Terra Core 2.0

Prepared for Terra, 24 May 2022

Table of Contents

Introduction

SCV was engaged by Terra 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.

Terra is launching a new blockchain *Terra 2.0* that is completely independent from the original legacy chain now called *Terra Classic*.

Terra 2.0 implementation consist of Cosmos SDK and native modules on top of Tendermint and CosmWasm (wasmd).

Scope

SCV performed the security assessment on the following Terra codebase:

- https://github.com/terra-money/core
- CodeHash: *d9be864deaa2367412041760d456ca0f444bc1ee*

Remediations were successfully applied into the following pull request:

- https://github.com/terra-money/core/pull/12

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 Terra. 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;
- Analysis of each line of the code base and inspect application perimeter;
- Review underlying infrastructure technologies and supply chain security posture;

Code Criteria and Test Coverage

SCV is using a scale from **0** to **10** that represents how *SUFFICIENT(6-10)* or *NOT SUFFICIENT(0-5)* each code criteria was assessed:

Criteria	Status	Scale Range	Notes
Provided Documentation	**Sufficient**	7-8	N\A
Code Coverage Test	**Sufficient**	6-8	N\A
Code Readability	**Sufficient**	8-9	N\A
Code Complexity	**Sufficient**	8-9	N\A

Vulnerabilities Summary

	Title and Summary	Risk	Status
1	Vesting auto-stake does not enforce max validator commissions	**Medium**	**Remediated**
2	Wrong chain name references used as placeholder	**Low**	**Remediated**
3	Lack of mempool prioritization and TTL	**Informational**	**Acknowledged**
4	CoinType can affect Interchain composability and UX	**Informational**	**Acknowledged**

Detailed Vulnerabilities

1. Vesting auto-stake does not enforce max validator commissions

Likelihood	Impact	Risk
Possible	Moderate	**Medium**

Description

In the `enforceStakingForVestingTokens` function, vesting tokens would be auto-staked across the validator set. However, the logic does not enforce key parameters such as, `max commission` and `max validators`. These parameters can be enforced into the logic using the SDK.

Recommendations

It's recommended to limit the `max commission` each validator can have for receiving the auto-staking. Also enforcing the `max validators` that appears to be 100 for all the set.

2. Wrong chain name references used as placeholder

Likelihood	Impact	Risk
Possible	Low	**Low**

Description

In the file `/app/app.go#L648` there is a wrong hardcoded reference name convention that could cause major problems during chain upgrades.

Recommendations

Ensure all placeholders and unnecessary code are removed and any word used as reference are replaced with it's correct value.

3. Lack of mempool prioritization and TTL

Likelihood	Impact	Risk
Likely	Informational	**Informational**

Description

Latest Tendermint release *(v0.35)* contains important security features that could be crucial when dealing with edge cases such as network congestion and spamming targeted attacks.

In the new release, Tendermint added mempool TTL *(time-to-live)* that once reached, automatically removes a particular transaction, preventing transactions from being stuck in the mempool and filling the entire mempool allocation. Transactions flow can also be designed around prioritization logic rather than FIFO *(first-in-first-out)* if necessary.

Recommendations

After a comprehensive test, Terra should implement the new Tendermint *(v0.35)* version or cherry pick it at later stage since there is not a consensus breaking change affecting the current implemented version.

4. CoinType can affect Interchain composability and UX

Likelihood	Impact	Risk
Likely	Informational	**Informational**

Description

Terra's address variation follows the same *Terra Classic* variation *CoinType (330)*. Besides the `CoinType` poses no security vulnerability, it can affect interchain composability and user experience when dealing with multiple chains.

Recommendations

It's recommended to use *CoinType 118* in order to apply the standardization for Cosmos chains. Additionally, an address prefix should also be taken into consideration to complete differentiate `Terra Classic` from `Terra`.

Document control

Document changes

Version	Date	Name	Changes
0.1	2022-05-22	Vinicius Marino	Initial report
0.2	2022-05-23	Vinicius Marino	Team communication and Pre-Release
1.0	2022-05-24	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