VIBRANIUM AUDITS

Security Assessment

Zodax_Token

Vibranium Audits Verified on Nov30th, 2024

Summary

Finding

DISCLAIMER

Vibranium audits verified on Nov 30th 2024

Zodax_Token

The security assessment was prepared by Vibranium audits , the leader in Web3 security

Executive Summary

TYPES	ECOSYSTEM	METHODS
DEFI	Binance smart chain / EVM	Formal Verification, Manual review

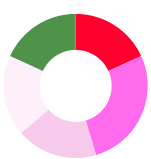
LANGUAGE

Solidity

Codebase

https://github.com/zodax-ai/Zodax_Token/blob/main/contracts/Zodax.sol
updated version ; https://amoy.polygonscan.com/address/0x55240a4dB5135B94B0949A0BF7F696b31945b10B#code

Vulnerability Summary



2	0	2	0	0	0
Total Findings	Critical	High	Medium	Minor	Informational

High	●	Resolved	Admin can withdraw tokens using the emergencyWithdraw function, which could lead to misuse or loss of funds if the admin is compromised.
High	●	Resolved	The PAUSER_ROLE can pause and unpause token transfers, which is a centralization risk and could lead to problems for the community if misused.

Codebase | **Zodax_Token**

Address

https://github.com/zodax-ai/Zodax_Token/blob/main/contracts/Zodax.sol
updated version : https://amoy.polygonscan.com/address/0x55240a4dB5135B94B0949A0BF7F696b31945b10B#code

Approach & Methods | Zodax_Token

This report has been prepared for Zodax_Token to identify potential issues and vulnerabilities in the source code of the project, including smart contracts and the token minting mechanism. A comprehensive examination has been conducted, utilizing Static Analysis and Manual Review techniques to ensure compliance with best security practices.

The auditing process pays special attention to the following considerations:

Testing the smart contracts against common and uncommon attack vectors such as reentrancy attacks, overflow vulnerabilities, and unauthorized access.

Assessing the codebase for compliance with industry best practices, ensuring code security, scalability, and maintainability.

Ensuring contract logic meets the specifications and requirements of the Zodax_Token project, specifically for token minting, access control, and transaction handling.

Cross-referencing contract structure and functionality against similar projects in the blockchain ecosystem to ensure adherence to standard practices.

Performing a line-by-line manual review of the entire codebase to identify any hidden or obscure vulnerabilities that automated tools may miss.

The security assessment identified vulnerabilities across a range of severity levels, from Critical to Informational. We recommend addressing these findings promptly to enhance the overall security of the Zodax_Token project. Key recommendations include:

Testing smart contracts against both common and uncommon attack vectors, ensuring robustness against real-world threats.

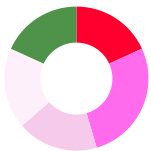
Implementing secure coding practices to enhance the quality and security of the codebase.

Expanding unit tests to cover all possible use cases and edge cases, especially for the token minting functions.

Improving code documentation and comments for better readability, particularly for critical functions involving token minting and transfers.

Ensuring transparency in privileged activities, such as the minting process, and implementing additional safeguards for authorization.

Zodax Token | Finding



2	0	2	0	0	0
Total Findings	Critical	High	Medium	Minor	Informational

This report provides a detailed audit of the Zodax Token project's codebase, focusing on the token contract . The objective of this audit is to uncover potential security vulnerabilities, optimize code efficiency, and identify areas for improvement to strengthen the project's security and reliability.
In total, two vulnerabilities were identified, categorized by severity as follows: 2 High .

ID	Title	Category	Severity	Status
ZO-01	Emergency Withdrawal	Access Control	High	Resolved
ZO-02	Centralized Control Over Pausing	Centralization Risk	High	Resolved

ZO-01 | Emergency Withdrawal

Category	Severity	Location	Status
Token Management	High	emergencyWithdraw()	Resolved

Description

- The emergencyWithdraw() function allows the contract admin to withdraw tokens from the contract. This could lead to misuse or loss of funds if the admin's credentials are compromised. If the private key of the admin is stolen or the admin acts maliciously, they could withdraw a significant amount of funds from the contract.

Mitigation

Consider implementing a multi-signature wallet or a more decentralized control mechanism for emergency withdrawals.

ZO-02 | Centralized Control Over Pausing

Category	Severity	Location	Status
Centralization Risk	High	pause() / unpause()	Resolved

Description

- The use of the pause() and unpause() functions for a token introduces a centralization risk. Pausing transfers gives an entity full control over the ability to freeze all transactions of the token, which could be problematic in decentralized systems. If pausing is triggered, it could prevent legitimate transactions, halt token transfers, or disrupt the normal operation of the token, leading to a breakdown of trust in the system. This centralization undermines the decentralization principles of blockchain systems and can create vulnerabilities where a single point of control can influence the token's availability in the market.

Mitigation

- Avoid Using pause() and unpause(): The best approach is to avoid the use of pause() and unpause() functions for token transfers. Instead, focus on designing mechanisms that can address emergency situations without halting the entire token system.
- Use Permissions for Critical Functions: If pausing is required for specific reasons (e.g., emergency actions), ensure that it's governed by a multi-signature or decentralized governance mechanism rather than a single entity. This reduces centralization and makes it more difficult for a single actor to disrupt the system.
- Implement Alternative Emergency Mechanisms: Rather than pausing token transfers, implement alternative emergency mechanisms that can mitigate issues without stopping all activity, such as blacklisting malicious addresses or temporarily restricting specific actions instead of halting the entire system.

DISCLAIMER | VIBRANIUM AUDITS

This security assessment has been prepared by Vibranium Audits for the Zodax_Token project to identify potential vulnerabilities in the project's codebase. Vibranium Audits applied its expertise in Web3 and smart contract security to perform a detailed analysis of the project, utilizing a combination of manual code review, automated tools, and industry best practices.

This report represents Vibranium Audits' assessment as of the verification date (November 30th, 2024). The findings and recommendations provided here in reflect the state of the project at the time of the audit. As blockchain technology and associated security risks continuously evolve, we strongly recommend ongoing monitoring, upgrades, and reassessments to maintain a robust security posture.

Vibranium Audits assumes no responsibility for any losses, damages, or consequences, whether financial or otherwise, resulting from the use, misuse, or reliance on this report. This document is intended solely for informational purposes and should not be construed as financial, legal, or investment advice, nor as an endorsement or guarantee of the project.

Vibranium Audits Securing the Web3 World

Vibranium Audits is a blockchain security company that was founded in 2021 by professors from the University of Greenwich and cyber-security engineers from ITI Capital. As pioneers in the field, Vibranium Audits utilizes best-in-class Formal Verification and AI technology to secure and monitor blockchains, smart contracts, and Web3 apps.