verichains

SECURITY AUDIT OF

BIT CASTLE WAR SMART CONTRACT

Public Report

Mar 08, 2022

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 prepared by Verichains Lab on Mar 08, 2022. We would like to thank the Bit Castle War 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 Bit Castle War Smart 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 had identified no vulnerable issues in the smart contracts code.

TABLE OF CONTENTS

1. MANAGEMENT SUMMARY

1.1. About Bit Castle War Smart Contract

BitCastleWar is an MMORPG NFT GAME built on the Binance Smart Chain platform, a game set in the medieval era when 3 races, Warrior, Magician, Archer. worshiping 4 elemental dragons: Medieval Dragon (Fire), Modemona Dragon (Ice), Angva Dragon (Storm), Gregen Dragon (Nature). To balance the BitCastleWar world. Until the dark mage Khozor of the dark guild Ilumia and his accomplices performed a ghostly ritual. Sacrifice 100 living creatures to corrupt Medieval Dragon, the most powerful of the 4 elemental dragons.

Bit Castle War Token is an ERC20 token that BitCastleWar players can use in the game.

1.2. Audit scope

This audit focused on identifying security flaws in code and the design of the smart contracts of Bit Castle War game. It was conducted on the source code provided by the Bit Castle War team.

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 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

1.4. 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

2.2. Contract codes

The Bit Castle War Smart Contract was written in Solidity language, with the required version to be 0.8.1.

2.2.1. Bit Castle War token contract

Bit Castle War token contract is an ERC20 token contract that only inherits ERC20 contract from OpenZeppelin. Currently, the symbol, name and initialSupply are not set. They are only set in the constructor by deployer through the contructor.

2.3. Findings

During the audit process, the audit team found no vulnerability in the given version of Bit Castle War Smart Contract.

APPENDIX

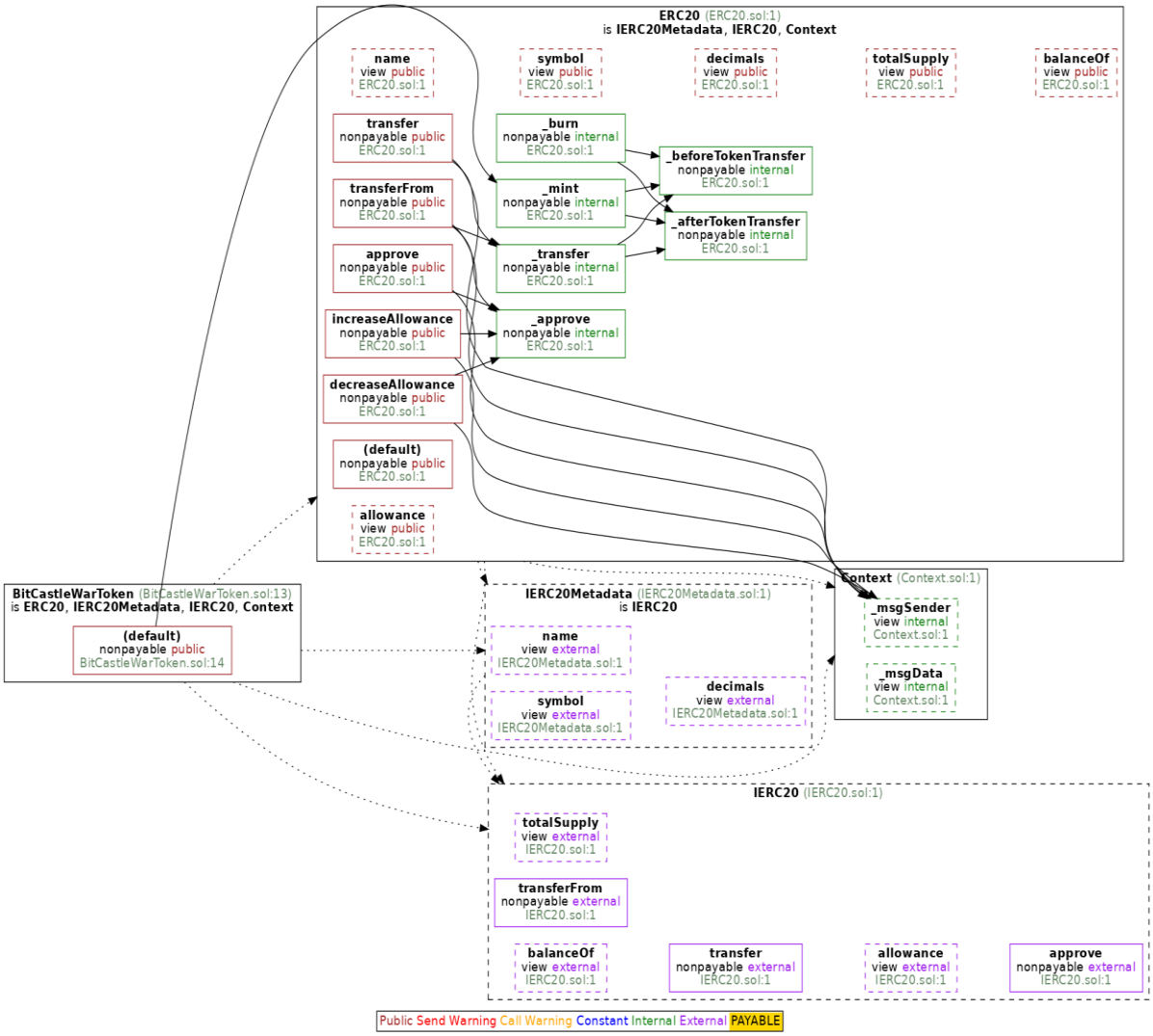

Image 1. Bit Castle War Smart Contract call graph

3. VERSION HISTORY

Version	Date	Status/Change	Created by
1.0	*Mar 08, 2022*	Public Report	Verichains Lab

Table 2. Report versions history