HackSafe

Smart Contract Security Audit Report

JokerFootball

March 2023

Security Status

★★★★☆

www.hacksafe.io

Audit Details

Audited project
JokerFootball

Deployer address
0x0b42398fb3739912f257033bf070c0ef5bfb91ea

Client contacts
JokerFootball Team

Blockchain
Binance Smart Chain

Website
Not Provided

Disclaimer

This is a limited report on our findings based on our analysis, in accordance with good industry practice as at the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the below disclaimer below – please make sure to read it in full.

DISCLAIMER: By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and TechRate and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (HackSafe) owe no duty of care towards you or any other person, nor does HackSafe make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and HackSafe hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, HackSafe hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against HackSafe, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report.

The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed.

Procedure

Step 1 - In-Depth Manual Review

Manual line-by-line code reviews to ensure the logic behind each function is sound and safe from various attack vectors. This is the most important and lengthy portion of the audit process (as automated tools often cannot find the nuances that lead to exploits such as flash loan attacks).

Step 2 - Automated Testing

Simulation of a variety of interactions with your Smart Contract on a test blockchain leveraging a combination of automated test tools and manual testing to determine if any security vulnerabilities exist.

Step 3 – Leadership Review

The engineers assigned to the audit will schedule meetings with our leadership team to review the contracts, any comments or findings, and ask questions to further apply adversarial thinking to discuss less common attack vectors.

Step 4 - Resolution of Issues

Consulting with the team to provide our recommendations to ensure the code's security and optimize its gas efficiency, if possible. We assist project team's in resolving any outstanding issues or implementing our recommendations.

Step 5 - Published Audit Report

Boiling down results and findings into an easy-to-read report tailored to the project. Our audit reports highlight resolved issues and any risks that exist to the project or its users, along with any remaining suggested remediation measures. Diagrams are included at the end of each report to help users understand the interactions which occur within the project.

Background

HackSafe was commissioned by JokerFootball to perform an audit of smart contracts:

- https://bscscan.com/token/0x20cc0f8139663d0233DeF10f9B3130588FFC66A9#code

The purpose of the audit was to achieve the following:

- Ensure that the smart contract functions as intended.
- Identify potential security issues with the smart contract.

The information in this report should be understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Contract Details

Token contract details for 31.03.2023

Type	: MEME
Contract name	: JokerFootball
Contract address	: 0x20cc0f8139663d0233DeF10f9B3130588FFC66A9
Total supply	: 100,000,000,000,000,000
Token Ticker	: JKF
Decimals	: 9
Token Holders	: 2,847
Transactions count	: 21,794
Compiler version	: v0.8.7+commit.e28d00a7
Contract deployer address	: 0x0b42398fb3739912f257033bf070c0ef5bfb91ea
Owner address	: 0x000000000000000000000000000000000000dead

Audit Summary

According to the standard audit assessment, Customer`s solidity smart contracts are **“Secure”.** This token contract does not contain owner control as ownership has been renounced, which do not make it fully decentralized.

Insecure	Poor secured	Secure	Well-secured

You are here 

We used various tools like Slither, Mythril and Remix IDE. At the same time this finding is based on critical analysis of the manual audit. All issues found during automated analysis were manually reviewed and applicable vulnerabilities are presented in the issues checking status.

We found 0 critical, 0 high, 1 medium and 0 low.

