VIBRANIUM AUDITS

Security Assessment

Token Mei Solutions

Vibranium Audits Verified on Oct 30th, 2024

Summary

Finding

DISCLAIMER

Vibranium audits verified on Oct 30th 2024

Token Mei Solutions

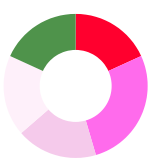
The security assesment was prepared by Vibranium audits , the leader in web3 security

Executive summary

TYPES	ECOSYSTEM	METHODS
Token	Solana	Formal Verification, Manual review

LANGUAGE	Codebase
Solana	Token Mei Solutions

Vulnerability Summay



2	0	1	1	0	0
Total Findings	Critical	High	Medium	Minor	Informational

High	Aknowledged	The initial supply (1B tokens) is entirely controlled by the creator, leading to risks of price manipulation, trust issues, and a single point of failure if the creator's wallet is compromised.
Medium	Aknowledged	The metadata immutability flag prevents any future changes to token details, which can result in irreversible issues if metadata is incorrect or if regulatory/branding needs require updates.

Codebase | **Token Mei Solutions**

Address

4MshgHvWGvxDs8mtFqPGKC8kX6kuhniWSYPguBb1p1bh

Approach & Methods | Token Mei Solutions

This report has been prepared for Token Mei Solutions to discover 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 Token Mei Solutions 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 Token Mei Solutions project. Key recommendations include:

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

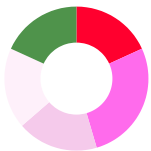
Implementing secure coding practices to enhance the quality and security of the codebase.

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.

Token Mei Solutions | Finding



2	0	1	1	0	0
Total Findings	Critical	High	Medium	Minor	Informational

This report provides a detailed audit of the Token Mei Solutions 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: 1 High and 1 Medium.

ID	Title	Category	Severity	Status
TM-S1	Centralization	Centralization problem	High	Acknowledged
TM-S1	Immutability Flag	Technical Limitation	Medium	Acknowledged

TM-S1 | Centralization

Category	Severity	Location	Status
Centralization Problem	High	4MshgHvWGvxDs8mtFqPGKC8kX6kuhniWSYPguBb1p1bh	Acknowledged

Description

The entire initial supply of 1 billion tokens is controlled by the creator, leading to a high centralization risk. This centralized control can allow the creator to influence token prices through large-scale token releases or withholding, potentially leading to price manipulation and instability in the market. Additionally, this centralization poses trust issues for holders and prospective investors, who may worry about unchecked control. Finally, if the creator's wallet is compromised, all tokens in their possession could be at risk, affecting the token's credibility and value stability.

Migitation

Set Up a Multisig Wallet for Token Control

- Transfer the entire initial supply (or a large portion) from the creator’s wallet to a multisig wallet. In Solana, multisig wallets can be set up using tools like Gnosis Safe or Squads, which allow multiple signers to jointly manage the wallet.
- Define the required number of signatures (e.g., 3 out of 5 or 4 out of 6 signers) for any transaction to ensure no single individual can unilaterally access or move tokens.

TM-S1 | Immutability Flag

Category	Severity	Location	Status
Technical Limitation	Medium	4MshgHvWGvxDs8mtFqPGKC8kX6kuhniWSYPguBb1p1bh	Acknowledged

Description

The immutability flag being true on the SPL token's metadata means that the metadata can be modified post-creation. This flexibility allows for potential updates, such as branding or additional information; however, it also introduces significant security risks. Specifically, it enables anyone with control over the metadata (usually the creator or an authorized party) to alter essential token information (such as the name, symbol, or other metadata), which could confuse token holders or harm the project's credibility. Furthermore, malicious actors could potentially alter metadata to mislead holders, especially if the control falls into the wrong hands.

Mitigation

- Consider Locking Metadata Later

After the project matures, consider setting the immutability flag to false to lock the metadata permanently, ensuring no further changes can be made. This can reassure holders that the token's identity and branding are stable and won't be altered unexpectedly.

DISCLAIMER

VIBRANIUM AUDITS

This security assessment has been prepared by Vibranium Audits for Token Mei Solutions to identify potential vulnerabilities in the project's codebase. Vibranium Audits applied its expertise in Web3 security to perform a thorough examination of the project, employing formal verification and manual review methods.

This report reflects Vibranium Audits' assessment as of the verification date (Oct 30th, 2024). It provides a snapshot of the security posture based on current findings and best practices at the time of the review. However, as blockchain technology and security landscapes evolve, ongoing vigilance and periodic reassessments are essential.

Vibranium Audits is not liable for any losses, financial or otherwise, resulting from the use or reliance on this report. This document is for informational purposes only and does not constitute financial advice, legal counsel, or an endorsement of any kind.

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.