Decentraland

Decentraland Collections Bridge Security Analysis

by Pessimistic

This report is private

10 September, 2021

Abstract

In this report, we consider the security of Collections Bridge smarts contracts of Decentraland project. Our task is to find and describe security issues in the smart contracts of the platform.

Disclaimer

The audit does not give any warranties on the security of the code. One audit cannot be considered enough. We always recommend proceeding with several independent audits and a public bug bounty program to ensure the security of smart contracts. Besides, security audit is not an investment advice.

Summary

In this report, we considered the security of Decentraland Collections Bridge smart contracts. We performed our audit according to the procedure described below.

The audit showed an Overpowered owner issue and one code quality issue of low severity.

The overall code quality is high.

General recommendations

We recommend limiting the powers of the owner.

Project overview

Project description

For the audit, we were provided with the pull request on a public GitHub repository. In this pull request, the bridge feature was added to the project.

The scope of the audit included only the following files:

- **contracts/bridge/***
- **contracts/validators/***
- **contracts/collections/v2/ERC721BridgedCollection.sol**

The project has a documentation, the code base has comments and detailed NatSpecs.

All the tests pass, the coverage is 100%.

Procedure

In our audit, we consider the following crucial features of the code:

1. Whether the code is secure.
2. Whether the code corresponds to the documentation (including whitepaper).
3. Whether the code meets best practices.

We perform our audit according to the following procedure:

- Automated analysis
    - We scan project’s code base with automated tool Slither.
    - We manually verify (reject or confirm) all the issues found by tools.
- Manual audit
    - We manually analyze code base for security vulnerabilities.
    - We assess overall project structure and quality.
- Report
    - We reflect all the gathered information in the report.

Manual analysis

The contracts were completely manually analyzed, their logic was checked. Besides, the results of the automated analysis were manually verified. All the confirmed issues are described below.

Critical issues

Critical issues seriously endanger smart contracts security. We highly recommend fixing them.

The audit showed no critical issues.

Medium severity issues

Medium issues can influence project operation in current implementation. We highly recommend addressing them.

Overpowered owner

The admin role of **ERC721BridgedCollection** contract can burn tokens or mint them to an arbitrary address. The admin role is considered to be controlled by a contract. However, the role is assigned by the owner and thus can be assigned to any address.

Therefore, there are scenarios that may result in undesirable consequences for the project and its users, e.g., if the owner's private keys become compromised.

We recommend designing contracts in a trustless manner or using proper key management system, e.g., multisig.

Low severity issues

Low severity issues can influence project operation in future versions of code. We recommend taking them into account.

Code quality

Consider using mappings with `boolean` type values to store validity status in **ERC721CollectionV1Validator** contract at line 10 and **ERC721CollectionV2Validator** contract at line 11.

This analysis was performed by Pessimistic:

Evgeny Marchenko, Senior Security Engineer
Vladimir Tarasov, Security Engineer
Boris Nikashin, Analyst
Irina Vikhareva, Project Manager

10 September, 2021