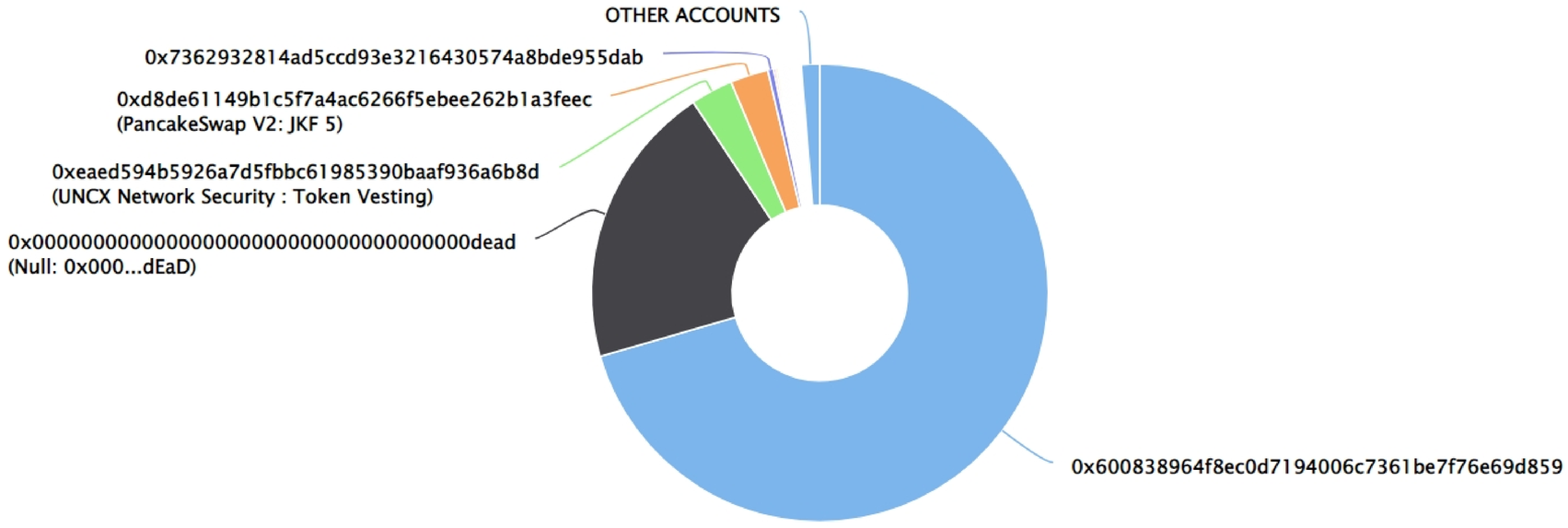
JokerFootball Token Distribution

The top 100 holders collectively own 98.71% (98,707,275,784,096,200.00 Tokens) of JokerFootball

Token Total Supply: 100,000,000,000,000,000.00 Token | Total Token Holders: 2,847

