MOTECH AUDIT

SMART CONTRACT SECURITY AUDIT

SECURITY ASSESSMENT

2021

MADHOUSE TOKEN AUDIT REPORT

11 NOV 2021

SECURITY ASSESMENT

TABLE OF CONTENTS

SECURITY ASSESMENT

SUMMARY

This report has been prepared for Madhouse to discover issues and vulnerabilities in the source code of the Madhouse project as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing Static Analysis, Manual Review, and Test net Deployment techniques.

The auditing process pays special attention to the following considerations:

- Testing the smart contracts against both common and uncommon attack vectors.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

The security assessment resulted in findings that ranged from critical to informational. We recommend addressing these findings to ensure a high level of security standards and industry practices. We suggest recommendations that could better serve the project from the security perspective:

- Enhance general coding practices for better structures of source codes;
- Add enough unit tests to cover the possible use cases given they are currently missing in the repository;
- Provide more comments per each function for readability, especially contracts are verified in public;
- Provide more transparency on privileged activities once the protocol is live.

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 MotechAudit and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (MotechAudit) owe no duty of care towards you or any other person, nor does MotechAudit 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 MotechAudit 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, MotechAudit hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against MotechAudit, 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.

SECURITY ASSESMENT

BACKGROUND

MotechAudit was commissioned by Madhouse to perform an audit of smart contracts:
https://bscscan.com/address/0x8c4885867d30f03ad04388cee01c65d11d192e61
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.

SECURITY ASSESMENT

AUDIT DETAILS

AUDITED PROJECT

Madhouse

DEPLOYER ADDRESS

0x03B32AbAB0d1EFd05CD707644cC0a0d687AfCD8F

CLIENT CONTACTS:

Madhouse team

BLOCKCHAIN

Binance Smart Chain Project

WEBSITE:

https://www.madhousetoken.com/

MOTECH AUDIT

SMART CONTRACT SECURITY AUDIT

SECURITY ASSESMENT

CONTRACT DETAILS

Token contract details for Sep-02-2021

Contract name	**Madhouse**
Contract address	**0x8c4885867D30F03AD04388cee01C65D11D192e61**
Total supply	**997,378,118.861766 MHTC**
Token ticker	**Madhouse Token (MHTC)**
Decimals	**9**
Token holders	**678**
Transactions count	**1,789**
Top 100 holders dominance	**0.967619%**
Contract deployer address	**0x03B32AbAB0d1EFd05CD707644cC0a0d687AfCD8F**
Contract's current owner address	**0x8c4885867d30f03ad04388cee01c65d11d192e61**

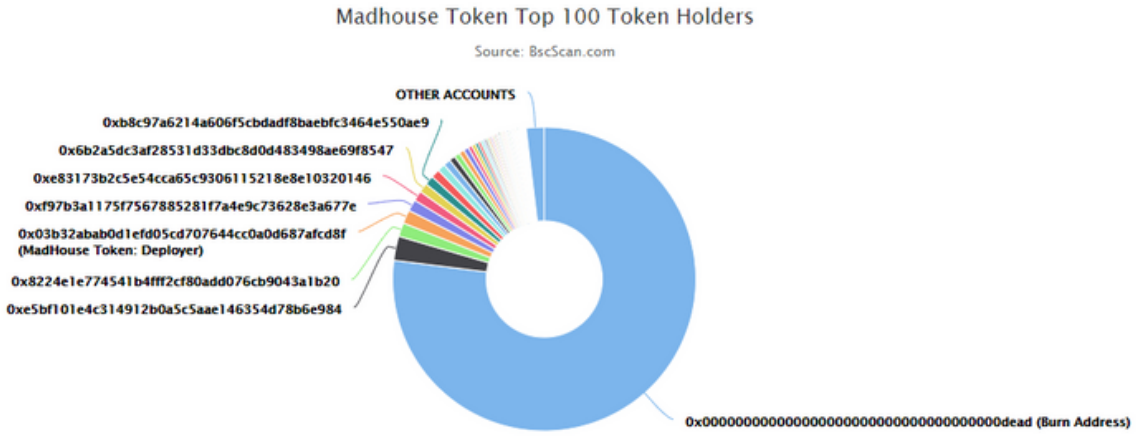
MOTECH AUDIT
SMART CONTRACT SECURITY AUDIT

SECURITY ASSESMENT

MADHOUSE TOKEN DISTRIBUTION

The top 100 holders collectively own 98.08% (978,192,408.01 Tokens) of Madhouse Token

