Techrate1 Techrate

TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

June, 2021

Audit Details

Audited project

StakeMars Protocol

Deployer address

0x89Ff50B890f4C07aB92C5B008551e737c3e846a2

Client contacts:

StakeMars Protocol team

Blockchain

Binance Smart Chain

Project website:

https://stakemars.com/

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 StakeMars Protocol to perform an audit of smart contracts:

https://bscscan.com/address/0x74f4ccdaEdb13b73754cf7Bb8CbABE74E2DD4B70

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.

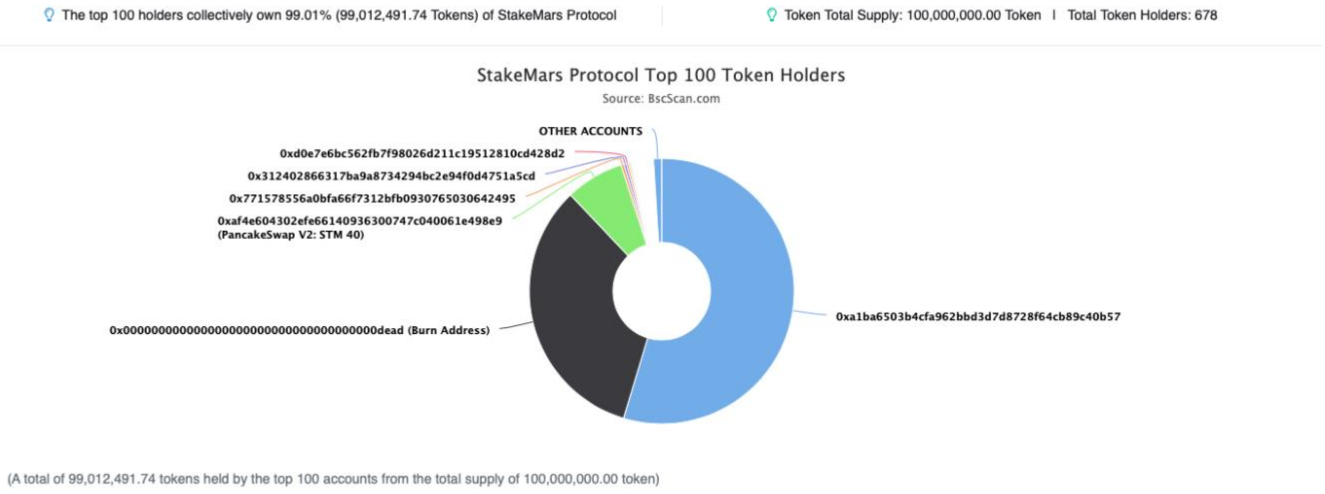
The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Contracts Details

Token contract details for 15.06.2021

Contract name	StakeMars Protocol
Contract address	0x74f4ccdaEdb13b73754cf7Bb8CbABE74E2DD4B70
Total supply	100,000,000
Token ticker	STM
Decimals	18
Token holders	678
Transactions count	17,311
Top 100 holders dominance	99.01%
Tax fee	10
Marketing address	0x18137263935bd44ea64fac1118cde4c0dde53e22
Staking address	0xa1ba6503b4cfa962bbd3d7d8728f64cb89c40b57
Uniswap V2 pair	0xaf4e604302efe66140936300747c040061e498e9
Contract deployer address	0x89Ff50B890f4C07aB92C5B008551e737c3e846a2
Contract’s current owner address	0x89ff50b890f4c07ab92c5b008551e737c3e846a2

StakeMars Protocol Token Distribution



The top 100 holders collectively own 99.01% (99,012,491.74 Tokens) of StakeMars Protocol

Token Total Supply: 100,000,000.00 Token | Total Token Holders: 678

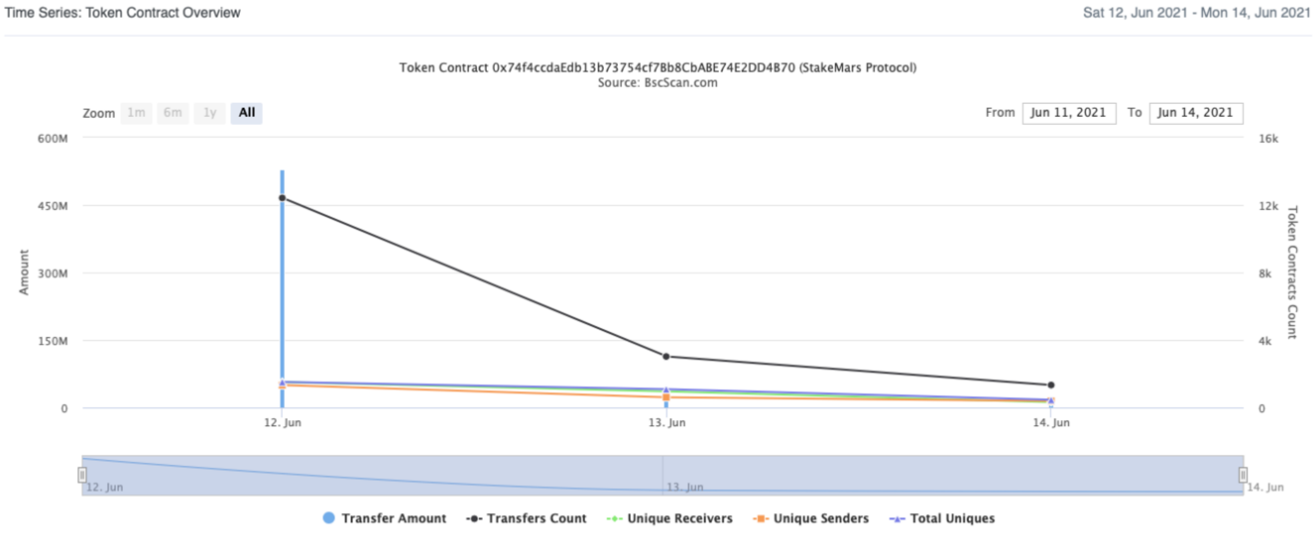
StakeMars Protocol Top 100 Token Holders

