OXSCANS

Project: Sourceblock

0x3eb85285ebc46780a8798149d271633210e61bad

05/05/2024

AUDIT REPORT

SAFETY SCORE: 85

1 - Arbitrary Jump/Storage Write

Result: Pass

2 - Centralization of Control

Result: Medium

Details: The contract has a function `renounceOwnership` that allows the owner to renounce their ownership, but there are also several functions that are only callable by the owner, which centralizes control. The owner can set fees, open trading, remove limits, and withdraw stuck tokens or ETH, which could be potentially harmful if misused.

Code:

```
function renounceOwnership() public virtual onlyOwner {
    emit OwnershipTransferred(_owner, address(0));
    _owner = address(0);
}
function setBuyFee(uint256 buyFeePercentage) external onlyOwner { ... }
function setSellFee(uint256 sellFeePercentage) external onlyOwner { ... }
function openTrading() external onlyOwner { ... }
function removeLimits() external onlyOwner { ... }
function setMaxWalletSize(uint256 amount) external onlyOwner { ... }
function setMaxTransactionSize(uint256 amount) external onlyOwner { ... }
function setMaxSwapAmountSize(uint256 amount) external onlyOwner { ... }
function withdrawStuckToken(address tokenContractAddress, address toRescueAddress, uint256 amount)
external { ... }
function withdrawStuckETH() external { ... }
function forceSwap() external { ... }
```

Correction:

```
// To mitigate centralization, consider implementing a multi-signature requirement for critical
functions or a time-locked admin function.
```

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 implement any anti-front running measures. The use of `swapExactTokensForETHSupportingFeeOnTransferTokens` could potentially be front-run by miners or bots.

Code:

```
function swapTokensForEth(uint256 tokenAmount) private lockTheSwap {
    ...
    uniswapV2Router.swapExactTokensForETHSupportingFeeOnTransferTokens(
        tokenAmount,
        0,
        path,
        _feeWallet,
        block.timestamp
    );
}
```

Correction:

```
// Implement measures to prevent front-running, such as using a commit-reveal scheme or adding slippage protection.
```

9 - Improper Events

Result: Pass

10 - Improper Authorization Scheme

Result: Pass

11 - Integer Over/Underflow

Result: Pass

Details: The contract uses SafeMath library which prevents integer overflows and underflows.

12 - Logical Issues

Result: Medium

Details: The contract allows the owner to set fees up to 35%, which is extremely high and could be considered a risk for investors.

Code:

```
function setBuyFee(uint256 buyFeePercentage) external onlyOwner {
    require(buyFeePercentage <= 35, "setBuyFee: buyFeePercentage shouldn't exceed 35%.");
    _initialBuyTax = buyFeePercentage;
}
function setSellFee(uint256 sellFeePercentage) external onlyOwner {
    require(sellFeePercentage <= 35, "setSellFee: sellFeePercentage shouldn't exceed 35%.");
    _initialSellTax = sellFeePercentage;
}
```

Correction:

```
// Consider setting a reasonable maximum fee percentage to protect investors.
```

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 function `sendETHToFee` is never called, which results in dead code that could be removed for gas optimization.

Code:

```
function sendETHToFee(uint256 amount) private {
    payable(_feeWallet).transfer(amount);
}
```

Correction:

```
// Remove the unused function to optimize contract efficiency.
```

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