SECURITY AUDIT OF

MAOBNB ERC20 TOKEN

Public Report

Sep 20, 2024

Verichains Lab

info@verichains.io

https://www.verichains.io

Driving Technology > Forward

ABBREVIATIONS

Name	Description
Ethereum	An open source platform based on blockchain technology to create and distribute smart contracts and decentralized applications.
Ether (ETH)	A cryptocurrency whose blockchain is generated by the Ethereum platform. Ether is used for payment of transactions and computing services in the Ethereum network.
Smart contract	A computer protocol intended to digitally facilitate, verify or enforce the negotiation or performance of a contract.
Solidity	A contract-oriented, high-level language for implementing smart contracts for the Ethereum platform.
Solc	A compiler for Solidity.
ERC20	ERC20 (BEP20 in Binance Smart Chain or *x*RP20 in other chains) tokens are blockchain-based assets that have value and can be sent and received. The primary difference with the primary coin is that instead of running on their own blockchain, ERC20 tokens are issued on a network that supports smart contracts such as Ethereum or Binance Smart Chain.

EXECUTIVE SUMMARY

This Security Audit Report was prepared by Verichains Lab on Sep 20, 2024. We would like to thank the MaoBNB for trusting Verichains Lab in auditing smart contracts. Delivering high-quality audits is always our top priority.

This audit focused on identifying security flaws in code and the design of the MaoBNB ERC20 Token. The scope of the audit is limited to the source code files provided to Verichains. Verichains Lab completed the assessment using manual, static, and dynamic analysis techniques.

During the audit process, the audit team had identified no vulnerable issues in the smart contracts code.

TABLE OF CONTENTS

1. MANAGEMENT SUMMARY

1.1. About MaoBNB ERC20 Token

MaoBNB ERC20 Token is a standard ERC20 token contract for Mao The Cat meme coin.

1.2. Audit scope

This audit focused on identifying security flaws in code and the design of the MaoBNB ERC20 Token that was deployed on BSC chain.

The latest version was made available in the course of the review:

FIELD	VALUE
Deployed Address	*https://bscscan.com/address/0xFd54E565e6de7509B07CDBa5769178045F212530*
Tx Deploy	*https://bscscan.com/tx/0x0afb79a93a4b31ecef34ebe0c95b08854012562d5819f078d3c18e4d830685d1*
Deployer	*https://bscscan.com/address/0xa0f26d7edf83dd033928d8c9e1ae7a9087058bf2*
Block Number	42131821

1.3. Audit methodology

Our security audit process for smart contract includes two steps:

- Smart contract codes are scanned/tested for commonly known and more specific vulnerabilities using public and RK87, our in-house smart contract security analysis tool.
- Manual audit of the codes for security issues. The contracts are manually analyzed to look for any potential problems.

Following is the list of commonly known vulnerabilities that were considered during the audit of the smart contract:

- Integer Overflow and Underflow
- Timestamp Dependence
- Race Conditions
- Transaction-Ordering Dependence
- DoS with (Unexpected) revert

- DoS with Block Gas Limit
- Gas Usage, Gas Limit and Loops
- Redundant fallback function
- Unsafe type Inference
- Reentrancy
- Explicit visibility of functions state variables (external, internal, private and public)
- Logic Flaws

For vulnerabilities, we categorize the findings into categories as listed in table below, depending on their severity level:

SEVERITY LEVEL	DESCRIPTION
CRITICAL	A vulnerability that can disrupt the contract functioning; creates a critical risk to the contract; required to be fixed immediately.
HIGH	A vulnerability that could affect the desired outcome of executing the contract with high impact; needs to be fixed with high priority.
MEDIUM	A vulnerability that could affect the desired outcome of executing the contract with medium impact in a specific scenario; needs to be fixed.
LOW	An issue that does not have a significant impact, can be considered as less important.

Table 1. Severity levels

1.4. Disclaimer

MaoBNB acknowledges that the security services provided by Verichains, are conducted to the best of their professional abilities but cannot guarantee 100% coverage of all security vulnerabilities. MaoBNB understands and accepts that despite rigorous auditing, certain vulnerabilities may remain undetected. Therefore, MaoBNB agrees that Verichains shall not be held responsible or liable, and shall not be charged for any hacking incidents that occur due to security vulnerabilities not identified during the audit process.

1.5. Acceptance Minute

This final report served by Verichains to the MaoBNB will be considered an Acceptance Minute. Within 7 days, if no any further responses or reports is received from the MaoBNB, the final report will be considered fully accepted by the MaoBNB without the signature.

2. AUDIT RESULT

2.1. Overview

The MaoBNB ERC20 Token was written in `Solidity` language, with the required version to be `^0.8.24`.

The contract makes use of the `OpenZeppelin` library's `ERC20` extension. Below is the contract's properties:

PROPERTY	VALUE
Name	MAO
Symbol	MAO
Decimals	18
Total Supply	1,000,000,000x10^{18} (It represents 1 billion tokens pre-minted to the contract deployer)

Table 2. The MaoBNB ERC20 Token properties

2.2. Findings

During the audit process, the audit team found no vulnerability in the given version of MaoBNB ERC20 Token.

3. VERSION HISTORY

Version	Date	Status/Change	Created by
1.0	*Sep 20, 2024*	Public Report	Verichains Lab

Table 3. Report versions history