HackSafe

Smart Contract Security Audit Report

VFOX

August 2022

Security Status

★★★★½

www.hacksafe.io

Audit Details

Audited project
VFOX

Deployer address
0x3154908af5FD763f319f19c73b79f3DAD3ff465f

Client contacts
VFOX

Blockchain
Binance Smart chain

Website
https://www.redfoxlabs.io/virtual-space

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 VFOX to perform an audit of smart contract:

- https://bscscan.com/address/0x4d61577d8fd2208a0afb814ea089fdeae19ed202#code

The purpose of the audit was to achieve the

- Ensutre 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 06.08.2022

Token Type	: BEP20
Contract name	: Token2
Contract address	: 0x4D61577d8Fd2208A0afb814ea089fDeAe19ed202
Compiler version	: v0.5.16+commit.9c3226ce
Total supply	: 21,000,000
Token Ticker	: VFOX
Decimals	: 18
Token Holders	: 3,195
Top 100 token holder's dominance	: 90.91%
Transactions count	: 397,672
Contract deployer address	: 0x3154908af5FD763f319f19c73b79f3DAD3ff465f
Owner address	: 0x5114a11ebee53f5b67cd70f8694f74a292ab1e51

Social profiles

Coingecko profile	: https://www.coingecko.com/en/coins/vfox/
Telegram profile	: https://t.me/redfoxlabs_announcements
Twitter profile	: https://twitter.com/redfoxlabs_io

Audit Summary

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

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, 0 medium and 1 low and some very low-level issues. These issues are not critical ones.

