verichains

SECURITY AUDIT OF

ANCIENT8 TOKEN

Public Report

May 04, 2024

Verichains Lab

info@verichains.io

https://www.verichains.io

Driving Technology > Forward

ABBREVIATIONS

Name	Description
Ethereum	An open source platform based on blockchain technology to create and distribute smart contracts and decentralized applications.
Ether (ETH)	A cryptocurrency whose blockchain is generated by the Ethereum platform. Ether is used for payment of transactions and computing services in the Ethereum network.
Smart contract	A computer protocol intended to digitally facilitate, verify or enforce the negotiation or performance of a contract.
Solidity	A contract-oriented, high-level language for implementing smart contracts for the Ethereum platform.
Solc	A compiler for Solidity.
ERC20	ERC20 (BEP20 in Binance Smart Chain or *x*RP20 in other chains) tokens are blockchain-based assets that have value and can be sent and received. The primary difference with the primary coin is that instead of running on their own blockchain, ERC20 tokens are issued on a network that supports smart contracts such as Ethereum or Binance Smart Chain.

EXECUTIVE SUMMARY

This Security Audit Report was prepared by Verichains Lab on May 04, 2024. We would like to thank the Ancient8 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 Ancient8 Token. 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 had identified no vulnerable issue in the smart contracts code.

TABLE OF CONTENTS

1. MANAGEMENT SUMMARY

1.1. About Ancient8 Token

Ancient8 is building a DAO that develops a community and software platform to enable everyone to play and build the Metaverse while earning rewards. As Vietnam's largest blockchain gaming guild, Ancient8 has helped tens of thousands of blockchain gamers and enthusiasts by providing scholarship and educational opportunities, community, and blockchain and software products. Ancient8's vision is to democratize social and financial access in the Metaverse, and is on a mission to reach, educate, and empower the next 100 million Metaverse citizens through the blockchain.

1.2. Audit scope

This audit focused on identifying security flaws in code and the design of the Ancient8 Token that was deployed on Ethereum.

The latest version was made available in the course of the review:

FIELD	VALUE
Address Deploy	0x3E5A19c91266aD8cE2477B91585d1856B84062dF
Tx Deploy	0x3cf242f5f56447c172f031523b5c4c28f421c597ac7e983d370d09537b12b2e2
Deployer	0xA9a3E32E18b2936702d466D02E77A1Fd64c9C4D4
Block Number	14722546

1.3. Audit methodology

Our security audit process for smart contract includes two steps:

- Smart contract codes are scanned/tested for commonly known and more specific vulnerabilities using public and RK87, 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 smart contract:

- Integer Overflow and Underflow
- Timestamp Dependence
- Race Conditions
- Transaction-Ordering Dependence
- DoS with (Unexpected) revert
- DoS with Block Gas Limit
- Gas Usage, Gas Limit and Loops
- Redundant fallback function
- Unsafe type Inference
- Reentrancy
- Explicit visibility of functions state variables (external, internal, private and public)
- 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

Ancient8 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. Ancient8 understands and accepts that despite rigorous auditing, certain vulnerabilities may remain undetected. Therefore, Ancient8 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 Ancient8 will be considered an Acceptance Minute. Within 7 days, if no any further responses or reports is received from the Ancient8, the final report will be considered fully accepted by the Ancient8 without the signature.

2. AUDIT RESULT

2.1. Overview

The Ancient8 Token was written in `Solidity` language, with the deployed compiler version is `0.8.13`.

The contract makes use of the `OpenZeppelin` library's `ERC20` extension. Below is the contract's properties:

PROPERTY	VALUE
Name	Ancient8
Symbol	A8
Decimals	18
Total Supply	1,000,000,000x10^{18} (It represents 1 billion tokens)
Allow Minter	Yes

Table 2. The Ancient8 Token properties

For the ERC20 token, the security audit team has the following checklist of centralization standards:

Checklist	Passed
No Upgradeable	Yes
No Fee modifiable	Yes
No Mintable	No
No Pausable	Yes
No Trading cooldown	Yes
No Blacklist	Yes
No Whitelist	Yes

Table 3. The decentralization checklist

2.2. Findings

During the audit process, the audit team found no vulnerability in the given version of Ancient8 Token.

