AUDIT REPORT

Alliance DAO

Alliance NFT Collection

Prepared by SCV-Security

On 14th May 2024

Table of Contents

Introduction

SCV has been engaged by Alliance DAO to conduct a comprehensive security review with the goal of identifying potential security threats and vulnerabilities within the codebase. The purpose of this audit is to evaluate the security posture of the codebase and provide actionable recommendations to mitigate any identified risks. This report presents an overview of the findings from our security audit, outlining areas of concern and proposing effective measures to enhance the codebase's security.

Scope Functionality

The scope of the audit integrates Eris Amplifier into the Alliance DAO NFT Collection contract. With these changes, rewards are denominated as `ampLUNA`, with the exchange rate determined by Eris Hub.

Submitted Codebase

alliance-nft-collection	
Repository	https://github.com/terra-money/alliance-nft-collection
Commit	`9598d4c60a634884533ef9f87b758a6f7a70a276`
Branch	PR#46

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 Alliance DAO. Testing includes, but is not limited to, the following:

- Understanding the application and its functionality 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

This section provides an evaluation of specific criteria aspects as described below:

- **Documentation:** Evaluating the presence and comprehensiveness of publicly available or provided explanatory information, diagram flowcharts, comments, and supporting documents to enhance code understanding.
- **Coverage:** Evaluating whether the code adequately addresses all necessary cases and scenarios, ensuring that the intended functionality or requirements are sufficiently covered.
- **Readability:** Assessing how easily the code can be understood and maintained, considering factors such as code structure, naming conventions, and overall organisation.
- **Complexity:** Evaluating the complexity of the code, including factors such as, number of lines, conditional statements, and nested structures.

The status of each criteria is categorised as either **SUFFICIENT** or **NOT-SUFFICIENT** based on the audit assessment. This categorisation provides insights to identify areas that may require further attention and improvement.

Criteria	Status	Notes
Documentation	**SUFFICIENT**	Documentation is detailed in `contracts/alliance-nft-collection/README.md`.
Coverage	**SUFFICIENT**	cargo tarpaulin reports a 70.66% coverage.
Readability	**SUFFICIENT**	N/A
Complexity	**SUFFICIENT**	N/A

Findings Summary

Summary Title	Risk Impact	Status
Potential division by zero error when updating rewards	LOW	ACKNOWLEDGED
Incorrect `REWARD_BALANCE` calculation when LST supply is zero	LOW	ACKNOWLEDGED
Edge case when current time equals the mint end time	INFO	ACKNOWLEDGED

Findings Technical Details

1. Potential division by zero error when updating rewards

RISK IMPACT: LOW	STATUS: PENDING

Revision Notes

The team suggests that there are no “active” NFTs left in the contract state.

Description

The `try_update_reward_callback` function in `contracts/alliance-nft-collection/src/contract/execute.rs:188-192` divides the amount of the collected rewards with `NUM_ACTIVE_NFTS` to compute the average rewards for active NFTs. In an edge case where there are no active NFTs (e.g., all NFTs are broken in `contracts/alliance-nft-collection/src/contract/execute.rs:352`), the function will fail due to a division by zero error.

Recommendation

Consider handling the edge case by increasing `REWARD_BALANCE` only if `NUM_ACTIVE_NFTS` is not zero.

2. Incorrect `REWARD_BALANCE` calculation when LST supply is zero

RISK IMPACT: LOW	STATUS: PENDING

Revision Notes

The team advises that they expect 1.1.0 migration to happen prior ERIS LST reaching zero.

Description

The `migrate_to_1_1_0` function in `contracts/alliance-nft-collection/src/contract/migrate.rs:64-67` computes the LST amount by manually multiplying the LUNA balance with the hub's total LST supply and dividing it with the hub's total staked LUNA.

In an edge case where the total LST supply is zero, `REWARD_BALANCE` will be computed as zero. This is incorrect because the LST amount minted will equal the LUNA balance sent to the hub based on the exchange rate.

Recommendation

Consider computing the LST amount by dividing the LUNA balance by the hub's exchange rate (`lst_hub_state.exchange_rate`).

3. Edge case when current time equals the mint end time

RISK IMPACT: INFORMATIONAL	STATUS: PENDING

Revision Notes

The team advises the probability of such a scenario is extremely unlikely and will not remediate at this point in time.

Description

The `is_minting_period` and `has_minting_period_finish` functions in `packages/alliance-nft-packages/src/state.rs:100-119` errors if the current time is larger or lesser than the mint end time. However, if the current time is equal to the mint end time, the `try_mint` and `try_send_to_dao_treasury` functions can be called, but only one will succeed.

Ideally, only one of the two functions can be called when the current time is equal to the mint end time. For example, if the user wants to mint the NFT with the `try_mint` function, their transaction will fail if someone calls the `try_send_to_dao_treasury` function first.

Recommendation

Consider modifying the implementation so that only one of the two functions can be called when the current time equals the mint end time.

Document Control

Version	Date	Notes
-	29th March 2024	Security audit commencement date.
0.1	6th May 2024	Initial report with identified findings delivered.
0.5	8th May 2024	Fixes remediations implemented and reviewed.
1.0	14th May 2024	Audit completed, final report delivered.

Appendices

A. Appendix - Risk assessment methodology

SCV-Security employs a risk assessment methodology to evaluate vulnerabilities and identified issues. This approach involves the analysis of both the LIKELIHOOD of a security incident occurring and the potential IMPACT if such an incident were to happen. For each vulnerability, SCV-Security calculates a risk level on a scale of 5 to 1, where 5 denotes the highest likelihood or impact. Consequently, an overall risk level is derived from combining these two factors, resulting in a value from 10 to 1, with 10 signifying the most elevated level of security risk

Risk Level	Range
CRITICAL	10
SEVERE	From 9 to 8
MODERATE	From 7 to 6
LOW	From 5 to 4
INFORMATIONAL	From 3 to 1

LIKELIHOOD and **IMPACT** would be individually assessed based on the below:

Rate	LIKELIHOOD	IMPACT
5	**Extremely Likely**	Could result in severe and irreparable consequences.
4	**Likely**	May lead to substantial impact or loss.
3	**Possible**	Could cause partial impact or loss on a wide scale.
2	**Unlikely**	Might cause temporary disruptions or losses.
1	**Rare**	Could have minimal or negligible impact.

B. Appendix - Report Disclaimer

This report should not be regarded as an "endorsement" or "disapproval" of any specific project or team. These reports do not indicate the economics or value of any "product" or "asset" created by a team or project that engages SCV-Security for a security review. The audit report does not make any statements or warranties about the code's utility, safety, suitability of the business model, regulatory compliance of the business model, or any other claims regarding the fitness of the implementation for its purpose or its bug-free status. The audit documentation is intended for discussion purposes only. The content of this audit report is provided "as is," without representations and warranties of any kind, and SCV-Security disclaims any liability for damages arising from or in connection with this audit report. Copyright of this report remains with SCV-Security.

THANK YOU FOR CHOOSING

SCV
SECURITY

🌐 scv.services

✉ contact@scv.services