Techrate1 Techrate

TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

September, 2021

Audit Details

Audited project

MiniUSDC

Deployer address

0x712cdcb7f7adb1aa9256dc6c76d4b3e79e9fe270

Client contacts:

MiniUSDC team

Blockchain

Binance Smart Chain

Project website:

https://linktr.ee/MiniUSDC

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 MiniUSDC to perform an audit of smart contracts:
https://bscscan.com/address/0xa39d4a24226102765f48678d87d80387dd0c5acb#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

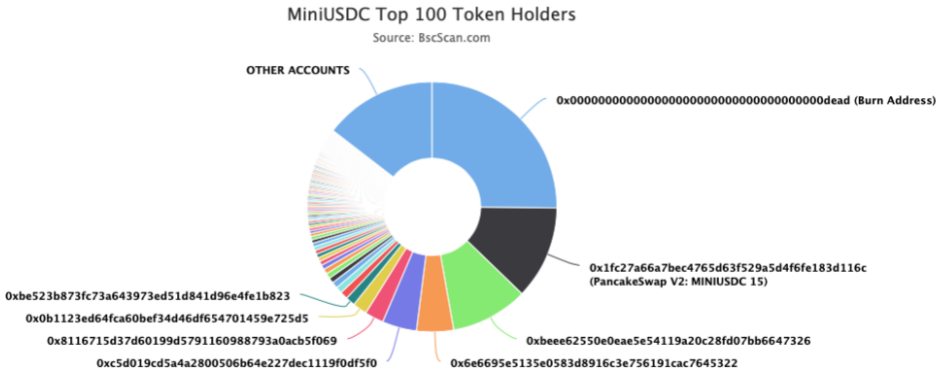
Token contract details for 01.09.2021

Contract name	MiniUSDC
Contract address	0xA39D4A24226102765f48678D87D80387DD0C5aCb
Total supply	1,000,000,000,000
Token ticker	MINIUSDC
Decimals	18
Token holders	1,461
Transactions count	17,988
Top 100 holders dominance	85.44%
Dividend token	0x8ac76a51cc950d9822d68b83fe1ad97b32cd580d
Total fees	20
Rewards fee	10
Uniswap V2 pair	0x1fc27a66a7bec4765d63f529a5d4f6fe183d116c
Contract deployer address	0x712cdcb7f7adb1aa9256dc6c76d4b3e79e9fe270
Contract's current owner address	0xb2f691f0e0cd928013702bcf509e4d56f95d507d

MiniUSDC Token Distribution

The top 100 holders collectively own 85.44% (854,404,154,698.61 Tokens) of MiniUSDC

Token Total Supply: 1,000,000,000,000.00 Token | Total Token Holders: 1,461

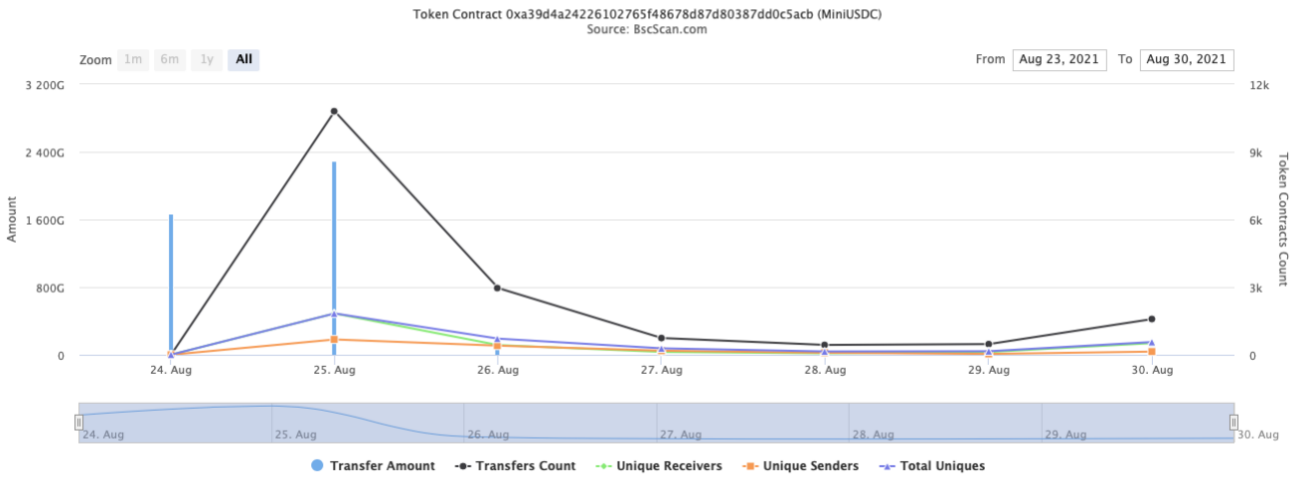


(A total of 854,404,154,698.61 tokens held by the top 100 accounts from the total supply of 1,000,000,000,000.00 token)