Token Total Supply: 997,375,711.98 Token | Total Token Holders: 689

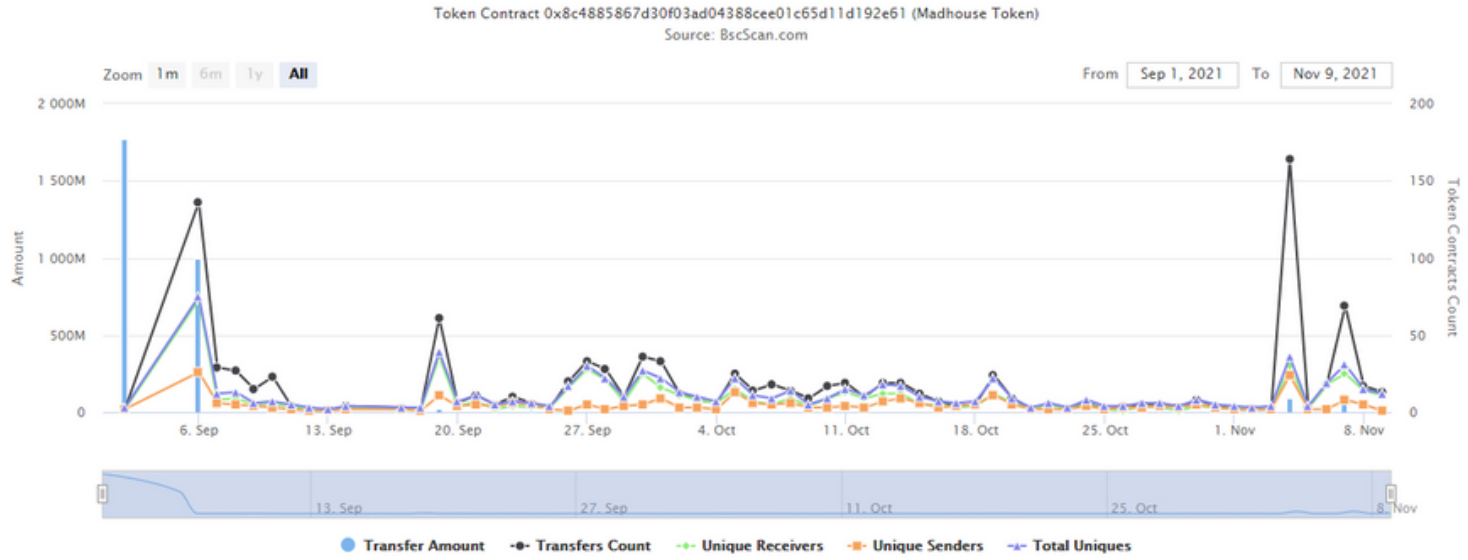


(A total of 978,192,408.01 tokens held by the top 100 accounts from the total supply of 997,375,711.98 token)

MADHOUSE TOKEN CONTRACT INTERACTION DETAILS

Time Series: Token Contract Overview

Thu 2, Sept 2021 - Tue 9, Nov 2021



MOTECH AUDIT

SMART CONTRACT SECURITY AUDIT

SECURITY ASSESMENT

TOP 10 TOKEN HOLDERS

Rank	Address	Quantity	Percentage	Analytics
1	Burn Address	767,729,203.567511126	76.9747%	
2	0xe5bf101e4c314912b0a5c5aae146354d78b6e984	25,730,776.34967675	2.5798%	
3	0x8224e1e774541b4fff2cf80add076cb9043a1b20	14,629,429.472049327	1.4668%	
4	MadHouse Token: Deployer	14,479,672.968421632	1.4518%	
5	0xf97b3a1175f7567885281f7a4e9c73628e3a677e	12,176,600.493998868	1.2209%	
6	0xe83173b2c5e54cca65c9306115218e8e10320146	10,770,356.567833981	1.0799%	
7	0x6b2a5dc3af28531d33dbc8d0d483498ae69f8547	10,089,424.908254211	1.0116%	
8	0xb8c97a6214a606f5cbdadf8baebfc3464e550ae9	9,809,151.832457206	0.9835%	
9	0x6ce50c6752c1461feef3cb92e209c794622372de	9,401,157.807814262	0.9426%	
10	0x8a99fe9092c02c7077d27abc9de4dab85bfd4059	8,285,201.266548698	0.8307%	

source:https://bscscan.com/

SECURITY ISSUES

Critical Severity Issues

No high severity issues found.

High Severity Issues

No high severity issues found.

Medium Severity Issues

No high severity issues found.

Low Severity Issues

1. No events on fees changes

   Changing fees should emit events so that could be easily tracked offchain.

   Recommendation: Please consider emitting events on changing fees.

   Fixed before the second review.

2. Unused state variable

   Contract MadhouseToken has a state variable **uniswapV2Router** which is never read in the code. Only writing is done in constructor and changeRouterVersion but it's never accessed for the reading which means it is just burning gas.

   Recommendation: Please consider removing the uniswapV2Router state variable.

   Fixed before the second review.

SECURITY ISSUES

3. Unused private method
   Contract MadhouseToken has a private method transferToAddressETH which is never called in the code.

   Recommendation: Please consider removing this method.

   Fixed before the second review.

4. Contracts that lock Ether
   Contract MadhouseToken has a payable function but without a withdrawal capacity.

   Recommendation: Remove the payable attribute or add a withdraw function.

   Fixed before the second review.

5. State variables that could be declared constant
   Constant state variables should be declared constant to save gas.

   Recommendation: Add the constant attributes to state variables that never change.

   Fixed before the second review.

6. Public functions that could be declared external
   public functions that are never called by the contract should be declared external to save gas.

   Recommendation: Use the external attribute for functions never called from the contract.

   Fixed before the second review.

SECURITY ASSESMENT

TOKEN LOGO

MOTECH AUDIT

SMART CONTRACT SECURITY AUDIT

SECURITY ASSESMENT

CONCLUSION

Smart contracts contain owner privileges!

Motech Audit 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.