verichains

SECURITY AUDIT OF

BOMBCRYPTO TOKEN SMART CONTRACTS

Public Report

October 5, 2021

Verichains Lab

info@verichains.io

https://www.verichains.io

Driving Technology > Forward

ACRONYMS AND 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 prepared by Verichains Lab on October 3, 2021. We would like to thank the Senspark 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 BombCrypto Token Smart Contracts. 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 issues in the smart contracts code.

TABLE OF CONTENTS

1. MANAGEMENT SUMMARY

1.1. About Senspark

Senspark is an indie game developer team founded in 2011, but developed games many years before. The team focuses on mobile games for both Android and iOS. Some titles are already top hits available on Apple AppStore and Google Play. They believe with a solid team and a goal to build qualified games Senspark can be a successful indie in Vietnam.

1.2. About BombCrypto Token Smart Contracts

BombCrypto is a Bomb game experiences to NFT collectibles on the blockchain by BCOIN. Players can collect, fight monsters and trade them for real money.

BCOIN is an ERC20 token that BombCrypto players can use to buy heros, upgrade them and earn rewards.

1.3. Audit scope

This audit focused on identifying security flaws in code and the design of the smart contracts of BombCrypto's BCOIN. It was conducted on commit 3fd5b6624e444f0dbde8413fb566f070499f4d6d from git repository *https://bitbucket.org/senspark/bombcrypto-vesting*.

1.4. 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 was 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

1.5. Disclaimer

Please note that security auditing cannot uncover all existing vulnerabilities, and even an audit in which no vulnerabilities are found is not a guarantee for a 100% secure smart contract. However, auditing allows discovering vulnerabilities that were unobserved, overlooked during development and areas where additional security measures are necessary.

2. AUDIT RESULT

2.1. Overview

The initial review was conducted in September 2021 and a total effort of 3 working days was dedicated to identifying and documenting security issues in the code base of the BombCrypto Token Smart Contracts.

The following files were made available in the course of the review:

FILE	SHA256 SUM
BCoinToken.sol	480f947222e4cd0f80bf135bfa5fc590d2a09d1cf1f60be97dc4d05e61681d20
BEP20.sol	f0565719857ee810408d1af17b9101ec54162bda335556271270a0e1ce1f1d75

2.2. Findings

The BombCrypto Token Smart Contracts was written in Solidity language, with the required version to be 0.8.0. The token was customized on template based on OpenZeppelin's library.

Senspark fixed the code according to Verichain's draft report in commit 7e1763234d87eb632d628657fcf3d15fe6cf0014.

2.3. Issues

The audit team found no vulnerability in the given version of BombCrypto Token Smart Contracts.

2.4. Additional notes and recommendations

2.4.1. Redundant of transfer and transferFrom function INFORMATIONAL

The transfer and transferFrom functions are checking duplicatted conditions with BEP20 contract.

```
require(_receiver != address(0));
```

Snippet 1. BCoinToken.sol, transfer function

```
require(_from != address(0));
require(_receiver != address(0));
require(_amount <= allowance(_from, msg.sender));
```

Snippet 2. BCoinToken.sol, transferFrom function

RECOMMENDATION

Removing 2 redudant functions transfer and transferFrom in BCoinToken contract.

UPDATES

- *2021-09-21*: Senspark has removed these functions in commit 7e1763234d87eb632d628657fcf3d15fe6cf0014.

3. VERSION HISTORY

Version	Date	Status/Change	Created by
1.0	*2021-10-03*	Public Report	Verichains Lab
1.1	*2011-10-05*	Update Project Information	Verichains Lab

Table 2. Report versions history