APPENDIX

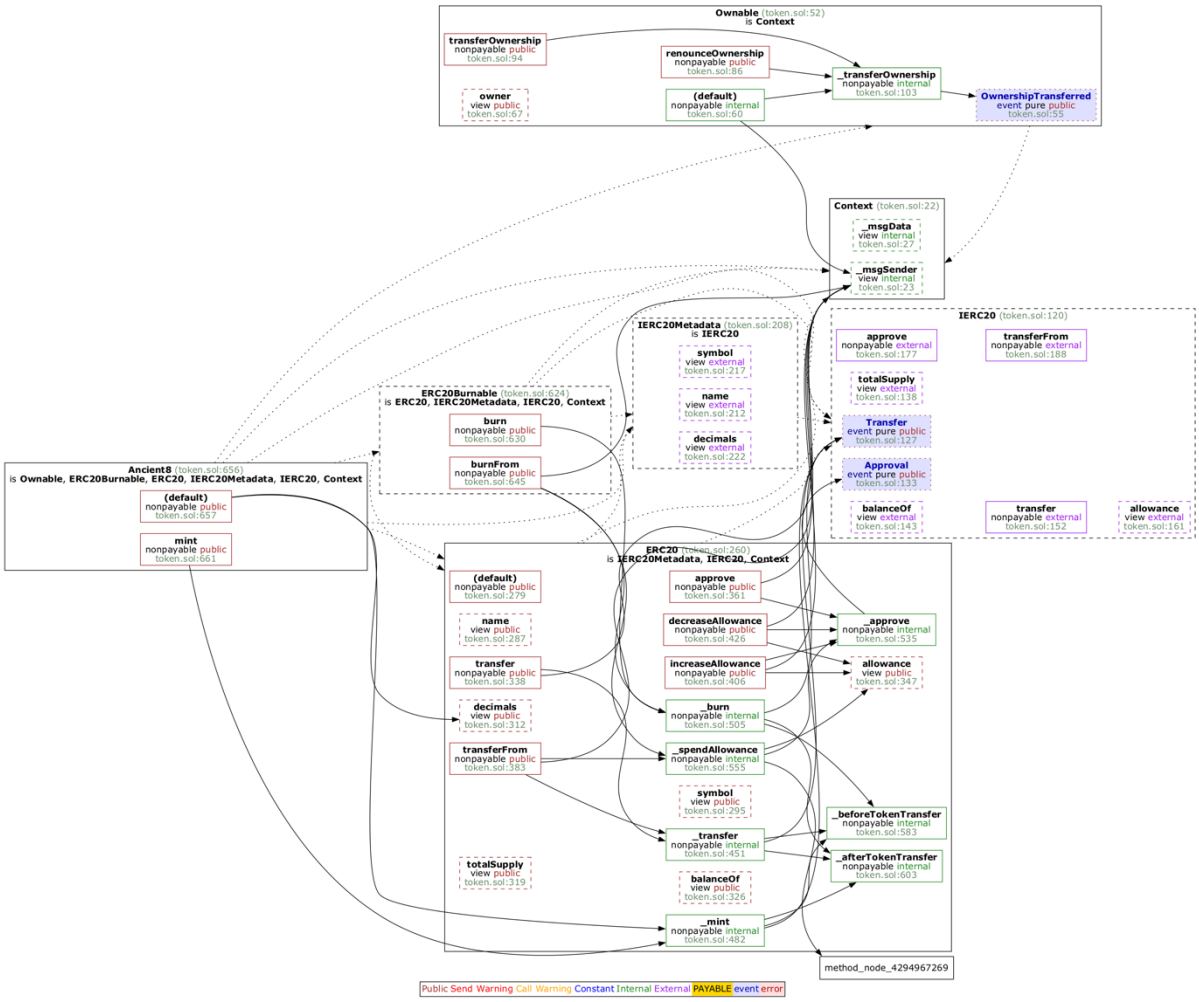

Image 1. ABI token smart contract call graph

3. VERSION HISTORY

Version	Date	Status/Change	Created by
1.0	*May 04, 2024*	Public Report	Verichains Lab

Table 4. Report versions history