CRACKEN

Smart Contract Security Audit

Project: MARIO INU

Apr 07, 2023

Contract Address

0x7b799e105b3152a3dc6ced8a9dd8dcb19f051fc8

Table of Contents

Disclaimer

The contents of this report reflect only the CRACKEN TECH audit team's understanding of the current progress and status of the security of the code audited, to verify the integrity of the code provided for the scope of this audit. You agree that your access and/or use, including but not limited to any associated services, products, protocols, platforms, content, and materials, will be at your sole risk. Given the size of the project, the findings detailed here are not to be considered exhaustive, and further testing and audit are recommended after the issues covered are fixed. We do not warrant, endorse, guarantee, or assume responsibility for any product or service advertised or offered by a third party through the product, any open source or third-party software, code, libraries, materials, or information linked to, called by, referenced by or accessible through the report, its content, and the related services and products, any hyperlinked websites, any websites or mobile applications appearing on any advertising, and we will not be a party to or in any way be responsible for monitoring any transaction between you and any third-party providers of products or services.

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.

The review does not address the compiler layer, any other areas beyond the programming language, or other programming aspects that could present security risks. If the audited source files are smart contract files, risks or issues introduced by using data feeds from off-chain sources are not extended by this review either.

Audit Review

The source code of the Mario Inu was audited in order to acquire a clear impression of how the project was implemented. The Cracken Tech audit team conducted in-depth research, analysis, and scrutiny, resulting in a series of observations. A detailed list of each issue found, and vulnerabilities in the source code will be included in the audit report. The problems and potential solutions are given in this report, we will identify common sources for such problems and comments for improvement.

The auditing process will follow a routine as special considerations by Cracken:

- Review of the specifications, sources, and instructions provided to Cracken to make sure the contract logic meets the intentions of the client without exposing the user's funds to risk.
- Manual review of the entire codebase by our experts, which is the process of reading source code line-by-line in an attempt to identify potential vulnerabilities.
- Specification comparison is the process of checking whether the code does what the specifications, sources, and instructions provided to Cracken describe.
- Test coverage analysis determines whether the test cases are covering the code and how much code is exercised when we run the test cases.
- Symbolic execution is analyzing a program to determine what inputs cause each part of a program to execute.
- Reviewing the codebase to improve maintainability, security, and control based on the established industry and academic practices.

Project Review

Token Summary

Parameter	Result
Token Name	**MARIOINU**
Token Symbol	MARIOINU
Token Decimal	9
Total Supply	420,000,000,000,000,000
Platform	BSC
Buy Tax Fee	10%
Sell Tax Fee	10%
Contract Creation Date	Apr 05, 2022
Liquidity Status	Locked for a month
Compiler Version	v0.8.17+commit.8df45f5f
Optimization	Yes with 200 runs
Contract Address	0x7b799e105b3152a3dc6ced8a9dd8dcb19f051fc8
Deployer Address	0x0d549196f42bcAf8EEb717c44987f5FEFE95BA18
Owner Address	0x0000000000000000000000000000000000000000

Source Code

CRACKEN was commissioned by Mario Inu to perform an audit based on the following smart contract:

https://bscscan.com/address/0x7B799E105B3152A3dc6cEd8a9dd8DCB19f051Fc8

Smart Contract Vulnerability Checks

Vulnerability	Auto-Scan	Manual-Scan	Result
Unencrypted Private Data On-Chain	Complete	Complete	Low / No Risk
Code With No Effects	Complete	Complete	Low / No Risk
Message call with hardcoded gas amount	Complete	Complete	Low / No Risk
Hash Collisions with Multiple Variable Length Arguments	Complete	Complete	Low / No Risk
Unexpected Ether balance	Complete	Complete	Low / No Risk
Presence of unused variables	Complete	Complete	Low / No Risk
Right-To-Left-Override control character (U+202E)	Complete	Complete	Low / No Risk
Typographical Error	Complete	Complete	Low / No Risk
DoS With Block Gas Limit	Complete	Complete	Low / No Risk
Arbitrary Jump with Function Type Variable	Complete	Complete	Low / No Risk
Insufficient Gas Grieving	Complete	Complete	Low / No Risk
Incorrect Inheritance Order	Complete	Complete	Low / No Risk
Write to Arbitrary Storage Location	Complete	Complete	Low / No Risk
Requirement Violation	Complete	Complete	Low / No Risk
Missing Protection against Signature Replay Attacks	Complete	Complete	Low / No Risk
Weak Sources of Randomness from Chain Attributes	Complete	Complete	Low / No Risk
Authorization through tx. origin	Complete	Complete	Low / No Risk
Delegate call to Untrusted Callee	Complete	Complete	Low / No Risk

Vulnerability	Auto-Scan	Manual-Scan	Result
Use of Deprecated Solidity Functions	Complete	Complete	Low / No Risk
Assert Violation	Complete	Complete	Low / No Risk
Reentrancy	Complete	Complete	Low / No Risk
Unprotected SELF-DESTRUCT Instruction	Complete	Complete	Low / No Risk
Unprotected Ether Withdrawal	Complete	Complete	Low / No Risk
Outdated Compiler Version	Complete	Complete	Low / No Risk
Integer Overflow and Underflow	Complete	Complete	Low / No Risk
Function Default Visibility	Complete	Complete	Low / No Risk

Manual Code Review

Classification of Issues

Severity	Description
High-Risk	A vulnerability that affects the desired outcome when using a contract, or provides the opportunity to use a contract in an unintended way.
Medium-Risk	A vulnerability that could affect the desired outcome of executing the contract in a specific scenario.
Low-Risk	A vulnerability that does not have a significant impact on possible scenarios for the use of the contract and is probably subjective.
Informational	A vulnerability that has an informational character but is not affecting any of the code.

Findings

Severity	Found
High-Risk	0
Medium-Risk	3
Low-Risk	0
Informational	0
Total	3

🟠 **Medium-Risk: functions make cause a few bugs of the project. Should be fixed.**

Set blacklist users

Description:

The owner can set blacklist users

[Medium-RISK] [Ownership Renounced]

```
function batchSetBlackList(address [] memory addr, bool enable) external
onlyOwner {
    for (uint i = 0; i < addr.length; i++) {
        _blackList[addr[i]] = enable;
    }
```

Recommendation:

We recommend that the owner should disable the blacklist function.

🟠 **Medium-Risk: functions make cause a few bugs of the project. Should be fixed.**

Set max buy / sell tax fee

Description:

The owner can set the buy & sell fees up to 100%

[Medium-Risk] [Ownership Renounced]

```
function setBuyFundFee(uint256 fundFee) external onlyOwner {
        _buyFundFee = fundFee;
}

function setSellFundFee(uint256 fundFee) external onlyOwner {
        _sellFundFee = fundFee;
}
```

🟠 **Medium-Risk: functions make cause a few bugs of the project. Should be fixed.**

Set trading function is enabled

Description:

The owner can set close trading

[Medium-Risk] [Ownership Renounced]

```
function closeTrade() external onlyOwner {

    startTradeBlock = 0;

}
```

Privileged Functions

onlyOwner

Function Name	Parameters	Visibility
approve	address spender, uint256 amount	public
batchSetBlackList	address [] memory addr, bool enable	external
claimBalance	none	external
claimToken	address token, uint256 amount, address to	external
closeTrade	none	external
renounceOwnership	none	public
setBlackList	address [] memory addr, bool enable	external
setBuyFundFee	uint256 fundFee	external
setExcludeHolder	address addr, bool enable	external
setFeeWhiteList	address addr, bool enable	external
setFundAddress	address addr	external
setLimitAmount	uint256 amount	public
setSellFundFee	uint256 fundFee	external
setSwapPairList	address addr, bool enable	external
setbb	uint16 _bb	external
startTrade	none	external
transfer	address recipient, uint256 amount	public
transferFrom	address sender, address recipient, uint256 amount	external
transferOwnership	address newOwner	public

Contract Ownership

The contract ownership of Mario Inu is currently being renounced. The ownership of the contract grants special powers to the protocol creators, making them the sole addresses that can call sensible ownable functions that may alter the state of the protocol.

