SECURITY AUDIT OF

LEISUREMETA TOKEN

Public Report

Feb 07, 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 Feb 07, 2023. We would like to thank the LeisureMeta 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 LeisureMeta 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 issues in the smart contracts code.

TABLE OF CONTENTS

1. MANAGEMENT SUMMARY

1.1. About LeisureMeta Token

The LeisureMeta Token (LM) is a ERC20 token used in the LeisureMetaverse ecosystem. The LM token is used as a form of payment for fees incurred from user activities within the LeisureMetaverse and all fees are burned, helping to prevent inflation and maintain a healthy ecosystem. The token also serves as a bridge between the virtual and real economies. Users are rewarded with LM tokens for participating in activities and collecting NFTs, with the rewards being based on the total user activity score. The Community Rewards have a maximum limit of 50,000,000 tokens per month and are subject to halving if this limit is reached.

1.2. Audit scope

This audit focused on identifying security flaws in code and the design of the LeisureMeta Token.

The audited contract is the LeisureMeta Token that deployed on Ethereum Mainnet at address `0x7BEC98609cB6378D6F995e8f8097Ee78376fbec9`. The details of the deployed smart contract are listed in Table 1.

FIELD	VALUE
Contract Name	LeisureMeta
Contract Address	0x7BEC98609cB6378D6F995e8f8097Ee78376fbec9
Compiler Version	v0.8.13+commit.abaa5c0e
Explorer	*https://etherscan.io/token/0x7bec98609cb6378d6f995e8f8097ee78376fbec9*

Table 1. The deployed smart contract details

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 2. 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

Table 2 lists some properties of the audited LeisureMeta Token (as of the report writing time).

PROPERTY	VALUE
Name	LeisureMeta Token
Symbol	LM
Decimals	18
Total Supply	5,000,000,000 x10^{18} Note: the number of decimals is 18, so the total representation token will be 5,000,000,000 or 5 billion.

Table 3. The LeisureMeta Token properties

2.2. Contract codes

LeisureMeta is an ERC20 token implemented on the Ethereum blockchain using the Solidity programming language. This token implements the ERC20 token standard and includes additional functionality from OpenZeppelin libraries: Ownable, Pausable, and ERC20Burnable.

The contract has an owner, and the token is pausable by the owner. The token is also burnable, meaning the owner or any other user can burn (permanently destroy) their tokens.

The contract has a mapping of locked items for each address, and a mapping of revocably locked items for each address. These locked items have an amount and a release time.

The contract has functions for transferring tokens, setting the D-Day (a date in the future), getting the D-Day, checking the locked items for an address, checking the revocably locked items for an address, checking the locked amount for an address, and clearing unnecessary locked items. The contract also includes events for setting the D-Day, sales lock, general lock, and revoke (that owner take all locked items was stored in mapping of revocablyLockedItems).

2.3. Findings

During the audit process, the audit team found no vulnerability in the given version of LeisureMeta Token.

