HackSafe

Smart Contract Security Audit Report

Vodi X

October 2022

Security Status

★ ★ ★ ★ ⯪

www.hacksafe.io

Audit Details

Audited project
Vodi X

Deployer address
0x698453d4a2944FB4eEfE1A5bf46849A22883d62D

Client contacts
Vodi X Team

Blockchain
Ethereum

Website
https://vodix.io/

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 Vodi X to perform an audit of smart contracts:

- https://etherscan.io/token/0x91e64f39c1fe14492e8fdf5a8b0f305bd218c8a1#code

The purpose of the audit was to achieve the following:

- 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 20.10.2022

Token Type	: ERC20
Contract name	: VodiX
Contract address	: 0x91e64F39C1FE14492e8FDf5A8B0f305BD218C8A1
Total supply	: 1,397,703,182.8411159
Token ticker	: VDX
Decimals	: 18
Token holders	: 917
Transactions count	: 20,476
Compiler version	: v0.5.0+commit.1d4f565a
Contract deployer address	: 0x698453d4a2944FB4eEfE1A5bf46849A22883d62D
Owner address	: 0x3c105058372694F30Af3ebbB922D9390e35427d5

Social profiles

Twitter profile	: https://twitter.com/vodi_app
Coinmarketcap Profile	: https://coinmarketcap.com/currencies/vodi-x/
Coingecko profile	: https://www.coingecko.com/en/coins/vodi-x/
Telegram profile	: https://t.me/Vodixgroup

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.

