Smart Contract Security Audit

Audit details:

Audited project:	HMfinance
Deployer address:	0x93052D51d56b324DC83fAE77C5de33543547e2F3
Client contacts:	HmFinanceteam
Blockchain:	Binance Smart Chain
Project website:	https://happymoney.finance

June, 2021
TechRate

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 HMFinance to perform an audit of smart contracts:

- https://bscscan.com/address/0x87eba250a34e7486eab140d89e2eb5d8d113ea2d#code
- https://bscscan.com/address/0x811A75bb32093683b51EC6bFe5D1CF42daC9305B#code
- https://bscscan.com/address/0xf6Aa87c741fffC94FB55546Ef9c5e1708977b1a4#code
- https://bscscan.com/address/0xF0eF5C1B87603ce369E9A03e847BeE410617Eb45#code
- https://bscscan.com/address/0x176E3D77c7712Bf830387e85855a5D7c11a2a725#code
- https://bscscan.com/address/0x0f456eE8553dd095Ad77B2f5e23DfeAb464c02A3#code
- https://bscscan.com/address/0x5a4df9242f45aDB061DF115F2ea2648Ea6FA7614#code
- https://bscscan.com/address/0x779d378A3C6C687A57e24E4Dc6C1b27B4e427CFd#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 22.06.2021

Contract name:	HMFinance
Contract address:	0x93052D51d56b324DC83fAE77C5de33543547e2F3
Total supply:	100_000_000_000_000_000_000_000_000
Token ticker:	HM
Decimals:	9
Token holders:	8
Transactions count:	8
Top 100 holders dominance:	100 %
Burn fee:	0
Tax fee:	0
Total fees:	0
Total burn:	0
Contract deployer address:	0x6544ca3303dca6f1ca8fa9bada44c2859b9d0333
Contract's current owner address:	0x6544ca3303dca6f1ca8fa9bada44c2859b9d0333

HMFinance token distribution

The top 100 holders collectively own 100.00% (100,000,000.00 Tokens) of Happy Money

Token Total Supply: 100,000,000.00 Token | Total Token Holders: 8

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

HMFinance top 10 token holders

Rank	Address	Quantity (Token)	Percentage
1	0x6544ca3303dca6f1ca8fa9bada44c2859b9d0333	83,600,000	83.6000%
2	0x21abc36ad7c9ca5b561be2f63154c444f132c798	2,400,000	2.4000%
3	0x3892abb3c5d06d67ac555edf4daca5af350bc629	2,400,000	2.4000%
4	0x5a6816374651e5e9cac613d437a58b0dcd672395	2,400,000	2.4000%
5	0x5b656ddf32ad898ec623475b7f52146abbcd158a	2,400,000	2.4000%
6	0x84cb39fcd979b96db4d8ee887cb315bf8b6ef1b8	2,400,000	2.4000%
7	0x0b1aa50a7bbfeb07bbea5fa7157dcfcebc5176c9	2,400,000	2.4000%
8	0x1add3e1fa45e0ed96bcf7adea6dab558d83820fb	2,000,000	2.0000%

Lock release times

Lock 1

- For: Team/Dev/Marketing 1
- Contract address: 0x21abc36ad7c9ca5b561be2f63154c444f132c798
- Release time: 1627776000
- Beneficiary: 0xcb3d1488c16f6ca622ee57194fb3cbe7baa317d7

Lock 2

- For: Team/Dev/Marketing 2
- Contract address: 0x3892abb3c5d06d67ac555edf4daca5af350bc629
- Release time: 1635724800
- Beneficiary: 0x850d94ab22a85ba787e3c0c247259179896a52c8

Lock 3

- For: Team/Dev/Marketing 3
- Contract address: 0x5a6816374651e5e9cac613d437a58b0dcd672395
- Release time: 1643673600
- Beneficiary: 0x2c9d50c5dbed45b4dbdb0133787492865010855d

Lock 4

- For: Team/Dev/Marketing 4
- Contract address : 0x5b656ddf32ad898ec623475b7f52146abbcd158a
- Release time: 1651363200
- Beneficiary: 0xf0067ae518ce512ad2335750922bd14eecbb0c85

Lock 5

- For: Team/Dev/Marketing 5
- Contract address: 0x84cb39fcd979b96db4d8ee887cb315bf8b6ef1b8
- Release time: 1659312000
- Beneficiary: 0x6cf37cc00a3de2316d72a26e854d3e2e85616c6c

Lock 6

- For: Community
- Contract address: 0x0b1aa50a7bbfeb07bbea5fa7157dcfcebc5176c9
- Release time: 1627776000
- Beneficiary: 0xf845407e8574f229c15d285f8f8f07af0a8ffcb4

Lock 7

- For: Community
- Contract address: 0x1add3e1fa45e0ed96bcf7adea6dab558d83820fb
- Release time: 1635724800
- Beneficiary: 0xf845407e8574f229c15d285f8f8f07af0a8ffcb4

Contract functions details

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

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

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

+ [Lib] SafeMath
  - [Int] tryAdd
  - [Int] trySub
  - [Int] tryMul
  - [Int] tryDiv
  - [Int] tryMod
  - [Int] add
  - [Int] sub
  - [Int] mul
  - [Int] div
  - [Int] mod
  - [Int] sub
  - [Int] div
  - [Int] mod

+ [Lib] Address
  - [Int] isContract
  - [Int] sendValue #
  - [Int] functionCall #
  - [Int] functionCall #
  - [Int] functionCallWithValue #
  - [Int] functionCallWithValue #
  - [Int] functionStaticCall
  - [Int] functionStaticCall

- [Int] functionDelegateCall #
- [Int] functionDelegateCall #
- [Prv] _verifyCallResult

+ ATToken (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] isExcluded
- [Pub] totalFees
- [Pub] totalBurn
- [Pub] payTax #
- [Pub] reflectionFromToken
- [Pub] tokenFromReflection
- [Ext] excludeAccount #
  - modifiers: onlyOwner
- [Ext] includeAccount #
  - modifiers: onlyOwner
- [Prv] _approve #
- [Prv] _transfer #
- [Prv] _transferStandard #
- [Prv] _transferToExcluded #
- [Prv] _transferFromExcluded #
- [Prv] _transferBothExcluded #
- [Prv] _burnAndRebase #
- [Prv] _getValues
- [Prv] _getTValues
- [Prv] _getRValues
- [Prv] _getRate
- [Prv] _getCurrentSupply
- [Prv] _setBurnFee #
- [Ext] setBurnFee #
  - modifiers: onlyOwner
- [Ext] setTaxFee #
  - modifiers: onlyOwner
- [Pub] getTaxFee
- [Pub] getBurnFee
- [Prv] getMaxTxSize

- [Pub] getTideCycle
- [Pub] getBurnCycle
- [Pub] getTradedCycle
- [Int] _rebase #
- [Int] _initializeFinalStage #

($) = 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 `includeAccount()` 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 includeAccount(address account⬆) external onlyOwner() {
    require(_isExcluded[account⬆], "Account is already included");
    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.

Owner privileges

- Owner can change the tax and burn fee in the range of 0 - 15 percent.

Conclusion

Smart contracts contain low severity issues and owner privileges.

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.