Techrate1 Techrate

TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

December, 2021

Audit Details

Audited project

SCARDust

Deployer address

0x9bda071ad0d5c38e7ffa8b0ea31c572426d94a68

Client contacts:

SCARDust team

Blockchain

Ethereum

Project website:

Not provided by SCARDust team

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 SCARDust to perform an audit of smart contracts:

https://etherscan.io/address/0xc10b30820f793e24733dc80da12c798dfbff0fff#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.

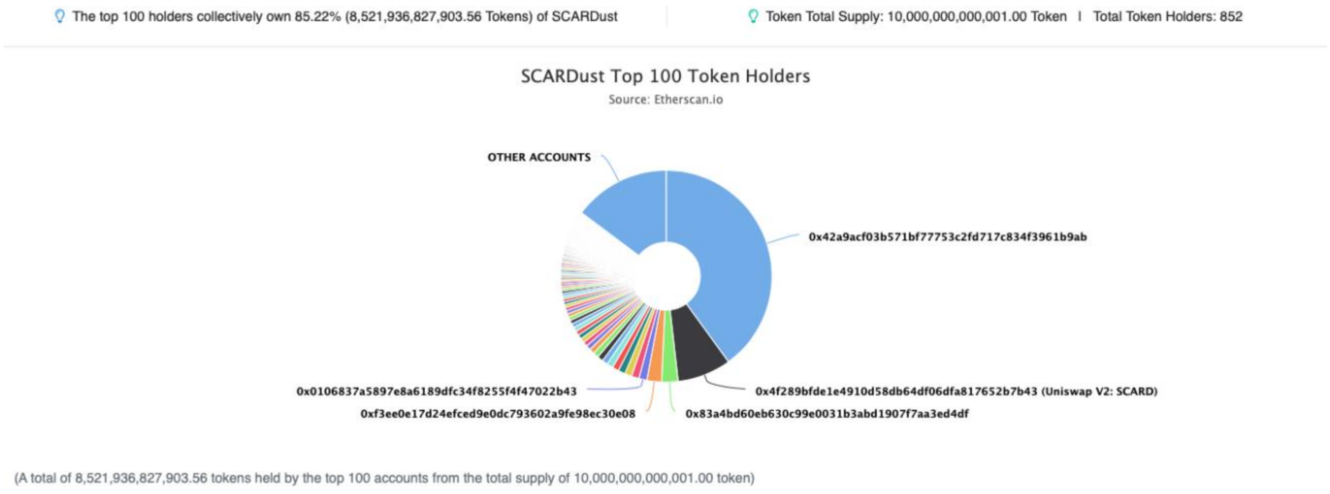
The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Contracts Details

Token contract details for 24.12.2021

Contract name	SCARDust
Contract address	0xC10b30820F793E24733dC80da12C798dfbFF0fFf
Total supply	10,000,000,000,001
Token ticker	SCARD
Decimals	9
Token holders	852
Transactions count	3,841
Top 100 holders dominance	85.22%
Current router	0x7a250d5630b4cf539739df2c5dacb4c659f2488d
marketing/ charity/ dev/ total ratios	4/1/6/11
Reflect/marketing/dev/ charity / totalSwap	100/400/600/100/1100
lpPair	0x4f289bfde1e4910d58db64df06dfa817652b7b43
Contract deployer address	0x9bda071ad0d5c38e7ffa8b0ea31c572426d94a68
Contract’s current owner address	0x59ceb6c1f1d04b75fa70d42c35b04e6cc0416990

SCARDust Token Distribution



The top 100 holders collectively own 85.22% (8,521,936,827,903.56 Tokens) of SCARDust

