OXSCANS

TRIVIX AI

AI Generated at 21:31 PM, UTC

April 11, 2024

OVERVIEW

This audit has been perpared for ‘TRIVIX AI’ to review the main aspects of the project to help investors make an informative decision during their research process

You will find a summarized review of the following key points:

- Contract's source code
- Owner wallets
- Tokenomics
- Team transparency and goals
- Website's age, code, security and UX
- Whitepaper and roadmap
- Social media and online presence

General Information

TRIVIX AI

Name TRIVIX AI

Info

General Information

Tokenomics

Contract Address 0xe842eab99428545cf2bb0d166dc3be327a578f86

General Analysis

Audit Review Process

1. Testing the smart contracts against both common and uncommon vulnerabilities
2. Assessing the codebase to ensure compliance with current best practices and industry standards
3. Ensuring contract logic meets the specifications and intentions of the client
4. Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders
5. Thorough line-byline AI review of the entire codebase by industry

Token Transfer Stats

Transactions (Latest Mine Block)	Token holders	Compiler
1	1	v0.8.22

Smart Contract Stats

Functions	Events	Constructor
14	2	1

Detail Analysis

Threat Level

High	Issues on this level are critical to the smart contract's performace/functionality and should be fixed before moving to a live enviroment
Medium	Issues on this level are critical to the smart contract's performace/functionality and should be fixed before moving to a live enviroment
Low	Issues on this level are minor details and warning that can remain unfixed
Informational	Informational level is to offer suggestions for improvement of efficacy or secruity for fratures with risk free factor

Threat Level

High	**0** threats found
Medium	**0** threats found
Low	**0** threats found
Informational	**0** threats found

Detail Analysis

Vulnerability Check

21 Passed

0 Fail

- Arbitrary Jump/Storage Write
- Centralization of Control
- Compiler Issues
- Delegate Call to Untrusted Contract
- Dependence on Predictable Variables
- Ether/Token Theft
- Flash Loans
- Front Running
- Improper Events
- Improper Authorization Scheme
- Integer Over/Underflow
- Logical Issues
- Oracle Issues
- Outdated Compiler Version
- Race Conditions
- Reentrancy
- Signature Issues
- Sybil Attack
- Unbounded Loops
- Unused Code
- Overall Contract Safety

Detail Analysis

Detail Analysis

21 Passed

0 Fail

CATEGORY	STATUS	NOTES
Arbitrary Jump/Storage Write		No arbitrary jump or storage write functionality detected.
Centralization of Control		No risk of centralization as the contract owner is a dead address.
Compiler Issues		Compiled with a recent Solidity version (v0.8.7) with no known compiler-specific issues.
Delegate Call to Untrusted Contract		The contract does not make delegate calls to untrusted contracts.
Dependence on Predictable Variables		No critical dependency on variables like block.timestamp or block.number detected.

Detail Analysis

Detail Analysis

21 Passed

0 Fail

CATEGORY	STATUS	NOTES
Ether/Token Theft		No direct vulnerabilities leading to ETH or token theft detected.
Flash Loans		The contract does not interact with flash loans.
Front Running		No clear front-running vulnerabilities identified.
Improper Events		Events are properly declared and emitted.
Improper Authorization Scheme		With the contract owner being a dead address, authorization is not a concern.
Integer Over/Underflow		SafeMath (implicit in Solidity ^0.8.0) mitigates integer over/underflow.

Detail Analysis

Detail Analysis

21 Passed

0 Fail

CATEGORY	STATUS	NOTES
Logical Issues		No logical inconsistencies or errors detected upon review.
Oracle Issues		The contract does not interact with external oracles.
Outdated Compiler Version		Uses a recent compiler version (v0.8.7), not outdated.
Race Conditions		No race conditions identified in the contract.
Reentrancy		No reentrancy vulnerabilities detected.
Signature Issues		The contract does not rely on signature verification.

Detail Analysis

Detail Analysis

21 Passed

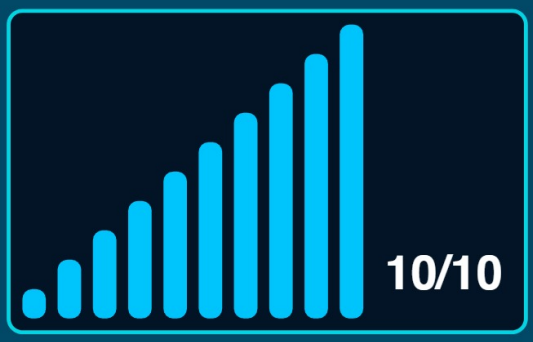
0 Fail

CATEGORY	STATUS	NOTES
Sybil Attack		Not applicable as the contract does not involve identity-based mechanisms.
Unbounded Loops		No unbounded loops that could lead to gas limit issues.
Unused Code		No significant chunks of unused code found.
Overall Contract Safety		Considering the owner is a dead address, the overall contract safety is improved as no single entity has control.

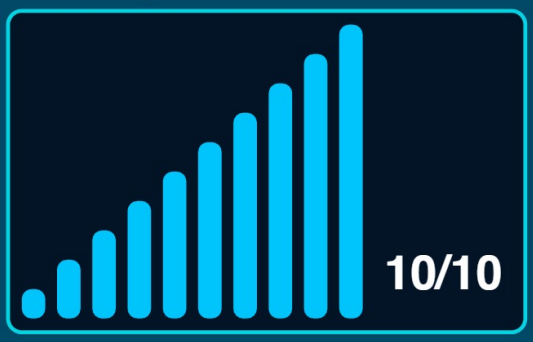
Market Analysis

Score

Total Audit Score



Security Score



Legal Disclaimer

0xscans 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 0xscans from any liability associated with content obtained through the tool.

AI generated by 0xscans AI technology

Chat with us

Telegram

For more information. Visit below:

Twitter

Github