verichains

*SECURITY AUDIT OF*

# LUNA RUSH TOKEN SMART CONTRACT


**Public Report**

*Jan 05, 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 Jan 05, 2022. We would like to thank the Luna Rush 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 Luna Rush Token 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 Luna Rush Token Smart Contract

Luna Rush is an idle RPG game based on blockchain technology. You can fight other players, team up with friends, win a tournament and earn money with your strategy and luck.

Summon your Warriors, TRAIN them to become powerful heroes, or convert them into Spirit material for EVOLVING.

Luna Rush is also a multiplayer RPG NFT GAME that lets the user engage in the combat arena and profit from battles.

## 1.2. Audit scope

This audit focused on identifying security flaws in code and the design of the Luna Rush Token Smart Contract.

It was conducted on commit ea8a2e388a54278f42e080272ea93b96baae33d9 from git repository *https://bitbucket.org/lunarush/contracts*.

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

| SHA256 SUM | FILE |
|---|---|
| **dd56e7cdc79c6f4e59d0d03af47e5b93d6e67e8945d41237ee94e223a97fe88e** | LUS.sol |

## 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

This table lists some properties of the audited Luna Rush Token Smart Contract (as of the report writing time).

| PROPERTY | VALUE |
|---|---|
| **Name** | Luna Rush Token |
| **Symbol** | LUS |
| **Decimals** | 18 |
| **Total Supply** | 350,000,000 ($x10^{18}$)<br>Note: the number of decimals is 18, so the total representation token will be 350,000,000 or 350 million. |

*Table 2. The Luna Rush Token Smart Contract properties*

Luna Rush Token Smart Contract is ERC20 token contract which is extended from OpenZeppelin ERC20 contract.

## 2.2. Findings

During the audit process, the audit team found no vulnerability in the given version of Luna Rush Token Smart Contract.

# APPENDIX

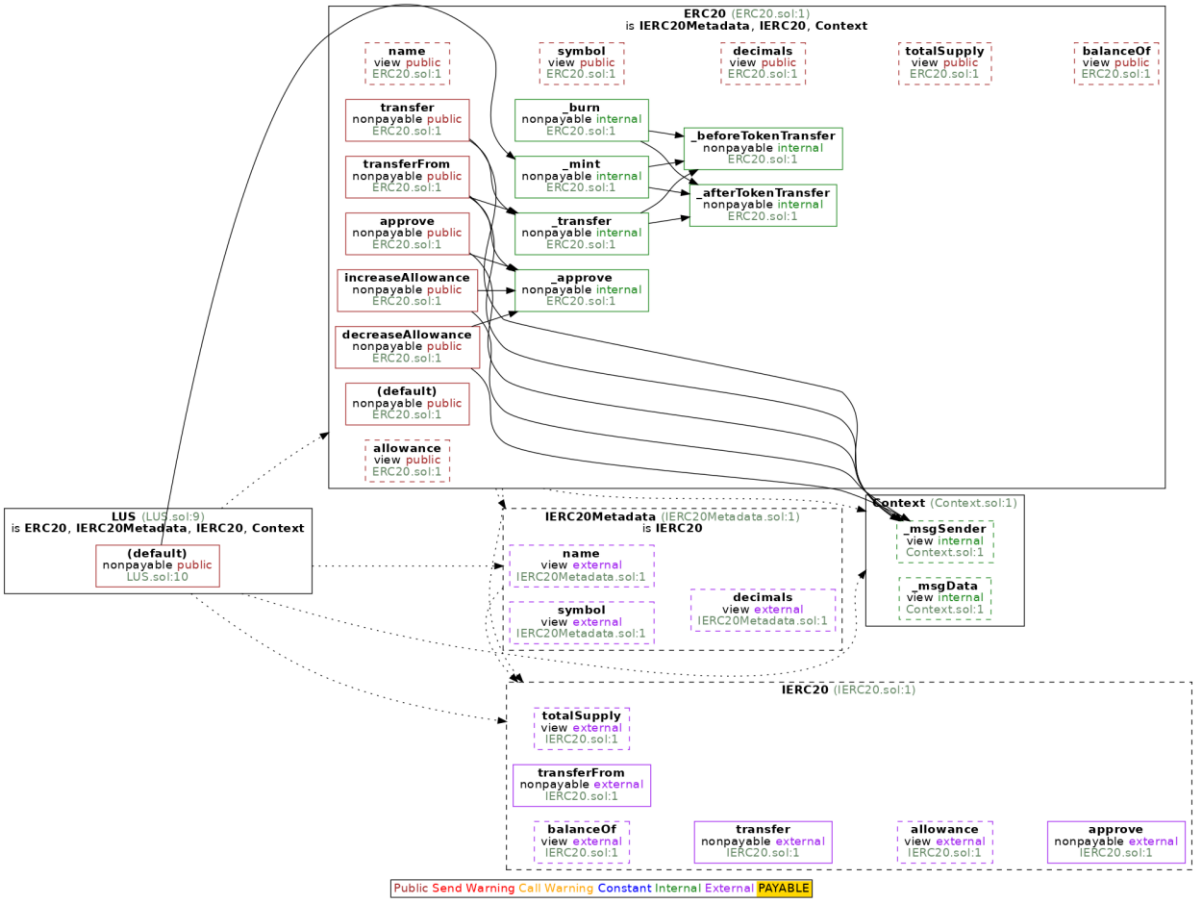


*Image 1. Luna Rush Token Smart Contract call graph*

# 3. VERSION HISTORY

| Version | Date | Status/Change | Created by |
|---|---|---|---|
| **1.0** | *Dec 16, 2021* | Public Report | Verichains Lab |
| **1.1** | *Jan 05, 2022* | Public Report | Verichains Lab |

*Table 3. Report versions history*