JokerFootball Top 100 Token Holders

Source: BscScan.com



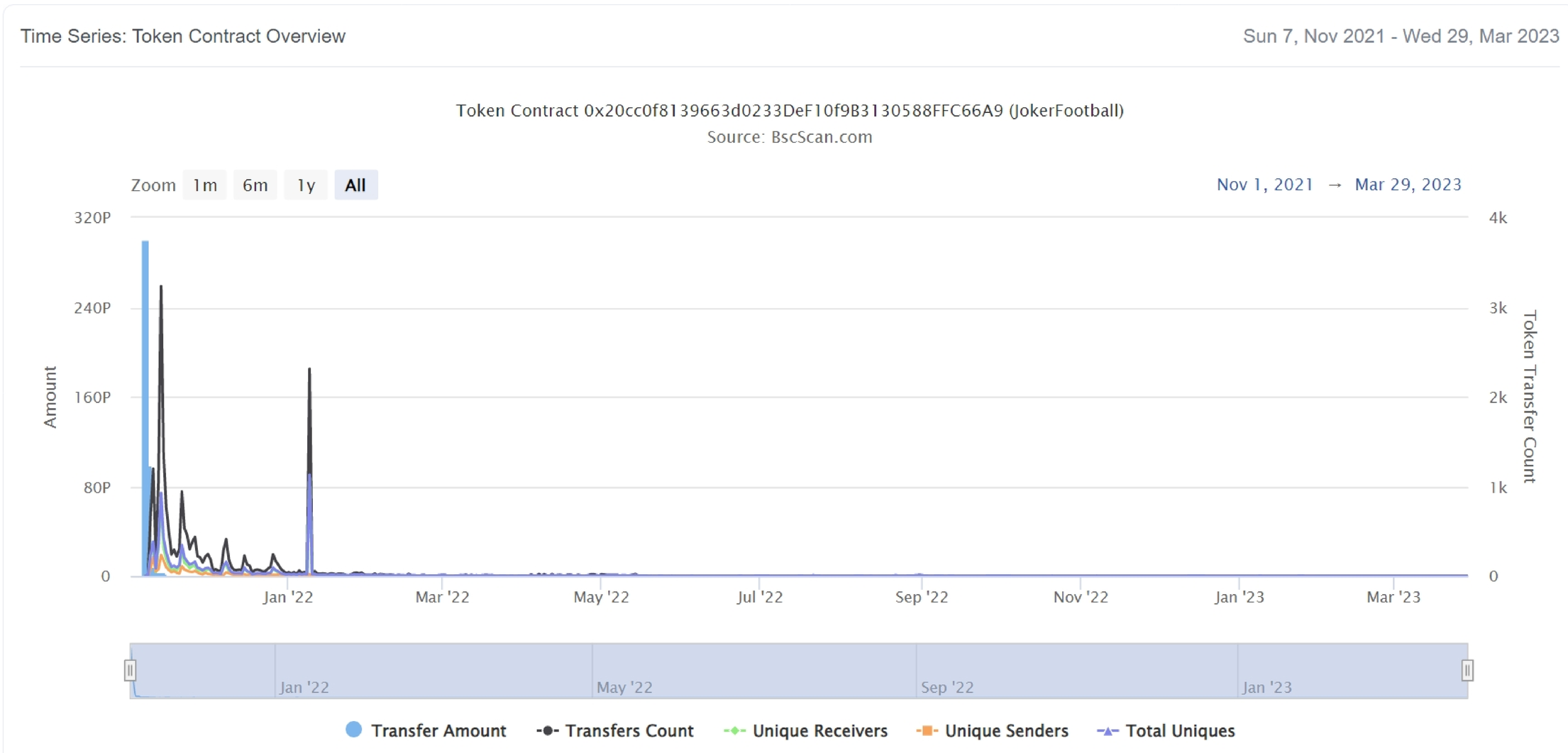
JokerFootball Token Top 20 Token Holders

(A total of 98,707,275,784,096,200.00 tokens held by the top 100 accounts from the total supply of 100,000,000,000,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0x600838964f8ec0d7194006c7361be7f76e69d859	70,530,525,594,199,999.2	70.5305%
2	Null: 0x000...dEaD	20,138,501,920,646,193.008275157	20.1385%
3	UNCX Network Security : Token Vesting	2,989,588,469,270,000	2.9896%
4	PancakeSwap V2: JKF 5	2,697,111,696,258,885.225459843	2.6971%
5	0x7362932814ad5ccd93e3216430574a8bde955dab	408,750,625,290,000	0.4088%
6	0x2dddce9e6ec945b2ed379baa26ddbca11cac78ba	159,710,280,301,337.174257677	0.1597%
7	0xcb3e0d479292fe9e61710d0f11d71a5b919e4174	158,340,746,322,983.77825187	0.1583%
8	0xadbc3a1fa9220cfc198e8ec441cc4d79c5150574	87,609,033,824,840.09128666	0.0876%
9	0x92ebeefeb901bdc2cc956840cadb1bbae3df6d15	86,250,642,696,048.779362866	0.0863%
10	0x0e12c5323ab58a78131275e891cecf9edf83b8d5	76,937,757,625,302.852312215	0.0769%
11	0xab5801a7d398351b8be11c439e05c5b3259aec9b	75,000,000,000,000	0.0750%
12	0xdefc0883759f20f52128bab34b0e45d3cdd8261a	59,782,253,425,367.677507079	0.0598%
13	0x5e50db52a13dfb6f3fd7cfecefd2e738c00a4aa6	59,059,751,239,074.880762172	0.0591%
14	0x9a247c2f472515f8da7bb794e200225bac717250	50,370,094,192,963.982602163	0.0504%
15	0x17ed2785937a49ca3496d04c5bd53eb98eae0efc	50,000,000,000,000	0.0500%
16	0x8bb03217ae9f27965dc210b3fcb361542df66bde	41,938,244,874,571.246590076	0.0419%
17	0x5e769ca4a24e6bd2bcd73e5b88920009b1c813bf	31,905,081,533,375.721603345	0.0319%
18	0x8438b69f5316c845701711cb80ea8c19c9ff7805	30,466,757,165,616.28	0.0305%
19	0xde07799f91dd0e66b3d91ea78baad5520ce860bb	29,986,000,000,000	0.0300%
20	0xca59cd0b0529461b7e1b353aea5bbe6bd0f3facd	29,198,782,435,358.246918322	0.0292%

