verichains

SECURITY AUDIT OF

AI POWNERS CONTRACT

AIPOWERS

Public Report

April 23, 2024

Verichains Lab

info@verichains.io

https://www.verichains.io

Driving Technology > Forward

ABBREVIATIONS

Name	Description
Solana Blockchain	Solana is a blockchain built for mass adoption. It's a high performance network that is utilized for a range of use cases, including finance, NFTs, payments, and gaming. Solana operates as a single global state machine, and is open, interoperable and decentralized.
Program	An app interacts with a Solana cluster by sending it transactions with one or more instructions. The Solana runtime passes those instructions to program.
Lamport	A fractional native token with the value of 0.000000001 sol.
SOL	A cryptocurrency whose blockchain is generated by the Solana platform.

EXECUTIVE SUMMARY

This Security Audit Report was prepared by Verichains Lab on April 23, 2024. We would like to thank the AI Powners for trusting Verichains Lab in auditing smart contracts. Delivering high-quality audits is always our top priority.

This audit focused on identifying security flaws in code and the design of the AI Powners Contract. The scope of the audit is limited to the source code files provided to Verichains. Verichains Lab completed the assessment using manual, static, and dynamic analysis techniques.

During the audit process, the audit team performs on-chain information gathering and conducts some data analysis.

TABLE OF CONTENTS

1. MANAGEMENT SUMMARY

1.1. About AI Powners Contract

AI Powers is an innovative platform designed to revolutionize the content creation landscape by leveraging advanced AI technologies. A powerful AI-driven application, enables users to effortlessly transform text and images into high-quality videos. This groundbreaking feature caters to a wide range of applications, from animated films and sci-fi videos to educational content and beyond. With team's commitment to continuous innovation, AI Powers is on the path to integrating Superintelligent Artificial General Intelligence (AGI) capabilities, promising to redefine creativity and content generation.

1.2. Audit scope

This audit focused on identifying security flaws in the code and the design of the AI Powners Contract. It was conducted on the token address `23fDC4u597wRHgTQjY9ikqYnqDc2RDPT3Tves8Z1RBLn` with on-chain data reviewed up to block `261637455`.

1.3. Audit methodology

Our security audit process for Solana smart contract includes two steps:

- Smart contract codes are scanned/tested for commonly known and more specific vulnerabilities using our in-house smart contract security analysis tool.
- Manual audit of the codes for security issues. The contracts are manually analyzed to look for any potential problems.

Following is the list of commonly known vulnerabilities that were considered during the audit of the Solana smart contract:

- Arithmetic Overflow and Underflow
- Signer checks
- Ownership checks
- Rent exemption checks
- Account confusions
- Bump seed canonicalization
- Closing account
- Signed invocation of unverified programs
- Numerical precision errors
- Logic Flaws

For vulnerabilities, we categorize the findings into categories as listed in table below, depending on their severity level:

SEVERITY LEVEL	DESCRIPTION
CRITICAL	A vulnerability that can disrupt the contract functioning; creates a critical risk to the contract; required to be fixed immediately.
HIGH	A vulnerability that could affect the desired outcome of executing the contract with high impact; needs to be fixed with high priority.
MEDIUM	A vulnerability that could affect the desired outcome of executing the contract with medium impact in a specific scenario; needs to be fixed.
LOW	An issue that does not have a significant impact, can be considered as less important.

Table 1. Severity levels

1.4. Disclaimer

AI Powners acknowledges that the security services provided by Verichains, are conducted to the best of their professional abilities but cannot guarantee 100% coverage of all security vulnerabilities. AI Powners understands and accepts that despite rigorous auditing, certain vulnerabilities may remain undetected. Therefore, AI Powners agrees that Verichains shall not be held responsible or liable, and shall not be charged for any hacking incidents that occur due to security vulnerabilities not identified during the audit process.

1.5. Acceptance Minute

This final report served by Verichains to the AI Powners will be considered an Acceptance Minute. Within 7 days, if no any further responses or reports is received from the AI Powners, the final report will be considered fully accepted by the AI Powners without the signature.

2. AUDIT RESULT

2.1. Overview

The AI Powers token program has been established using the Metaplex Token Metadata program.

The audited version of the AI Powers token program has identified the below information:

Field	Value
Website	*https://aipowers.app*
Token Symbol	AIP
Token Mint Address	23fDC4u597wRHgTQjY9ikqYnqDc2RDPT3Tves8Z1RBLn
Data URI	*https://ipfs.io/ipfs/ QmPgxz95JjAbVQRPrdVQ24KcG9vT7TPrZ7WyHVHpiRcpYX*
Current Supply	500,000,000 $x10^8$
Extensions	No
Created At	April 18, 2024
Creator	3ss6QPJubw3b8iaYM4B16WXhvptZk7D7JQ8xH5cHLRE8
Holder	99,99% by 3ss6QPJubw3b8iaYM4B16WXhvptZk7D7JQ8xH5cHLRE8
Mutable Program	Yes
Market	Not Listed Yet
Update Authority	3ss6QPJubw3b8iaYM4B16WXhvptZk7D7JQ8xH5cHLRE8
Mint authority	3ss6QPJubw3b8iaYM4B16WXhvptZk7D7JQ8xH5cHLRE8
Freeze authority	3ss6QPJubw3b8iaYM4B16WXhvptZk7D7JQ8xH5cHLRE8
Token Account	6S8ezPF5NRS87zk5fkAoNZnd2tx9m5TN4cf1gsEVRLFW
Owner of Token Account	3ss6QPJubw3b8iaYM4B16WXhvptZk7D7JQ8xH5cHLRE8

Field	Value
Close Authority Token Account	Not Set
Delegate Token Account	Not Set

Table 2. Program Information

The AI Powers token program with ownership vested in a sole holder.

This single owner enjoys exclusive privileges, including the ability to manipulate token metadata, mint new tokens, freeze existing ones, and execute program upgrades at their discretion.

It's important to note that, as of now, the token program hasn't been infused with liquidity and hasn't made its list on any market.

Given the comprehensive control wielded by the owner, they hold considerable sway over the program's direction and administration.

Expanding on the program's centralized authority, it's crucial to highlight how the single owner's exclusive privileges centralize decision-making and governance. With the ability to manipulate token metadata, mint new tokens, freeze existing ones, and execute program upgrades at their discretion, the owner holds unparalleled control over the program's operations. This centralized authority consolidates power in the hands of a single entity, enabling swift and decisive action without the need for consensus or approval from external stakeholders. However, while this centralization offers efficiency and agility in decision-making, it also raises concerns about transparency, accountability, and the potential for misuse of power. As such, it underscores the importance of robust governance mechanisms and oversight to ensure the fair and responsible management of the program for the benefit of all stakeholders.

2.2. Findings

During the audit process, the audit team has not identified any security issues in the contract code.

3. VERSION HISTORY

Version	Date	Status/Change	Created by
1.0	*Apr 23, 2024*	Public Report	Verichains Lab

Table 3. Report versions history