Techrate1 Techrate

TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

December, 2021

Audit Details

Audited project

MultiGenCapital

Deployer address

0x2141524eb535a97544c73ac87d909004277997df

Client contacts:

MultiGenCapital team

Blockchain

Ethereum

Project website:

https://multigencapital.io/

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 MultiGenCapital to perform an audit of smart contracts:

https://etherscan.io/address/0x494cd82786a86ea842f8d80545ff841bcbf42ded#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 09.12.2021

Contract name	MultiGenCapital
Contract address	0x494Cd82786a86eA842f8D80545Ff841Bcbf42dED
Total supply	1,000,000,000,000
Token ticker	MGC
Decimals	9
Token holders	480
Transactions count	2,078
Top 100 holders dominance	92.27%
Max wallet size	45000000000000000000
_mgcaddress	0x6fbbdfd6b8358b82a2daedfa0ff3b09ae3c9147f
_mktgaddress	0xc96f450784b294153a9f8d41a0235758c1adc9e7
Uniswap V2 pair	0x471de74ecf3f5837c119cb4e2607dadd3e72a49d
Contract deployer address	0x2141524eb535a97544c73ac87d909004277997df
Contract's current owner address	0x2141524eb535a97544c73ac87d909004277997df

MultiGenCapital Token Distribution

The top 100 holders collectively own 92.27% (922,707,564,577.53 Tokens) of MultiGenCapital

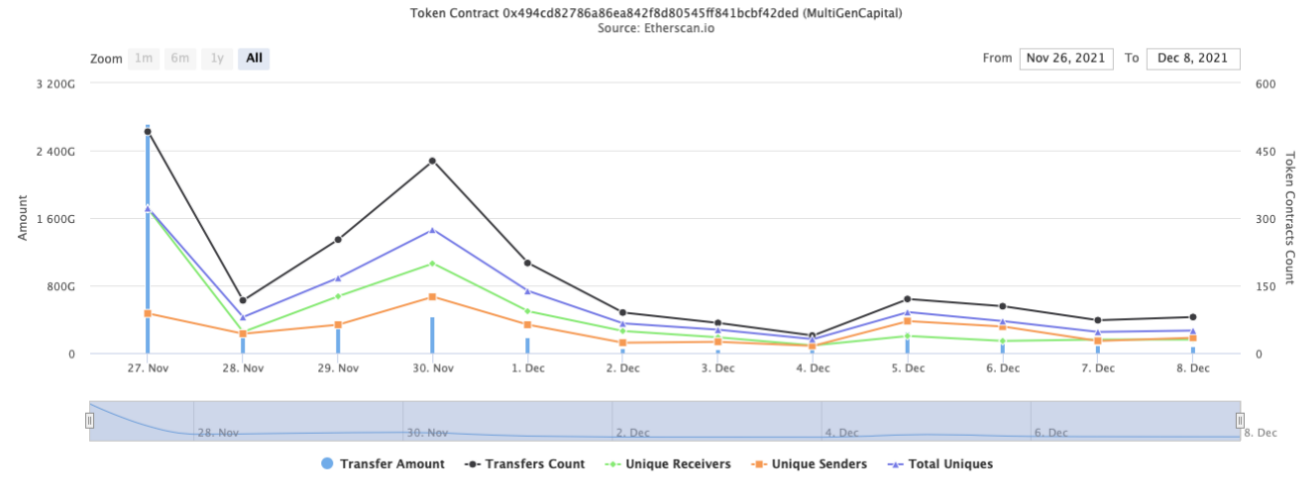
Token Total Supply: 1,000,000,000,000.00 Token | Total Token Holders: 480

(A total of 922,707,564,577.53 tokens held by the top 100 accounts from the total supply of 1,000,000,000,000.00 token)