Token Total Supply: 10,000,000,000,001.00 Token | Total Token Holders: 852

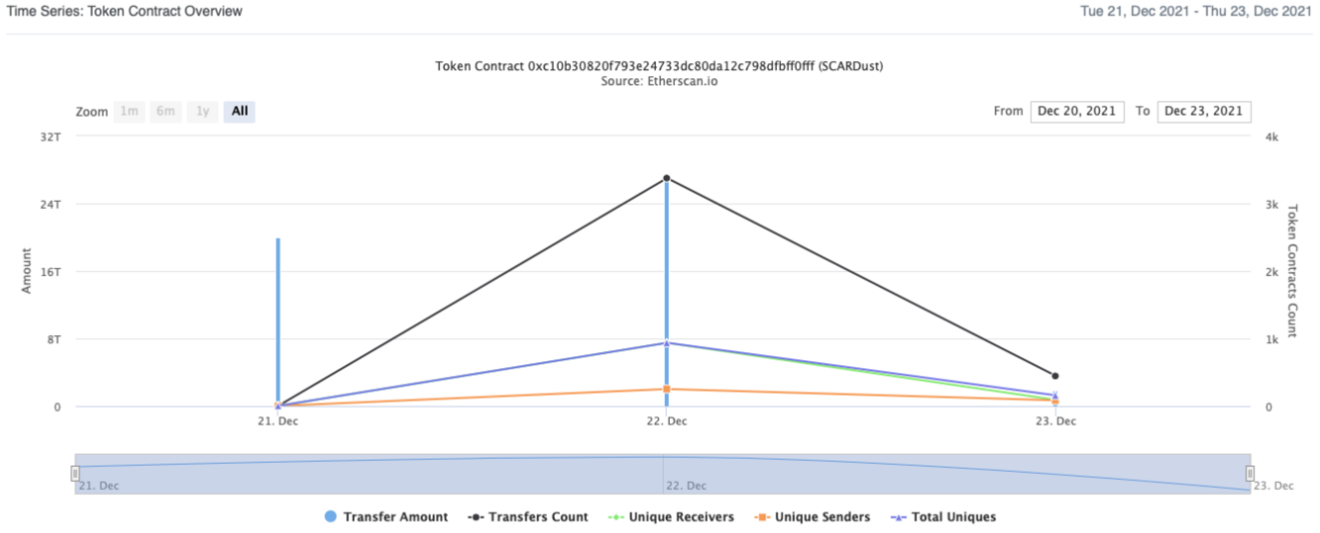
SCARDust Top 100 Token Holders

Source: Etherscan.io

OTHER ACCOUNTS
0x42a9acf03b571bf77753c2fd717c834f3961b9ab
0x0106837a5897e8a6189dfc34f8255f4f47022b43
0x4f289bfde1e4910d58db64df06dfa817652b7b43 (Uniswap V2: SCARD)
0xf3ee0e17d24efced9e0dc793602a9fe98ec30e08
0x83a4bd60eb630c99e0031b3abd1907f7aa3ed4df

(A total of 8,521,936,827,903.56 tokens held by the top 100 accounts from the total supply of 10,000,000,000,001.00 token)

SCARDust Contract Interaction Details



Time Series: Token Contract Overview

Tue 21, Dec 2021 - Thu 23, Dec 2021

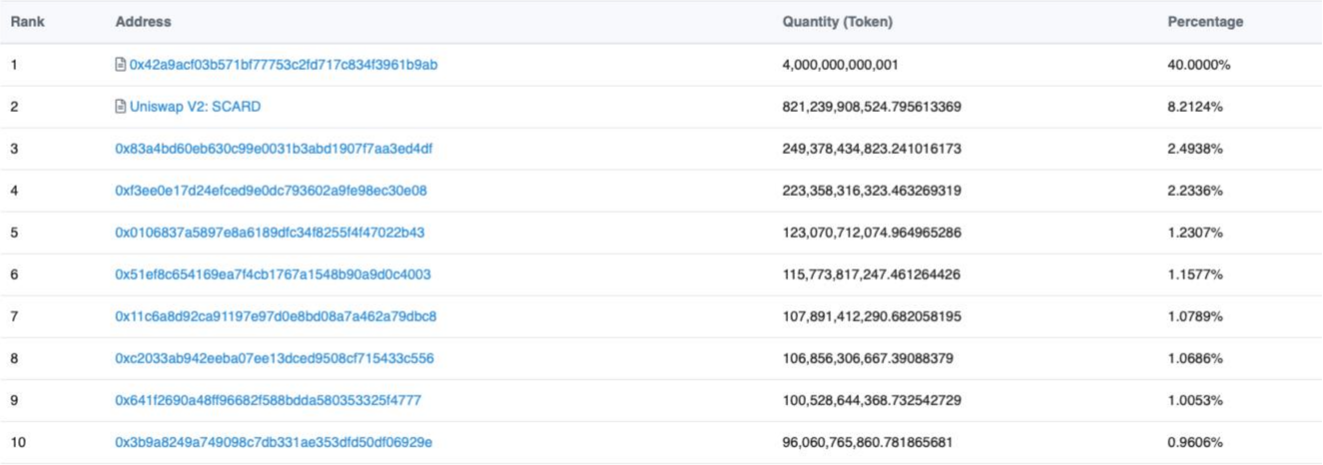
Token Contract 0xc10b30820f793e24733dc80da12c798dfbff0fff (SCARDust)