APPENDIX

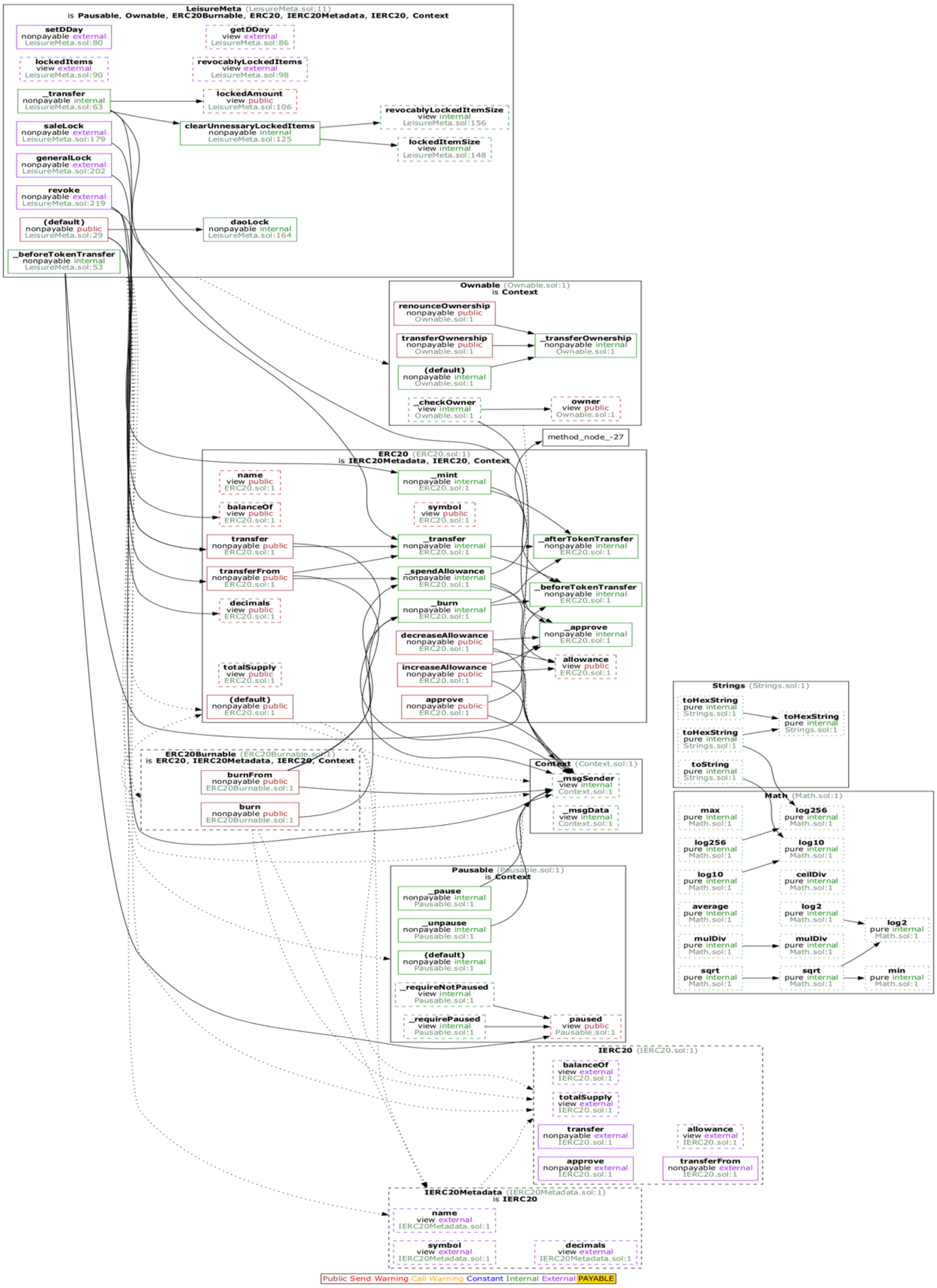
LeisureMeta (LeisureMeta.sol:11)
is Pausable, Ownable, ERC20Burnable, ERC20, IERC20Metadata, IERC20, Context
setDDay nonpayable external LeisureMeta.sol:80
getDDay view external LeisureMeta.sol:86
lockedItems view external LeisureMeta.sol:90
revocablyLockedItems view external LeisureMeta.sol:98
_transfer nonpayable internal LeisureMeta.sol:63
lockedAmount view public LeisureMeta.sol:106
revocablyLockedItemSize view internal LeisureMeta.sol:156
saleLock nonpayable external LeisureMeta.sol:179
clearUnnessaryLockedItems nonpayable internal LeisureMeta.sol:125
lockedItemSize view internal LeisureMeta.sol:148
generalLock nonpayable external LeisureMeta.sol:202
revoke nonpayable external LeisureMeta.sol:219
(default) nonpayable public LeisureMeta.sol:29
daoLock nonpayable internal LeisureMeta.sol:164
_beforeTokenTransfer nonpayable internal LeisureMeta.sol:53
Ownable (Ownable.sol:1)
is Context
renounceOwnership nonpayable public Ownable.sol:1
transferOwnership nonpayable public Ownable.sol:1
_transferOwnership nonpayable internal Ownable.sol:1
(default) nonpayable internal Ownable.sol:1
_checkOwner view internal Ownable.sol:1
owner view public Ownable.sol:1
method_node_-27
ERC20 (ERC20.sol:1)
is IERC20Metadata, IERC20, Context
name view public ERC20.sol:1
_mint nonpayable internal ERC20.sol:1
balanceOf view public ERC20.sol:1
symbol view public ERC20.sol:1
transfer nonpayable public ERC20.sol:1
_transfer nonpayable internal ERC20.sol:1
_afterTokenTransfer nonpayable internal ERC20.sol:1
transferFrom nonpayable public ERC20.sol:1
_spendAllowance nonpayable internal ERC20.sol:1
_beforeTokenTransfer nonpayable internal ERC20.sol:1
decimals view public ERC20.sol:1
_burn nonpayable internal ERC20.sol:1
_approve nonpayable internal ERC20.sol:1
decreaseAllowance nonpayable public ERC20.sol:1
allowance view public ERC20.sol:1
totalSupply view public ERC20.sol:1
increaseAllowance nonpayable public ERC20.sol:1
