



MOTECH AUDIT

SMART CONTRACT SECURITY AUDIT

SECURITY ASSESSMENT

MONSTERS CLAN TOKEN AUDIT REPORT

2021

12 NOV 2021

SECURITY ASSESMENT

TABLE OF CONTENTS

Summary	3
Disclaimer	4
Background	5
Audit Details	6
Contract Details	7
Monsters Clan Token Distribution	8
Monsters Clan Token Contract Interaction Details	8
Top 10 Token Holders	9
Security Issue	10
Token Logo	11
Conclusion	12



SECURITY ASSESMENT

SUMMARY

This report has been prepared for Monsters Clan to discover issues and vulnerabilities in the source code of the Monsters Clan 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 Testnet 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.



MOTECH AUDIT
SMART CONTRACT SECURITY AUDIT

SECURITY ASSESSMENT

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 ASSESSMENT

BACKGROUND

MotechAudit was commissioned by Monsters Clan to perform an audit of smart contracts:

<https://bscscan.com/address/0xe4c797d43631f4d660ec67b5cb0b78ef5c902532>

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.

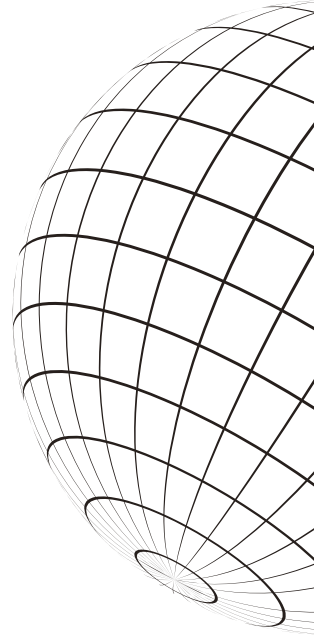
The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.



MOTECH AUDIT
SMART CONTRACT SECURITY AUDIT

SECURITY ASSESSMENT

AUDIT DETAILS



AUDITED PROJECT

Monsters Clan



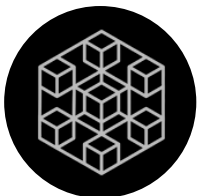
DEPLOYER ADDRESS

0x2C11b6f491b72BC4579b931D8CFc07BAAb6035deD



CLIENT CONTACTS:

Monsters Clan team



BLOCKCHAIN

Binance Smart Chain Project



WEBSITE:

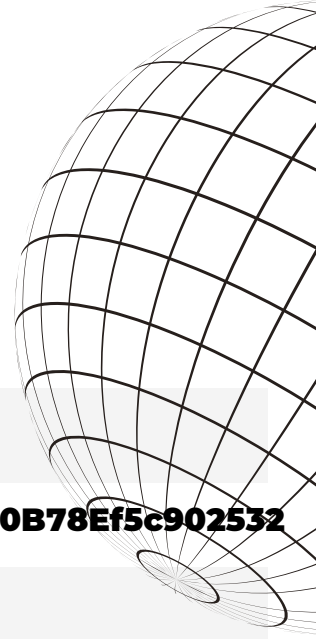
<http://www.monstersclan.com/>



SECURITY ASSESSMENT

CONTRACT DETAILS

Token contract details for Jul-27-2021



Contract name	Monsters Clan
Contract address	0xE4c797d43631F4d660EC67B5CB0B78Ef5c902532
Total supply	100,000,000 MONS
Token ticker	Monsters Clan Token (MONS)
Decimals	18
Token holders	7,209
Transactions count	136,463
Top 100 holders dominance	98.1079%
Contract deployer address	0x2C11b6f491b72BC4579b931D8CFc07BAAb6035deD
Contract's current owner address 0x2C11b6f491b72BC4579b931D8CFc07BAAb6035deD	

