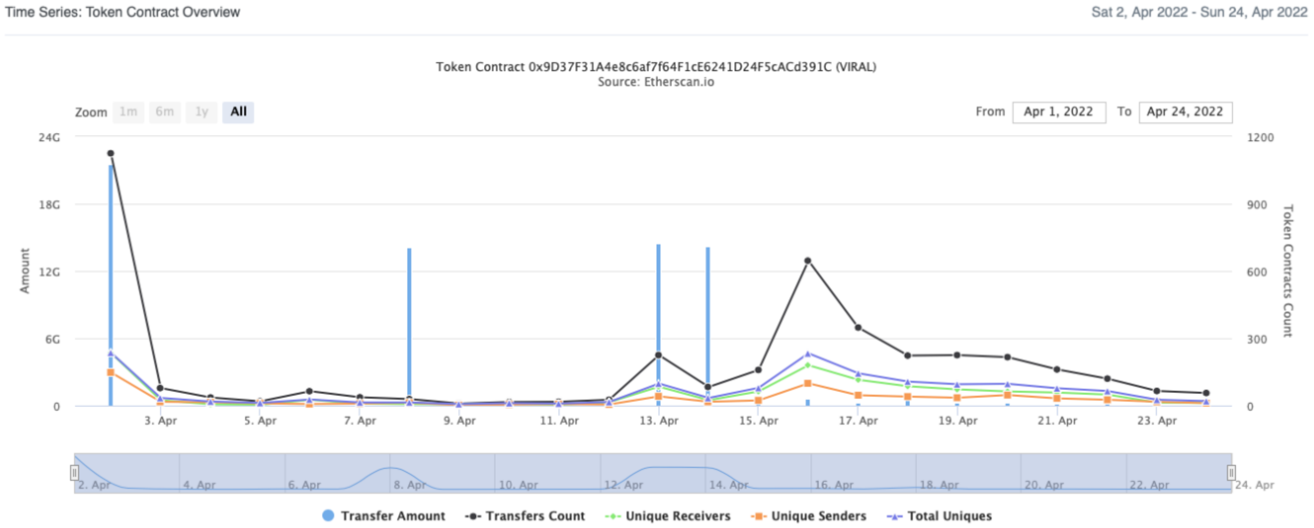
VIRAL Top 100 Token Holders

Source: Etherscan.io

OTHER ACCOUNTS
0x73fa5ddf2ab78d92bb723d92ab98af7a0a4fde8f
0xb3336d324ed828dbc87644db8158466297997c45
0xf232e570f27ad07fc7f27f7d2ce34279eb1530d2
0xfaead58e6e2efb71daeafa98048f3e5fd8fee512
0x2efa525b14539eea83adcee4e6578a35905fe8bc (Uniswap V2: VIRAL 2)
0xe2fe530c047f2d85298b07d9333c05737f1435fb (SNAP!: Liquidity Pools)
0xb6ef076ce327d886e298559c0c65f483bb913d81

(A total of 9,814,547,476.96 tokens held by the top 100 accounts from the total supply of 10,000,000,000.00 token)

VIRAL Contract Interaction Details



Time Series: Token Contract Overview

Sat 2, Apr 2022 - Sun 24, Apr 2022

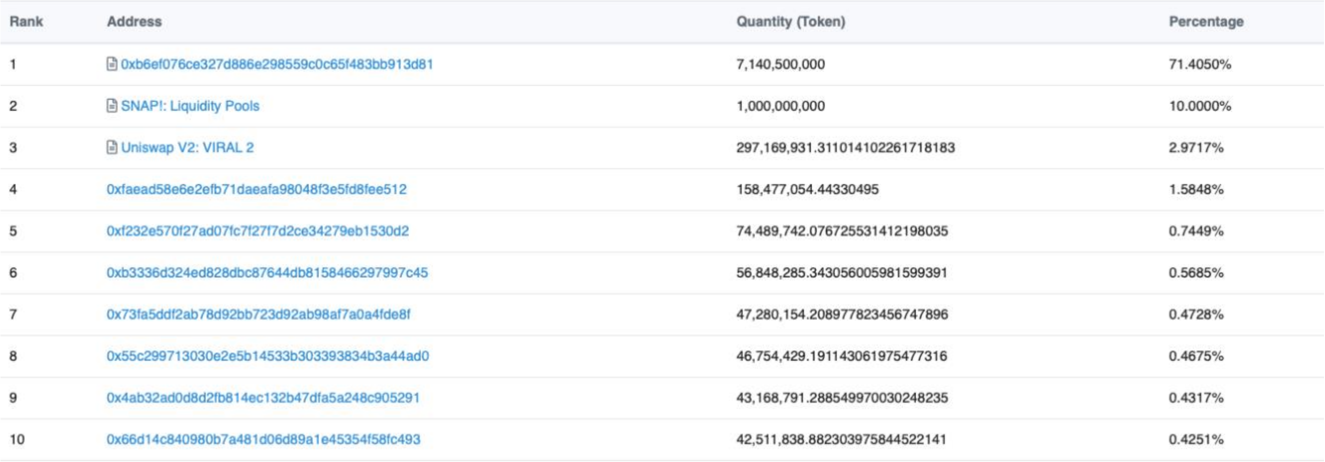
Token Contract 0x9D37F31A4e8c6af7f64F1cE6241D24F5cACd391C (VIRAL)

