SECURITY AUDIT OF

WORLD OF MASTERS SMART CONTRACTS

Public Report

Mar 03, 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 03, 2022. We would like to thank the World of Masters 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 World of Masters 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 World of Masters Smart Contracts

World Of Masters is a completely new generation of Card Battle turn-based mobile games based on Blockchain technology. You can participate in a world of Kungfu - martial arts - mythology in the most authentic way. Together with the extremely famous legendary heroes from Jin Yong's top novels in the world, to create a unique worldview of their own. Fight with evil forces or compete with other players to conquer the heights in the game.

1.2. Audit scope

This audit focused on identifying security flaws in code and the design of the World of Masters Smart Contracts.

It was conducted on commit 414b6b508c72a9e27e779d42ee2a3669020d6df6 from git repository *https://github.com/wofmteam/smart-contract*.

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

World of Masters Smart Contracts contains 2 main contracts: WofM and WoMPaymentGateway.

2.1.1. WofM contract

This is ERC20 token contract in the World of Masters Smart Contracts, which extends WoM20Payable, ERC20Burnable and WoMWithdrawable contracts. With WoMWithdrawable, WITHDRAWER_ROLE role can withdraw all tokens, NFT (ERC20, ERC721, ERC1155) and native tokens from this contract.

WoM20Payable supports user paying invoices with this token. Invoices are generated and signed in backend server, users can only pay for a valid signature invoice.

The total supply of this token is 1,000,000,000 (x10^{18}) (Note: the number of decimals is 18, so the total representation token will be 1,000,000,000 or 1 billion.)

2.1.2. WoMPaymentGateway contract

This is the payment gateway contract in the World of Masters Smart Contracts, which extends WoMWithdrawable and EIP712 contracts.

WoMPaymentGateway supports user paying invoices with any ERC20 token. Invoices are generated and signed in backend server, users can only pay for a valid signature invoice. It also supports withdrawing tokens, users can only withdraw tokens with a valid invoice signed by backend server.

2.2. Findings

During the audit process, the audit team found no vulnerability in the given version of the World of Masters Smart Contracts.

3. VERSION HISTORY

Version	Date	Status/Change	Created by
1.0	*Mar 2, 2022*	Public Report	Verichains Lab
1.1	*Mar 3, 2022*	Public Report	Verichains Lab

Table 2. Report versions history