



Smart Contract Security Audit Report

Memeflate

December 2022

Security Status



www.hacksafe.io



Audit Details



Audited project

Memeflate



Deployer address

0xfe3b9bc6e3ad8294a5196144cef52e9167c63f02



Client contacts

Memeflate Team



Blockchain

Binance smart chain



Website

<http://www.memeflate.io/>

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.

Procedure

Step 1 - In-Depth Manual Review

Manual line-by-line code reviews to ensure the logic behind each function is sound and safe from various attack vectors. This is the most important and lengthy portion of the audit process (as automated tools often cannot find the nuances that lead to exploits such as flash loan attacks).

Step 2 - Automated Testing

Simulation of a variety of interactions with your Smart Contract on a test blockchain leveraging a combination of automated test tools and manual testing to determine if any security vulnerabilities exist.

Step 3 – Leadership Review

The engineers assigned to the audit will schedule meetings with our leadership team to review the contracts, any comments or findings, and ask questions to further apply adversarial thinking to discuss less common attack vectors.

Step 4 - Resolution of Issues

Consulting with the team to provide our recommendations to ensure the code's security and optimize its gas efficiency, if possible. We assist project team's in resolving any outstanding issues or implementing our recommendations.

Step 5 - Published Audit Report

Boiling down results and findings into an easy-to-read report tailored to the project. Our audit reports highlight resolved issues and any risks that exist to the project or its users, along with any remaining suggested remediation measures. Diagrams are included at the end of each report to help users understand the interactions which occur within the project.

Background

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

- <https://bscscan.com/token/0xaFE3321309A994831884fc1725F4c3236AC79f76#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 understood 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.

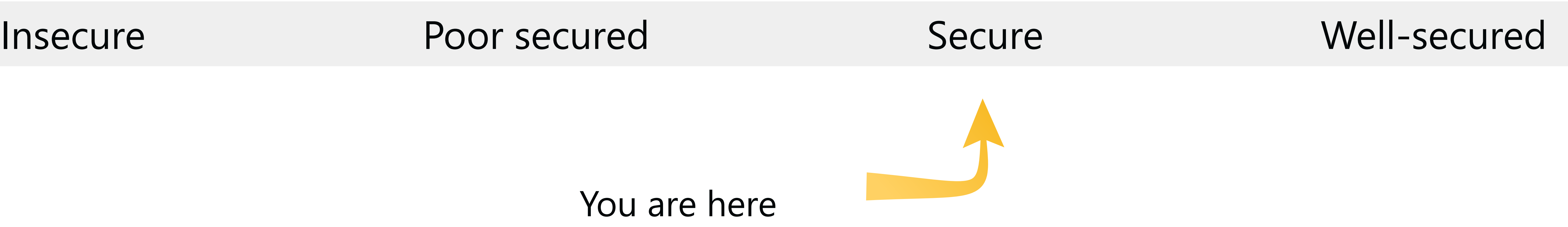
Contract Details

Token contract details for 14.12.2022

Token Type	: Marketplace
Contract name	: MEMEFLATE
Contract address	: 0xaFE3321309A994831884fc1725F4c3236AC79f76
Total supply	: 1,000,000,000,000,000,000
Token ticker	: \$MFLATE
Decimals	: 9
Token Holders	: 7,301
Transactions count	: 27,769
Compiler version	: v0.7.6+commit.7338295f
Contract deployer address	: 0xfe3b9bc6e3ad8294a5196144cef52e9167c63f02
Owner address	: 0x43642e03c4fc87c73ee2cf648196fb4909c415ac

Audit Summary

According to the standard audit assessment, Customer`s solidity smart contracts are **“Secure”**. This token contract does contain owner control, which do not make it fully decentralized.



We used various tools like Slither, Mythril and Remix IDE. At the same time this finding is based on critical analysis of the manual audit. All issues found during automated analysis were manually reviewed and applicable vulnerabilities are presented in the issues checking status.

We found 0 critical, 0 high, 1 medium and 2 low.

