HackSafe

Smart Contract Security Audit Report

Orbs

July 2022

Security Status

★★★★☆

www.hacksafe.io

Audit Details

Audited project
Orbs

Deployer address
0x54F5A04417E29FF5D7141a6d33cb286F50d5d50e

Client contacts
Orbs team

Blockchain
Binance Smart Chain

Website
https://www.orbs.com/

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 Orbs to perform an audit of smart contracts:

- https://bscscan.com/address/0xebd49b26169e1b52c04cfd19fcf289405df55f80#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 29.07.2022

Token Type	: BEP20
Contract name	: AnyswapV4ERC20
Contract address	: 0xeBd49b26169e1b52c04cFd19FCf289405dF55F80
Compiler version	: v0.8.2+commit.661d1103
Total supply	: 9,604,201.143711
Token Ticker	: ORBS
Decimals	: 18
Token Holders	: 1,747
Top 100 token holder's	: 99.69%
Transactions count	: 41,537
Contract deployer address	: 0x54F5A04417E29FF5D7141a6d33cb286F50d5d50e
Owner address	: 0x533e3c0e6b48010873b947bddc4721b1bdff9648
Vault address	: 0x533e3c0e6b48010873b947bddc4721b1bdff9648 (primary controller of the token contract)

Social profiles

Twitter Profile	: https://twitter.com/orbs_network
Facebook Profile	: https://www.facebook.com/OrbsNetwork/
Telegram Profile	: https://t.me/orbs_network
Coinmarketcap profile	: https://coinmarketcap.com/currencies/orbs/
Coingecko profile	: https://www.coingecko.com/en/coins/orbs/

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. Owner have full access over the smart contract.

Insecure	Poor	Secure	Well-secured

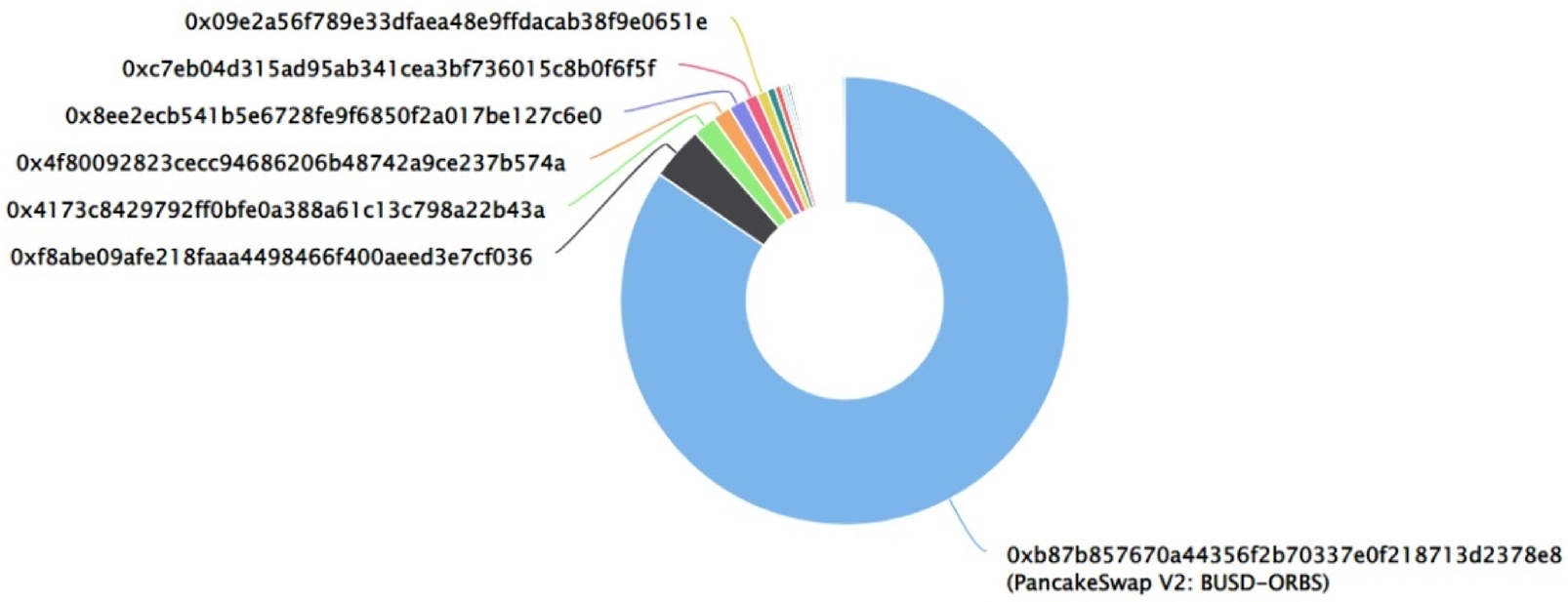
You are here 

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.

