Cyberscope

Audit Report
RaffleRefund

August 2022

SHA256 ddbf66cd6cfcad3aa98e3aaebc88139a63e8d2aa105ecf1cd8e8c93c7c36615d

Audited by © cyberscope

Table of Contents

Table of Contents 1

Contract Review 2

Source Files 2

Audit Updates 2

Introduction 3

Request Verification 4

Contract Roles 5

Contract Diagnostics 6

USB - User Sufficient Balance 7

Description 7

Recommendation 7

CSB - Contract Sufficient Balance 8

Description 8

Recommendation 8

L04 - Conformance to Solidity Naming Conventions 9

Description 9

Recommendation 9

Contract Functions 10

Contract Flow 11

Summary 12

Disclaimer 13

About Cyberscope 14

Contract Review

Contract Name	RaffleRefund
Test Deploy	https://testnet.bscscan.com/address/0x83F4A44D061d8407fF2Dc408Ead0e563ca4C034d
Domain	https://battleworld.game

Source Files

Filename	**SHA256**
contract.sol	ddbf66cd6cfcad3aa98e3aaebc88139a63e8d2aa105ecf1cd8e8c93c7c36615d

Audit Updates

Initial Audit	4th August 2022
Corrected	

Introduction

The RaffleFund contract implements a ticket redeem mechanism. The users can redeem their tickets in order to receive native tokens. During the redeem process, the corresponding tickets are burned. The value of each ticket is defined by the contract owners during the contract deployment. During the redeem princess, the users have to provide a message that must be verified in order to proceed with the transaction.

Request Verification

The verification process is based on an off-chain configuration. The contract owners are responsible for updating the in-chain factor in order to validate correctly the provided message.

The verification algorithm is using the markle tree mechanism.

https://github.com/protofire/zeppelin-solidity/blob/master/contracts/MerkleProof.sol

According to the markle algorithm, the off-chain mechanism pre-defines all the `index, recipient, amount` combinations.

Hence, only predefined users have the ability to redeem tickets in specific amounts.

Contract Roles

Role owner:

- The contract owners can pause the redeem mechanism.
- The contract owners can invalidate the validation factor and reset the saved address that claimed tickets.

Contract Diagnostics

● Critical ● Medium ● Informative

Severity	Code	Description
●	USB	User Sufficient Balance
●	CSB	Contract Sufficient Balance
●	L04	Conformance to Solidity Naming Conventions

USB - User Sufficient Balance

Criticality	informative
Location	contract.sol#L297

Description

The contract is baked on the fact that the burnFrom method will revert if the user’s balance is insufficient.

```
require(
            IRaffleTicket(RAFFLE_TICKET_ADDRESS).burnFrom(_msgSender(), amount),
            "RaffleRefund#claimRaffleRefund: Burning Raffle Ticket Failed"
        );
```

Recommendation

The contract could proactively check if the user's ticket balance is sufficient for the transaction.

CSB - Contract Sufficient Balance

Criticality	informative
Location	contract.sol#L301

Description

The contract is based on the fact that the Vault contract will revert the transaction if the required balance is insufficient.

```
require(
            IVault(VAULT).transferFromVault(
                _msgSender(),
                amount * RAFFLE_TICKET_PRICE
            ),
            "RaffleRefund#claimRaffleRefund: Payment from Vault Failed"
        );
```

Recommendation

The contract could proactively check if the Vault's balance is sufficient

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contract.sol#L115,111,112,113

Description

Solidity defines a naming convention that should be followed. Rule exceptions:

- Allow constant variable name/symbol/decimals to be lowercase.
- Allow _ at the beginning of the mixed_case match for private variables and unused parameters.

```
RAFFLE_TICKET_PRICE
VAULT
RAFFLE_TICKET_ADDRESS
RefundMerkleRoot
```

