COINSCOPE

Audit Report

Cashio

December 2021

Type	BEP20
Address	0x54ef94bEb6f890860F6bcEE78B16B58613034771
Audited by	© coinscope

Table of Contents

Contract Review

Contract Name	KeyCashGame
Compiler Version	v0.8.7+commit.e28d00a7
Optimization	200 runs
Licence	MIT
Explorer	https://bscscan.com/token/0x54ef94bEb6f890860F6bcEE78B16B58613034771
Symbol	CASHIO
Website	https://cashio.io

Audit Updates

Initial Audit	18th of December 2021
Corrected	

Contract Analysis

🔴 Critical 🟠 Medium 🔵 Pass

Severity	Code	Description
🔴	MT	Whitelist Addresses
🔴	BT	Exceed Limit Fees Manipulation to Team Wallet
🔵	ELFM	Reusable Code Segments

Whitelist Addresses

Criticality	high
Location	https://bscscan.com/address/0x54ef94beb6f890860f6bcee78b16b58613034771#code#L631

Description

The contract owner has the authority to whitelist addresses from the maximum acceptable ticket amount. Also the contract owner has the ability set the `maxKeysPerTx` to zero. That means that an excluded address can buy a huge amount of tickets and always be the winner.

```
require(noTicket <= maxKeysPerTx || maxKeysPerTxWhitelist[msg.sender] , "Number ticket must be less than maxAmount");
```

Recommendation

Since it is a game, there is no actual benefit for the game progress to have whitelisted addresses. This functionality can be eliminated from the contract.

The team should carefully manage the private keys of the owner’s account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions. That risk can be prevented by temporarily locking the contract or renouncing ownership.

Exceed Limit Fees Manipulation to Team Wallet

Criticality	high
Location	https://bscscan.com/address/0x54ef94beb6f890860f6bcee78b16b58613034771#code#L727,L734

Description

The contract owner has the authority to arbitrarily increase the amount that is accumulated to the team wallet. The owner may take advantage of it by calling the `setPrizePoolShare` function with a high percentage value on `_earningPlatform`.

```
function setPrizePoolShare(uint256 _prizeShare, uint256 _nextRound, uint256
_distributionForPlayers, uint256 _earningPlatform) public onlyOwner {
    require(_prizeShare + _nextRound + _distributionForPlayers +
_earningPlatform == 100);
    sharePrizePoolForPrize = _prizeShare;
    sharePrizePoolForNextRound = _nextRound;
    sharePrizePoolAllPlayers = _distributionForPlayers;
    sharePrizePoolForEarningPlatform = _earningPlatform;
}
```

The same manipulation can happen on `setTicketPriceShare` setting a high value on the `_earningPlatform` argument.

Recommendation

The contract could embody a check for the maximum acceptable value, for instance 10%.

The team should carefully manage the private keys of the owner's account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions. That risk can be prevented by temporarily locking the contract or renouncing ownership.

Reusable Code Segments

Criticality	low
Location	https://bscscan.com/address/0x54ef94beb6f890860f6bcee78b16b58613034771#code#L614,L659

Description

There are similar code segments in the application. The creation of the round structure is a good example. Both in the `startGame` and `buyTicket` functions, a `round` structure is created. The only different variation is the `prizePool`.

```
Round storage curRound = rounds[currentRound];
curRound.ticketPrice = startPrice;
curRound.prizePool = 0;
curRound.startTimestamp = block.timestamp;
curRound.closeTimestamp = block.timestamp + roundPeriod;
curRound.additionalTime = increaseTimePerTicket;
```

Recommendation

The author could create reusable functions that will make the contract code smaller and more readable.

Contract Diagnostics

Pass	Name
✓	Integer Underflow
✓	Parity Multisig Bug
✓	Callstack Depth Attack
✓	Transaction-Ordering Dependency
✓	Timestamp Dependency
✓	Re-Entrancy

