Security Audit Report

Ta-da prize-pool
smart contract

by ARDA

on July 16, 2024

Table of Content

Disclaimer

The report makes no statements or warranties, either expressed or implied, regarding the security of the code, the information herein or its usage. It also cannot be considered as a sufficient assessment regarding the utility, safety and bugfree status of the code, or any other statements.

This report does not constitute legal or investment advice. It is for informational purposes only and is provided on an "as-is" basis. You acknowledge that any use of this report and the information contained herein is at your own risk. The authors of this report shall not be liable to you or any third parties for any acts or omissions undertaken by you or any third parties based on the information contained herein.

Terminology

Inherent risk: A risk for users that comes from a behavior inherent to the smart contract design.

Inherent risks only represent the risks inherent to the smart contract design, which are a subset of all the possible risks. **No inherent risk doesn't mean no risk.** It only means that no risk inherent to the smart contract design has been identified. Other kind of risks could still be present. For example, the issues not fixed incur risks for the users, or the smart contracts deployed as upgradeable also incur risks for the users.

Issue: A behavior unexpected by the users or by the project, or a practice that increases the chances of unexpected behaviors to appear.

Critical issue: An issue intolerable for the users or the project, that must be addressed.

Major issue: An issue undesirable for the users or the project, that we strongly recommend to address.

Medium issue: An issue uncomfortable for the users or the project, that we recommend to address.

Minor issue: An issue imperceptible for the users or the project, that we advise to address for the overall project security.

Audit Summary

Scope of initial audit

- **Repository:** https://gitlab.com/ta-da2/smart-contracts/sc-tada
- **Commit:** `ce92218211a82b3bfcc815ddf2d5c83557846d07`
- **Path to Smart contract:** `./prize_pool/`

Scope of final audit

- **Repository:** https://gitlab.com/ta-da2/smart-contracts/sc-tada
- **Commit:** `2e74f4ab6d5f51fec189d873113d1f68aa658c27`
- **Path to Smart contract:** `./prize_pool/`

Report objectives

1. Reporting all **inherent risks** of the smart contract.
2. Reporting all **issues** in the smart contract **code**.
3. Reporting all **issues** in the smart contract **test**.
4. Reporting all **issues** in the **other** parts of the smart contract.
5. Proposing **recommendations** to address all issues reported.

1 inherent risk in the final commit

1 issue in the final commit

11 issues reported from the initial commit and 1 remaining in the final commit:

Severity	Reported			Remaining		
	Code	Test	Other	Code	Test	Other
Critical	1	0	0	0	0	0
Major	0	0	0	0	0	0
Medium	5	1	0	1	0	0
Minor	3	0	1	0	0	0

Inherent Risks

R1: Users must trust that rewards will be correctly distributed to them.

This is because rewards distributions are performed by privileged addresses whitelisted by the Ta-da team. If they are inactive or wrongly allocate rewards between users, then some users might not earn rewards at all or less rewards than they should. In particular, if a whitelisted address is compromised, then it could steal all users' rewards by sending them to an unwanted address.

Code Issues & Recommendations

Since the smart contract code is not open-source, only the remaining issues are published.

C6: Can have more than 1 whitelisted address and increase risks of rewards being stolen

Severity: Medium **Status:** Won't fix

Location

`prize_pool/src/lib.rs`

Description

Current behavior: The list `get_whitelist` of addresses whitelisted by Ta-da can be arbitrarily big, however whitelisted addresses have a sensitive role, namely they can distribute the TADA rewards held in the smart contract to the users they want.

Therefore, the more whitelisted addresses there are, the higher the risk that one is corrupted or makes a mistake, and that rewards are incorrectly distributed.

Expected behavior: Since the Ta-da team needs to whitelist only 1 address for distributing rewards, this should be enforced in the smart contract in order to reduce the risk that a problem arises with a whitelisted address.

Worst consequence: One of the multiple whitelisted addresses is forgotten by the Ta-da team, and its private keys are not sufficiently secured. In turn, an attacker succeeds to get access to the private keys and steals all the TADA rewards held in the smart contract.

Recommendation

We recommend enforcing that there is only one whitelisted address, by making `get_whitelist` into a `SingleValueMapper<ManagedAddress>` instead of a `UnorderedSetMapper<ManagedAddress>`.

Resolution notes

The issue has not been fixed.

Test Issues & Recommendations

Since the smart contract code is not open-source, only the remaining issues are published.

Other Issues & Recommendations

Since the smart contract code is not open-source, only the remaining issues are published.