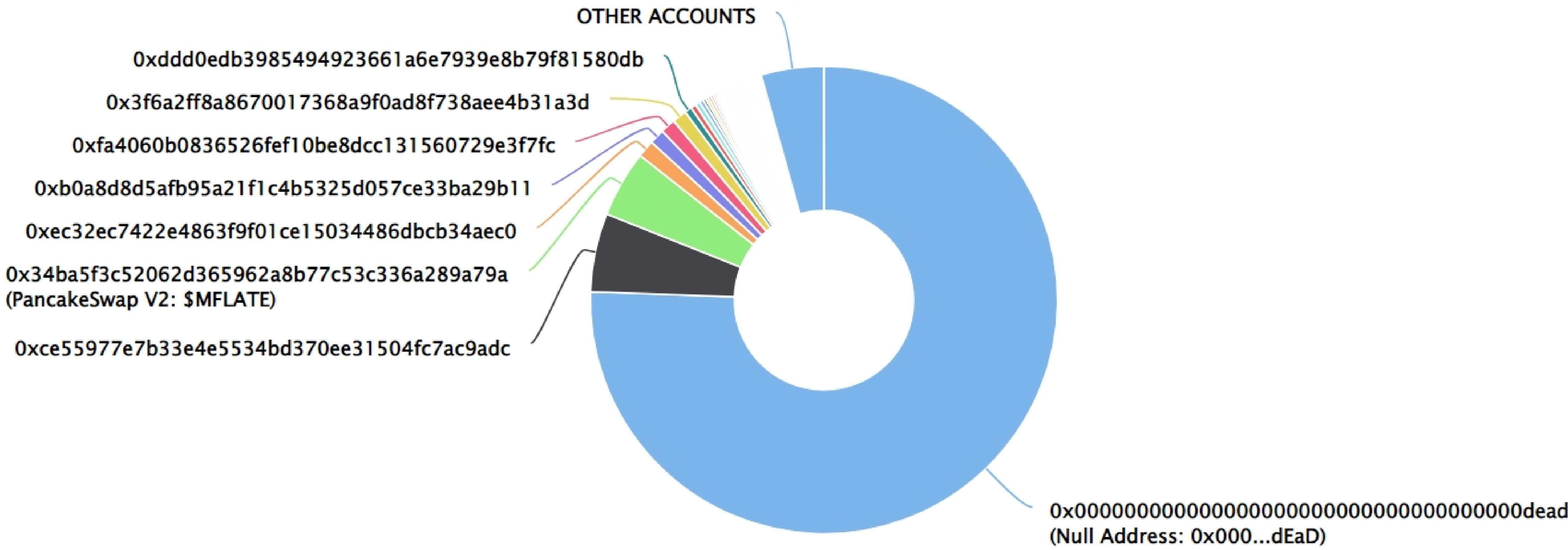
Memeflate Token Distribution

💡 The top 100 holders collectively own 95.67% (95,667,950,610,726,200.00 Tokens) of Memeflate

💡 Token Total Supply: 100,000,000,000,000,000.00 Token | Total Token Holders: 7,300