Contract Functions

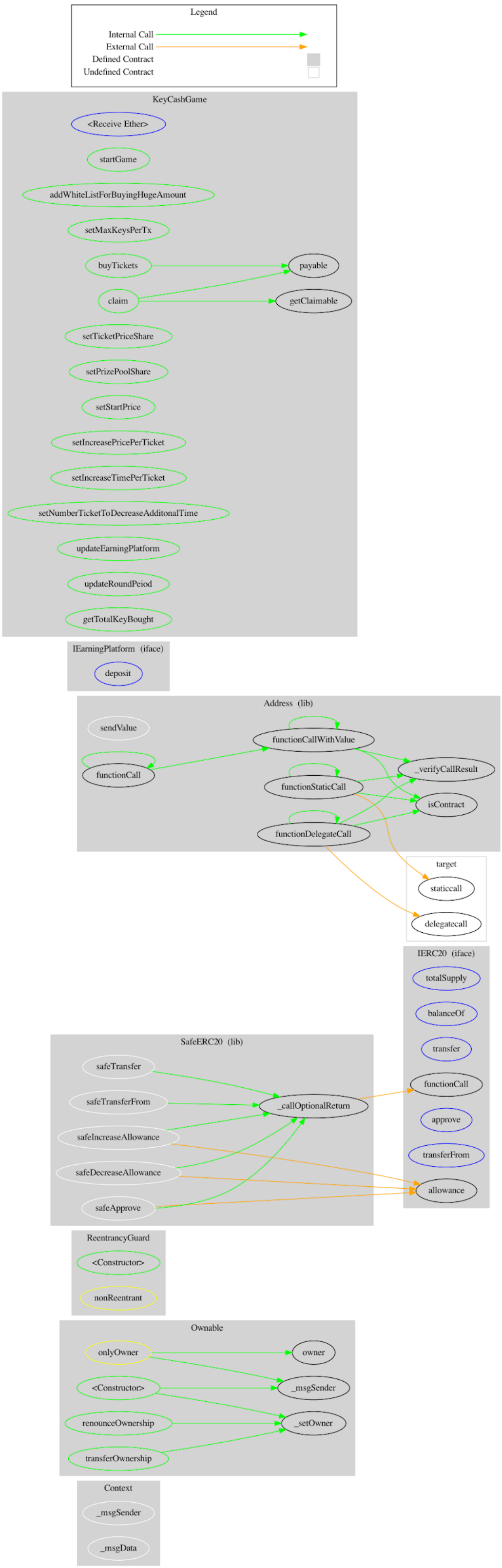
Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
Ownable	Implementation	Context		
		Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	_setOwner	Private	✓	
ReentrancyGuard	Implementation			
		Public	✓	-

IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
Address	Library			
	isContract	Internal		
	sendValue	Internal	✓	
	functionCall	Internal	✓	
	functionCall	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionStaticCall	Internal		
	functionStaticCall	Internal		
	functionDelegateCall	Internal	✓	
	functionDelegateCall	Internal	✓	

	_verifyCallResult	Private		
SafeERC20	Library			
	safeTransfer	Internal	✓	
	safeTransferFrom	Internal	✓	
	safeApprove	Internal	✓	
	safeIncreaseAllowance	Internal	✓	
	safeDecreaseAllowance	Internal	✓	
	_callOptionalReturn	Private	✓	
IEarningPlatform	Interface			
	deposit	External	Payable	-
KeyCashGame	Implementation	Ownable, ReentrancyGuard		
		External	Payable	-
	startGame	Public	✓	onlyOwner
	addWhiteListForBuyingHugeAmount	Public	✓	onlyOwner
	setMaxKeysPerTx	Public	✓	onlyOwner

	buyTickets	Public	Payable	nonReentrant
	getClaimable	Public		-
	claim	Public	✓	-
	setTicketPriceShare	Public	✓	onlyOwner
	setPrizePoolShare	Public	✓	onlyOwner
	setStartPrice	Public	✓	onlyOwner
	setIncreasePricePerTicket	Public	✓	onlyOwner
	setIncreaseTimePerTicket	Public	✓	onlyOwner
	setNumberTicketToDecreaseAdditonalTime	Public	✓	onlyOwner
	updateEarningPlatform	Public	✓	onlyOwner
	updateRoundPeiod	Public	✓	onlyOwner
	getTotalKeyBought	Public		-

Contract Flow



Domain Info

Domain Name	cashio.io
Registry Domain ID	e041f250570c430e8cf1ebe039997145-DONUTS
Registrar WHOIS Server	whois.godaddy.com
Registrar URL	http://www.godaddy.com/domains/search.aspx?ci=8990
Updated Date	2021-11-23T15:55:47Z
Creation Date	2021-07-19T05:40:06Z
Registry Expiry Date	2022-07-19T05:40:06Z
Registrar	GoDaddy.com, LLC
Registrar IANA ID	146

The domain was created about half a year before the creation of the audit. It will expire in one year.

There is no public billing information, the creator is protected by the privacy settings.

Summary

Keycash Game is an interesting game that is running in the BSC. The players should buy tickets in order to participate in the game. The player with the highest buy is the winner. The game is played periodically in rounds.

There are some functions that can be abused by the owner, like manipulating fees, transferring funds to the team’s wallet and whitelisting addresses. A multi-wallet signing pattern, renouncing the ownership, or periodically locks will eliminate all the contract threats.

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.

Coinscope 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 Coinscope 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 Coinscope 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 Coinscope team disclaims any liability for the resulting losses.

About Coinscope

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.

Coinscope is aiming to make crypto discoverable and efficient globally. It provides all the essential tools to assist users draw their own conclusions.

The Coinscope.co team

https://www.coinscope.co