Nebula Protocol - Emergency Vesting Contract - Audit Report

Prepared for Nebula Protocol, 15 June 2022

Table of Contents

Introduction

SCV was engaged by Nebula Protocol to assist in identifying security threats and vulnerabilities that have the potential to affect their security posture. Additionally, SCV will assist the team in understanding the risks and identifying potential mitigations.

Scope

SCV performed the security assessment on the following codebase:

- https://github.com/nebula-protocol/terra-emergency-alloc-vesting

Code freeze hash: *0e7798d8f07000e7d862d4c5a7b3d61f236660ab*

Remediation were applied into the following PR:

- https://github.com/nebula-protocol/terra-emergency-alloc-vesting/pull/1

Methodologies

SCV performs a combination of automated and manual security testing based on the scope of testing. The testing performed is based on the extensive experience and knowledge of the auditor to provide the greatest coverage and value to Nebula Protocol. Testing includes, but is not limited to, the following:

- Understanding the application and its code base purpose;
- Deploying SCV in-house tooling to automate dependency analysis and static code review;
- Analyse each line of the code base and inspect application security perimeter;
- Review underlying infrastructure technologies and supply chain security posture;

Code Criteria and Test Coverage

SCV used a scale from **0** to **10** that represents how **SUFFICIENT(6-10)** or **NOT SUFFICIENT(0-5)** each code criteria was during the assessment:

Criteria	Status	Scale Range	Notes
Provided Documentation	**Sufficient**	7-8	N\A
Code Coverage Test	**Sufficient**	7-8	N\A
Code Readability	**Sufficient**	7-8	N\A
Code Complexity	**Sufficient**	7-8	N\A

Vulnerabilities Summary

	Title and Summary	Risk	Status
1	Explicitly define vesting asset denom as static variable	**Low**	**Remediated**
2	English word typos found in the codebase	**Informational**	**Remediated**
3	Potential division by zero case can cause a Panic	**Informational**	**Remediated**

Detailed Vulnerabilities

1. Explicitly define vesting asset denom as static variable

Likelihood	Impact	Risk
Rare	Low	**Low**

Description

In the file */src/contract.rs#51*, there is a check to ensure the received coins from the contract matches with the specified denom defined during in the instantiation *(msg.denom)*.

This can be problematic because there is no validation when defining a denom. As example, it could be mistaken defined as `ULUNA` rather than `uluna`.

Recommendations

Consider explicitly define the denom as a *const* since a single denom is expected.

2. English word typos found in the codebase

Likelihood	Impact	Risk
Rare	Informational	**Informational**

Description

The codebase contains typos in comments that can affect overall code quality and makes it more difficult to understand.

- `paramters` at `/src/state#31` should be `parameters`;

Also, in the `/src/state#68` the naming convention of the `VESTING_INFO MAP` refers to *loan_info* where there is no such loan functionality.

Recommendations

Rename words to the correct values.

3. Potential division by zero case can cause a Panic

Likelihood	Impact	Risk
Rare	Informational	**Informational**

Description

In the */src/contract.rs#93* there is no check to ensure the `vesting.amount` is valid to avoid division by zero case from the instantiation data. Any error or typo made during the instantiation could cause the contract to panic and might result in the funds to be locked.

SCV notes that, this edge case would be extreme unlikely to happen.

Recommendations

Ensure there is a check `.is_zero()` before performing arithmetic division operations.

Document control

Document changes

Version	Date	Name	Changes
0.1	2022-06-14	Vinicius Marino	Initial report
0.2	2022-06-15	Vinicius Marino	Team communication and Pre-Release
1.0	2022-06-15	Vinicius Marino	Document Release

Document contributors

Name	Role	Email address
Vinicius Marino	Security Specialist	vini@scv.services

Appendices

Appendix A: Report Disclaimer

The content of this audit report is provided “As is”, without representations and warranties of any kind.

The author and their employer disclaim any liability for damage arising out of, or in connection with, this audit report.

Appendix B: Risk assessment methodology

A qualitative risk assessment is performed on each vulnerability to determine the impact and likelihood of each.

Risk rate will be calculated on a scale. As per criteria Likelihood vs Impact table below:

Impact \ Likelihood	Rare	Unlikely	Possible	Likely
Critical	Medium	High	Critical	Critical
Severe	Low	Medium	High	High
Moderate	Low	Medium	Medium	High
Low	Low	Low	Low	Medium
Informational	Informational	Informational	Informational	Informational

LIKELIHOOD:

- **Likely**: likely a security incident will occur;
- **Possible**: It is possible a security incident can occur;
- **Unlikely**: Low probability a security incident will occur;
- **Rare**: In rare situations, a security incident can occur;

IMPACT:

- **Critical**: May cause a significant and critical impact;
- **Severe**: May cause a severe impact;
- **Moderate**: May cause a moderated impact;
- **Low**: May cause low or none impact;
- **Informational**: May cause very low impact or none.


SCV