HackSafe

Smart Contract Security Audit Report

Musk Melon

April **2022**

Security Status

★ ★ ★ ★ ★

www.hacksafe.io

Audit Details

Audited project
Musk Melon

Deployer address
0xAEA1258D9D8801B0425132D37ef6F15932573DAD

Client contacts
Musk Melon team

Blockchain
Binance smartchain

Website
www.muskmelon.org

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) (HackSafe) owe no duty of care towards you or any other person, nor does HackSafe 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 HackSafe 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, HackSafe hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against HackSafe, 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

HackSafe was commissioned by Musk Melon to perform an audit of smart contracts:

- https://bscscan.com/address/0xb14784b2a56945aed7b8cd41661d68f8b6ccec8b#code

The purpose of the audit was to achieve the following:

- Ensure that the smart contract functions as intended.
- Identify potential security issue 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 17.04.2022

Contract name	: Musk Melon
Contract address	: 0xb14784b2a56945AED7b8CD41661D68F8b6CCeC8b
Total supply	: 10 billion
Token ticker	: MELON
Decimals	: 18
Network	: BSC
Transactions count	: 5,688
Token Holders	: 5,683 addresses
Contract deployer address	: 0xAEA1258D9D8801B0425132D37ef6F15932573DAD
Owner address	: 0xAEA1258D9D8801B0425132D37ef6F15932573DAD

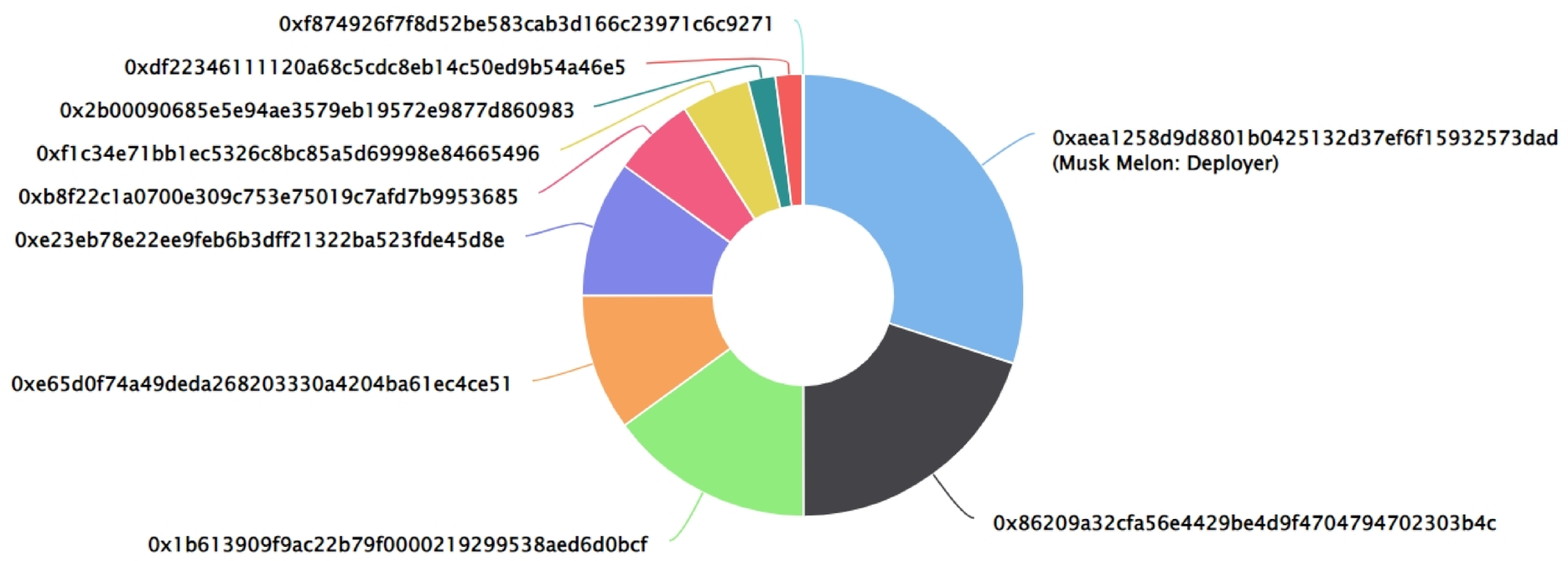
Musk Melon Token Distribution

The top 500 holders collectively own 100.00% (9,999,994,817.50 Tokens) of Musk Melon