Source: Etherscan.io

Zoom 1m 6m 1y **All**

From Apr 1, 2022 To Apr 24, 2022

VIRAL Top 10 Token Holders



Rank	Address	Quantity (Token)	Percentage
1	0xb6ef076ce327d886e298559c0c65f483bb913d81	7,140,500,000	71.4050%
2	SNAP!: Liquidity Pools	1,000,000,000	10.0000%
3	Uniswap V2: VIRAL 2	297,169,931.311014102261718183	2.9717%
4	0xfaead58e6e2efb71daeafa98048f3e5fd8fee512	158,477,054.44330495	1.5848%
5	0xf232e570f27ad07fc7f27f7d2ce34279eb1530d2	74,489,742.076725531412198035	0.7449%
6	0xb3336d324ed828dbc87644db8158466297997c45	56,848,285.343056005981599391	0.5685%
7	0x73fa5ddf2ab78d92bb723d92ab98af7a0a4fde8f	47,280,154.208977823456747896	0.4728%
8	0x55c299713030e2e5b14533b303393834b3a44ad0	46,754,429.191143061975477316	0.4675%
9	0x4ab32ad0d8d2fb814ec132b47dfa5a248c905291	43,168,791.288549970030248235	0.4317%
10	0x66d14c840980b7a481d06d89a1e45354f58fc493	42,511,838.882303975844522141	0.4251%

Contract functions details

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

 + [Int] DividendPayingTokenInterface
   - [Ext] dividendOf
   - [Ext] withdrawDividend #
   - [Ext] withdrawableDividendOf
   - [Ext] withdrawnDividendOf
   - [Ext] accumulativeDividendOf

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

 + [Lib] SafeMathInt
   - [Int] mul
   - [Int] div
   - [Int] sub
   - [Int] add
   - [Int] abs
   - [Int] toUint256Safe

 + [Lib] SafeMathUint
   - [Int] toInt256Safe

 +  ERC20 (Context, IERC20, IERC20Metadata)
   - [Pub] <Constructor> #
   - [Pub] name
   - [Pub] symbol
   - [Pub] decimals
   - [Pub] totalSupply
   - [Pub] balanceOf
   - [Pub] transfer #
   - [Pub] allowance
   - [Pub] approve #
   - [Pub] transferFrom #
   - [Pub] increaseAllowance #
   - [Pub] decreaseAllowance #
   - [Int] _transfer #
   - [Int] _mint #
   - [Int] _burn #
   - [Int] _approve #
   - [Int] _beforeTokenTransfer #

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

 + [Int] IERC20Metadata (IERC20)
   - [Ext] name
   - [Ext] symbol
   - [Ext] decimals

 + [Int] IPair
   - [Ext] getReserves
   - [Ext] token0

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

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

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

```
    - modifiers: onlyOwner

 +  DividendPayingToken (ERC20, DividendPayingTokenInterface, Ownable)
   - [Pub] <Constructor> #
    - modifiers: ERC20
   - [Pub] distributeLPDividends #
    - modifiers: onlyOwner
   - [Pub] withdrawDividend #
   - [Int] _withdrawDividendOfUser #
   - [Pub] dividendOf
   - [Pub] withdrawableDividendOf
   - [Pub] withdrawnDividendOf
   - [Pub] accumulativeDividendOf
   - [Int] _transfer #
   - [Int] _mint #
   - [Int] _burn #
   - [Int] _setBalance #

 + [Lib] Address
   - [Int] sendValue #

 +  VIRAL (ERC20, Ownable)
   - [Pub] <Constructor> #
    - modifiers: ERC20
   - [Ext] <Fallback> ($)
   - [Pub] updateDividendTracker #
    - modifiers: onlyOwner
   - [Ext] claim #
   - [Ext] rescueETH20Tokens #
    - modifiers: onlyOwner
   - [Ext] forceSend #
   - [Ext] trackerRescueETH20Tokens #
    - modifiers: onlyOwner
   - [Ext] trackerForceSend #
    - modifiers: onlyOwner
   - [Ext] updateRouter #
    - modifiers: onlyOwner
   - [Pub] excludeFromFees #
    - modifiers: onlyOwner
   - [Pub] excludeMultipleAccountsFromFees #
    - modifiers: onlyOwner
   - [Ext] excludeFromDividends #
    - modifiers: onlyOwner
   - [Ext] setTreasuryWallet #
    - modifiers: onlyOwner
```