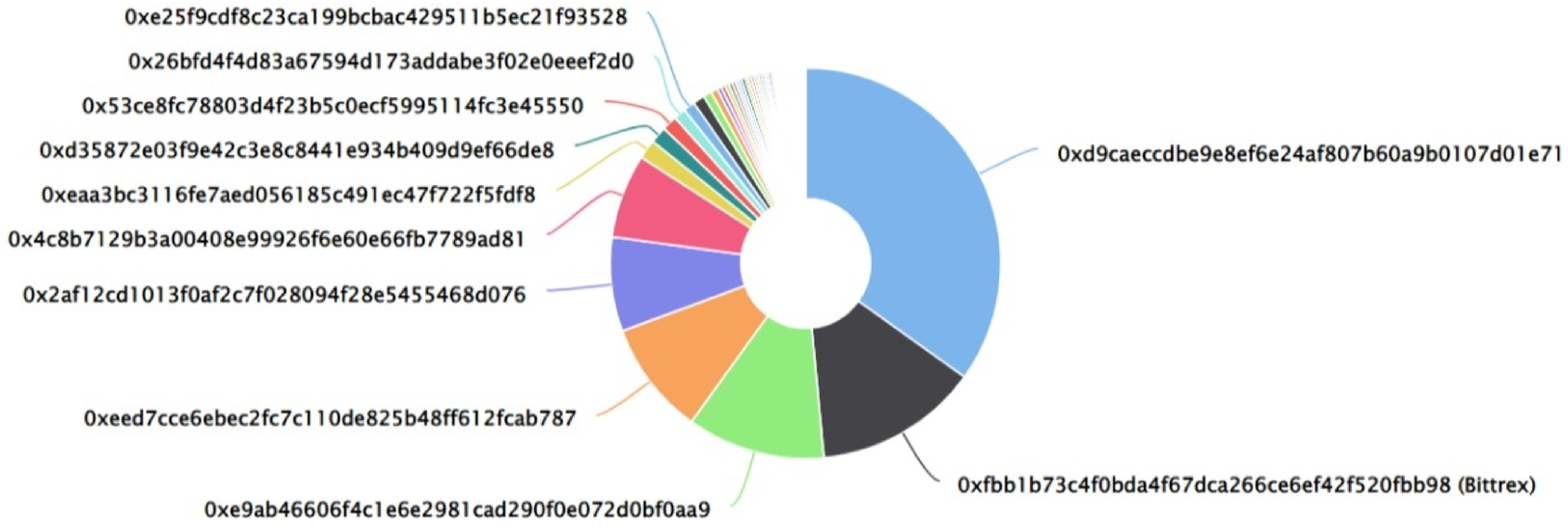
Vodi X Token Distribution

The top 100 holders collectively own 99.95% (1,396,994,314.12 Tokens) of Vodi X

Token Total Supply: 1,397,703,182.84 Token | Total Token Holders: 917

Vodi X Top 100 Token Holders

Source: Etherscan.io



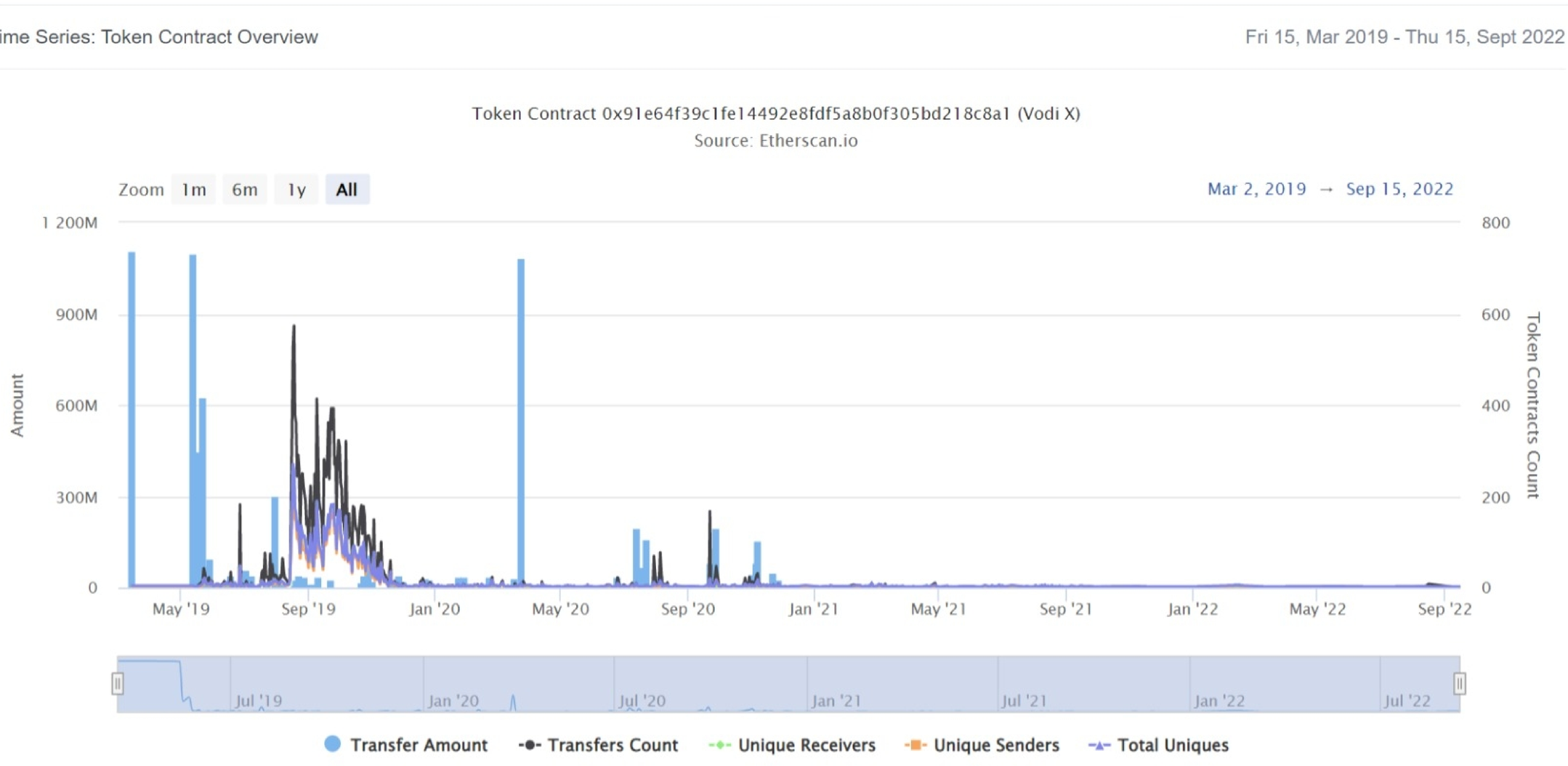
Vodi X 20 Token Holders

(A total of 1,396,994,314.12 tokens held by the top 100 accounts from the total supply of 1,397,703,182.84 token)