JokerFootball Token Distribution

JokerFootball Token Contract Overview



Contract functions details

+[Int] IUniswapV2Router01
    -[Ext] factory
    -[Ext] WETH
    -[Ext] addLiquidity #
    -[Ext] addLiquidityETH ($)
    -[Ext] removeLiquidity #
    -[Ext] removeLiquidityETH #
    -[Ext] removeLiquidityWithPermit #
    -[Ext] removeLiquidityETHWithPermit #
    -[Ext] swapExactTokensForTokens #
    -[Ext] swapTokensForExactTokens #
    -[Ext] swapExactETHForTokens ($)
    -[Ext] swapTokensForExactETH #
    -[Ext] swapExactTokensForETH #
    -[Ext] swapETHForExactTokens ($)
    -[Ext] quote
    -[Ext] getAmountOut
    -[Ext] getAmountIn
    -[Ext] getAmountsOut
    -[Ext] getAmountsIn

+[Int] IUniswapV2Router02 (IUniswapV2Router01)
    -[Ext] removeLiquidityETHSupportingFeeOnTransferTokens #
    -[Ext] removeLiquidityETHWithPermitSupportingFeeOnTransferTokens #
    -[Ext] swapExactTokensForTokensSupportingFeeOnTransferTokens #
    -[Ext] swapExactETHForTokensSupportingFeeOnTransferTokens ($)
    -[Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #

+[Int] IUniswapV2Factory
    -[Ext] feeTo
    -[Ext] feeToSetter
    -[Ext] getPair
    -[Ext] allPairs
    -[Ext] allPairsLength
    -[Ext] createPair #
    -[Ext] setFeeTo #
    -[Ext] setFeeToSetter #

+[Lib] SafeMath

Contract functions details

-[Int] tryAdd
-[Int] trySub
-[Int] tryMul
-[Int] tryDiv
-[Int] tryMod
    -[Int] add
    -[Int] sub
    -[Int] mul
    -[Int] div
    -[Int] mod
    -[Int] sub
    -[Int] div
    -[Int] mod

+[Int] IERC20
    -[Ext] totalSupply
    -[Ext] balanceOf
    -[Ext] transfer #
    -[Ext] allowance
    -[Ext] approve #
    -[Ext] transferFrom #

+[Int] IERC20Metadata (IERC20)
    -[Ext] name
    -[Ext] symbol
    -[Ext] decimals

+Context
    -[Int] _msgSender
    -[Int] _msgData

+Ownable (Context)
    -[Pub] <Constructor > #
    -[Pub] owner
    -[Pub] renounceOwnership #
     - modifiers: onlyOwner
    -[Pub] transferOwnership #
     - modifiers: onlyOwner
    -[Pvt] _setOwner #

Contract functions details

+ERC20 (Context, IERC20, IERC20Metadata)
  - -[Pub] <Constructor > #
  - -[Pub] name
  - -[Pub] symbol
  - -[Pub] decimals
  - -[Pub] totalSupply
  - -[Pub] balanceOf
  - -[Pub] transfer #
  - -[Pub] allowance
  - -[Pub] approve #
  - -[Pub] transferFrom #
  - -[Pub] increaseAllowance #
  - -[Pub] decreaseAllowance #
  - -[Int] _transfer #
  - -[Int] _mint #
  - -[Int] _burn #
  - -[Int] _approve #
  - -[Int] _beforeTokenTransfer #
  - -[Int] _afterTokenTransfer #

