



# Smart Contract Security Audit

## Audit details:

Audited project:	YieldMoon
Deployer address:	0x44ed84b915427204e5d99583daccb8ad0b1bcec3
Client contacts:	YieldMoon team
Blockchain:	Binance Smart Chain
Project website:	<a href="https://yieldmoon.org">https://yieldmoon.org</a>

# 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 YieldMoon to perform an audit of smart contracts:

- <https://bscscan.com/address/0x2f23b8cdcc4068975325210615292768683b6951#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

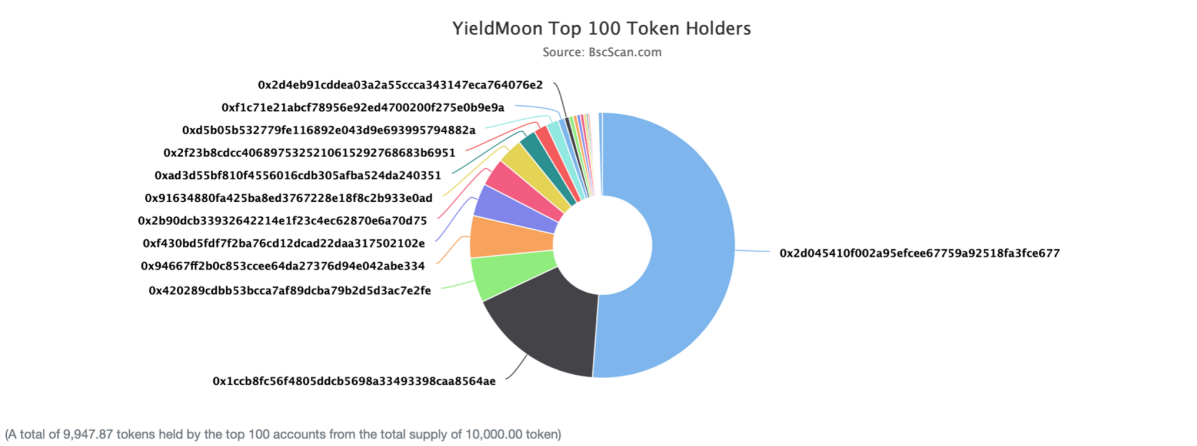
Token contract details for 04.05.2021.

Contract name:	YieldMoon
Contract address:	0x2f23b8cdcc4068975325210615292768683b6951
Total supply:	10_000_000_000_000_000_000_000
Token ticker:	YMOON
Decimals:	18
Token holders:	40
Transactions count:	120
Top 100 holders dominance:	99.48 %
Liquidity fee:	5
Tax fee:	5
Total fees:	260_473_928_912_329_634_549
Uniswap V2 pair:	0x1ccb8fc56f4805ddcb5698a33493398caa8564ae
Contract deployer address:	0x44ed84b915427204e5d99583daccb8ad0b1bcec3
Contract's current owner address:	0x00

# YieldMoon token distribution

The top 100 holders collectively own 99.48% (9,947.87 Tokens) of YieldMoon

Token Total Supply: 10,000.00 Token | Total Token Holders: 40



# YieldMoon top 10 token holders

Rank	Address	Quantity (Token)	Percentage
1	0x2d045410f002a95efcee67759a92518fa3fce677	5,120.836872658315604489	51.2084%
2	0x1ccb8fc56f4805ddcb5698a33493398caa8564ae	1,680.276896659060258106	16.8028%
3	0x420289cddb53bcca7af89dcb97b2d5d3ac7e2fe	543.035249333030928826	5.4304%
4	0x94667ff2b0c853ccee64da27376d94e042abe334	515.749681796650329992	5.1575%
5	0xf430bd5fd7f2ba76cd12dcad22daa317502102e	399.150329473993507963	3.9915%
6	0x2b90dcb33932642214e1f23c4ec62870e6a70d75	346.169329564546220209	3.4617%
7	0x91634880fa425ba8ed3767228e18f8c2b933e0ad	313.277174919426116835	3.1328%
8	0xad3d55bf810f4556016cdb305afba524da240351	221.41858051520286663	2.2142%
9	0x2f23b8dcc4068975325210615292768683b6951	162.539719136935992185	1.6254%
10	0xd5b05b532779fe116892e043d9e693995794882a	152.927495924695123305	1.5293%

# YieldMoon LP token holders

Rank	Address	Quantity	Percentage
1	0xeb3a9c56d963b971d320f889be2fb8b59853e449	59.160797830996159425	96.6028%
2	0x00	1.833297549347256023	2.9936%
3	0x07d80ae6f36a5e08dca74ce884a24d39db9934ed	0.247177010265064231	0.4036%

# Contract functions details

## + [Int] IERC20

- [Ext] totalSupply
- [Ext] balanceOf
- [Ext] transfer #
- [Ext] allowance
- [Ext] approve #
- [Ext] transferFrom #

