verichains

SECURITY AUDIT OF

F3 TOKEN

Public Report

Oct 24, 2023

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 Oct 24, 2023. We would like to thank the DevTrek 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 F3 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 F3 Token

The $F3 is a digital asset that serves as a currency within the gaming world of F3 Play. In this game, F3 Token plays a pivotal role, enabling players to engage in exciting battles and upgrading their in-game NFTs. F3 Token can be acquired through the process of opening the F3 Box or the Lottery tickets that are earned as rewards through battles.

1.2. Audit scope

This audit focused on identifying security flaws in code and the design of the smart contracts of F3 Token. It was conducted on commit `98c3d1b7d036969c0853eb575cb56c95fbff1041` from git repository *https://github.com/mimett/f3-smart-contracts*.

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

SHA256 Sum	File
`21fe758c562404a99290b6f78ed3a023fab2eb06ad9f563c60a7fddc5b3145d9`	`F3Token.sol`

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

DevTrek 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. DevTrek understands and accepts that despite rigorous auditing, certain vulnerabilities may remain undetected. Therefore, DevTrek 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.

2. AUDIT RESULT

2.1. Overview

The F3 Token was written in `Solidity` language, with the required version to be `^0.8.19`. The source code was written based on OpenZeppelin's libraries: `AccessControl`, `ERC20`.

The accounts with MINTER_ROLE role are allowed to mint tokens with the condition that `totalSupply()` cannot be greater than 4,206,900,000 tokens.

The smart contract is `ERC20` implementation that have some properties (as of the report writing time):

PROPERTY	VALUE
Name	F3 Token
Symbol	F3
Decimals	18
Total Supply	4,206,900,000

Table 2. The F3 Token properties

2.2. Findings

During the audit process, the audit team had identified no vulnerable issue in the smart contracts code.

3. VERSION HISTORY

Version	Date	Status/Change	Created by
1.0	*Oct 24, 2023*	Public Report	Verichains Lab

Table 3. Report versions history