Eris Protocol - Amplified Staking - Audit Report

Prepared for Eris Protocol, 23 September 2022

Table of Contents

Introduction

SCV was engaged by Eris 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/erisprotocol/contracts-terra-classic
- Code Freeze: *4c866a74ea8033c804fffc5698a8bf3b735648ac*
- https://github.com/erisprotocol/contracts-terra
- Code Freeze: *218b61fd252e3ab200fddb5572d1ef91e0708e30*

Remediations were applied into several commits up to the following hash commit:

- Code Freeze *aefbeb38b69018adaac3a4e45f0160affdcaf51a* (contracts-terra)
- Code Freeze *211e47f2772410433e946585c649cfcaad8eb314* (contracts-terra-classic)

SCV notes that the Terra Classic Tax Burn component were also part of remedation and audit scope:

- https://github.com/erisprotocol/contracts-terra-classic/tree/feature/burn-tax

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 Eris 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**	6-7	N/A
Code Coverage Test	**Sufficient**	7-8	N/A
Code Readability	**Sufficient**	6-8	N/A
Code Complexity	**Sufficient**	6-7	N/A

Vulnerabilities Summary

	Title and Summary	Risk	Status
1	Additional validations necessary	**Low**	**Remediated**
2	Ensure CW20 minter is supplied	**Low**	**Remediated**
3	add_validator does not properly validator address	**Low**	**Remediated**
4	Remove unused commented code blocks	**Informational**	**Remediated**
5	Reply entry-point returns incorrect error	**Informational**	**Remediated**

Detailed Vulnerabilities

1. Additional validations necessary

Likelihood	Impact	Risk
Unlikely	Low	**Low**

Description

The `instantiate` functions in `terra:contracts/hub/src/execute.rs:32` and `classic:contracts/hub/src/execute.rs:33` are lacking validations which may lead to potential misconfigurations. `msg.validators` is a vector of validator addresses, these addresses should be checked to ensure they are valid and that the vector does not contain duplicate values.

In addition, in `classic:contracts/hub/src/execute.rs:64` is lacking validation on `msg.swap_config`. This swap config is directly saved without proper validation. There should be checks that confirm that the `msg.swap_config` does not contain duplicates and that each swap router contract address is validated.

The `update_config` function in `classic:contracts/hub/src/execute.rs:796` does not confirm that the vector of `SwapConfig` is deduplicated.

Recommendations

We recommend implementing the validations mentioned above to ensure that no misconfigurations could be introduced during the instantiation.

2. Ensure CW20 minter is supplied

Likelihood	Impact	Risk
Unlikely	Low	**Low**

Description

The `instantiate` function in `terra:contracts/token/src/lib.rs:13` and `classic:contracts/token/src/lib.rs:13` directly passes the `InstantiateMsg` to the `cw20_instantiate` function but it does not ensure that `msg.mint` is `Some`. If this value is `None` it will prevent vital operations in the contract and will not allow for new assets to be minted. We classify this as low impact because it required the instantiator to make introduce this misconfiguration which is unlikely to occur.

Recommendations

We recommend ensuring that `msg.mint` is `Some` before passing the msg to `cw20_instantiate`.

3. add_validator does not properly validator address

Likelihood	Impact	Risk
Unlikely	Low	**Low**

Description

The `add_validator` functions in `terra:contracts/hub/src/execute.rs:632` and `classic:contracts/hub/src/execute.rs:678` does not properly validate the validator address being added to `state.validators`. Even though the owner is the only address that may call this function, it is best practice to validate the address before saving to avoid errors that this may cause in other functions.

Recommendations

We recommend performing an address validation on validator before adding the string to validators in both the terra and terra-classic contracts.

4. Remove unused commented code blocks

Likelihood	Impact	Risk
Rare	Informational	**Informational**

Description

The codebase contains unused code blocks that are commented. It is best practice to remove this code to clean the code base and improve its readability and maintainability.

- *terra*:contracts/hub/src/execute.rs:371-375
- *terra*:contracts/hub/src/contract.rs:132-139
- *classic*:contracts/hub/src/contract.rs:144-152

Recommendations

We recommend removing the instances mentioned above before the code is deployed.

5. Reply entry-point returns incorrect error

Likelihood	Impact	Risk
Unlikely	Informational	**Informational**

Description

The reply entry-point in `terra:contracts/hub/src/contract.rs:140` returns an incorrect error `"invalid reply id: {}; must be 1-3"`. There are only 2 possible reply ids so this error is incorrect and may be misleading for anyone attempting to debug errors.

Recommendations

We recommend updating the error to `"invalid reply id: {}; must be 1-2"` in `terra:contracts/hub/src/contract.rs:140`.

Document control

Document changes

Version	Date	Name	Changes
0.1	2022-09-20	Vinicius Marino	Initial report
0.2	2022-09-21	Vinicius Marino	Team communication and Pre-Release
1.0	2022-09-23	Vinicius Marino	Revisions and 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