(default) nonpayable public ERC20.sol:1
approve nonpayable public ERC20.sol:1
ERC20Burnable (ERC20Burnable.sol:1)
is ERC20, IERC20Metadata, IERC20, Context
burnFrom nonpayable public ERC20Burnable.sol:1
burn nonpayable public ERC20Burnable.sol:1
Context (Context.sol:1)
_msgSender view internal Context.sol:1
_msgData view internal Context.sol:1
Strings (Strings.sol:1)
toHexString pure internal Strings.sol:1
toHexString pure internal Strings.sol:1
toHexString pure internal Strings.sol:1
toString pure internal Strings.sol:1
Math (Math.sol:1)
max pure internal Math.sol:1
log256 pure internal Math.sol:1
log256 pure internal Math.sol:1
log10 pure internal Math.sol:1
log10 pure internal Math.sol:1
ceilDiv pure internal Math.sol:1
average pure internal Math.sol:1
log2 pure internal Math.sol:1
log2 pure internal Math.sol:1
mulDiv pure internal Math.sol:1
mulDiv pure internal Math.sol:1
sqrt pure internal Math.sol:1
sqrt pure internal Math.sol:1
min pure internal Math.sol:1
Pausable (Pausable.sol:1)
is Context
_pause nonpayable internal Pausable.sol:1
_unpause nonpayable internal Pausable.sol:1
(default) nonpayable internal Pausable.sol:1
_requireNotPaused view internal Pausable.sol:1
_requirePaused view internal Pausable.sol:1
paused view public Pausable.sol:1
IERC20 (IERC20.sol:1)
balanceOf view external IERC20.sol:1
totalSupply view external IERC20.sol:1
transfer nonpayable external IERC20.sol:1
allowance view external IERC20.sol:1
approve nonpayable external IERC20.sol:1
transferFrom nonpayable external IERC20.sol:1
IERC20Metadata (IERC20Metadata.sol:1)
is IERC20
name view external IERC20Metadata.sol:1
symbol view external IERC20Metadata.sol:1
decimals view external IERC20Metadata.sol:1
Public Send Warning Call Warning Constant Internal External PAYABLE

Image 1. LeisureMeta Token call graph

3. VERSION HISTORY

Version	Date	Status/Change	Created by
1.0	*Feb 07, 2023*	Public Report	Verichains Lab

Table 4. Report versions history