Smart Contract Audit
Sovryn CSOV Token

Franklin Richards

15th January 2021

Index

Note: Some threat levels or headings might be empty if there is no vulnerability/updates/suggestions found.

Introduction

The contract audited here and the supporting contracts is/are:
https://github.com/DistributedCollective/Genesis-Sale/blob/5c7d879/contracts/main/CSOVToken.sol

and was shared by Sovryn for auditing purposes while working with them.

Based on the audit, we were able to find 0 High threats, 0 Medium threat, and 0 Low threat with some other changes in the optimization, readability, typos, and comments section.

High Threats

1. None

Medium Threats

1. None

Low Threats

1. None

Optimization & Readability

1. No need to import IERC20 if ERC20 is imported from Openzeppelin at line 7.

Typo's & Comments

1. Many functions are without any comments. Please make sure every function follows the NatSpec Format.

Suggestions

1. The saleClosure() can only be used once to close the sale, then the if condition is useless and also, no need to pass the bool parameter, as we could directly pass `true` to the variable.

2. The setSaleAdmin() could completely be removed, if we use the constructor to set the saleAdmin parameter, and mint the tokens directly to saleAdmin's address if it is known at the time of deployment of the contract. Best to remove complexity as much as possible.

3. Instead of onlyAllowed() custom function which we created and due to which we had to edit the transfer() and transferFrom(), we could use openzeppelin's _beforeTokenTransfer() which we are anyway inheriting. Thus, we won't have to edit the transfer and transferFrom as well.