Memeflate Top 100 Token Holders

Source: BscScan.com



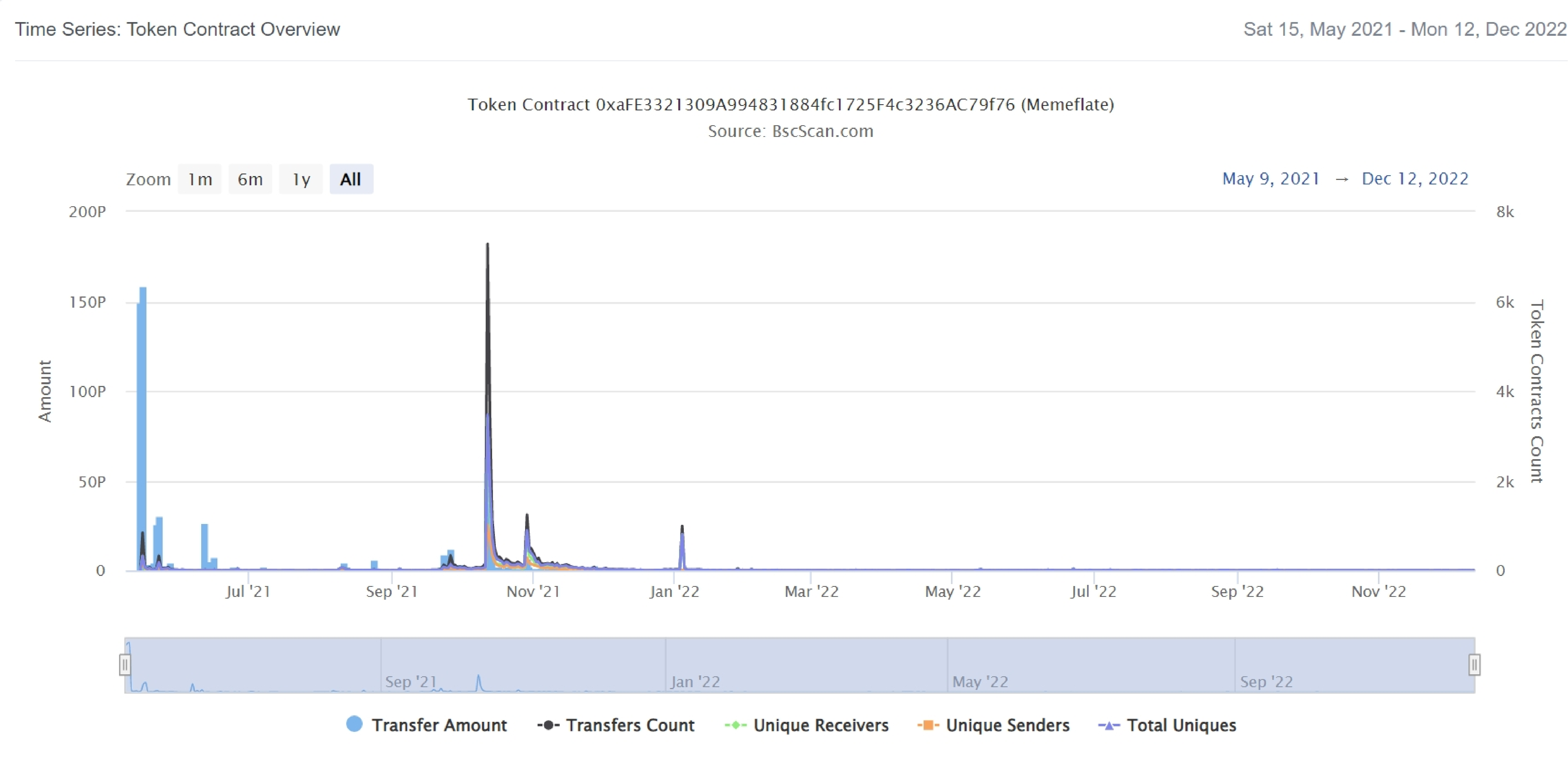
Memeflate Top 20 Token Holders

(A total of 95,667,950,610,726,200.00 tokens held by the top 100 accounts from the total supply of 100,000,000,000,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	Null Address: 0x000...dEaD	75,579,478,759,612,100.068049465	75.5795%
2	0xce55977e7b33e4e5534bd370ee31504fc7ac9adc	5,425,903,506,048,000.16344166	5.4259%
3	 PancakeSwap V2: \$MFLATE	4,599,925,606,743,370.913393888	4.5999%
4	0xec32ec7422e4863f9f01ce15034486dbcb34aec0	1,195,763,366,288,130.493818719	1.1958%
5	0xb0a8d8d5afb95a21f1c4b5325d057ce33ba29b11	1,050,112,293,201,670.162701651	1.0501%
6	0xfa4060b0836526fef10be8dcc131560729e3f7fc	1,030,896,293,669,610.888140212	1.0309%
7	0x3f6a2ff8a8670017368a9f0ad8f738aee4b31a3d	1,001,919,880,844,070.564928808	1.0019%
8	0xdd0edb3985494923661a6e7939e8b79f81580db	500,215,269,811,279.200754157	0.5002%
9	0x388963ca9ce19adca4ec4058c24df85639f5ef7c	356,321,993,697,502.93428816	0.3563%
10	0x68421a3e2521f35731f6432b978fc3dfb4d4e9da	335,233,865,150,238.000634342	0.3352%
11	0xd153b6e1ff4fbdc8cef59d5633d915887a22288f	272,178,665,765,886.477193837	0.2722%
12	0xbe4b59f18fe0e842d86c1edb8abdc8023588b0f	196,142,357,437,132.308870925	0.1961%
13	0x484edcf57306a0f73f9588269eeba858ab1188e4	191,193,841,008,362.477190955	0.1912%
14	 0x32e81e780568c3b6597e24ab3355d46987bb07e2	190,000,000,000,000	0.1900%
15	0x30f3f2fe25e75de8f1a3cff5acd65b01f9d4a928	169,617,877,423,559.864162094	0.1696%
16	0xe3bce7b15d213d9b8d6122db64fa792981e69357	166,834,326,285,187.56323027	0.1668%
17	0xe6ece98424545323d0fd0f09b02a83c13d962f7f	152,160,296,294,116.347777863	0.1522%
18	0xd93ef487e2fe1b04771d14fb4bcb65621f864bbe	145,795,335,955,234.267444435	0.1458%
19	0x2767b8326836b76b650fdf8db3506c307e8fd8bf	132,474,956,847,914.632184043	0.1325%
20	0x5a906ca72471f2da119cb591cf9e0e9d9d23ffab	120,682,754,841,560.420632994	0.1207%