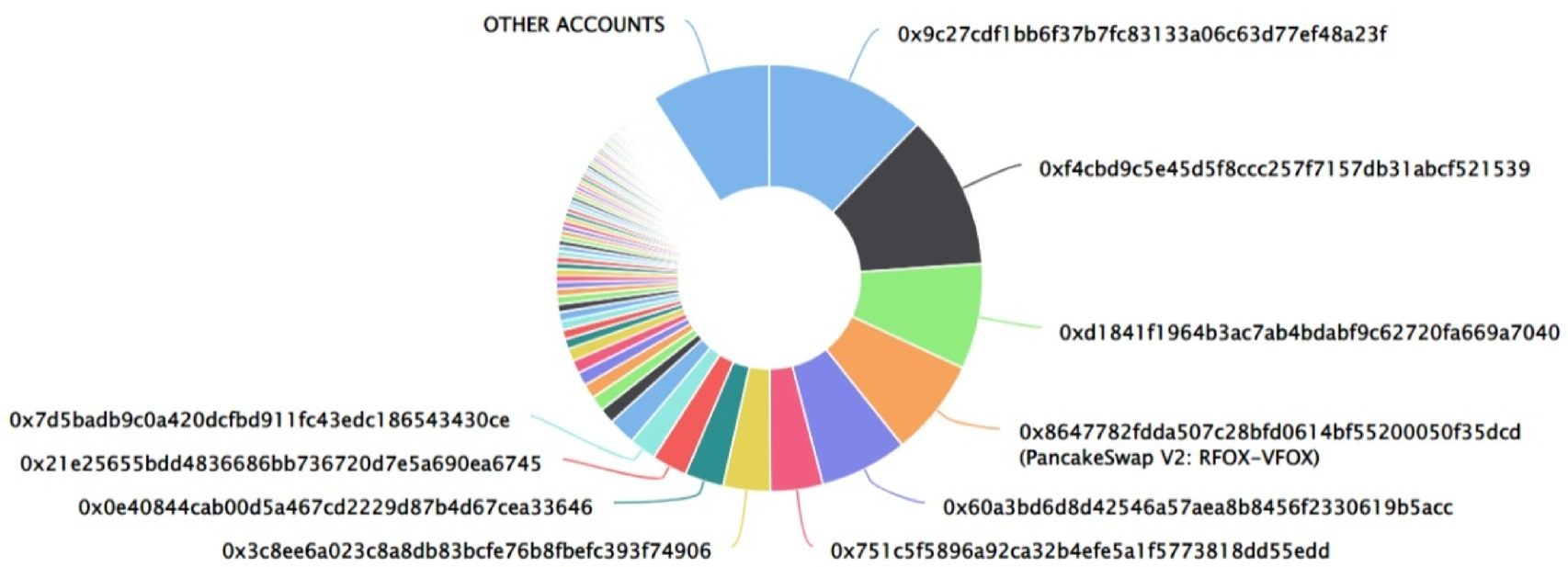
VFOX Token Distribution

The top 100 holders collectively own 90.91% (19,090,859.71 Tokens) of VFOX

Token Total Supply: 21,000,000.00 Token | Total Token Holders: 3,195

VFOX Top 100 Token Holders

Source: BscScan.com



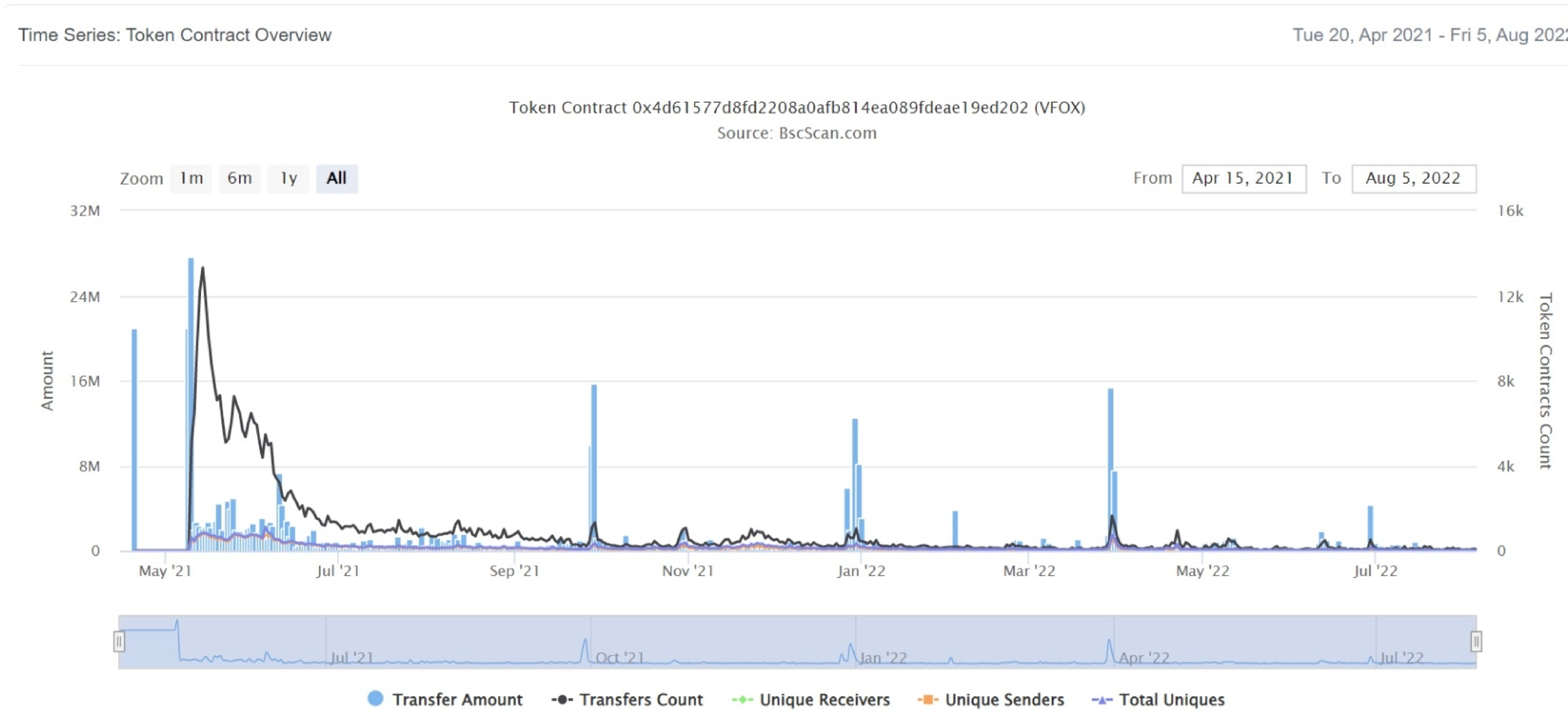
VFOX Token Top 20 Token Holders

(A total of 19,090,859.71 tokens held by the top 100 accounts from the total supply of 21,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0x9c27cdf1bb6f37b7fc83133a06c63d77ef48a23f	2,571,108.986658086580636254	12.2434%
2	0xf4cbd9c5e45d5f8ccc257f7157db31abcf521539	2,453,741.620998446538219025	11.6845%
3	0xd1841f1964b3ac7ab4bdabf9c62720fa669a7040	1,682,967.089375905694736323	8.0141%
4	PancakeSwap V2: RFOX-VFOX	1,546,844.255946398697758545	7.3659%
5	0x60a3bd6d8d42546a57aea8b8456f2330619b5acc	1,398,352.582650833928147936	6.6588%
6	0x751c5f5896a92ca32b4efe5a1f5773818dd55edd	830,599.013605802622130623	3.9552%
7	0x3c8ee6a023c8a8db83bcfe76b8fbefc393f74906	752,402.680871443225696789	3.5829%
8	0x0e40844cab00d5a467cd2229d87b4d67cea33646	617,247.50654272783785529	2.9393%
9	0x21e25655bdd4836686bb736720d7e5a690ea6745	564,355.729603295728456327	2.6874%
10	0x7d5badb9c0a420dcfbd911fc43edc186543430ce	433,494.248549721549394856	2.0643%
11	0xe1dff72b704ee6a0d3f447747006597612034076	430,841.383837777923040661	2.0516%
12	0x871879501aae945a6484ceee9246290933676418	242,399.526456459087200006	1.1543%
13	0xebcc34134dc3107f0fb285629c041606cfa1f5be	238,098.549121481136247555	1.1338%
14	0xf3f95fb20bd50895bbb4fc2e9c63c3b5772a26f6	235,311.282804340372192405	1.1205%
15	0xde0ada1a303517c3320e180601d14f135052e12c	211,482.312298889814423563	1.0071%
16	0x89417d68cd6e679953342e7843a365d8ca017cc1	209,083.268979440724900587	0.9956%
17	0xefed375ab776227614a58fd999b01f5b9fe5ecf8	203,905.253870856835224613	0.9710%
18	0x4998bcc70c0ac5af857dd08d1f3feb401362eb14	156,234.943985340092565093	0.7440%
19	0xe28d6ccdb970c0934b266c29a5172ff099ecb7de	146,599.355528316035843021	0.6981%
20	0x2f082c3abe4745d93087339ee7c4df159f5a0cfa	143,529.149344044927014453	0.6835%

VFOX Token Distribution

VFOX Token Contract Overview



Contract functions details

VFOX.sol
+ Token2 (BEP20Token)
    -[Pub] <constructor>

BEP20Token.sol
