AUDITMOS

Secure your space

TERRALAND

audit / code review report

November 4, 2021

TABLE OF CONTENTS

contact@auditmos.com

AUDITMOS

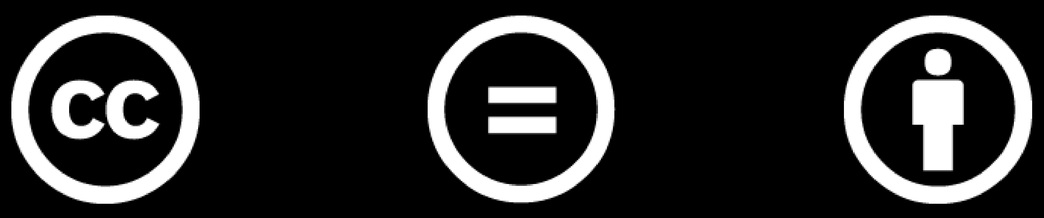
Secure your space

TERRALAND

audit / code review report

November 4, 2021

LICENSE



contact@auditmos.com

AUDITMOS

Secure your space

TERRALAND

audit / code review report

November 4, 2021

DISCLAIMER

contact@auditmos.com

AUDITMOS

Secure your space

TERRALAND

audit / code review report

November 4, 2021

APPROACH AND METHODOLOGY

PURPOSE

1. Determine the correct operation of the protocol, according to the design specification.
2. Identify possible vulnerabilities that could be exploited by an attacker.
3. Detect errors in the smart contract that could lead to unexpected behavior.
4. Analyze whether best practices were followed during development.
5. Make recommendations to improve security and code readability.

CODEBASE

Repository	https://github.com/FCQPlatform-com/terra-fcq
Branch	master
Commit hash	c76f1aa67a9cb2309034ee642594f9fe9a390a1e

METHODOLOGY

1. Reading the available documentation and understanding the code.
2. Doing automated code analysis and reviewing dependencies.
3. Checking manually source code line by line for security vulnerabilities.
4. Following guildlines and recommendations.
5. Preparing this report.

AUDITMOS

Secure your space

TERRALAND

audit / code review report

November 4, 2021

DESCRIPTION

Issues Categories:

Severity	Description
CRITICAL	vulnerability that can lead to loss of funds, failure to recover blocked funds, or catastrophic denial of service.
HIGH	vulnerability that can lead to incorrect contract state or unpredictable operation of the contract.
MEDIUM	failure to adhere to best practices, incorrect usage of primitives, without major impact on security.
LOW	recommendations or potential optimizations which can lead to better user experience or readability.

Each issue can be in the following state:

State	Description
PENDING	still waiting for resolving
ACKNOWLEDGED	know but not planned to resolve for some reasons
RESOLVED	fixed and deployed

contact@auditmos.com

AUDITMOS

Secure your space

TERRALAND

audit / code review report

November 4, 2021

FINDINGS

Finding	Severity	Status
#1 - Better gas optimization for MEMBERS	LOW	PENDING
#2 - Fees are not enforced in any way	LOW	PENDING
#3- Update terraland_token_address	LOW	PENDING
#4- Use plural action name	LOW	PENDING
#5- Better testing and code coverage	LOW	PENDING

contact@auditmos.com

AUDITMOS

Secure your space

TERRALAND

audit / code review report

November 4, 2021

#1 - BETTER GAS OPTIMIZATION FOR MEMBERS

For gas optimization it would be better to store CanonicalAddr instead of String.

It is recommended for MEMBERS as it is is frequently changed and store lots of data.

Severity	Status
LOW	PENDING

RECOMMENDATION

Please change the current code:

```
pub const MEMBERS: Map<&Addr, Member> = Map::new("members");
```

to this one below:

```
pub const MEMBERS: Map<CanonicalAddr, Member> = Map::new(“members”);
```

PROOF OF SOURCE

https://github.com/FCQPlatform-com/terra-fcq/blob/c76f1aa67a9cb2309034ee642594f9fe9a390a1e/contracts/airdrop/src/state.rs#L40

contact@auditmos.com

AUDITMOS

Secure your space

TERRALAND

audit / code review report

November 4, 2021

#2 - FEES ARE NOT ENFORCED IN ANY WAY

In execute_claim function comment mention that sender has to pay 1 UST to claim but it is not enforced in any way.

Severity	Status
LOW	PENDING

RECOMMENDATION

Fee for claim operation might be not obligatory if not set in constructor and/or updat_config function.

PROOF OF SOURCE

https://github.com/FCQPlatform-com/terra-fcq/blob/c76f1aa67a9cb2309034ee642594f9fe9a390a1e/contracts/airdrop/src/contract.rs#L188

contact@auditmos.com

TERRALAND

audit / code review report

November 4, 2021

#3 - UPDATE TERRALAND_TOKEN_ADDRESS

Severity	Status
LOW	PENDING

In update_config you don't allow to update terraland_token address.

Whether this is intentional?

RECOMMENDATION

This is just a thing to consider.

PROOF OF SOURCE

https://github.com/FCQPlatform-com/terra-fcq/blob/c76f1aa67a9cb2309034ee642594f9fe9a390a1e/contracts/airdrop/src/msg.rs#L24

TERRALAND

audit / code review report

November 4, 2021

#4 - USE PLURAL ACTION NAME

Severity	Status
LOW	PENDING

It might be better to use plural action name in some cases to make the code of smart contract more readable.

RECOMMENDATION

Please change the current code:

```
Ok(Response::new()
.add_attribute("action", "register_member")
.add_attribute("sender", info.sender))
```

to this one below:

```
Ok(Response::new()
.add_attribute("action", "register_members")
.add_attribute("sender", info.sender))
```

PROOF OF SOURCE

https://github.com/FCQPlatform-com/terra-fcq/blob/c76f1aa67a9cb2309034ee642594f9fe9a390a1e/contracts/airdrop/src/contract.rs#L177

TERRALAND

audit / code review report

November 4, 2021

#5 - BETTER TESTING AND CODE COVERAGE

Severity	Status
LOW	PENDING

In the current contract implementation not all functions with restricted access to contract owner are covered by tests. It might lead to some unpredictable behaviour during this function call by some address which is not owner address.

It is highly recommended to test all of the functions which should have restriceted access and/or should be called only by contract owner.

RECOMMENDATION

Output name collisions in test target.

For all contracts in example directory you produce schema binary. It might be better to rename it. For e.g rename vesting/example/schema.rs to vesting_schema.rs.

PROOF OF SOURCE

None

contact@auditmos.com

auditmos.com

Secure your space

contact@auditmos.com