Source: Etherscan.io

Zoom 1m 6m 1y All

From Dec 20, 2021 To Dec 23, 2021

SCARDust Top 10 Token Holders



Rank	Address	Quantity (Token)	Percentage
1	📄 0x42a9acf03b571bf77753c2fd717c834f3961b9ab	4,000,000,000,001	40.0000%
2	📄 Uniswap V2: SCARD	821,239,908,524.795613369	8.2124%
3	0x83a4bd60eb630c99e0031b3abd1907f7aa3ed4df	249,378,434,823.241016173	2.4938%
4	0xf3ee0e17d24efced9e0dc793602a9fe98ec30e08	223,358,316,323.463269319	2.2336%
5	0x0106837a5897e8a6189dfc34f8255f4f47022b43	123,070,712,074.964965286	1.2307%
6	0x51ef8c654169ea7f4cb1767a1548b90a9d0c4003	115,773,817,247.461264426	1.1577%
7	0x11c6a8d92ca91197e97d0e8bd08a7a462a79dbc8	107,891,412,290.682058195	1.0789%
8	0xc2033ab942eeba07ee13dced9508cf715433c556	106,856,306,667.39088379	1.0686%
9	0x641f2690a48ff96682f588bdda580353325f4777	100,528,644,368.732542729	1.0053%
10	0x3b9a8249a749098c7db331ae353dfd50df06929e	96,060,765,860.781865681	0.9606%

Contract functions details

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

 + [Int] IERC20
   - [Ext] totalSupply
   - [Ext] decimals
   - [Ext] symbol
   - [Ext] name
   - [Ext] getOwner
   - [Ext] balanceOf
   - [Ext] transfer #
   - [Ext] allowance
   - [Ext] approve #
   - [Ext] transferFrom #

 + [Int] IFactoryV2
   - [Ext] getPair
   - [Ext] createPair #

 + [Int] IV2Pair
   - [Ext] factory
   - [Ext] getReserves

 + [Int] IRouter01
   - [Ext] factory
   - [Ext] WETH
   - [Ext] addLiquidityETH ($)
   - [Ext] quote
   - [Ext] getAmountOut
   - [Ext] getAmountIn
   - [Ext] getAmountsOut
   - [Ext] getAmountsIn

 + [Int] IRouter02 (IRouter01)
   - [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #

 + [Int] AntiSnipe
   - [Ext] checkUser #
   - [Ext] setLaunch #
   - [Ext] setLpPair #
   - [Ext] setProtections #
   - [Ext] setGasPriceLimit #
   - [Ext] removeSniper #
   - [Ext] getSniperAmt
   - [Ext] removeBlacklisted #
   - [Ext] isBlacklisted
   - [Ext] transfer #
   - [Ext] setBlacklistEnabled #
   - [Ext] setBlacklistEnabledMultiple #
   - [Ext] getSellCooldown
```