SECURITY ASSESSMENT

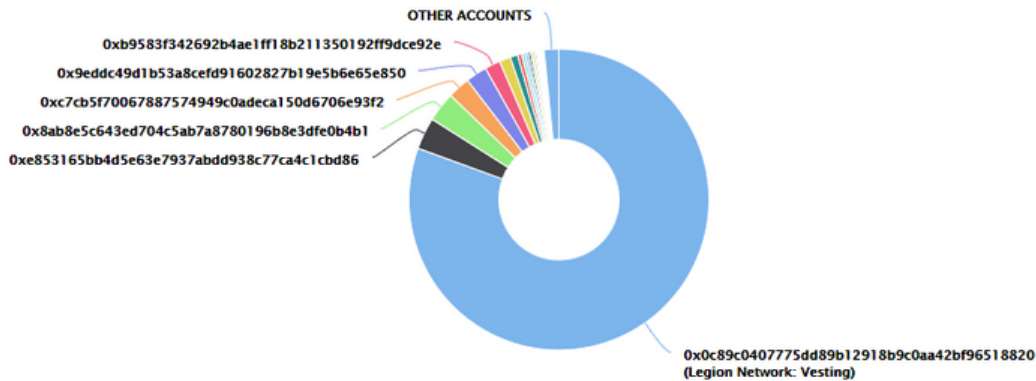
MONSTERS CLAN TOKEN DISTRIBUTION

The top 100 holders collectively own 98.41% (98,411,749.43 Tokens) of Monsters Clan Token

Token Total Supply: 100,000,000.00 Token | Total Token Holders: 7,209

Monsters Clan Token Top 100 Token Holders

Source: BscScan.com



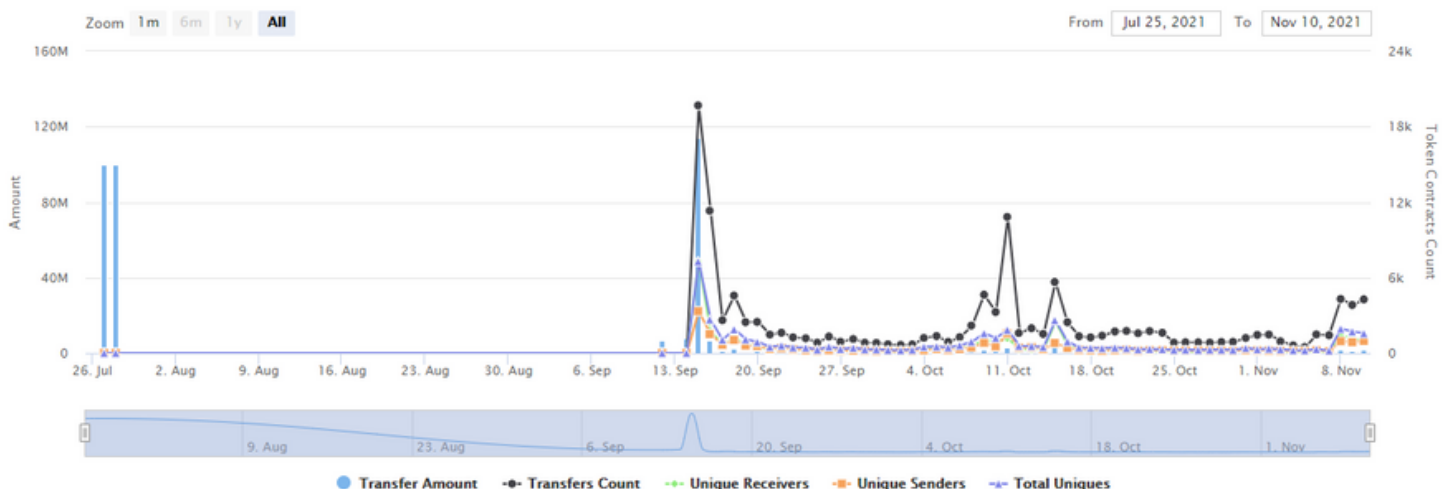
(A total of 98,411,749.43 tokens held by the top 100 accounts from the total supply of 100,000,000.00 token)

