Limestone ERC20 Token Smart Contract
Security Audit Report

July 14, 2020

Table Of Contents

Executive Summary

Limestone Network Pte Ltd requested a security audit of the Limestone ERC20 Token smart contract by Taka Security. The security audit focused on verifying that the token contract fully adheres to the ERC20 token standard. During the security audit performed by Taka Security on July 13/14 2020 no issues were discovered. The Limestone ERC20 Token smart contract is fully compliant with the ERC20 token standard.

Audit Overview

Scope

Git repo	`https://github.com/limestone-network/limex`
Git commit	`a9ee9098ce3e997796fc19cd62e67438257a10f0`
Compiler version	0.6.2
Mainnet address	`0x400b1d8a7dd8C471026B2c8CBe1062b27d120538`

Review Methodology

During an audit Taka Security will execute Ethereum security analysis tools, as well as perform a thorough manual review. The manual review will focus on finding security related issues, as well as flagging bad practices or inefficient designs. If a specification is provided Taka Security will verify it reflects the implementation. Each issue found will be written into a separate finding in the report.

Findings Resolution

After the initial report has been sent to the client, it is up to the client to update the source code to resolve the reported findings. Once client has provided the updated source code to Taka Security, each resolved finding will be updated accordingly with a short description of the applied code changes.

Findings Severities

Each finding is assigned one out of four severities: low, medium, high, or critical, The severity depends on the impact of the finding, as well as the likelihood of the finding, each also receiving one of the four severities. The impact depends on the consequences of the finding being exploited/triggered. The likelihood takes into account malicious actors deliberately exploiting the finding, as well as users inadvertently triggering the finding.

Limitations

Security auditing cannot uncover all existing vulnerabilities: even a contract in which no vulnerabilities are found during the audit is not a guarantee of a secure smart contract. However, auditing enables the discovery of vulnerabilities that were overlooked during development and areas where additional security measures are necessary.

Project Overview

The Limestone ERC20 Token smart contract implements an ERC20 token built on top of the OpenZeppelin `ERC20.sol` smart contract. Furthermore, the token contract is pausable, and tokens can be minted or burned.

Token Info

Token standard(s)	ERC20
Name	Limestone
Symbol	LIMEX
Decimals	8
Max total supply	no
Pausable	yes
Mintable	yes
Burnable	yes

Roles

The token contract adds three functions (`mint`, `burn`, `pause`) that can only be called by an account that has been granted the correct role. To implement Role-Based Access Control, the token contract inherits from OpenZeppelin `AccessControl.sol`. Three custom roles are created at deployment, and each of these is granted to the deployer. Furthermore, the `DEFAULT_ADMIN_ROLE` is also granted to the deployer. The four granted roles and their power(s) are:

MINTER_ROLE Can mint tokens to any account by calling `mint`.

BURNER_ROLE Can burn tokens of any account by calling `burn`.

PAUSER_ROLE Can pause the token contract by calling `pause`.

- Note that pausing is irreversible as there is no unpause function.
- When the contract is paused no transfers of tokens, minting of tokens, or burning of tokens is possible.

DEFAULT_ADMIN_ROLE Can grant/revoke any of the above three roles, as well as the `DEFAULT_ADMIN_ROLE` itself, by calling `grantRole` and `revokeRole`, respectively.

Any account that has been granted any of the above roles can at any time renounce its role by calling `renounceRole`.

Findings

This section lists the issues found during the audit of the Limestone ERC20 Token smart contract.

Taka Security did not find any issues.

Disclaimer

UPON REQUEST BY LIMESTONE NETWORK PTE LTD, TAKA SECURITY AGREES TO MAKE THIS AUDIT REPORT PUBLIC. THE CONTENT OF THIS AUDIT REPORT IS PROVIDED "AS IS", WITHOUT REPRE-SENTATIONS AND WARRANTIES OF ANY KIND, AND TAKA SECURITY DISCLAIMS ANY LIABILITY FOR DAMAGE ARISING OUT OF, OR IN CONNECTION WITH, THIS AUDIT REPORT. COPYRIGHT OF THIS REPORT REMAINS WITH TAKA SECURITY.

Contact:

https://takasecurity.com
contact@takasecurity.com