## + [Lib] SafeMath

- [Int] add
- [Int] sub
- [Int] sub
- [Int] mul
- [Int] div
- [Int] div
- [Int] mod
- [Int] mod

## + Context

- [Int] \_msgSender
- [Int] \_msgData

## + [Lib] Address

- [Int] isContract
- [Int] sendValue #
- [Int] functionCall #
- [Int] functionCall #
- [Int] functionCallWithValue #
- [Int] functionCallWithValue #
- [Prv] \_functionCallWithValue #

## + Ownable (Context)

- [Int] <Constructor> #
- [Pub] owner
- [Pub] renounceOwnership #
  - modifiers: onlyOwner
- [Pub] transferOwnership #
  - modifiers: onlyOwner
- [Pub] geUnlockTime
- [Pub] lock #
  - modifiers: onlyOwner
- [Pub] unlock #

## + [Int] IUniswapV2Factory

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

#### + [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] 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 #

+ YieldMoon (Context, IERC20, Ownable)

- [Pub] <Constructor> #
- [Pub] name
- [Pub] symbol
- [Pub] decimals
- [Pub] totalSupply
- [Pub] balanceOf
- [Pub] transfer #
- [Pub] allowance
- [Pub] approve #
- [Pub] transferFrom #
- [Pub] increaseAllowance #
- [Pub] decreaseAllowance #
- [Pub] isExcludedFromReward
- [Pub] totalFees
- [Pub] deliver #
- [Pub] reflectionFromToken
- [Pub] tokenFromReflection
- [Pub] excludeFromReward #
  - modifiers: onlyOwner
- [Ext] includeInReward #
  - modifiers: onlyOwner
- [Prv] \_transferBothExcluded #
- [Pub] excludeFromFee #
  - modifiers: onlyOwner
- [Pub] includeInFee #
  - modifiers: onlyOwner
- [Ext] setTaxFeePercent #



- modifiers: onlyOwner
- [Ext] setLiquidityFeePercent #
  - modifiers: onlyOwner
- [Ext] setMaxTxPercent #
  - modifiers: onlyOwner
- [Pub] setSwapAndLiquifyEnabled #
  - modifiers: onlyOwner
- [Ext] <Fallback> (\$)
- [Prv] \_reflectFee #
- [Prv] \_getValues
- [Prv] \_getTValues
- [Prv] \_getRValues
- [Prv] \_getRate
- [Prv] \_getCurrentSupply
- [Prv] \_takeLiquidity #
- [Prv] calculateTaxFee
- [Prv] calculateLiquidityFee
- [Prv] removeAllFee #
- [Prv] restoreAllFee #
- [Pub] isExcludedFromFee
- [Prv] \_approve #
- [Prv] \_transfer #
- [Prv] swapAndLiquify #
  - modifiers: lockTheSwap
- [Prv] swapTokensForEth #
- [Prv] addLiquidity #
- [Prv] \_tokenTransfer #
- [Prv] \_transferStandard #
- [Prv] \_transferToExcluded #
- [Prv] \_transferFromExcluded #

(\$ ) = 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 `includeInReward()` 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.

```
function includeInReward(address account↑) external onlyOwner() {
    require(!_isExcluded[account↑], "Account is already excluded");
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (_excluded[i] == account↑) {
            _excluded[i] = _excluded[_excluded.length - 1];
            tOwned[account↑] = 0;
            _isExcluded[account↑] = false;
            _excluded.pop();
            break;
        }
    }
}
```

- ❑ The function `_getCurrentSupply` also uses the loop for evaluating total supply. It also could be aborted with `OUT_OF_GAS` exception if there will be a long excluded addresses list.

```
function _getCurrentSupply() private view returns(uint256, uint256) {
    uint256 rSupply = _rTotal;
    uint256 tSupply = _tTotal;
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (_rOwned[_excluded[i]] > rSupply || _tOwned[_excluded[i]] > tSupply) return (_rTotal, _tTotal);
        rSupply = rSupply.sub(_rOwned[_excluded[i]]);
        tSupply = tSupply.sub(_tOwned[_excluded[i]]);
    }
    if (rSupply < _rTotal.div(_tTotal)) return (_rTotal, _tTotal);
    return (rSupply, tSupply);
}
```

Recommendation:

Use `EnumerableSet` instead of array or do not use long arrays.

# Conclusion

Smart contracts contain low severity issues! Liquidity pair contract is not checked.

Liquidity locking details on DXSale provided by the team until 4 May 2023 at 15:22 -

<https://dxsale.app/app/pages/dxlockview?id=0&add=0x44Ed84B915427204E5D99583dAcCb8aD0B1Bcec3&type=lplock&chain=BSC>

Tokens reserved for airdrop locked on DXSale details provided by the team -

<https://dxsale.app/app/pages/dxlockview?id=0&add=0x44Ed84B915427204E5D99583dAcCb8aD0B1Bcec3&type=tokenlock&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.*