OXSCANS

Project Address

0xDF3D893BE686731D606B503D8BD904F15EE090c4

01/27/2024

OXSCANS

AUDIT REPORT

SAFETY SCORE: 85

1 - Arbitrary Jump/Storage Write

Result: Pass

2 - Centralization of Control

Result: Medium

Details: The contract has an onlyOwner modifier which centralizes control over certain functions such as launch, pause, removeLimits, updateSwapTokensAtAmount, updateMaxTxnAmount, updateMaxWalletAmount, excludeFromMaxTransaction, updateSwapEnabled, updateBuyFees, updateSellFees, excludeFromFees, setAutomatedMarketMakerPair, updateMarketingWallet, addSniperInList, removeSniperFromList, airdrop, withdrawETH, and withdrawToken. This level of control by a single address can pose a risk to the protocol's decentralization and trust.

3 - Compiler Issues

Result: Pass

4 - Delegate Call to Untrusted Contract

Result: Pass

5 - Dependence on Predictable Variables

Result: Pass

6 - Ether/Token Theft

Result: Pass

7 - Flash Loans

Result: Pass

8 - Front Running

Result: Medium

Details: The contract does not appear to have specific mechanisms to prevent front-running attacks, especially in the swapBack function where the outcome of transactions can be predicted and exploited by miners or bots.

OXSCANS

9 - Improper Events

Result: Pass

10 - Improper Authorization Scheme

Result: Pass

11 - Integer Over/Underflow

Result: Pass

Details: The contract uses SafeMath library for all arithmetic operations, which prevents integer overflows and underflows.

12 - Logical Issues

Result: Medium

Details: The contract has a function swapBack that is called within the _transfer function. This can lead to a scenario where the swapBack function fails (due to gas price fluctuations or other issues), causing all transfers to fail as well. This can be improved by decoupling the swap logic from the transfer logic.

13 - Oracle Issues

Result: Pass

14 - Outdated Compiler Version

Result: Pass

15 - Race Conditions

Result: Pass

16 - Reentrancy

Result: Pass

17 - Signature Issues

Result: Pass

18 - Sybil Attack

Result: Pass

19 - Unbounded Loops

Result: Pass

20 - Unused Code

Result: Low

Details: The contract includes the pragma experimental ABIEncoderV2 directive, which is no longer necessary as of Solidity 0.8.0 since the ABI coder v2 is activated by default.

Code:
pragma experimental ABIEncoderV2;
Correction:
// Removed as it's no longer needed in Solidity 0.8.0 and above

LEGAL DISCLAIMER

Oxscans operates as an automated system for smart contract due diligence, acknowledging the possibility of bugs or vulnerabilities impacting token values. We do not hold specific obligations regarding your trading outcomes or the utilization of audit content. Users release Oxscans from any liability associated with content obtained through the tool.

AI GENERATED BY OXSCANS AI TECHNOLOGY

chat with us

Telegram

For more information. Visit below:

Twitter

Github

OXSCANS