



Byte Detective

Smart Contract Audit & Blockchain Development

<https://bytedetective.tech>

Types of Severities

High

A high severity issue or vulnerability means that your smart contract can be exploited. Issues on this level are critical to the smart contract's performance or functionality, and we recommend these issues be fixed before moving to a live environment.

Medium

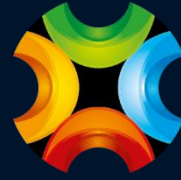
The issues marked as medium severity usually arise because of errors and deficiencies in the smart contract code. Issues on this level could potentially bring problems, and they should still be fixed.

Low

Low-level severity issues can cause minor impact and or are just warnings that can remain unfixed for now. It would be better to fix these issues at some point in the future.

PROJECT NAME: **LOTTOOperator**

OFFICIAL LOGO:



Team Doxed: **Yes**

WEBSITE: <https://www.cryptolotterynt.com>

Checked Vulnerabilities

- | | |
|----------------------------|-------------------------------|
| ✓ Reentrancy | ✓ ERC20 API violation |
| ✓ Timestamp Dependence | ✓ Malicious libraries |
| ✓ Gas Limit and Loops | ✓ Old Compiler version |
| ✓ DoS with Block Gas Limit | ✓ Redundant fallback function |
| ✓ Transaction-Ordering | ✓ Backdoors & Hidden Address |
| ✓ Use of tx.origin | ✓ Style guide violation |
| ✓ Exception disorder | ✓ Unchecked external call |

Contract Audit: 0x81Eb8246FC4c0aBb6aB38DeD5E10F02Cf8F7b25D

Can Set Fees

Safe

Can Mint

Safe

Can Burn

Safe

Can Blacklist

Safe

Can Blacklist Massively

Safe

Can Whitelist

Safe

Can Cooldown Transfers

Safe

Can Pause Transfers

Safe

Can change max tx amount

No

LOTTOOperator.sol Smart Contract Report

Summary:

The smart contract appears to be a basic implementation of an ERC-20 token with additional functionality to burn tokens and change ownership. It inherits from the OpenZeppelin contracts, which is generally a good practice for security.

Positive Aspects:

1. Inheritance from Standard Interfaces: The contract correctly inherits from the IERC20 interface and Ownable from the OpenZeppelin library. This ensures compatibility with other ERC-20 tokens and provides basic access control.

2. SafeMath Usage: SafeMath is used to prevent overflows and underflows, which is a good security practice.

Potential Issues:

No issues found!

Smart Contract is Safe!

- Free of Backdoors
- No Malicious Code
- Owner Manipulation Prevention
- Transparent and Secure

Associate links :

- <https://t.me/CryptoguaridaOficial>
- <https://metamask.io/>
- <https://twitter.com/Manuel36677856>
- <https://twitter.com/CRYPTOLottery91>
- <https://discord.gg/jfbFbXvg>
- https://www.tiktok.com/@cryptolottery_nft?is_from_webapp=1&sender_device=pc
- <https://discord.gg/9ZFgHzBh>
- <https://www.youtube.com/channel/UCA8ZpKwypoN67hGX0upUIEg>
- <https://www.genesys.network/>
- https://t.me/cryptolottery_nft



THANK YOU!

10/17/2023