Rank	Address	Quantity (Token)	Percentage
1	0xd9caeccdbe9e8ef6e24af807b60a9b0107d01e71	487,879,930	34.9058%
2	Bittrex	190,088,277.48458188	13.6000%
3	0xe9ab46606f4c1e6e2981cad290f0e072d0bf0aa9	160,000,000	11.4474%
4	0xeed7cce6ebec2fc7c110de825b48ff612fcab787	131,611,274	9.4163%
5	0x2af12cd1013f0af2c7f028094f28e5455468d076	109,090,908	7.8050%
6	0x4c8b7129b3a00408e99926f6e60e66fb7789ad81	97,045,833	6.9432%
7	0xeaa3bc3116fe7aed056185c491ec47f722f5fdf8	22,400,000	1.6026%
8	0xd35872e03f9e42c3e8c8441e934b409d9ef66de8	19,307,590	1.3814%
9	0x53ce8fc78803d4f23b5c0ecf5995114fc3e45550	17,471,623.10899107	1.2500%
10	0x26bfd4f4d83a67594d173addabe3f02e0eeef2d0	14,230,290.15404038	1.0181%
11	0xe25f9cdf8c23ca199bcbac429511b5ec21f93528	13,318,725	0.9529%
12	0x2cbf80bed3d7cc2769637c894ab11087f4992c73	13,315,580	0.9527%
13	0x12439e12923e2bcc4e4b4882256e8985d0eff352	9,733,800.26859776	0.6964%
14	0x2da2bb5600e8f93978723c9d4dbff35bbc47edc1	8,000,000	0.5724%
15	0x5d7142c223ced450fafe5979f75f59aa08e18c11	5,000,000.000000000131422084	0.3577%
16	0x2956bcfd62083af5bf803e04c6a613ce8dd29ac8	4,525,243.75496728	0.3238%
17	0xdbb31d133f933b0cfb2551e94960bd97b1149226	4,459,150	0.3190%
18	0xd8a8da7788b24714669c64ef3b26f77b9e758357	4,135,430.37574318	0.2959%
19	0xc26337d82554777562943d5ea492f53ea42c8417	4,000,000	0.2862%
20	0x02fde175a31b9f07469620232e0b5ee0febcf9c3	3,999,645.69825436	0.2862%

Vodi X Token Distribution

Vodi X Contract Overview



Contract functions details

+ Ownable
    -[Int] <constructor>
    -[Pub] owner
    -[Pub] isOwner
    -[Pub] renounceOwnership #
      -modifiers: onlyOwner
    -[Pub] transferOwnership #
      -modifiers: onlyOwner
    -[Int] _transferOwnership #

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

+[Int] IController
    -[Ext] totalSupply
    -[Ext] balanceOf
    -[Ext] allowance
    -[Ext] approve
    -[Ext] transfer
    -[Ext] transferFrom
    -[Ext] mint
    -[Ext] increaseAllowance
    -[Ext] decreaseAllowance
    -[Ext] burn
    -[Ext] burnFrom

+ERC20 (Ownable, IERC20)
    -[Pub] balanceOf
    -[Pub] totalSupply
    -[Pub] allowance
    -[Pub] mint #
      -modifiers: onlyOwner
    -[Pub] mintToggle #

Contract functions details

-modifiers: onlyOwner
-[Pub] approve #
-[Pub] increaseAllowance #
-[Pub] decreaseAllowance #
-[Pub] transfer #
-[Pub] transferFrom #
-[Pub] burn #
-[Pub] burnFrom #

+VodiX (ERC20)
-[Pub] name
-[Pub] symbol
-[Pub] decimals

($) = 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 issues found.
- **Medium Severity Issues**
  No medium severity issues found.
- **Low Severity Issues**
  One low severity issue found.

1.Old compiler version

- **Description**
  Contract has been deployed using too old solidity version.
- **Recommendation**
  It is advisable to deploy contract using any of the latest version of solidity.

Centralization

Owner Privileges:

- Vodi X Contract:
    - Owner can transfer and renounce ownership.
    - Owner can mint tokens.

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 as smart contract ownership has not been renounced. Following are Admin functions:

- Transferownership
- Renounceownership
- Minttoggle
- Mint

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.