```
  - [Ext] setCooldownTimeEnabled #
  - [Ext] setCooldownTimeDuration #

+ SCARDust (Context, IERC20)
  - [Pub] <Constructor> ($)
  - [Ext] <Fallback> ($)
  - [Pub] owner
  - [Ext] transferOwner #
    - modifiers: onlyOwner
  - [Pub] renounceOwnership #
    - modifiers: onlyOwner
  - [Ext] totalSupply
  - [Ext] decimals
  - [Ext] symbol
  - [Ext] name
  - [Ext] getOwner
  - [Ext] allowance
  - [Pub] balanceOf
  - [Pub] transfer #
  - [Pub] approve #
  - [Prv] _approve #
  - [Pub] approveContractContingency #
    - modifiers: onlyOwner
  - [Ext] transferFrom #
  - [Pub] increaseAllowance #
  - [Pub] decreaseAllowance #
  - [Pub] setNewRouter #
    - modifiers: onlyOwner
  - [Ext] setLpPair #
    - modifiers: onlyOwner
  - [Ext] changeRouterContingency #
    - modifiers: onlyOwner
  - [Pub] getCirculatingSupply
  - [Pub] isExcludedFromFees
  - [Pub] setExcludedFromFees #
    - modifiers: onlyOwner
  - [Pub] isExcludedFromReward
  - [Pub] setExcludedFromReward #
    - modifiers: onlyOwner
  - [Pub] tokenFromReflection
  - [Ext] setInitializer #
    - modifiers: onlyOwner
  - [Ext] setBlacklistEnabled #
    - modifiers: onlyOwner
  - [Ext] setBlacklistEnabledMultiple #
    - modifiers: onlyOwner
  - [Ext] removeBlacklisted #
    - modifiers: onlyOwner
  - [Pub] isBlacklisted
  - [Pub] getSniperAmt
  - [Ext] removeSniper #
    - modifiers: onlyOwner
  - [Ext] setProtectionSettings #
    - modifiers: onlyOwner
  - [Ext] setGasPriceLimit #
```

  - modifiers: onlyOwner
- [Pub] getSellCooldown
- [Ext] setCooldownTimeEnabled #
  - modifiers: onlyOwner
- [Ext] setCooldownTimeDuration #
  - modifiers: onlyOwner
- [Ext] setTaxesBuy #
  - modifiers: onlyOwner
- [Ext] setTaxesSell #
  - modifiers: onlyOwner
- [Ext] setTaxesTransfer #
  - modifiers: onlyOwner
- [Ext] setRatios #
  - modifiers: onlyOwner
- [Ext] setMaxTxPercent #
  - modifiers: onlyOwner
- [Ext] setMaxWalletSize #
  - modifiers: onlyOwner
- [Pub] getMaxTX
- [Pub] getMaxWallet
- [Ext] setSwapSettings #
  - modifiers: onlyOwner
- [Ext] setWallets #
  - modifiers: onlyOwner
- [Pub] setContractSwapEnabled #
  - modifiers: onlyOwner
- [Prv] _hasLimits
- [Int] _transfer #
- [Prv] contractSwap #
  - modifiers: lockTheSwap
- [Prv] _checkLiquidityAdd #
- [Pub] enableTrading #
  - modifiers: onlyOwner
- [Ext] sweepContingency #
  - modifiers: onlyOwner
- [Prv] _finalizeTransfer #
- [Prv] _getValues #
- [Int] _getRate

($) = 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

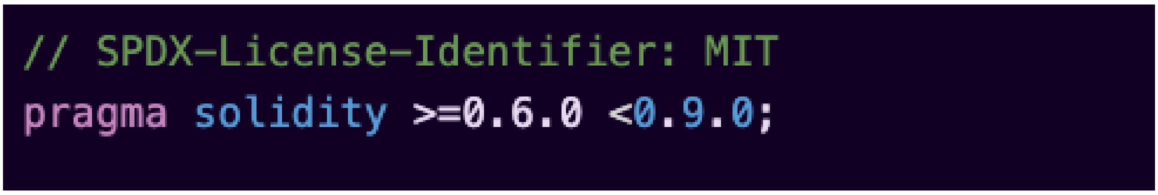
No medium severity issues found.

Low Severity Issues

1. Non fixed solidity version

Issue:

- Solidity version is not fixed. Contract use operators, that works different way on different solidity versions.



