expelee

Building the Futuristic Blockchain Ecosystem

SECURITY AUDIT REPORT

RaceGame

TABLE OF CONTENTS

02 Overview
03 Table of Contents
04 Overview
05 Risk Classification
06 About Expelee
07 Disclaimer

expelee

OVERVIEW

Report for RaceGame Contract.
All unit tests were performed using Forge from foundry.

expelee

RISK FINDING

- Medium : createRace function requires (according to error message) entryFee to be more than 0 but entryFee still can be set to 0 if balance of msg.sender is zero or msg.value is 0

require(_entryFee >= IERC20(_tokenToPlay).balanceOf(msg.sender),"Value sent has to be greater than 0");

require(_entryFee >= msg.value, "Value sent has to be greater than 0");

Suggestion:

Do not compare entryFee to msg.value or balance of msg.sender, instead check entryFee to be more than 0
require(_entryFee > 0,"Value sent has to be greater than 0");
require(_entryFee > 0, "Value sent has to be greater than 0");

RISK FINDING

- Low : A malicious actor is able to add a contract that rejects ETH into a race, when owner tries to remove that race (using cancelRace), he wont be able to do so, since one of players (malicious contract) rejects receiving ether

```
  function cancelRace(uint _raceId) public onlyOwner {
    require(_raceId > 0 && _raceId <= raceCounter, "Invalid race ID");
require(!races[_raceId].started, "Race has already started");

IERC20(races[_raceId].tokenUsed).approve(
        address(this),
IERC20(races[_raceId].tokenUsed).balanceOf(address(this))
    );
    // Refund all players if not giveAway
    if (!races[_raceId].isGiveAway) {
      for (uint i = 0; i < races[_raceId].players.length; i++) {
        if (races[_raceId].tokenUsed != DEAD) {
 IERC20(races[_raceId].tokenUsed).transfer(
races[_raceId].players[i],
races[_raceId].entryFee
            );
        } else {
payable(races[_raceId].players[i]).transfer(
races[_raceId].entryFee
            );
        }
      }
    }

races[_raceId].players = new address[](0);
races[_raceId].status = 3;
  }
```

Suggestion:
Instead of using “transfer’ in this case, use a low-level call for sending ETH (empty data) and ignore return value, but protect cancelRace function with a non-reentrancy guard

ABOUT EXPELEE

Expelee is a product-based aspirational Web3 start-up. Coping up with numerous solutions for blockchain security and constructing a Web3 ecosystem from deal making platform to developer hosting open platform, while also developing our own commercial and sustainable blockchain.

www.expelee.com

expeleeofficial

expelee

Expelee

expelee

expelee_official

expelee-co

expelee

Building the Futuristic Blockchain Ecosystem

DISCLAIMER

All the content provided in this document is for general information only and should not be used as financial advice or a reason to buy any investment. Team provides no guarantess against the sale of team tokens or the removal of liquidity by the project audited in this document.

Always do your own research and project yourselves from being scammed. The Expelee team has audited this project for general information and only expresses their opinion based on similar projects and checks from popular diagnostic tools.

Under no circumstances did Expelee receive a payment to manipulate those results or change the awarding badge that we will be adding in our website. Alway do your own research and protect yourselves from scams.

This document should not be presented as a reason to buy or not buy any particular token. The Expelee team disclaims any liability for the resulting losses.