+ BEP20Token (Context, IBEP20, Ownable)
-[Int] _initialize #
-[Ext] mintable #
-[Ext] decimals
-[Ext] symbol
-[Ext] name
-[Ext] getOwner
-[Ext] totalSupply
-[Ext] balanceOf
-[Ext] transfer #
-[Ext] allowance
-[Ext] approve #
-[Ext] transferFrom #
-[Ext] increaseAllowance
-[Ext] decreaseAllowance
-[Ext] mint #
  -modifiers: onlyOwner
-[Ext] burn #
-[Ext] recoverBEP20 #
  -modifiers: onlyOwner
-[Int] _transfer #
-[Int] _mint#
-[Int] _burn #
-[Int] _approve #

Context.sol
+ Context
    -[Int] < constructor>
    -[Int] _msgSender
    -[Int] _msgData

IBEP20.sol
+ [Int] IBEP20
    -[Ext] totalSupply
    -[Ext] decimals

Contract functions details

-[Ext] symbol
-[Ext] name
-[Ext] getOwner
-[Ext] balanceOf
-[Ext] transfer
-[Ext] allowance
-[Ext] approve
-[Ext] transferFrom

Ownable.sol
+Ownable (Context)
-<constructor>
-[Pub] owner
-[Pub] renounceOwnership #
-modifiers: onlyOwner
-[Pub] transferOwnership
-modifiers: onlyOwner
-[Int] _transferOwnership #

SafeMath.sol
+[Lib] SafeMath
-[Int] add
-[Int] sub
-[Int] sub
-[Int] mul
-[Int] div
-[Int] div
-[Int] mod
-[Int] mod

($) = payable function
= non-constant function

Issues Checking Status

No.	Title	Status
1.	Unlocked Compiler Version	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.	Passed
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	Low issue

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

No medium severity issues found.

Low Severity Issues

One low severity issue found.

1. Too old compiler version.

- **Description**

  Contract has been deployed using too old compiler version.

- **Recommendation**

  It is advisable that the compiler version of solidity should be among the new compiler versions.

Centralization

Owner privileges:

- VFOX Contract:
    - Owner can remove and transfer ownership.
    - Owner can mint new tokens.
    - Owner can recover token by transferring token amount to owner address.

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 create trouble but smart contract ownership has been renounced. Following are Admin functions functions:

- Transferownership
- Renounceownership
- Mint
- Recoverbep20

Conclusion

Smart contract contains low 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.