Source: BscScan.com

OTHER ACCOUNTS
0xd0e7e6bc562fb7f98026d211c19512810cd428d2
0x312402866317ba9a8734294bc2e94f0d4751a5cd
0x771578556a0bfa66f7312bfb0930765030642495
0xaf4e604302efe66140936300747c040061e498e9 (PancakeSwap V2: STM 40)
0x000000000000000000000000000000000000dead (Burn Address)
0xa1ba6503b4cfa962bbd3d7d8728f64cb89c40b57

(A total of 99,012,491.74 tokens held by the top 100 accounts from the total supply of 100,000,000.00 token)

StakeMars Protocol Contract Interaction Details



Time Series: Token Contract Overview

Sat 12, Jun 2021 - Mon 14, Jun 2021

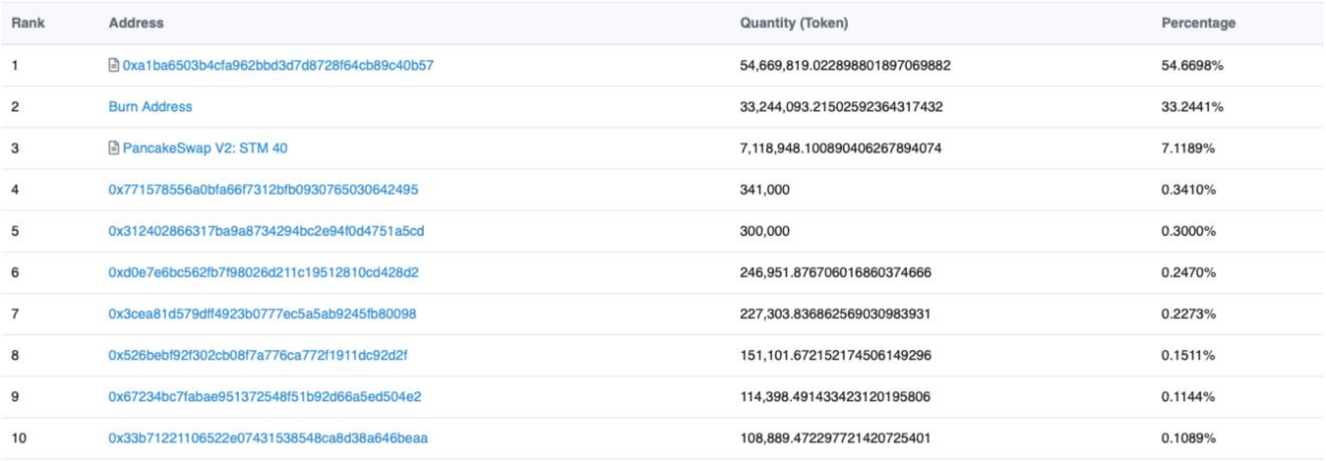
Token Contract 0x74f4ccdaEdb13b73754cf7Bb8CbABE74E2DD4B70 (StakeMars Protocol)

Source: BscScan.com

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

From Jun 11, 2021 To Jun 14, 2021

StakeMars Protocol Top 10 Token Holders



Rank	Address	Quantity (Token)	Percentage
1	0xa1ba6503b4cfa962bbd3d7d8728f64cb89c40b57	54,669,819.022898801897069882	54.6698%
2	Burn Address	33,244,093.21502592364317432	33.2441%
3	PancakeSwap V2: STM 40	7,118,948.100890406267894074	7.1189%
4	0x771578556a0bfa66f7312bfb0930765030642495	341,000	0.3410%
5	0x312402866317ba9a8734294bc2e94f0d4751a5cd	300,000	0.3000%
6	0xd0e7e6bc562fb7f98026d211c19512810cd428d2	246,951.876706016860374666	0.2470%
7	0x3cea81d579dff4923b0777ec5a5ab9245fb80098	227,303.836862569030983931	0.2273%
8	0x526bebf92f302cb08f7a776ca772f1911dc92d2f	151,101.672152174506149296	0.1511%
9	0x67234bc7fabae951372548f51b92d66a5ed504e2	114,398.491433423120195806	0.1144%
10	0x33b71221106522e07431538548ca8d38a646beaa	108,889.472297721420725401	0.1089%

