Kujira – Governance Contract

Audit Report

Prepared for Kujia, 14 October 2022

Table of Contents

Introduction

SCV was engaged by Kujira 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.

Audit Brief

The Governance contracts for the Kujira blockchain was originally forked from cw-plus. These are broken down into two contracts as per below:

CW3 Multisig:

- cw3-flex-multisig builds on cw3-fixed-multisig, with a more powerful implementation of the cw3 spec. It's a multisig contract backed by a cw4 (group) contract, which independently maintains the voter set.
- Implementation of *max_weight* and a *min_weight* to the contract config, to constrain the total amount of voting power that the membership can contain
- Implementation of an *identity* field to Member, so that members of this voting set can be identified by community members

CW4 Group:

- It handles elected membership, by admin or multisig. It fulfils all elements of the spec, including raw query lookups, and is designed to be used as a backing storage for cw3 compliant contracts.
- The requirement of membership to create proposals is removed, instead replacing it with a deposit requirement;
- Extended the proposal status to respect a *Veto* result, subsequently burning the deposit if these conditions are met.

Scope

SCV performed the security assessment on the following codebase forked from [cw-plus.]

- https://github.com/Team-Kujira/gov
- Code Freeze: *7a5bd13a6376e3b6d4cf7b414c0a1eb7919a6946*

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* or *NOT SUFFICIENT* each code criteria was during the assessment:

Criteria	Status	Notes
Provided Documentation	SUFFICIENT 🟢	N/A
Code Coverage Test	SUFFICIENT 🟢	N/A
Code Readability	SUFFICIENT 🟢	N/A
Code Complexity	SUFFICIENT 🟢	N/A

Vulnerabilities Summary

#	Summary Title	Risk Impact	Status
1	Consider enforcing validation checks on members and max and min weight	**Informational**	**Acknowledged**

Detailed Vulnerabilities

1 – Consider enforcing validation checks on members and max and min weight.

Risk Impact: Informational - **Status**: Acknowledgement

Description

In the *cw-group/src/contract.rs:31* there is no check or validation to ensure the max_weight is greater than min_weight.

SCV also notes that in the identify struct it could be optimised to a min and max length since its a expected input from a keybase PGP fingerprint.

Recommendations

Consider adding the following checks:

1. Ensure *msg.max_weight* is greater than *msg.min_weight*.
2. Expect a min of 16 char and max of 40 char for the *member.identity* PGP fingerprint.

Document control

Version	Date	Approved by	Changes
0.1	13/10/2022	Vinicius Marino	Initial Report
0.2	14/10/2022	Vinicius Marino	Document Pre-Release
1.0	14/10/2022	Vinicius Marino	Revisions and Document Release

Appendices

A. Appendix – 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:

	Rare	Unlikely	Possible	Likely
Critical	**Medium**	**Severe**	**Critical**	**Critical**
Severe	**Low**	**Medium**	**Severe**	**Severe**
Moderate	**Low**	**Medium**	**Medium**	**Severe**
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.

B. Appendix – 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.