Cyberscope

# Audit Report

# Monkey Shit Inu

June 2024

Network ETH

Address 0x2Be8e422cb4A5A7f217a8F1b0658952a79132F28

Audited by © cyberscope

# Analysis

Critical Medium Minor / Informative Pass

| Severity | Code | Description | Status |
|---|---|---|---|
| ● | ST | Stops Transactions | Passed |
| ● | OTUT | Transfers User's Tokens | Passed |
| ● | ELFM | Exceeds Fees Limit | Passed |
| ● | MT | Mints Tokens | Passed |
| ● | BT | Burns Tokens | Passed |
| ● | BC | Blacklists Addresses | Passed |

# Diagnostics

Critical Medium Minor / Informative

| Severity | Code | Description | Status |
|---|---|---|---|
| ● | MEE | Missing Events Emission | Unresolved |
| ● | L19 | Stable Compiler Version | Unresolved |

# Table of Contents

# Review

| | |
|---|---|
| **Contract Name** | MSIToken |
| **Compiler Version** | v0.8.23+commit.f704f362 |
| **Optimization** | 200 runs |
| **Explorer** | https://etherscan.io/address/0x2be8e422cb4a5a7f217a8f1b0658952a79132f28 |
| **Address** | 0x2Be8e422cb4A5A7f217a8F1b0658952a79132F28 |
| **Network** | ETH |
| **Symbol** | $MSI |
| **Decimals** | 18 |
| **Total Supply** | 3,000,000,000,000 |
| **Badge Eligibility** | Yes |

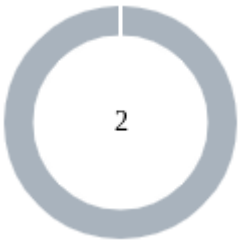
## Audit Updates

| | |
|---|---|
| **Initial Audit** | 14 Jun 2024 |

## Source Files

| **Filename** | SHA256 |
|---|---|
| **contracts/errors.sol** | cc3c970d7d5833744d978712c28c3e39a95aafa0124992e4945113665359a810 |
| **contracts/MSIToken.sol** | 9431bf9ee3b29b62b76fea2b8cc1524b7179abbc22df2015f36ac16143b99b50 |

# Findings Breakdown




| | |
|---|---|
| Critical | 0 |
| Medium | 0 |
| Minor / Informative | 2 |

| Severity | Unresolved | Acknowledged | Resolved | Other |
|---|---|---|---|---|
| Critical | 0 | 0 | 0 | 0 |
| Medium | 0 | 0 | 0 | 0 |
| Minor / Informative | 2 | 0 | 0 | 0 |

# MEE - Missing Events Emission

| | |
|---|---|
| **Criticality** | Minor / Informative |
| **Location** | contracts/MSIToken.sol#L125 |
| **Status** | Unresolved |

## Description

The contract performs actions and state mutations from external methods that do not result in the emission of events. Emitting events for significant actions is important as it allows external parties, such as wallets or dApps, to track and monitor the activity on the contract. Without these events, it may be difficult for external parties to accurately determine the current state of the contract.

```
    function changeTaxWallet(address newTaxWallet) external
onlyOwner isZeroAddress(newTaxWallet) {
        taxWallet = newTaxWallet;
    }
```

## Recommendation

It is recommended to include events in the code that are triggered each time a significant action is taking place within the contract. These events should include relevant details such as the user's address and the nature of the action taken. By doing so, the contract will be more transparent and easily auditable by external parties. It will also help prevent potential issues or disputes that may arise in the future.

