Security and Design audit
Decentraland Burner Contract

03/06/2019

Agustín Aguilar

Introduction

The Decentraland Team requested the review of the project on the repository *https://github.com/decentraland/aux-contracts/tree/master/burner*, the commit referenced for this audit is 0x7aa82fc37e70989577b9e6d86f7152f76dfe5195.

The audited contracts are:

- DecentralandBurner.sol Allows any Ethereum address to burn the mana tokens received in this address.

Issues

Low severity

1 - Burn front running by the owner

The owner of the burner contract could choose to withdraw the MANA tokens without calling the *burn()* method.

Proposed Solution:

Internally call *burn()* before executing any command using *execute(). (See Issue 3)*

Notes

2 - Discarded revert message on execute method

If a proxied call using the method *execute()* fails, the revert message is "Call error", consider forwarding the real revert message contained in the *response* variable.

3 - Avoid calling burn() if current balance is zero

The MANA Token contract fails if the burn method is called with _value zero, avoid the call to burn() if the result of *balanceOf(address(this))* is zero.

Final thoughts

The burner contract is well written, documented, and have unit testing with good coverage; no critical vulnerabilities or bugs were found on DecentralandBurner.sol.

June 2019, Madrid, Spain - by Agustin Esteban Aguilar