MiniUSDC Contract Interaction Details

Time Series: Token Contract Overview

Tue 24, Aug 2021 - Mon 30, Aug 2021



MiniUSDC Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	Burn Address	251,444,151,191.262215319742956691	25.1444%
2	PancakeSwap V2: MINIUSDC 15	120,800,275,450.243927055881397371	12.0800%
3	0xbeee62550e0eae5e54119a20c28fd07bb6647326	100,000,000,110.00000000096	10.0000%
4	0x6e6695e5135e0583d8916c3e756191cac7645322	47,904,680,001	4.7905%
5	0xc5d019cd5a4a2800506b64e227dec1119f0df5f0	44,432,813,642.75622393774970335	4.4433%
6	0x8116715d37d60199d5791160988793a0acb5f069	24,493,560,000	2.4494%
7	0x0b1123ed64fca60bef34d46df654701459e725d5	18,593,824,612.085869372059567421	1.8594%
8	0xbe523b873fc73a643973ed51d841d96e4fe1b823	12,184,766,537.594331514565635401	1.2185%
9	0x7d058ae7b6be91b03ee80e6d7e41013830ba7c87	10,000,000,000	1.0000%
10	0xe2561dcbfa67615cfec58d3de6e2b68cdcfca6fa	8,500,000,000.000000006643777536	0.8500%

Contract functions details

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

+ [Int] IUniswapV2Pair
  - [Ext] name
  - [Ext] symbol
  - [Ext] decimals
  - [Ext] totalSupply
  - [Ext] balanceOf
  - [Ext] allowance
  - [Ext] approve #
  - [Ext] transfer #
  - [Ext] transferFrom #
  - [Ext] DOMAIN_SEPARATOR
  - [Ext] PERMIT_TYPEHASH
  - [Ext] nonces
  - [Ext] permit #
  - [Ext] MINIMUM_LIQUIDITY
  - [Ext] factory
  - [Ext] token0
  - [Ext] token1
  - [Ext] getReserves
  - [Ext] price0CumulativeLast
  - [Ext] price1CumulativeLast
  - [Ext] kLast
  - [Ext] mint #
  - [Ext] burn #
  - [Ext] swap #
  - [Ext] skim #
  - [Ext] sync #
  - [Ext] initialize #

+ [Int] IUniswapV2Factory
  - [Ext] feeTo
  - [Ext] feeToSetter
  - [Ext] getPair
  - [Ext] allPairs
  - [Ext] allPairsLength
  - [Ext] createPair #
  - [Ext] setFeeTo #
  - [Ext] setFeeToSetter #

+ [Lib] IterableMapping
  - [Pub] get
  - [Pub] getIndexOfKey
  - [Pub] getKeyAtIndex
  - [Pub] size
  - [Pub] set #
  - [Pub] remove #

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

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

+ 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] DividendPayingTokenOptionalInterface
  - [Ext] withdrawableDividendOf
  - [Ext] withdrawnDividendOf
  - [Ext] accumulativeDividendOf

+ [Int] DividendPayingTokenInterface
  - [Ext] dividendOf
  - [Ext] distributeDividends ($)
  - [Ext] withdrawDividend #

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

+ Ownable (Context)
  - [Pub] <Constructor> #
  - [Pub] owner

  - [Pub] renounceOwnership #
    - modifiers: onlyOwner
  - [Pub] transferOwnership #
    - modifiers: onlyOwner

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

+ [Lib] SafeMathUint
  - [Int] toInt256Safe

+ [Int] IUniswapV2Router01
  - [Ext] factory
  - [Ext] WETH
  - [Ext] addLiquidity #
  - [Ext] addLiquidityETH ($)
  - [Ext] removeLiquidity #
  - [Ext] removeLiquidityETH #
  - [Ext] removeLiquidityWithPermit #
  - [Ext] removeLiquidityETHWithPermit #
  - [Ext] swapExactTokensForTokens #
  - [Ext] swapTokensForExactTokens #
  - [Ext] swapExactETHForTokens ($)
  - [Ext] swapTokensForExactETH #
  - [Ext] swapExactTokensForETH #
  - [Ext] swapETHForExactTokens ($)
  - [Ext] quote
  - [Ext] getAmountOut
  - [Ext] getAmountIn
  - [Ext] getAmountsOut
  - [Ext] getAmountsIn

+ [Int] IUniswapV2Router02 (IUniswapV2Router01)
  - [Ext] removeLiquidityETHSupportingFeeOnTransferTokens #
  - [Ext] removeLiquidityETHWithPermitSupportingFeeOnTransferTokens #
  - [Ext] swapExactTokensForTokensSupportingFeeOnTransferTokens #
  - [Ext] swapExactETHForTokensSupportingFeeOnTransferTokens ($)
  - [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #

+ DividendPayingToken (ERC20, DividendPayingTokenInterface, DividendPayingTokenOptionalInterface, Ownable)
  - [Pub] <Constructor> #
    - modifiers: ERC20
  - [Ext] <Fallback> ($)
  - [Pub] distributeDividends ($)
  - [Pub] distributeTokenDividends #
    - modifiers: onlyOwner
  - [Pub] withdrawDividend #
  - [Int] _withdrawDividendOfUser #
  - [Pub] dividendOf

- [Pub] withdrawableDividendOf
- [Pub] withdrawnDividendOf
- [Pub] accumulativeDividendOf
- [Int] _transfer #
- [Int] _mint #
- [Int] _burn #
- [Int] _setBalance #

+ MiniUSDC (ERC20, Ownable)
- [Pub] <Constructor> #
  - modifiers: ERC20
- [Ext] <Fallback> ($)
- [Ext] addPresaleAddressForExclusions #
  - modifiers: onlyOwner
- [Ext] emergencyPresaleAddressUpdate #
  - modifiers: onlyOwner
- [Ext] updateDividendTracker #
  - modifiers: onlyOwner
- [Ext] excludeFromDividends #
  - modifiers: onlyOwner
- [Ext] includeInDividends #
  - modifiers: onlyOwner
- [Ext] enableTrading #
  - modifiers: onlyOwner
- [Ext] updateMaxAmount #
  - modifiers: onlyOwner
- [Ext] updateFees #
  - modifiers: onlyOwner
- [Ext] updateUniswapV2Router #
  - modifiers: onlyOwner
- [Pub] excludeFromMaxTransaction #
  - modifiers: onlyOwner
- [Pub] excludeFromFees #
  - modifiers: onlyOwner
- [Ext] excludeMultipleAccountsFromFees #
  - modifiers: onlyOwner
- [Pub] setAutomatedMarketMakerPair #
  - modifiers: onlyOwner
- [Prv] _setAutomatedMarketMakerPair #
- [Ext] updateMarketingWallet #
  - modifiers: onlyOwner
- [Ext] updateTeamWallet #
  - modifiers: onlyOwner
- [Ext] updateLiquidityWallet #
  - modifiers: onlyOwner
- [Ext] updateGasForProcessing #
  - modifiers: onlyOwner
- [Ext] updateClaimWait #
  - modifiers: onlyOwner
- [Ext] getClaimWait
- [Ext] getTotalDividendsDistributed
- [Pub] isExcludedFromFees
- [Pub] withdrawableDividendOf
- [Pub] dividendTokenBalanceOf
- [Ext] getAccountDividendsInfo

  - [Ext] getAccountDividendsInfoAtIndex
  - [Ext] processDividendTracker #
  - [Ext] claim #
  - [Ext] getLastProcessedIndex
  - [Ext] getNumberOfDividendTokenHolders
  - [Ext] getNumberOfDividends
  - [Ext] removeLimits #
    - modifiers: onlyOwner
  - [Int] _transfer #
  - [Prv] swapTokensForEth #
  - [Prv] swapAndLiquify #
  - [Prv] addLiquidity #
  - [Prv] swapBnbForRewardToken #
  - [Prv] swapAndSendDividends #
  - [Ext] buyBackTokens #
    - modifiers: onlyOwner

+ DividendTracker (DividendPayingToken)
  - [Pub] <Constructor> #
    - modifiers: DividendPayingToken
  - [Int] _transfer
  - [Pub] withdrawDividend
  - [Ext] excludeFromDividends #
    - modifiers: onlyOwner
  - [Ext] includeInDividends #
    - modifiers: onlyOwner
  - [Ext] updateClaimWait #
    - modifiers: onlyOwner
  - [Ext] getLastProcessedIndex
  - [Ext] getNumberOfTokenHolders
  - [Pub] getAccount
  - [Pub] getAccountAtIndex
  - [Prv] canAutoClaim
  - [Ext] setBalance #
    - modifiers: onlyOwner
  - [Pub] process #
  - [Pub] 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:
Be careful about accounts array length.

Notes:

- Owner can change dividend tracker that could be not audited and some functions may work in different ways.

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

- Owner can add addresses to multiple exclusions.
- Owner can airdrop to wallets.
- Owner can change presale and presale router address.
- Owner can change dividend tracker.
- Owner can exclude from dividends.
- Owner can enable trading.
- Owner can change maxSell amount.
- Owner can change fees.
- Owner can change Uniswap router address.
- Owner can exclude from max transaction amount.
- Owner can exclude from the fees.
- Owner can exclude and include addresses in automatedMarketMakerPairs array.
- Owner can change marketing, team and liquidity wallets.
- Owner can change gas for processing.
- Owner can update claimWait value.
- Owner can remove limits.
- Owner can manually buyback tokens.

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 provided by the team:
https://dxsale.app/app/v3/dxlockview?id=0&add=0xB2f691F0E0Cd928013702bcf509E4d56f95d507d&type=lplock&chain=BSC

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.