Memeflate Token Distribution

Memeflate Contract Overview



Contract functions details

+Context

- [Int] _msgSender
- [Int] _msgData

+ [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

+ [Lib] Address

- [Int] isContract
- [Int] sendValue
- [Int] functionCall
- [Int] functionCall
- [Int] functionCallWithValue
- [Int] functionCallWithValue
- [Pvt] _functionCallWithValue

+Ownable (Context)

- [Pub] <constructor>
- [Pub] owner
- [Pub] renounceOwnership #
 - modifiers: onlyOwner
- [Pub] transferOwnership #
 - modifiers: onlyOwner

Contract functions details

+ MEMEFLATE (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] reflect #
- [Pub] reflectionFromToken
- [Pub] tokenFromReflection
- [Pub] taxVote #
- [Pub] currentTax
- [Ext] changeTax #
 - modifiers: onlyOwner
- [Pvt] burnVotes #
 - modifiers: onlyOwner
- [Pub] leadingVote
- [Pub] currentVotes
- [Ext] voteClose #
 - modifiers: onlyOwner
- [Ext] excludeAccount #
 - modifiers: onlyOwner
- [Ext] includeAccount #
 - modifiers: onlyOwner
- [Pvt] _approve #
- [Pvt] _transfer #
- [Pvt] _transferStandard #
- [Pvt] _transferToExcluded #
- [Pvt] _transferFromExcluded #
- [Pvt] _transferBothExcluded #
- [Pvt] _reflectFee #

Contract functions details

- [Pvt] _getValues
- [Pvt] _getTValues
- [Pvt] _getRValues
- [Pvt] _getRate
- [Pvt] _getCurrentSupply

(\$) = payable function

Issues Checking Status

No.	Title	Status
1.	Unlocked Compiler Version	Low issue
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.	Medium Issue
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.	Low issue
17.	Design Logic.	Passed
18.	Safe Open Zeppelin contracts implementation and usage.	Passed
19.	Incorrect Naming State Variable	Passed
20.	Too old version	Passed

Severity Definitions

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to assets loss or data manipulations.
High	High-level vulnerabilities are difficult to exploit; however, they also have a significant impact on smart contract execution, e.g., public access to crucial functions
Medium	Medium-level vulnerabilities are important to fix; however, they can't lead to assets loss or data manipulations.
Low	Low-level vulnerabilities are mostly related to outdated, unused, etc. code snippets that can't have a significant impact on execution.

Security Issues

✔ Critical Severity Issues

No critical severity issue found.

✔ High Severity Issues

No high severity issue found.

✔ Medium Severity Issues

One medium severity issue found.

1. Out of gas error

• **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.

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.

• **Recommendation**

Check that the excluded array length is not too big.

✔ Low Severity Issues

Two low severity issue found

1. Rounding error

• **Issue:**

At each calculation with division, it is goes first. In Solidity we don't have floating points, but instead we get rounding errors

• **Recommendation**

Do division after multiplication.

2. 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.

Security Issues

- **Recommendation**

It is advisable that the compiler version is alternatively locked at the lowest version possible so that the contract can be compiled. For example, for version ^0.7.6 the contract should contain the following line:

```
pragma solidity 0.7.6;
```


Centralization

Owner privileges :

- Memeflate Contract:
 - Owner can transfer/renounce ownership.
 - Owner can change tax fee.
 - Owner can close vote.
 - Owner can include in and exclude from reward.

This smart contract has some functions which can be executed by the admin (Owner) only. If the admin wallet private key would be compromised, then it would not create trouble, as smart contract ownership has been renounced. Following are Admin functions:

- renounceOwnership
- transferOwnership
- changeTax
- burnVotes
- voteClose
- excludeAccount
- includeAccount

Conclusion

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

Liquidity locking details NOT provided by the team.

HackSafe 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.