REALPrivateSale.sol

* **Owner Role / Centralized Risk**

Only the owner role has authority over the functions shown below. Any compromise to the \_owner account may allow the hacker to take advantage of this authority.

Text

Description automatically generated

* **Recommendation**

The risk describes the current project design and potentially makes iterations to improve the security operation and level of decentralization, which in most cases cannot be resolved entirely at the present stage. We advise the client to carefully manage the privileged account's private key to avoid any potential risks of being hacked. In general, we strongly recommend centralized privileges or roles in the protocol be improved via a decentralized mechanism or smart-contract-based accounts with enhanced security practices, e.g., multi-signature wallets.

REALPublicSale.sol

* **Owner Role / Centralized Risk**

Only the owner role has authority over the functions shown below. Any compromise to the \_owner account may allow the hacker to take advantage of this authority.

Text

Description automatically generated

* **Recommendation**

The risk describes the current project design and potentially makes iterations to improve the security operation and level of decentralization, which in most cases cannot be resolved entirely at the present stage. We advise the client to carefully manage the privileged account's private key to avoid any potential risks of being hacked. In general, we strongly recommend centralized privileges or roles in the protocol be improved via a decentralized mechanism or smart-contract-based accounts with enhanced security practices, e.g., multi-signature wallets.

REALSeedSale.sol

* **Owner Role / Centralized Risk**

Only the owner role has authority over the functions shown below. Any compromise to the \_owner account may allow the hacker to take advantage of this authority.

Text

Description automatically generated

* **Recommendation**

The risk describes the current project design and potentially makes iterations to improve the security operation and level of decentralization, which in most cases cannot be resolved entirely at the present stage. We advise the client to carefully manage the privileged account's private key to avoid any potential risks of being hacked. In general, we strongly recommend centralized privileges or roles in the protocol be improved via a decentralized mechanism or smart-contract-based accounts with enhanced security practices, e.g., multi-signature wallets.

RealTeamAndAdvisor.sol

* **Owner Role / Centralized Risk**

Only the owner role has authority over the functions shown below. Any compromise to the \_owner account may allow the hacker to take advantage of this authority.

Text

Description automatically generated

* **Recommendation**

The risk describes the current project design and potentially makes iterations to improve the security operation and level of decentralization, which in most cases cannot be resolved entirely at the present stage. We advise the client to carefully manage the privileged account's private key to avoid any potential risks of being hacked. In general, we strongly recommend centralized privileges or roles in the protocol be improved via a decentralized mechanism or smart-contract-based accounts with enhanced security practices, e.g., multi-signature wallets.

REALREALM-token.sol

# **Medium severity issues**

* **Initial Token Distribution / Centralization**

In the constructor function, the deployer is minting tokens for multiple hardcoded addresses. This could be a centralization risk, the deployer can distribute those tokens without obtaining the consensus of the community.



* **Recommendation**

We recommend the team to be transparent regarding the initial token distribution process, and the team shall make enough efforts to restrict the access of the private key, We also advise the client to adopt Multisig, Timelock, and/or DAO in the project to manage the specific account in this case.

* **Owner Role / Centralized Risk**

Only the owner role has authority over the functions shown below. Any compromise to the \_owner account may allow the hacker to take advantage of this authority.

Graphical user interface, text, application, chat or text message

Description automatically generated

Graphical user interface, text, application

Description automatically generated

* **Recommendation**

The risk describes the current project design and potentially makes iterations to improve the security operation and level of decentralization, which in most cases cannot be resolved entirely at the present stage. We advise the client to carefully manage the privileged account's private key to avoid any potential risks of being hacked. In general, we strongly recommend centralized privileges or roles in the protocol be improved via a decentralized mechanism or smart-contract-based accounts with enhanced security practices, e.g., multi-signature wallets.

# **Low severity issues**

* **Unchecked Value of ERC-20 transfer()**

**In function** incurDebt**,the external call to transfer of ERC20 contracts and the return value is not checked in either case.**

Graphical user interface, text, application

Description automatically generated

* **Recommendation**

We advise the team to use SafeERC20 or make sure that the value returned from **transfer**()' is checked.