+JokerFootball (ERC20, Ownable)
  - -[Pub] <Constructor >#
    - modifiers: ERC20
  - -[Ext] <Fallback >($)
  - -[Ext] updateUniswapV2Router #
    - modifiers: onlyOwner
  - -[Ext] setSwapTokensAmt #
    - modifiers: onlyOwner
  - -[Pub] excludeFromFees #
    - modifiers: onlyOwner
  - -[Pub] excludeMultipleAccountsFromFees #
    - modifiers: onlyOwner
  - -[Ext] blacklistAddress #
    - modifiers: onlyOwner
  - -[Ext] setTeamWallet #
    - modifiers: onlyOwner
  - -[Ext] setProjectWallet #
    - modifiers: onlyOwner

Contract functions details

  - modifiers: onlyOwner
-[Ext] setProjectWallet #
  - modifiers: onlyOwner
-[Ext] setBuyFee #
  - modifiers: onlyOwner
-[Ext] setSellFee #
  - modifiers: onlyOwner
-[Pub] setAutomatedMarketMakerPair #
  - modifiers: onlyOwner
-[Ext] setSwapEnabled #
  - modifiers: onlyOwner
-[Pvt] _setAutomatedMarketMakerPair #
-[Pub] isExcludedFromFees
-[Int] _transfer #
-[Pvt] swapAndSend #
-[Pvt] swapTokensForEth #

($) = payable function
= non-constant function

Issues Checking Status

No.	Title	Status
1.	Compiler error	Passed
2.	Missing Input Validation	Passed
3.	Race conditions and Reentrancy. Cross-function race conditions.	Passed
4.	Possible delays in data delivery	Passed
5.	Oracle calls.	Passed
6.	Timestamp dependence.	Passed
7.	Integer Overflow and Underflow	Passed
8.	DoS with Revert.	Passed
9.	DoS with block gas limit.	Medium Issues
10.	Methods execution permissions.	Passed
11.	Economy model of the contract.	Passed
12.	Private use data leaks.	Passed
13.	Malicious Event log.	Passed
14.	Scoping and Declarations.	Passed
15.	Uninitialized storage pointers.	Passed
16.	Arithmetic accuracy.	Passed
17.	Design Logic.	Passed
18.	Safe Open Zeppelin contracts implementation and usage.	Passed
19.	Incorrect Naming State Variable	Passed
20.	Too old version	Passed

Severity Definitions

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to assets loss or data manipulations.
High	High-level vulnerabilities are difficult to exploit; however, they also have a significant impact on smart contract execution, e.g., public access to crucial functions
Medium	Medium-level vulnerabilities are important to fix; however, they can't lead to assets loss or data manipulations.
Low	Low-level vulnerabilities are mostly related to outdated, unused, etc. code snippets that can't have a significant impact on execution.

Security Issues

- **Critical Severity Issues**
  No critical severity issue found.
- **High Severity Issues**
  No high severity issue found.
- **Medium Severity Issues**
  One medium severity issue found.

1. Out of gas

- **Issue:**
  - The function excludeMultipleAccountsFromFees() uses the loop to exclude multiple accounts from fees. Function will be aborted with OUT_OF_GAS exception if there will be a long addresses list.
- **Recommendation**
  - Be careful about accounts array length.

- **Low Severity Issues**
  No low severity issue found.

Centralization

Owner privileges :

- JokerFootball Contract:
    - Owner can change Uniswap router address.
    - Owner can change swap tokens amount value.
    - Owner can include in and exclude from fees.
    - Owner can add / remove addresses from blacklist.
    - Owner can change team and project wallet addresses.
    - Owner can exclude and include addresses in automatedMarketMakerPairs array.
    - Owner can change buy project, buy team, sell project and sell team fees.
    - Owner can enable / disable swap.

This smart contract has some functions which can be executed by the admin (Owner) only. If the admin wallet private key would be compromised, then it would not create trouble as smart contract ownership has been renounced.

Conclusion

Smart contract contains medium severity issues! The further transfer and operations with the fund raised are not related to this particular contract.

HackSafe note: Please check the disclaimer above and note, the audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is provided for the only contract mentioned in the report and does not include any other potential contracts deployed by Owner.