ORBS Token Distribution

The top 100 holders collectively own 99.79% (9,574,832.85 Tokens) of Orbs

Token Total Supply: 9,594,904.59 Token | Total Token Holders: 1,747



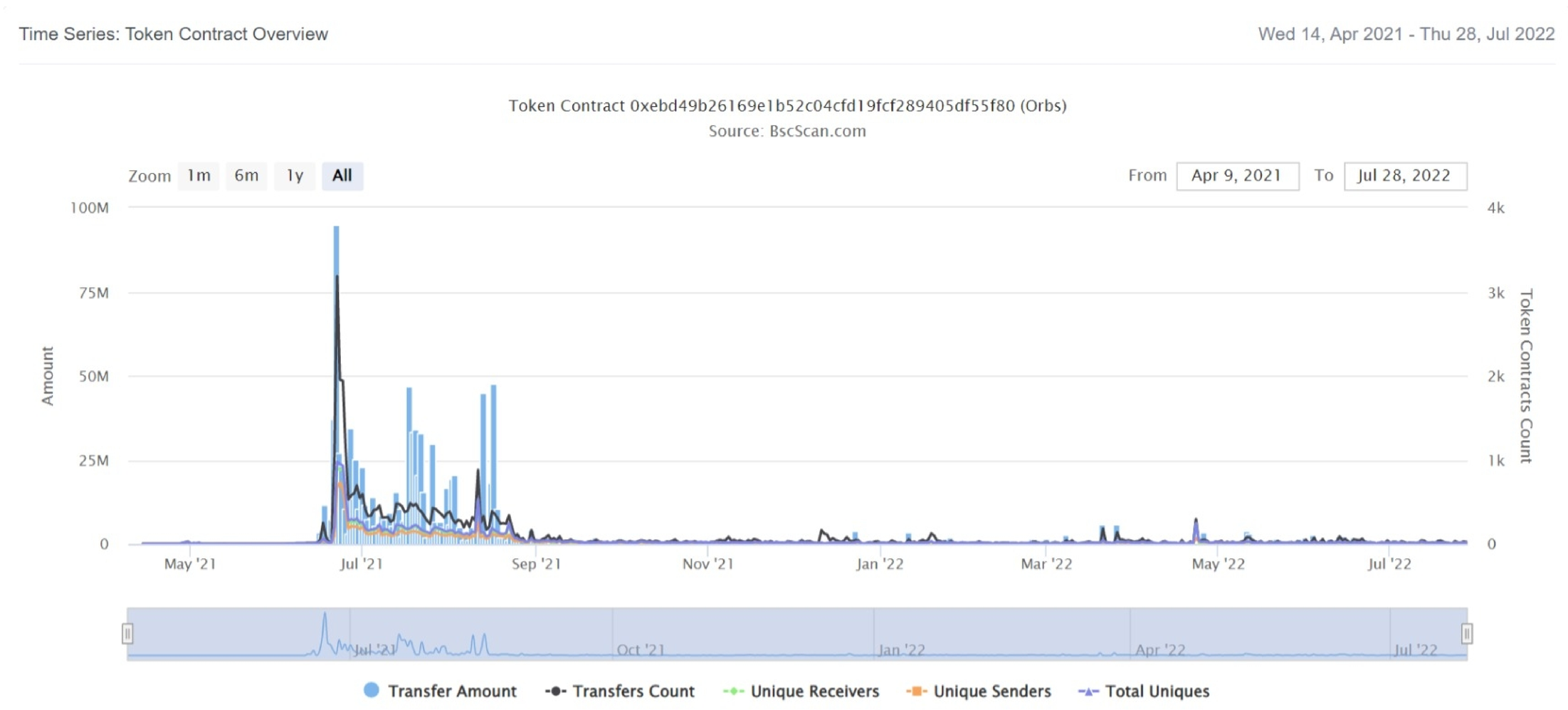
ORBS Top 20 Token Holders

(A total of 9,574,832.85 tokens held by the top 100 accounts from the total supply of 9,594,904.59 token)