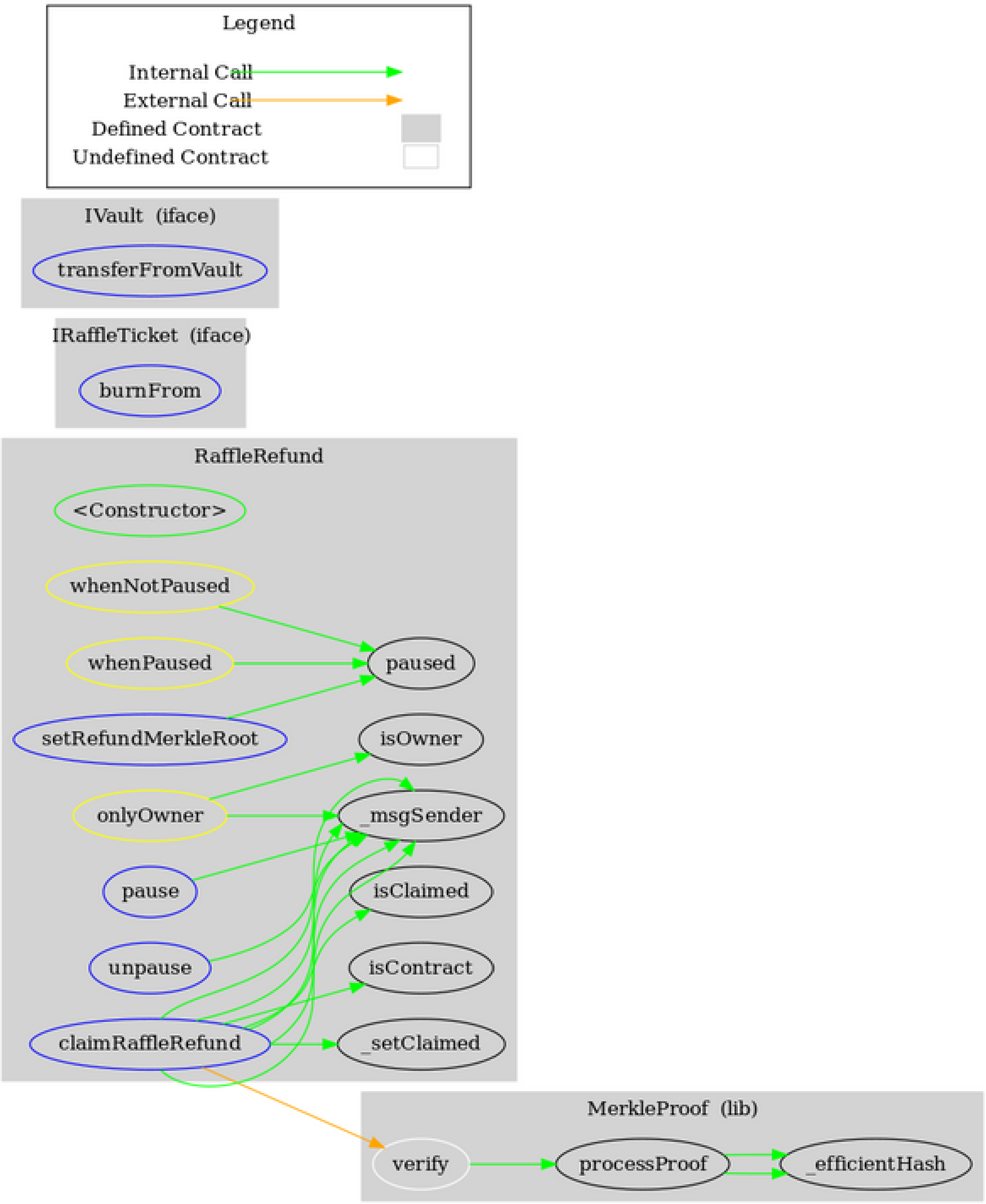
Recommendation

Follow the Solidity naming convention.
https://docs.soliditylang.org/en/v0.4.25/style-guide.html#naming-conventions.

Contract Functions

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
MerkleProof	Library			
	verify	Internal		
	processProof	Internal		
	_efficientHash	Private		
IRaffleTicket	Interface			
	burnFrom	External	✓	-
IVault	Interface			
	transferFromVault	External	✓	-
RaffleRefund	Implementation			
	<Constructor>	Public	✓	-
	_msgSender	Internal		
	isOwner	Public		-
	paused	Public		-
	pause	External	✓	onlyOwner
	unpause	External	✓	onlyOwner
	isContract	Internal		
	setRefundMerkleRoot	External	✓	onlyOwner
	isClaimed	Public		-
	_setClaimed	Private	✓	
	claimRaffleRefund	External	✓	whenNotPaused

Contract Flow



Summary

The Vault contract implements a redeem mechanism. It provides functionality to redeem tickets.The contract should thoroughly check balances before every transaction. The audit investigates the main features, mentions security recommendation, performance improvements and potential optimizations.

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.

Cyberscope team provides no guarantees against the sale of team tokens or the removal of liquidity by the project audited in this document. Always Do your own research and protect yourselves from being scammed.

The Cyberscope 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 Cyberscope receive a payment to manipulate those results or change the awarding badge that we will be adding in our website.

Always 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 Cyberscope team disclaims any liability for the resulting losses.

About Cyberscope

Coinscope audit and K.Y.C. service has been rebranded to Cyberscope.

Coinscope is the leading early coin listing, voting and auditing authority firm. The audit process is analyzing and monitoring many aspects of the project. That way, it gives the community a good sense of security using an informative report and a generic score.

Cyberscope and Coinscope are aiming to make crypto discoverable and efficient globally. They provide all the essential tools to assist users draw their own conclusions.

The Cyberscope team

https://www.cyberscope.io