MONSTERS CLAN TOKEN CONTRACT INTERACTION DETAILS

Time Series: Token Contract Overview

Tue 27, Jul 2021 - Wed 10, Nov 2021













Token Contract 0xe4c797d43631f4d660ec67b5cb0b78ef5c902532 (Monsters Clan Token)
Source: BscScan.com



MOTECH AUDIT
SMART CONTRACT SECURITY AUDIT

SECURITY ASSESSMENT

TOP 10 TOKEN HOLDERS

Rank	Address	Quantity	Percentage	Analytics
1	 Legion Network: Vesting	80,550,000	80.5500%	
2	0xe853165bb4d5e63e7937abdd938c77ca4c1cbd86	3,417,272	3.4173%	
3	0x8ab8e5c643ed704c5ab7a8780196b8e3dfe0b4b1	3,193,650	3.1937%	
4	0xc7cb5f70067887574949c0adeca150d6706e93f2	2,410,512	2.4105%	
5	0x9eddc49d1b53a8cefd91602827b19e5b6e65e850	2,292,911	2.2929%	
6	0xb9583f342692b4ae1ff18b211350192ff9dce92e	1,671,049.24	1.6710%	
7	0x7e4d0a8ec32b57251d096df058881106074dd8cc	1,212,613	1.2126%	
8	0x22853a5d653ed285a4533e7f79dae7afb78cf937	799,138	0.7991%	
9	0xa7fa0e5638a25f15bcf0af7326cbb2201043dc4b	439,649.738533343204266	0.4396%	
10	 PancakeSwap V2: MONS-BUSD 2	398,690.396437340855080823	0.3987%	

source:<https://bscscan.com/>

SECURITY ASSESSMENT

SECURITY ISSUES

✓ High Severity Issues

No high severity issues found.

✓ Medium Severity Issues

No medium severity issues found.

Low Severity Issues

1. Possible incorrect pausable usage

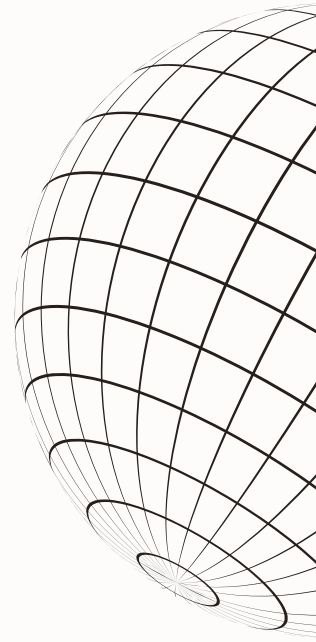
MonsterClanToken contract inherits ERC20Pausable contract but has no functions to pause/unpause the contract.

Recommendation: Please consider either removing ERC20Pausable or add pause/unpause functions and restrict the call by Timelock or DAO contract.



MOTECH AUDIT
SMART CONTRACT SECURITY AUDIT

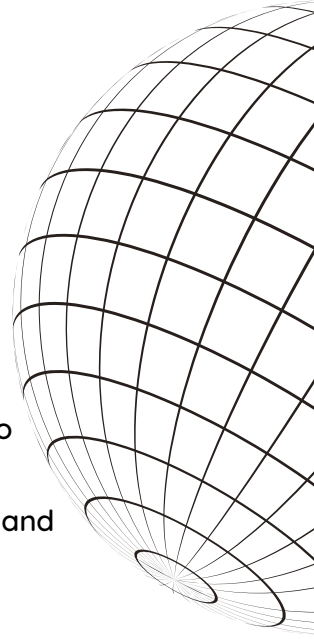
SECURITY ASSESMENT
TOKEN LOGO



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.



MOTECH AUDIT
SMART CONTRACT SECURITY AUDIT