RISK AUDIT

for

PB&J
CONSULTING

on

Jun 02, 2025

FIDESIUM

Executive Summary

Report

24
/100

TOTAL
Low risk
June 02, 2025

Abstract

Fidesium's automated risk assessment service was requested to perform a risk posture audit on TriviTourney **contracts**

Repository Link: https://github.com/PBJ-JWeb3/Trivi-Contracts

Initial Commit Hash:

`d537ed717155e3fa6257fc0b6d721f721f778932`

Issue Summary

Critical	High	Medium	Low	Info
0 Issues	2 Issues	3 Issues	1 Issues	2 Issues

Caveats

PBJ's codebase is generally well written, but does incur a handful of flaws.

Test Approach

Fidesium performed both Whitebox and Blackbox testing, as per the scope of the engagement, and relied on automated security testing.

Methodology

The assessment methodology covered a range of phases and employed various tools, including but not limited to the following:

- Mapping Content and Functionality of API
- Application Logic Flaws
- Access Handling
- Authentication/Authorization Flaws
- Brute Force Attempt
- Input Handling
- Source Code Review
- Fuzzing of all input parameter
- Dependency Analysis

Severity Definitions

Critical	The issue can cause large economic losses, large-scale data disorder or loss of control of authority management.
High	The issue puts users' sensitive information at risk or is likely to lead to catastrophic financial implications.
Medium	The issue puts a subset of users' sensitive information at risk, reputation damage or moderate financial impact.
Low	The risk is relatively small and could not be exploited on a recurring basis, or is low-impact to the client's business.
Informational	The issue does not pose an immediate risk but is relevant to security best practices or defence in Depth.

Risk Issues

Vulnerability	Description	Risk	Probability	Status
Data Corruption: Storage Slot Collision	The `TriviTournament` contract nests a mapping in a struct, which can lead to storage slot collision.	High	Medium	Active
DoS: Unbounded Loop	The `TriviTournament.cancelTournament` function iterates without a gas limit, and can be used to DOS the contract.	High	Medium	Active
One step ownership transfer	The `TriviTournament` contract relies on `Ownable` to manage ownership, which is not secure.	Medium	Medium	Active
Centralization	The `backendService` has significant modification rights over the contracts and their state.	Medium	Medium	Active
Missing bounds validation	The `enterTournament` does not validate against `maxPlayers`.	Medium	Medium	Active
Gas Vulnerability: Permanent Storage Bloat	The `TriviTournament` contract uses a mapping to store the tournaments.	Low	Low	Active
Gas Inefficiency: Repeated storage reads	The `TriviTournament` contract reads the `tournament` variable repeatedly.	Info	Info	Active
Gas Inefficiency: String Comparison as Existence Check	The `TriviTournament` contract uses a string comparison to check for existence.	Info	Info	Active

Risk Overview

Team Risk

Low risk: 1

No issues found in founding team

Doxxing Status	Team Experience	Risk Summary
Public	Highly relevant	Low

Smart Contract Risks

Risk summary: 27

The contracts are well written, and secure with only a few minor issues..

Vulnerabilities Critical

Current scan criticals Clear

During this scan no critical security vulnerabilities were identified. The assessment covered all key components of the project, including smart contract logic, access controls, and potential attack vectors. While no critical issues were found, we recommend ongoing security monitoring and best practices to maintain the integrity and resilience of the system.

Vulnerabilities High

Data Corruption: Storage Slot Collision

Vulnerability severity: **High**

Vulnerability probability: **Medium**

The `TriviTournament` contract nests a mapping in a struct, which can lead to storage slot collision.

Nested Mappings and dynamic arrays in a struct do not use the struct's slot, instead they calculate the slot based on the hash of the struct and the mapping/array's key. If an attacker crafts a second tournament id that collides with the first tournament id, the second tournament will overwrite the first tournament's data. This can lead to manipulation, DoS, and, in extreme cases, protocol failure

Recommendations:

Separate the mapping and array from the struct, and use a different slot for the mapping.

```
mapping(string => mapping(address => bool)) public tournamentParticipants;
mapping(string => address[]) public tournamentPlayers;
```

DoS: Unbounded Loop

Vulnerability severity: **High**

Vulnerability probability: **Medium**

The `TriviTournament.cancelTournament` function iterates without a gas limit, and can be used to DOS the contract. The function iterates over the `tournaments` array, and for each tournament, it iterates over the `players` array. If the `players` array is large, the function will run out of gas and revert. This can be used to DOS the contract, and prevent users from cancelling tournaments.

