SLOWMIST

Smart Contract
Security Audit Report

The SlowMist Security Team received the team's application for smart contract security audit of the TRALA OG NFT(TON) on 2024.03.08. The following are the details and results of this smart contract security audit:

Token Name :

TRALA OG NFT(TON)

File name and hash (SHA256) :

ERC721vTrala2.zip: 4113066a4b6d3f8f09b1ecf4cac394b214baa48ea63b072cede4f3f697fbd6fe

The audit items and results :

(Other unknown security vulnerabilities are not included in the audit responsibility scope)

NO.	Audit Items	Result
1	Replay Vulnerability	Passed
2	Denial of Service Vulnerability	Passed
3	Race Conditions Vulnerability	Passed
4	Authority Control Vulnerability Audit	Passed
5	Integer Overflow and Underflow Vulnerability	Passed
6	Gas Optimization Audit	Passed
7	Design Logic Audit	Passed
8	Uninitialized Storage Pointers Vulnerability	Passed
9	Arithmetic Accuracy Deviation Vulnerability	Passed
10	"False top-up" Vulnerability	Passed
11	Malicious Event Log Audit	Passed
12	Scoping and Declarations Audit	Passed
13	Safety Design Audit	Passed
14	Non-privacy/Non-dark Coin Audit	Passed

Audit Result : Passed

Audit Number : 0X002403110002

Audit Date : 2024.03.08 - 2024.03.11

Audit Team : SlowMist Security Team

Summary conclusion : This is an ERC721 Token contract and does not contain the dark coin section. The total amount of NFT remains unchangeable. The contract does not have the Overflow and the Race Conditions issue. During the audit, we found the following information:

1. Only the owner role can call the safeMultiMint function and the max total amount of the NFT is 2222.
2. Only the owner role can call the setTokenURI function to modify the _tokenURI.

The source code:

```
// SPDX-License-Identifier: MIT
//SlowMist// The contract does not have the Overflow and the Race Conditions issue
pragma solidity 0.8.20;

import "@openzeppelin/contracts/token/ERC721/extensions/ERC721URIStorage.sol";
import "@openzeppelin/contracts/access/Ownable.sol";
import "@openzeppelin/contracts/utils/Counters.sol";

contract TralaOgNft is ERC721URIStorage, Ownable {
    uint256 private _maxTokenId;
    string private _tokenURI;

    using Counters for Counters.Counter;
    Counters.Counter private _tokenIdCounter;
    event SetTokenURI(string preURI, string setURI);

    constructor(
        string memory tokenURI,
        address initialOwner
    ) ERC721("TRALA OG NFT", "TON") Ownable(initialOwner) {
        _maxTokenId = 2222;
        _tokenURI = tokenURI;
    }
    //SlowMist// Only the owner can mint NFT
    function safeMultiMint(uint count) public onlyOwner {
        uint256 tokenId;
        for (uint i = 0; i < count; i++) {
            _tokenIdCounter.increment();
            tokenId = _tokenIdCounter.current();
            require(tokenId <= _maxTokenId, "Minting is over");
            _safeMint(msg.sender, tokenId);
            _setTokenURI(tokenId, _tokenURI);
        }
    }
    //SlowMist// The owner role can change the _tokenURI
    function setTokenURI(string memory tokenURI) public onlyOwner {
        string memory preURI = _tokenURI;
        _tokenURI = tokenURI;
        emit SetTokenURI(preURI, _tokenURI);
    }
}
```

Statement

SlowMist issues this report with reference to the facts that have occurred or existed before the issuance of this report, and only assumes corresponding responsibility based on these.

For the facts that occurred or existed after the issuance, SlowMist is not able to judge the security status of this project, and is not responsible for them. The security audit analysis and other contents of this report are based on the documents and materials provided to SlowMist by the information provider till the date of the insurance report (referred to as "provided information"). SlowMist assumes: The information provided is not missing, tampered with, deleted or concealed. If the information provided is missing, tampered with, deleted, concealed, or inconsistent with the actual situation, the SlowMist shall not be liable for any loss or adverse effect resulting therefrom. SlowMist only conducts the agreed security audit on the security situation of the project and issues this report. SlowMist is not responsible for the background and other conditions of the project.

SLOWMIST

Official Website

www.slowmist.com

✉

E-mail

team@slowmist.com

Twitter

@SlowMist_Team

Github

https://github.com/slowmist