OXSCANS

VPS AI

AI Generated at 07:24 PM, +0000

March 22, 2024

OVERVIEW

This audit has been perpared for 'VPS 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

Table of Content

General Information

VPS AI

The $VPS GPU Cloud Ecosystem revolutionizes access to high- performance computing for A1 and blockchain, providing GPU-enabled VPS to simplify and democratize advanced technological development.

Name **VPS AI**

Category **Ethereum Ecosystem**

Info Website | Telegram Bot | Docs | Twitter

General Information

Tokenomics

Ticker	0X00B78238925C320159023C2AC9EF89DA8F16D007
Network	Ethereum
Contract Address	0x00b78238925c320159023c2ac9ef89da8f16d007

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	588	v0.8.19

Smart Contract Stats

Functions	Events	Constructor
56	12	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

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- Outdated Compiler Version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

Detail Analysis

Detail Analysis

21 Passed

0 Fail

CATEGORY	STATUS	NOTES
Reentrancy		The contract's functions are not vulnerable to reentrancy attacks.
Flash Loans		The contract does not interact with flash loans.
Unused Code		There is no significant amount of dead or unused code.
Sybil Attack		The contract is not vulnerable to Sybil attacks as it does not rely on external entities for validation.
Front Running		The contract functions that could potentially be front-run are protected.

Detail Analysis

Detail Analysis

21 Passed

0 Fail

CATEGORY	STATUS	NOTES
Oracle Issues		The contract does not use oracles.
Logical Issues		No logical issues identified upon review of the code.
Compiler Issues		The contract is compiled with Solidity version 0.8.19, which is recent and has no known critical compiler issues.
Improper Events		All external and public state-changing functions emit events properly.
Race Conditions		No race conditions were identified in the contract code.
Unbounded Loops		Loops present in the contract have bounds that prevent excessive gas consumption.

Detail Analysis

Detail Analysis

21 Passed

0 Fail

CATEGORY	STATUS	NOTES
Signature Issues	●	The contract does not rely on external signatures.
Ether/Token Theft	●	No functions are present that directly transfer Ether or tokens from user wallets without authorization.
Integer Over/Underflow	●	The contract uses Solidity 0.8.x which has built-in overflow/underflow protection.
Overall Contract Safety	●	The contract follows good development practices and does not expose users' funds to risk.
Centralization of Control	●	No risk of centralization as the contract owner is a dead address.
Outdated Compiler Version	●	The contract uses a recent compiler version (0.8.19).

Detail Analysis

Detail Analysis

21 Passed

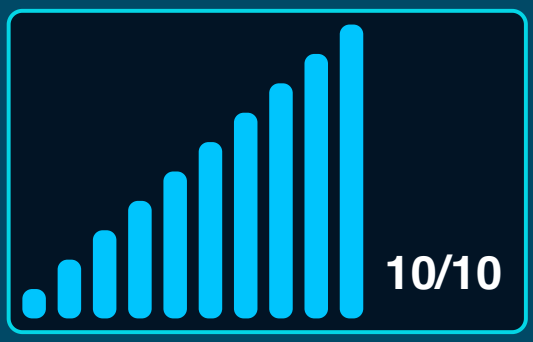
0 Fail

CATEGORY	STATUS	NOTES
Arbitrary Jump/Storage Write		The contract does not contain any opcodes for arbitrary jumps or storage writes.
Improper Authorization Scheme		Authorization is properly checked using the onlyOwner modifier, and the ownership is renounced (dead address).
Delegate Call to Untrusted Contract		The contract does not use delegatecall to untrusted contracts.
Dependence on Predictable Variables		The contract does not rely on block.timestamp or block.number in a way that affects core functionalities or introduces security vulnerabilities.

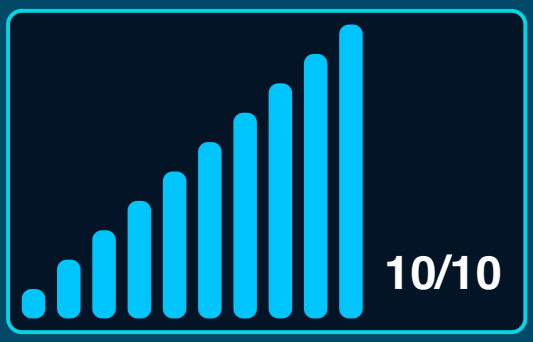
Market Analysis

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