  - [Ext] setDevWallet #
    - modifiers: onlyOwner
  - [Ext] setSwapTokensAtAmount #
    - modifiers: onlyOwner
  - [Ext] setBuyTaxes #
    - modifiers: onlyOwner
  - [Ext] setSellTaxes #
    - modifiers: onlyOwner
  - [Ext] setMaxBuyAndSell #
    - modifiers: onlyOwner
  - [Ext] setSwapEnabled #
    - modifiers: onlyOwner
  - [Ext] activateTrading #
    - modifiers: onlyOwner
  - [Ext] setClaimEnabled #
    - modifiers: onlyOwner
  - [Ext] setBot #
    - modifiers: onlyOwner
  - [Ext] setBulkBot #
    - modifiers: onlyOwner
  - [Ext] setLP_Token #
    - modifiers: onlyOwner
  - [Ext] setAutomatedMarketMakerPair #
    - modifiers: onlyOwner
  - [Prv] _setAutomatedMarketMakerPair #
  - [Ext] getTotalDividendsDistributed
  - [Pub] isExcludedFromFees
  - [Pub] withdrawableDividendOf
  - [Pub] dividendTokenBalanceOf
  - [Ext] getAccountInfo
  - [Ext] airdropTokens #
    - modifiers: onlyOwner
  - [Int] _transfer #
  - [Prv] swapAndLiquify #
  - [Prv] swapTokensForETH #
  - [Prv] addLiquidity #

+ VIRALDividendTracker (Ownable, DividendPayingToken)
  - [Pub] <Constructor> #
    - modifiers: DividendPayingToken
  - [Ext] trackerRescueETH20Tokens #
    - modifiers: onlyOwner
  - [Ext] trackerForceSend #
    - modifiers: onlyOwner
  - [Ext] updateLP_Token #

    - modifiers: onlyOwner
  - [Int] _transfer
  - [Ext] excludeFromDividends #
    - modifiers: onlyOwner
  - [Pub] getAccount
  - [Ext] setBalance #
    - modifiers: onlyOwner
  - [Ext] processAccount #
    - modifiers: onlyOwner

($) = 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.**	Low issues
10.	**Methods execution permissions.**	Passed
11.	**Economy model of the contract.**	Passed
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. Out of gas

Issue:

- The function excludeMultipleAccountsFromFees() uses the loop to exclude multiple accounts from fees. Function will be aborted with OUT_OF_GAS exception if there will be a long addresses list.

Recommendation:

Check that the array length is not too big.

Issue:

- The function setBulkBot() uses the loop to mark multiple accounts as bots. Function will be aborted with OUT_OF_GAS exception if there will be a long addresses list.

Recommendation:

Check that the array length is not too big.

Issue:

- The function airdropTokens() uses the loop to distribute token amounts to multiple accounts. Function will be aborted with OUT_OF_GAS exception if there will be a long addresses list.

Recommendation:

Check that the array length is not too big.

Notes:

- updateDividendTracker() function doesn’t exclude from dividends dead address as in contructor.
- Transfer function hasn’t automatic dividend distribution logic, exclude in swap logic.

Owner privileges (In the period when the owner is not renounced)

- Owner can change dividendTracker.
- Owner can withdraw contract and dividend tracker’s ERC20 and native tokens.
- Owner can change router address.
- Owner can exclude from the fees and dividends.
- Owner can exclude and include addresses in automatedMarketMakerPairs array.
- Owner can change devWallet and treasuryWallet addresses.
- Owner can change swapTokensAtAmount.
- Owner can change fees.
- Owner can change maxBuyAmount and maxSellAmount.
- Owner can enable/disable swap.
- Owner can enable trading.
- Owner can enable/disable claimEnabled.
- Owner can mark addresses as bots.
- Owner can change dividend tracker’s LP token.

Conclusion

Smart contracts contain low severity issues! Liquidity pair contract's security is not checked due to out of scope. The further transfers and operations with the funds raise are not related to this particular contract.

Liquidity locking details are provided by the team:

- https://app.unicrypt.network/amm/uni-v2/pair/0x2efa525b14539eea83adcee4e6578a35905fe8bc
- https://www.team.finance/view-coin/0x9D37F31A4e8c6af7f64F1cE6241D24F5cACd391C?name=VIRAL&symbol=VIRAL

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.