Recommendations:

- Add a gas limit to the function.
- Implement a pull over push strategy for the `players` array.

```
mapping(string => mapping(address => uint256)) public refunds;
...
function cancelTournament(string memory tournamentId) external {
    ...
    for (uint256 i = 0; i < tournament.players.length; i++) {
        refunds[tournamentId][tournament.players[i]] = tournament.entryFee;
    }
    tournament.isActive = false;
}

function claimRefund(string memory tournamentId) external nonReentrant {
    uint256 refundAmount = refunds[tournamentId][msg.sender];
    require(refundAmount > 0, "No refund available");
    refunds[tournamentId][msg.sender] = 0;
    triviToken.safeTransfer(msg.sender, refundAmount);
}
```

Vulnerabilities Medium

One Step Ownership Transfer

Vulnerability severity: **Medium**

Vulnerability probability: **Medium**

The `TriviTournament` contract relies on `Ownable` to manage ownership, which is not secure.

The `Ownable` pattern is vulnerable to a one step ownership transfer. This exposes these contracts to accidental ownership transfer to malicious or invalid wallets.

Recommendations:

Implement `Ownable2Step` to drive a two step ownership transfer. This will require applying `Upgradeable` independently.

Centralization

Vulnerability severity: **Medium**

Vulnerability probability: **Medium**

The `backendService` has significant modification rights over the contracts and their state.

Recommendations:

Ensure that these roles are tied to well maintained Multisig wallets, and consider implementing a timelock.

Missing bounds validation

Vulnerability severity: **Medium**

Vulnerability probability: **Medium**

The `enterTournament` does not validate against `maxPlayers`.

Recommendations:

Validate the `maxPlayers` parameter.

Vulnerabilities Low

Gas Vulnerability: Permanent Storage Bloat

Vulnerability severity: **Low**

Vulnerability probability: **Low**

The `TriviTournament` contract uses a mapping to store the tournaments.

This can lead to permanent storage bloat, and can be used to DOS or grief the contract via storage exhaustion in extreme cases.

Recommendations:

- Implement tournament cleanup
- Use incremental tournament ids
- For large player counts, use merkle trees.

Vulnerabilities Info

Gas Inefficiency: Repeated storage reads

Vulnerability severity: **Info**

Vulnerability probability: **Info**

The `TriviTournament` contract reads the `tournament` variable repeatedly.

Recommendations:

Cache the `tournament` reference.

```
Tournament storage tournament = tournaments[tournamentId];
```

Gas Inefficiency: String Comparison as Existence Check

Vulnerability severity: **Info**

Vulnerability probability: **Info**

The `TriviTournament` contract uses a string comparison to check for existence.

`bytes(tournamentId).length > 0` is gas intensive.

Recommendations:

Use a separate existence mapping.

Disclaimer

Disclaimer

This report is governed by the Fidesium terms and conditions.

This report does not constitute an endorsement or disapproval of any project or team, nor does it reflect the economic value or potential of any related product or asset. It is not investment advice and should not be used as the basis for investment decisions. Instead, this report provides an assessment intended to improve code quality and mitigate risks inherent in cryptographic tokens and blockchain technology.

Fidesium does not guarantee the absence of bugs or vulnerabilities in the technology assessed, nor does it comment on the business practices, models, or regulatory compliance of its creators. All services, reports, and materials are provided "as is" and "as available," without warranties of any kind, including but not limited to merchantability, fitness for a particular purpose, or non-infringement.

Cryptographic assets and blockchain technologies are novel and carry inherent technical risks, uncertainties, and the possibility of unpredictable outcomes. Assessment results may contain inaccuracies or depend on third-party systems, and reliance on them is solely at the Customer’s risk.

Fidesium assumes no liability for content inaccuracies, personal injuries, property damages, or losses related to the use of its services, reports, or materials. Third-party components are provided "as is," and any warranties are strictly between the Customer and the third-party provider.

These services and materials are intended solely for the Customer's use and benefit. No third party or their representatives may claim rights to or rely on these services, reports, or materials under any circumstances.