## L19 - Stable Compiler Version

| | |
|---|---|
| **Criticality** | Minor / Informative |
| **Location** | contracts/MSIToken.sol#L2 |
| **Status** | Unresolved |

### Description

The `^` symbol indicates that any version of Solidity that is compatible with the specified version (i.e., any version that is a higher minor or patch version) can be used to compile the contract. The version lock is a mechanism that allows the author to specify a minimum version of the Solidity compiler that must be used to compile the contract code. This is useful because it ensures that the contract will be compiled using a version of the compiler that is known to be compatible with the code.

```
pragma solidity ^0.8.23;
```

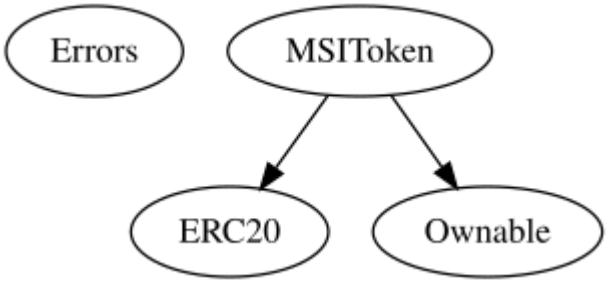
### Recommendation

The team is advised to lock the pragma to ensure the stability of the codebase. The locked pragma version ensures that the contract will not be deployed with an unexpected version. An unexpected version may produce vulnerabilities and undiscovered bugs. The compiler should be configured to the lowest version that provides all the required functionality for the codebase. As a result, the project will be compiled in a well-tested LTS (Long Term Support) environment.

