verichains

SECURITY AUDIT OF

WORLD MOBILE TOKEN NFT OWNERSHIP SMART CONTRACT

Public Report

Nov 1, 2022

Verichains Lab

info@verichains.io

https://www.verichains.io

Driving Technology > Forward

ABBREVIATIONS

Name	Description
Smart contract	A computer protocol intended to digitally facilitate, verify or enforce the negotiation or performance of a contract.
ADA	The native cryptocurrency of the Cardano platform.
Lovelace	The smallest unit of ADA, equivalent to one millionth of one token.
Plutus	Plutus is the smart contract platform of the Cardano blockchain. It allows you to write applications that interact with the Cardano blockchain.

EXECUTIVE SUMMARY

This Security Audit Report was prepared by Verichains Lab on Nov 1, 2022. We would like to thank the World Mobile Token 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 Mobile Token NFT Ownership 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 found no vulnerability in the given version of World Mobile Token NFT Ownership Smart Contract, only some notes and recommendations.

TABLE OF CONTENTS

1. MANAGEMENT SUMMARY

1.1. About World Mobile Token NFT Ownership Smart Contract

World Mobile Token (WMT) is the fuel for the unstoppable World Mobile network.

It's used to reward users and node operators, powering the sharing economy by providing incentives for securing the network, processing transactions, and delivering connectivity.

Whether it's through staking, operating an EarthNode, connecting others, securing the network, or providing value-added services, WMT's tokenomics offer many ways for users to benefit from holding and staking WMT in their Vault.

1.2. Audit scope

This audit focused on identifying security flaws in code and the design of the World Mobile Token NFT Ownership Smart Contract. It was conducted on the source code provided by the World Mobile Token team.

It was conducted on commit `c26a0890ee0cf8107fa4ddac5404535d8e2e4569` from git repository *https://github.com/worldmobilegroup/ennft-mgr/commit/*.

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

SHA256 Sum	File
`0f8f0830f033a3ea1d905e2792936a34e8e1b17d272e6003709b3258c471991b`	`Contract/Ownership/Admin/Attributions.hs`
`a1cc37d30c83bd8a8182c2b974df41e38b45bf897f580e360b27668486326f20`	`Contract/Ownership/Admin/Command.hs`
`c8fb2664bbfb6b04dd31ec035e3f09cbccc1d18cc0a722c732162cc59c086681`	`Contract/Ownership/Admin/Console.hs`
`79cd9db4d91ddcb5aab3a97a57985745f3d9bf7e3e8c94cce1ed10060ad26cd0`	`Contract/Ownership/Admin/TxBuilder/AttributeNFTs.hs`
`6f7ef2ec599ed3d5d8122f61fe2d0b8568c8f0c14f85debdae08ac4266bcea0b`	`Contract/Ownership/Admin/TxBuilder/RetrieveAllNonConformedAssets.hs`
`5783e9bcb94a66c815e55949017783a0b1f00ebf01ac9bcbe3b6442f13f9a46f`	`Contract/Ownership/Admin/TxBuilder/RetrieveAttributedNFTs.hs`
`8a9c491a7e8fc5586cb4d2bea91b272cf6b97837ae03b6297ff9f4c372caf8aa`	`Contract/Ownership/Admin/TxBuilder/RetrieveReleasedNFTs.hs`

ec89448d3ec92fa03fe6ed84e4a3f0355593539f539d289d2531e41f0427114e	Contract/Ownership/Admin/TxBuilder/SetNFTsOwnerShip.hs
94d155911414834d39f5b29471590a97b78d3847b7e6cd795dc4e91f3d7dd29c	Contract/Ownership/Admin/TxBuilder/TransferNFTsOwnerShip.hs
6502b58371aa488ff88a056d0bc176f1a6bf3e69b1ae6e193d6acfc094b4d0fb	Contract/Ownership/OnChain/Validator.hs
6cd3743c6dae8a0ba5b08e78cb9beb43f65dad1c36992aecf72f55bb2c688d58	Contract/Ownership/Owner/Command.hs
ba271907fe2d235ae4a5ebe0dd68fad8ba8aa005a0cce5dbf238a942272dbfc5	Contract/Ownership/Owner/Console.hs
445be64747f86e8ae1a931826b145e8cda907b1f038e499e668bc8346b02dcde	Contract/Ownership/Owner/Server.hs
ffdf28902fc2f4ed26c4d712e25c5f60caaff014827990de1419233da42a7c77	Contract/Ownership/Owner/TxBuilder/ReleaseNFTs.hs
5e66d740d958ff4561bae469e6de83c5bd56f63392454786b3f258b7b80c6881	Contract/Ownership/Owner/TxBuilder/RetrieveAttributedNFTs.hs
6be916b48aabc24b9e144a4bad4a2ec2ad6114f754dd01406a87b748565e6e7d	Contract/Ownership/Server.hs
8bbc4a723a2562fb440a6a2fd54d28cb736482d08ba97833c40c93762d9bef32	Contract/Ownership/Types.hs

1.3. Audit methodology

Our security audit process for Cardano smart contract includes two steps:

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

- Double Satisfaction
- Hard Limits
- Datum Hijacking
- 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

The World Mobile Token NFT Ownership Smart Contract was written in `Haskell` programming language with `Plutus` platform. It is a Semi-Centralized Plutus Script for managing the distribution of NFTs previously minted by Admin.

Users can retrieve NFTs locked in the contract in exchange for a specific amount (set by Admin) of their fungible tokens to be locked. At any time, owners of NFTs can retrieve their fungible tokens by releasing their NFTs back to the contract.

2.2. Findings

During the audit process, the audit team found no vulnerability in the given version of World Mobile Token NFT Ownership Smart Contract, only some notes and recommendations.

2.2.1. Unused `filterValueByDatum` function INFORMATIVE

Affected files:

- `OnChain/Validator.hs`

RECOMMENDATION

Removing unused function.

UPDATES

- *Nov 1, 2022*: This issue has been acknowledged by the World Mobile Token team.

3. VERSION HISTORY

Version	Date	Status/Change	Created by
1.0	*Sep 23, 2022*	Private Report	Verichains Lab
1.1	*Nov 1, 2022*	Public Report	Verichains Lab

Table 2. Report versions history