Rank	Address	Quantity (Token)	Percentage
1	PancakeSwap V2: BUSD-ORBS	8,111,513.854863542349087309	84.5398%
2	0xf8abe09afe218faaa4498466f400aeed3e7cf036	372,200	3.8791%
3	0x4173c8429792ff0bfe0a388a61c13c798a22b43a	161,010.433221737023382422	1.6781%
4	0x4f80092823cecc94686206b48742a9ce237b574a	126,580.616582693589129435	1.3192%
5	0x8ee2ecb541b5e6728fe9f6850f2a017be127c6e0	116,900	1.2184%
6	0xc7eb04d315ad95ab341cea3bf736015c8b0f6f5f	91,898.294115206871523567	0.9578%
7	0x09e2a56f789e33dfaea48e9ffdacab38f9e0651e	73,857.006387423024888073	0.7698%
8	0x9ac31c624d23a1902023b413eb6745d745c6e7a5	56,004.424652490014529586	0.5837%
9	0x8594d8e9483473626908648a5539d9d65ca2fe8d	44,450.922817613241456289	0.4633%
10	0xfd3f7dccbe439b353169afc1bce11587430a0962	24,072.614613658155255009	0.2509%
11	0x9ffb54b5f11f7fdd759bf678ea4c1200a8c6605e	21,546.9668225228	0.2246%
12	0x5c7a3671471d9505808de6e78ba1d3bd7c5c800a	20,745.201735642936918282	0.2162%
13	0xbc6a4bc0f7987ba7413c6c001524bacc49bba224	17,382.173758508642776822	0.1812%
14	Anyswap: ORBS Token	16,458.682405068237824484	0.1715%
15	0x0c9ef9e0d06fcc4639cfb99b6c0aa6a6964938c6	15,695.454291485563259847	0.1636%
16	0xfb5d242a968bc3f5b10069dcfb2914e7ed052e55	15,594.159007712459336923	0.1625%
17	0x01b50c90e015230be610e6d89c9c72e737cdda93	13,830.697191303079217508	0.1441%
18	0x16bba5071600502cd641bfa5820dc7e8b8126a7a	12,562.017193082749564128	0.1309%
19	PancakeSwap V2: ORBS	11,606.129106738319212065	0.1210%
20	0xba94f0f09c1a19f91dbc4d46adf660b67604d4db	11,433.811054611072183792	0.1192%

ORBS Token Distribution

ORBS Contract Overview



Contract functions details

+ [Int] IERC20
    -[Ext] totalSupply
    -[Ext] decimals
    -[Ext] balanceOf
    -[Ext] transfer
    -[Ext] allowance
    -[Ext] approve
    -[Ext] transferFrom
    -[Ext] permit
    -[Ext] transferWithPermit

+[Int] IERC2612
    -[Ext] nonces

+[Int] IAnyswapV3ERC20 (IERC20, IERC2612)
    -[Ext] approveAndCall
    -[Ext] transferAndCall

+[Int] ITransferReceiver
    -[Ext] onTokenTransfer

+[Int] IApprovalReceiver
    -[Ext] onTokenApproval

+ [Lib] Address
    -[Int] isContract

+[Lib] SafeERC20
    -[Int] safeTransfer
    -[Int] safeTransferFrom
    -[Int] safeApprove
    -[Pvt] callOptionalReturn

+ AnyswapV4ERC20 (IAnyswapV3ERC20)
    -[Pub] owner
    -[Pub] mpc
    -[Ext] setVaultOnly #
      -modifiers: onlyVault
    -[Ext] initVault #
      -modifiers: onlyVault
    -[Ext] setMinter #
      -modifiers: onlyVault

Contract functions details

-[Ext] setVault #
  -modifiers: onlyVault
-[Ext] applyVault #
  -modifiers: onlyVault
-[Ext] applyMinter #
  -modifiers: onlyVault
-[Ext] revokeMinter #
  -modifiers: onlyVault
-[Ext] getAllMinters
-[Ext] changeVault #
  -modifiers: onlyVault
-[Pub] changeMPCOwner #
  -modifiers: onlyVault
-[Ext] mint #
  -modifiers: onlyAuth
-[Ext] burn #
  -modifiers: onlyAuth
-[Pub] Swapin #
-[Pub] Swapout #
-<constructor>
-[Ext] depositWithPermit #
-[Ext] depositWithTransferPermit #
-[Ext] deposit #
-[Ext] deposit #
-[Ext] deposit #
-[Ext] depositVault #
  -modifiers: onlyVault
-[Int] _deposit #
-[Ext] withdraw #
-[Ext] withdraw #
-[Ext] withdraw #
-[Ext] withdrawVault #
  -modifiers: onlyVault
-[Int] _withdraw #
-[Int] _mint #
-[Int] _burn #
-[Ext] approve #
-[Ext] approveAndCall #

Contract functions details

-[Ext] permit #
-[Ext] transferWithPermit #
-[Int] verifyEIP712 #
-[Int] verifyPersonalSign #
-[Int] prefixed #
-[Ext] transfer #
-[Ext] transferFrom #
-[Ext] transferAndCall #

($) = 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	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

No medium severity issues found.

Low Severity Issues

No low severity issue found.

Centralization

Vault address privileges:

- ORBS Contract:
    - Vault can set minter.
    - Vault can set other vault address.
    - Vault can apply vault and minter.
    - Vault can change vault address.
    - Vault can change MPC owner.
    - Vault can withdraw tokens.

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

- Setvaultonly
- Initvault
- Setminter
- Setvault
- Applyvault
- Applyminter
- Revokeminter
- Changevault
- Changempcowner
- Depositvault
- Withdrawvault

Conclusion

Smart contract contains low severity issues but the owner’s access to the contract which do not make it full decentralized! 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.