Token Total Supply: 10,000,000,000.00 Token | Total Token Holders: 5,683

Musk Melon Top 500 Token Holders

Source: BscScan.com



Musk Melon Top 10 Token Holders

(A total of 9,999,684,680.00 tokens held by the top 10 accounts from the total supply of 10,000,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	Musk Melon: Deployer	2,999,094,800	29.9909%
2	0x86209a32cfa56e4429be4d9f4704794702303b4c	2,000,000,000	20.0000%
3	0x1b613909f9ac22b79f0000219299538aed6d0bcf	1,500,000,000	15.0000%
4	0xe65d0f74a49deda268203330a4204ba61ec4ce51	1,000,000,000	10.0000%
5	0xe23eb78e22ee9feb6b3dff21322ba523fde45d8e	1,000,000,000	10.0000%
6	0xb8f22c1a0700e309c753e75019c7afd7b9953685	600,000,000	6.0000%
7	0xf1c34e71bb1ec5326c8bc85a5d69998e84665496	500,000,000	5.0000%
8	0x2b00090685e5e94ae3579eb19572e9877d860983	200,000,000	2.0000%
9	0xdf22346111120a68c5cdc8eb14c50ed9b54a46e5	199,989,880	1.9999%
10	0xf874926f7f8d52be583cab3d166c23971c6c9271	600,000	0.0060%

Contract functions details

+ Context
    -[int]_msgsender
    -[Int] _msgdata

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

+ [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)
    <Constructor>#
    -[Pub] name
    -[Pub] symbol
    -[Pub] decimals
    -[Pub] totalsupply
    -[Pub] balanceOf
    -[Pub] transfer#
    -[Pub] allowance
    -[Pub] approv#
    -[Pub] transferFrom#
    -[Pub] increaseAllowance#
    -[Pub] decreaseAllowance#

Contract functions details

-[Int] _transfer
-[Int] _mint#
-[Int] _burn#
-[Int] _approve#
-[Int] _spendAllowance#
-[Int] _beforeTokenTransfer
-[Int] _afterTokenTransfer

+ ERC20Burnable (Context, ERC20)
-[Pub] burn#
-[Pub] burnFrom#

+ MuskMelon (ERC20, ERC20Burnable, Ownable)
<constructor>#
-[Pub] mint
-Modifier: onlyOwner

($) = payable function
= non-constant function

Issues Checking Status

No.	Title	Status
1.	Unlocked Compiler Version	Low issues
2.	Missing Input Validation	Passed
3.	Race conditions and Reentrancy. Cross-function race conditions.	Passed
4.	Possible delays in data delivery	Passed
5.	Oracle calls.	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.	Private use data leaks.	Passed
13.	Malicious Event log.	Passed
14.	Scoping and Declarations.	Passed
15.	Uninitialized storage pointers.	Passed
16.	Arithmetic accuracy.	Passed
17.	Design Logic.	Passed
18.	Safe Open Zeppelin contracts implementation and usage.	Passed
19.	Incorrect Naming State Variable	Passed

Security Issues

- **High Severity Issues**
  No high severity issue found.
- **Medium Severity Issues**
  No medium severity issue found.
- **Low Severity Issues**
  One low severity issue found.

1. Unlocked Compiler Version

- **Description**

  The contract utilizes an unlocked compiler version. An unlocked compiler version in the contract's source code permits the user to compile it at or above a particular version. This, in turn, leads to differences in the generated bytecode between compilations due to differing compiler version numbers. This can lead to ambiguity when debugging as compiler-specific bugs may occur in the codebase that would be difficult to identify over a span of multiple compiler versions rather than a specific one.

- **Recommendation**

  We advise to use only one compiler version instead multi pragma which is alternatively locked at the lowest version possible so that the contract can be compiled. Use following line instead of pragma solidity ^0.8.4;

  pragma solidity 0.8.4;

Owner Privileges

Owner Privileges (in the period when the owner is not renounced) :

- MuskMelon Contract:
    - Owner can renounce ownership.
    - Owner can transfer ownership.
    - Owner can mint tokens.

Conclusion

Smart contract contains low severity issues!