MultiGenCapital Contract Interaction Details

Time Series: Token Contract Overview

Sat 27, Nov 2021 - Wed 8, Dec 2021



MultiGenCapital Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	0xfcac9d8e8fc28e4ee5effeaea7e2bf795d1df911	193,339,532,332.269480759	19.3340%
2	Uniswap V2: MGC 10	165,102,119,454.793593617	16.5102%
3	0xb3f3658bf332ba6c9c0cc5bc1201caba7ada819b	48,092,210,082.514004769	4.8092%
4	0x81272c72da45b7f362f2790821c9862ba5b5ae12	43,335,506,352.771976477	4.3336%
5	0xad9886e81a08276388f0384aed8f01ee84813f31	33,437,605,538.6894308	3.3438%
6	0x43557e6baa8e82484a43f058a541ec1b5d54a861	29,146,793,989.402427133	2.9147%
7	0x1d67afde08c1ab53f17768d43c5b943821c0ea25	28,749,370,385.320325575	2.8749%
8	0xbe23cbb62064b8b1550ae5ada59c39d45b1e2081	23,434,381,718.407864744	2.3434%
9	Multi Gen Capital: Deployer	23,300,379,644.985816027	2.3300%
10	0xab147e14e024ba21e9008578d919937845080548	18,865,226,835.294427066	1.8865%

Contract functions details

+ Context
  - [Int] _msgSender

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

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

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

+ [Int] IUniswapV2Factory
  - [Ext] createPair #

+ [Int] IUniswapV2Router02
  - [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #
  - [Ext] factory
  - [Ext] WETH
  - [Ext] addLiquidityETH ($)

+ MultiGenCapital (Context, IERC20, Ownable)
  - [Pub] <Constructor> #
  - [Pub] name
  - [Pub] symbol
  - [Pub] decimals
  - [Pub] totalSupply
  - [Pub] balanceOf
  - [Pub] transfer #
  - [Ext] excludeFromFee #
    - modifiers: onlyOwner
  - [Ext] includeInFee #
    - modifiers: onlyOwner
  - [Pub] excludeFromReflection #
    - modifiers: onlyOwner
  - [Pub] includeInReflection #
    - modifiers: onlyOwner
  - [Pub] allowance

- [Pub] approve #
- [Pub] transferFrom #
- [Prv] tokenFromReflection
- [Prv] removeAllFee #
- [Prv] restoreAllFee #
- [Prv] _approve #
- [Prv] _transfer #
- [Prv] swapTokensForEth #
  - modifiers: lockTheSwap
- [Prv] sendETHToFee #
- [Ext] manualSwap #
- [Ext] manualSend #
- [Pub] blockBots #
  - modifiers: onlyOwner
- [Pub] unblockBot #
  - modifiers: onlyOwner
- [Prv] _tokenTransfer #
- [Prv] _transferStandard #
- [Prv] _takeTeam #
- [Prv] _reflectFee #
- [Ext] <Fallback> ($)
- [Prv] _getValues
- [Prv] _getTValues
- [Prv] _getRValues
- [Prv] _getRate
- [Prv] _getCurrentSupply
- [Pub] setFee #
  - modifiers: onlyOwner
- [Int] enableTrading #
  - modifiers: onlyOwner
- [Ext] airdrop #
  - modifiers: onlyOwner
- [Pub] setMinSwapTokensThreshold #
  - modifiers: onlyOwner
- [Pub] setMaxTxAmount #
  - modifiers: onlyOwner
- [Pub] excludeFromMaxTxAmount #
  - modifiers: onlyOwner
- [Pub] setMaxWalletSize #
  - modifiers: onlyOwner
- [Ext] _setMGCAddress #
  - modifiers: onlyOwner
- [Ext] _setMktgAddress #
  - 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.	Low issues
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 `includeInReflection()` 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.

Recommendation:
Check that the excluded array length is not too big.

- The function `blockBots()` uses the loop to add bot addresses from the list. 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.

2. _getCurrentSupply issue

Issue:

- The function `_getCurrentSupply()` do not consider excluded from reflection addresses in calculations.

Recommendation:
Consider excluded from reflection addresses in calculations.

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

- Owner can exclude from the reflection.
- Owner can exclude from the fee.
- Owner can block/unblock bot addresses.
- Owner can change fees.
- Owner can enable trading.
- Owner can airdrop to addresses.
- Owner can change _swapTokensAtAmount.
- Owner can change the maximum transaction amount.
- Owner can exclude from the maximum transaction amount.
- Owner can change _maxWalletSize.
- Owner can change mgcAddress and mktgAddress.

Conclusion

Smart contracts contain low severity issues! Liquidity pair contract's security is not checked due to out of scope.

Liquidity locking details are provided by the team: https://www.team.finance/view-coin/0x494Cd82786a86eA842f8D80545Ff841Bcbf42dED?name=MultiGenCapital&symbol=MGC

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.