Contract functions details

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

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

+ [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] 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 #

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

+  BaseERC20 (Context, Ownable)
  - [Pub] <Constructor> #
  - [Pub] name
  - [Pub] symbol
  - [Pub] decimals
  - [Pub] totalSupply
  - [Pub] balanceOf
  - [Pub] approve #
  - [Pub] allowance
  - [Pub] transfer #
  - [Pub] transferFrom #
  - [Int] _transfer #
  - [Int] _approve #

+ [Int] IStaking
  - [Ext] distribute ($)

+  StakeMars (BaseERC20)
  - [Pub] <Constructor> #
    - modifiers: BaseERC20
  - [Int] _transfer #
  - [Prv] _feeTransfer #
  - [Prv] _noFeeTransfer #
  - [Prv] _isWhitelisted
  - [Ext] <Fallback> ($)
  - [Prv] _swap #
  - [Prv] swapTokensForEth #
```

- [Prv] addLiquidity #
- [Ext] setStakingAddress #
  - modifiers: onlyOwner
- [Ext] updateWhitelist #
  - modifiers: onlyOwner
- [Ext] setMktAddress #
  - 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.	Passed
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 high severity issues found.

Low Severity Issues

1. Wrong burning

Issue:

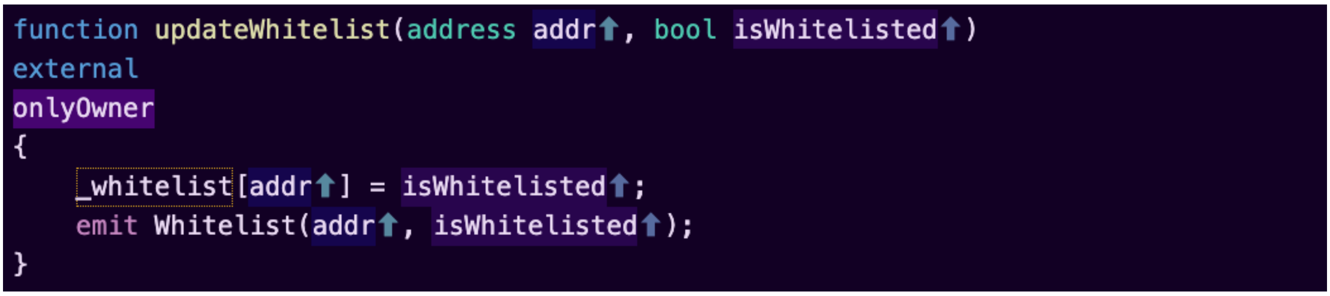
- The function _feeTransfer () sends burn amount to burnAddress instead of decreasing totalSupply.

Recommendation:

Decrease total supply value instead of sending burn amount to zero address.

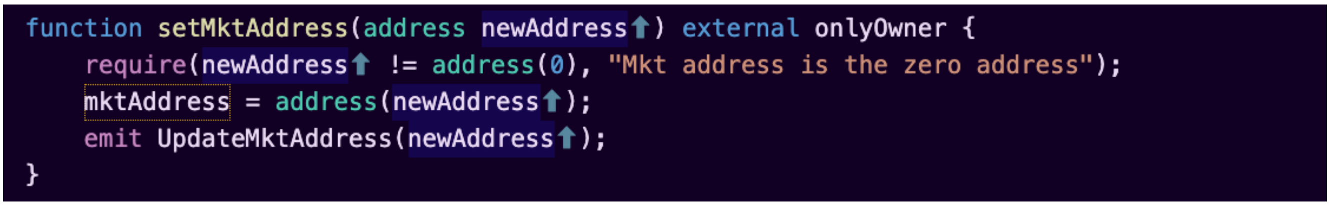
Owner privileges (In the period when the owner is not renounced)

- Owner can remove from fees.



```
function updateWhitelist(address addr, bool isWhitelisted)
external
onlyOwner
{
    _whitelist[addr] = isWhitelisted;
    emit Whitelist(addr, isWhitelisted);
}
```

- Owner can change marketing address.



```
function setMktAddress(address newAddress) external onlyOwner {
    require(newAddress != address(0), "Mkt address is the zero address");
    mktAddress = address(newAddress);
    emit UpdateMktAddress(newAddress);
}
```

Conclusion

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

Liquidity locking details provided by the team:
https://dxsale.app/app/pages/dxlockview?id=0&add=0x89Ff50B890f4C07aB92C5B008551e737c3e846a2&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.