The current owner is the address 0x0000000000000000000000000000000000000000 which can be viewed: HERE

The owner wallet has the power to call the functions displayed on the privileged functions list above, if the owner wallet is compromised these privileges could be exploited.

We recommend the team renounce ownership at the right time if possible, or gradually migrate to a time lock with governing functionalities in respect of transparency and safety considerations.

Liquidity Overview

Liquidity Information

Parameter	Result
Pair Address	0xe259b0cd4dcbd3351ebc59b883d59c70474c7371
MARIOINU Reserves	100,783,114.06B MARIOINU
WBNB Reserves	20.16 WBNB
Liquidity Value	$12.49K USDT
Liquidity Ownership	The token does not have liquidity at the moment of the audit

Tokenomics

Rank	Address	Quantity (Token)	Percentage
1	PancakeSwap V2: MARIOINU 5	100,881,696,774,571,646.36284546	24.0195%
2	0x84690bcf6ddc82d5fa0460f5bfb89bd0c182b476	9,940,308,532,758,493.766551099	2.3667%
3	0xc5a0db034e4870c7fc61d599fdce730ee2fd7987	9,698,231,572,125,199.590294971	2.3091%
4	0xce37276258a78feedcd8a2e7137ca4892119f513	9,619,171,489,414,007.571390148	2.2903%
5	0xbe0f9c199a340bf7dc0aeea799352b13f54ed226	9,298,164,078,670,617.102800113	2.2138%

Social Media Check

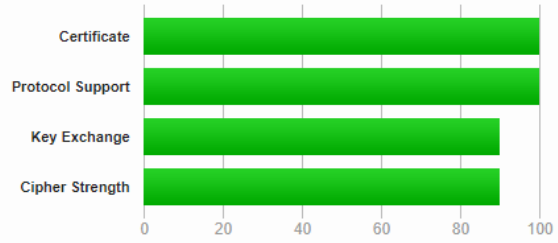
Social Media Type	Link	Result
Website	https://www.marioinu.online/	Checked
Twitter	https://twitter.com/Mario_inuMeme	Checked
Telegram	https://t.me/MarioInuMeme	Checked

Website Review

Summary

Overall Rating

A



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This site works only in browsers with SNI support.

This server supports TLS 1.3.

Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	www.marioinu.online Fingerprint SHA256: 403ce4bfc6f0c5c8dcbd876bbf070f93bac574994183ac372e0520e6d4d020d6 Pin SHA256: Buc05gisIpVndNKO11jNp3dmSTQCBlg60ZvinTKvCpc=
Common names	www.marioinu.online
Alternative names	www.marioinu.online marioinu.online
Serial Number	00bdfb7d1286f9a82114dbb08e6c7940df
Valid from	Thu, 06 Apr 2023 00:00:00 UTC
Valid until	Fri, 05 Apr 2024 23:59:59 UTC (expires in 11 months and 29 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	Sectigo RSA Domain Validation Secure Server CA AIA: http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	OCSP OCSP: http://ocsp.sectigo.com
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows

- Mobile Friendly
- Contains no code errors
- SSL is secured
- No spelling errors

Audit Conclusion

- **The owner can pause trading [Medium-Risk] [Ownership Renounced]**
- The owner cannot mint new tokens
- **The owner can blacklist users [Medium-Risk] [Ownership Renounced]**
- The owner cannot change the max tx amount
- **The owner can change buy/sell fees up to 100%[Medium-Risk] [Ownership Renounced]**
- The owner can set whitelist wallets.

(No functions can be used due to the ownership is renounced)

AUDIT IS PASSED