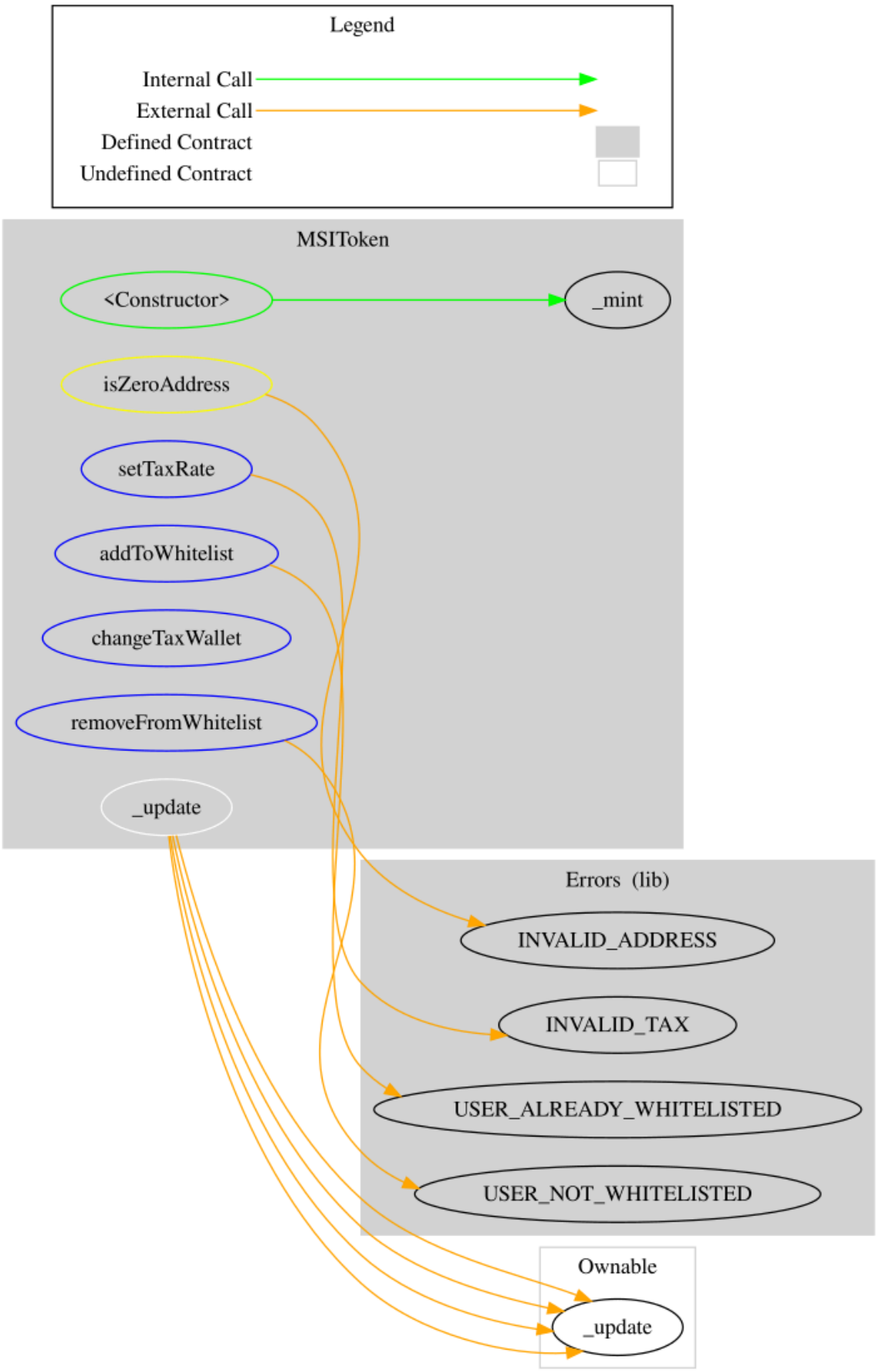
# Functions Analysis

| Contract | Type | Bases | | |
|---|---|---|---|---|
| | **Function Name** | **Visibility** | **Mutability** | **Modifiers** |
| | | | | |
| **MSIToken** | Implementation | ERC20, Ownable | | |
| | | Public | ✓ | isZeroAddress isZeroAddress ERC20 Ownable |
| | _update | Internal | ✓ | |
| | setTaxRate | External | ✓ | onlyOwner |
| | changeTaxWallet | External | ✓ | onlyOwner isZeroAddress |
| | addToWhitelist | External | ✓ | onlyOwner isZeroAddress |
| | removeFromWhitelist | External | ✓ | onlyOwner isZeroAddress |

# Inheritance Graph



# Flow Graph


Legend
Internal Call
External Call
Defined Contract
Undefined Contract
MSIToken
<Constructor>
_mint
isZeroAddress
setTaxRate
addToWhitelist
changeTaxWallet
removeFromWhitelist
_update
Errors (lib)
INVALID_ADDRESS
INVALID_TAX
USER_ALREADY_WHITELISTED
USER_NOT_WHITELISTED
Ownable
_update

# Summary

Monkey Shit Inu contract implements a token mechanism. This audit investigates security issues, business logic concerns and potential improvements. Monkey Shit Inu is an interesting project that has a friendly and growing community. The Smart Contract analysis reported no compiler error or critical issues. The contract Owner can access some admin functions that can not be used in a malicious way to disturb the users' transactions. There is also a limit of max 10% fees.

# Disclaimer

The information provided in this report does not constitute investment, financial or trading advice and you should not treat any of the document's content as such. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes nor may copies be delivered to any other person other than the Company without Cyberscope's prior written consent. This report is not nor should be considered an "endorsement" or "disapproval" of any particular project or team. This report is not nor should be regarded as an indication of the economics or value of any "product" or "asset" created by any team or project that contracts Cyberscope to perform a security assessment. This document does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors' business, business model or legal compliance. This report should not be used in any way to make decisions around investment or involvement with any particular project. This report represents an extensive assessment process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk Cyberscope's position is that each company and individual are responsible for their own due diligence and continuous security Cyberscope's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies and in no way claims any guarantee of security or functionality of the technology we agree to analyze. The assessment services provided by Cyberscope are subject to dependencies and are under continuing development. You agree that your access and/or use including but not limited to any services reports and materials will be at your sole risk on an as-is where-is and as-available basis Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives false negatives and other unpredictable results. The services may access and depend upon multiple layers of third parties.

# About Cyberscope

Cyberscope is a blockchain cybersecurity company that was founded with the vision to make web3.0 a safer place for investors and developers. Since its launch, it has worked with thousands of projects and is estimated to have secured tens of millions of investors' funds.

Cyberscope is one of the leading smart contract audit firms in the crypto space and has built a high-profile network of clients and partners.

**The Cyberscope team**

https://www.cyberscope.io