DEFENCERT
BLOCKCHAIN SECURITY

Maru Neko

20 Feb 2022

Smart Contract Audit Report

www.defencert.com

Table of Contents

Contents

Disclaimer

Defencert Blockchain Security (“Defencert”) has conducted an independent audit to verify the integrity of and highlight any vulnerabilities or errors, intentional or unintentional, that may be present in the codes that were provided for the scope of this audit. This audit report does not constitute agreement, acceptance, or advocation for the Project that was audited, and users relying on this audit report should not consider this as having any merit for financial advice in any shape, form, or nature. The contracts audited do not account for any economic developments that may be pursued by the Project in question, and that the veracity of the findings thus presented in this report relate solely to the proficiency, competence, aptitude and discretion of our independent auditors, who make no guarantees nor assurance that the contracts are completely free of exploits, bugs, vulnerabilities or deprecation of technologies. Further, this audit report shall not be disclosed nor transmitted to any persons or parties on any objective, goal, or justification without due written assent, acquiescence, or approval by Defencert.

All information provided in this report does not constitute financial or investment advice, nor should it be used to signal that any persons reading this report should invest their funds without sufficient individual due diligence regardless of the findings presented in this report. Information is provided ‘as is’, and Defencert is under no covenant to the completeness, accuracy, or solidity of the contracts audited. In no event will Defencert or its partners, employees, agents, or parties related to the provision of this audit report be liable to any parties for, or lack thereof, decisions and/or actions with regards to the information provided in this audit report.

Cryptocurrencies and any technologies by extension directly or indirectly related to cryptocurrencies are highly volatile and speculative by nature. All reasonable due diligence and safeguards may yet be insufficient, and users should exercise considerable caution when participating in any shape or form in this nascent industry.

The audit report has made all reasonable attempts to provide clear and articulate recommendations to the Project team with respect to the rectification, amendment, and/or revision of any highlighted issues, vulnerabilities, or exploits within the contracts provided. It is the sole responsibility of the Project team to sufficiently test and performs checks, ensuring that the contracts are functioning as intended, specifically that the functions therein contained within said contracts have the desired intended effects, functionalities, and outcomes of the Project team.

1. Overview

This report has been prepared for Maru Neko on the Binance Smart Chain network. Defencert provides a user-centered examination of the smart contracts to look for vulnerabilities, logic errors, or other issues from both an internal and external perspective.

1.1 Summary

Project Name	Maru Neko
URL	maruneko.org
Platform	Binance Smart Chain
Language	Solidity

Contracts Assessed

Name	Contract	Live Code Match
MARU	0x1134310dcf17071f461e7c7b68f1916b678f0357	Yes

1.2 Findings Summary

Severity	Found	Resolved	Partially Resolved	Acknowledged
High	0	0	0	0
Medium	0	0	0	0
Low	2	0	0	2
Informational	0	0	0	0
Total	2	0	0	2

Severity	Description
High	Exploits, vulnerabilities or errors that will certainly or probabilistically lead towards loss of funds, control, or impairment of the contract and its functions. Issues under this classification are recommended to be fixed with utmost urgency.
Medium	Bugs or issues with that may be subject to exploit, though their impact is somewhat limited. Issues under this classification are recommended to be fixed as soon as possible.
Low	Effects are minimal in isolation and do not pose a significant danger to the project or its users. Issues under this classification are recommended to be fixed nonetheless.
Informational	Consistency, syntax or style best practices. Generally, pose a negligible level of risk, if any.

1.3 MARU

ID	Severity	Summary	Status
01	Low	A floating pragma is set.	Acknowledged
02	Low	State variable visibility is not set.	Acknowledged

2 Findings

2.1 MARU

Maru Neko (MARU) is a BEP20 Token in Binance Smart Chain Mainnet. Token is implemented as BEP20 smart contract. This token has a 10% of transaction tax which consist of 6% reflection, 3% burn and 1% marketing fee.

2.1.1 Token Overview

Address	0x1134310dcf17071f461e7c7b68f1916b678f0357
Token Supply	1,000,000,000,000,000
Decimal	18
Transfer Max Size	-
Transfer Min Size	-
Transfer Fees	10%

2.1.2 Privileged Roles

The following functions can be called by the owner of the contract:

a) Include/Exclude from rewards

b) Set fees

c) Set marketing address

d) Transfer/renounce ownership

e) Withdraw any token and BNB balance in the token contract.

2.1.3 Issues & Recommendations

Issue #01	A floating pragma is set.
Severity	Low
Line	883
Description	The current pragma Solidity directive is ""^0.8.0"". It is recommended to specify a fixed compiler version to ensure that the bytecode produced does not vary between builds. This is especially important if you rely on bytecode-level verification of the code.
Recommendation & Resolution	Consider to set solidity version to a fix variable. Change the current pragma to “0.8.0”.
Status	Acknowledged

Issue #02	State variable visibility is not set.
Severity	Low
Line	927
Description	It is best practice to set the visibility of state variables explicitly. The default visibility for "inSwap" is internal. Other possible visibility settings are public and private.
Recommendation & Resolution	Consider to set inSwap visibility to public. Change inSwap visibility to public.
Status	Acknowledged


DEFENCERT
BLOCKCHAIN SECURITY