```
// SPDX-License-Identifier: MIT
pragma solidity >=0.6.0 <0.9.0;
```

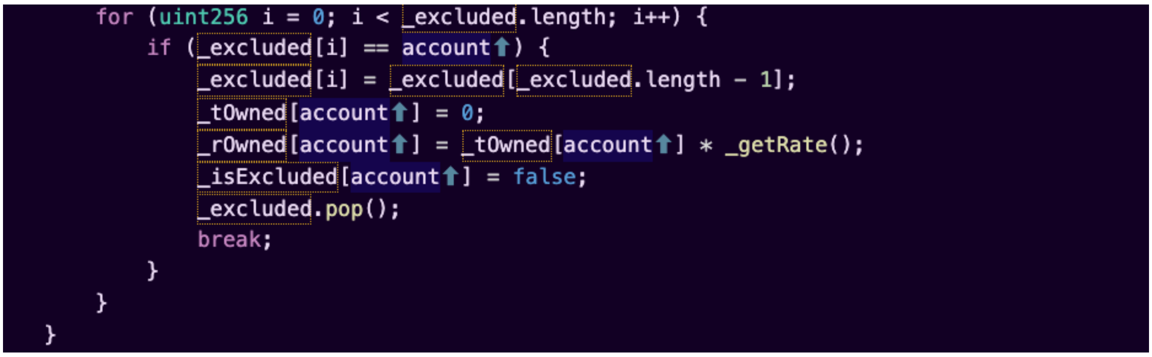
Recommendation:

Fix solidity version to one or reduce versions range.

2. Out of gas

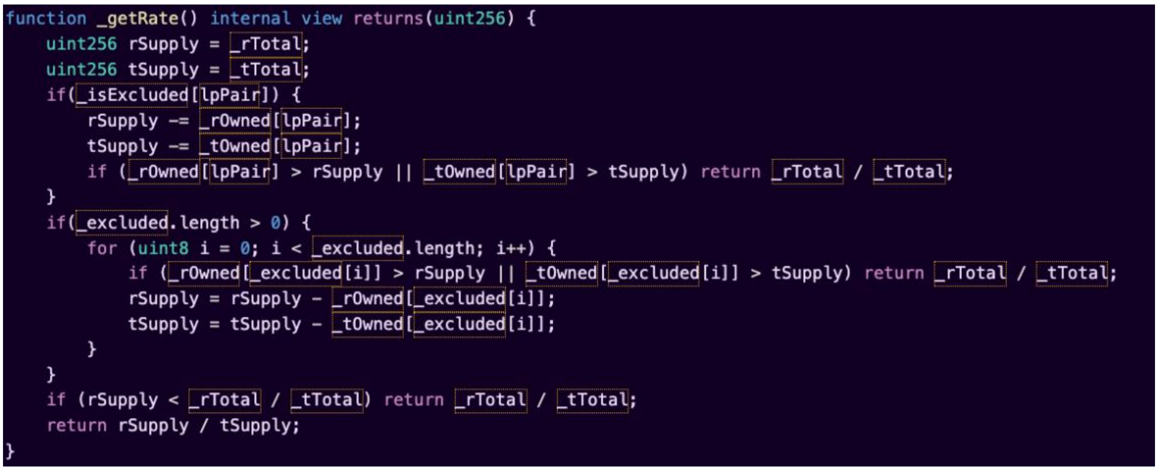
Issue:

- The function setExcludedFromReward() 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.



```
        for (uint256 i = 0; i < _excluded.length; i++) {
            if (_excluded[i] == account) {
                _excluded[i] = _excluded[_excluded.length - 1];
                _tOwned[account] = 0;
                _rOwned[account] = _tOwned[account] * _getRate();
                _isExcluded[account] = false;
                _excluded.pop();
                break;
            }
        }
    }
```

- The function _getRate() also uses the loop for evaluating reflect rate. It also could be aborted with OUT_OF_GAS exception if there will be a long excluded addresses list.



```
function _getRate() internal view returns(uint256) {
    uint256 rSupply = _rTotal;
    uint256 tSupply = _tTotal;
    if(_isExcluded[lpPair]) {
        rSupply -= _rOwned[lpPair];
        tSupply -= _tOwned[lpPair];
        if (_rOwned[lpPair] > rSupply || _tOwned[lpPair] > tSupply) return _rTotal / _tTotal;
    }
    if(_excluded.length > 0) {
        for (uint8 i = 0; i < _excluded.length; i++) {
            if (_rOwned[_excluded[i]] > rSupply || _tOwned[_excluded[i]] > tSupply) return _rTotal / _tTotal;
            rSupply = rSupply - _rOwned[_excluded[i]];
            tSupply = tSupply - _tOwned[_excluded[i]];
        }
    }
    if (rSupply < _rTotal / _tTotal) return _rTotal / _tTotal;
    return rSupply / tSupply;
}
```

Recommendation:

Check that the excluded array length is not too big.

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

- Owner can transfer whole ownership.
- Owner can change Uniswap router address.
- Owner can include in LpPair array.
- Owner can exclude from the fee.
- Owner can change antisnipe address.
- Owner can enable/disable antisnipe blacklist.
- Owner can remove sniper addresses.
- Owner can change protection settings.
- Owner can change antisnipe gas limit.
- Owner can change antisnipe cooldown settings.
- Owner can change fees and ratios.
- Owner can change max wallet size.
- Owner can change max transaction amount.
- Owner can change swapThreshold and swapAmount.
- Owner can change marketing, charity and development address.
- Owner can enable/disable contractSwapEnabled.
- Owner can enable trading.
- Owner can withdraw contract ETHs.

Conclusion

Smart contracts contain low severity issues! Liquidity pair contract's security is not checked due to out of scope. Contract contain interfaces that is not audited, some functions may work different ways.

Liquidity locking details NOT provided by the team.

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.