HackSafe

Smart Contract Security Audit Report

Truedeck

September 2022

Security Status

★ ★ ★ ★ ★

www.hacksafe.io

Audit Details

Audited project
TrueDeck

Deployer address
0x301Df3Ab354249b4179be4F4e4ab6E5A6a570738

Client contacts
TrueDeck Team

Blockchain
Ethereum

Website
https://truedeck.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 TrueDeck to perform an audit of smart contract:

- https://etherscan.io/token/0x5b11aacb6bddb9ffab908fdce739bf4aed554327#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 17.09.2022

Token Type	: ERC20
Contract name	: TrueDeckToken
Contract address	: 0x5b11aAcB6Bddb9ffab908FDCE739Bf4aed554327
Compiler version	: v0.4.23+commit.124ca40d
Total supply	: 200,000,000
Token ticker	: TDP
Decimals	: 18
Token holders	: 3,595
Transactions count	: 15,862
Contract deployer address	: 0x301Df3Ab354249b4179be4F4e4ab6E5A6a570738
Owner address	: No owner

Social profiles

Telegram profile	: https://t.me/thetruedeck
Coinmarketcap profile	: https://coinmarketcap.com/currencies/truedeck/
Coingecko profile	: https://www.coingecko.com/en/coins/truedeck/

Claimed Smart Contract Features

Claimed Feature Detail

Tokenomics :

- **Name** : TrueDeckToken
- **Symbol** : TDP
- **Decimals** : 18
- **Protocol** : ERC20
- **Total supply** : 200,000,000
- **Contract address** : 0x5b11aAcB6Bddb9ffab908FDCE739Bf4aed554327

Our Observation

YES, this is valid.

Audit Summary

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

Insecure	Poor	Secure	Well-secured

You are here 

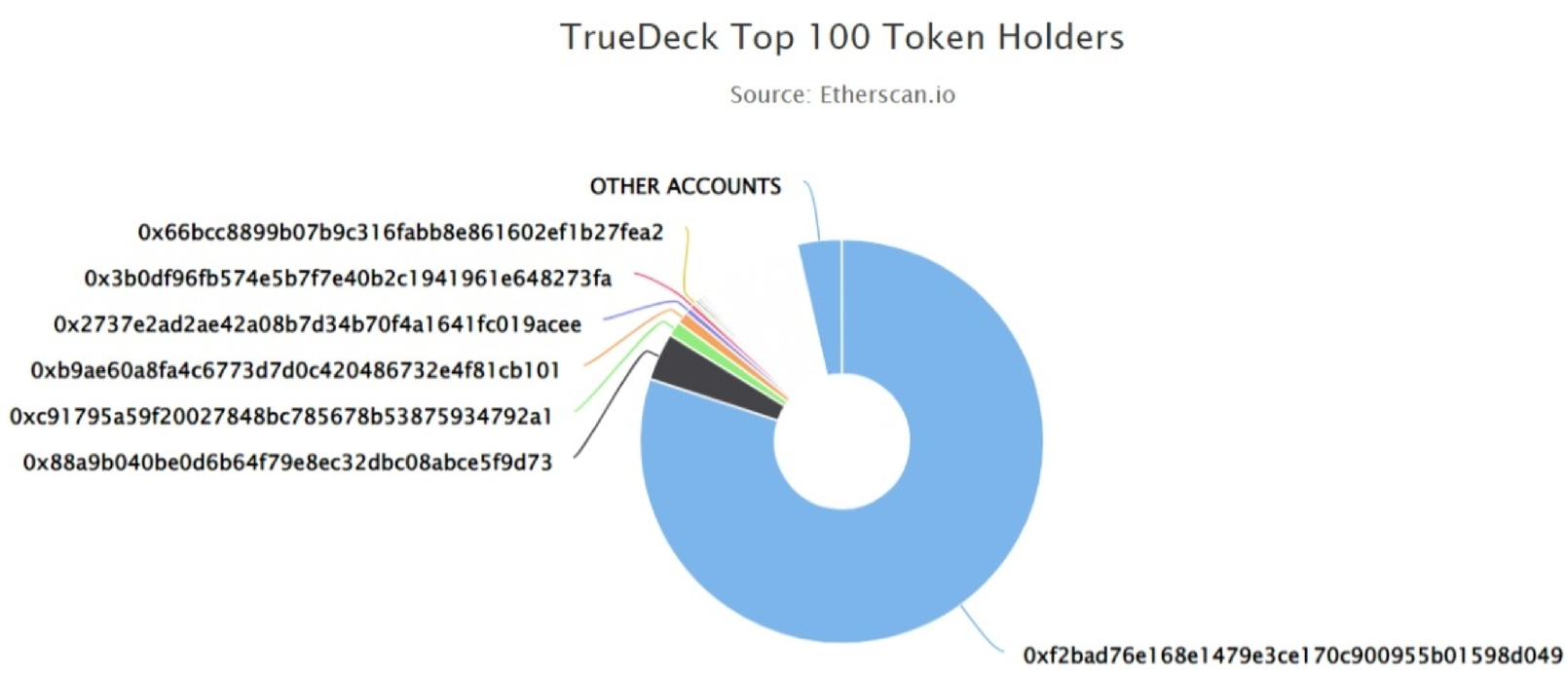
We used various tools like Slither, Mythril and Remix IDE. At the same time this finding is based on critical analysis of the manual audit. All issues found during automated analysis were manually reviewed and applicable vulnerabilities are presented in the issues checking status.

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

TrueDeck Token Distribution

The top 100 holders collectively own 96.42% (192,845,749.61 Tokens) of TrueDeck

Token Total Supply: 200,000,000.00 Token | Total Token Holders: 3,595



TrueDeck Top 20 Token Holders

(A total of 192,845,749.61 tokens held by the top 100 accounts from the total supply of 200,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0xf2bad76e168e1479e3ce170c900955b01598d049	160,000,000	80.0000%
2	0x88a9b040be0d6b64f79e8ec32dbc08abce5f9d73	7,654,419.1581	3.8272%
3	0xc91795a59f20027848bc785678b53875934792a1	2,369,770	1.1849%
4	0xb9ae60a8fa4c6773d7d0c420486732e4f81cb101	1,920,151.434195	0.9601%
5	0x2737e2ad2ae42a08b7d34b70f4a1641fc019acee	978,065.29785908199623499	0.4890%
6	0x3b0df96fb574e5b7f7e40b2c1941961e648273fa	855,314.807364	0.4277%
7	0x66bcc8899b07b9c316fabb8e861602ef1b27fea2	500,000	0.2500%
8	0x4204144629bea3c9feae34b877503057aa394483	468,939.5989698	0.2345%
9	0x46db0dec99c784103f89059d3f38a29b36098621	444,303.467508	0.2222%
10	0x64d6e73f96dd421af2eb88c251e3970118f92aab	403,272.586305	0.2016%
11	0x92ea678d0d9db01c067d19e57dd5e1ba78712979	378,915.92054595984	0.1895%
12	Mercatox	349,380.092912186577366763	0.1747%
13	0xfe226bc9286f7db3cb235cc256873e90569f844b	340,769.573074470919941776	0.1704%
14	0x795d70269280b2051949fd80578fd4961bd075c1	309,149.57928193	0.1546%
15	0xa321aae0cd7cb5b6d721de31eb6ea697e661ed01	305,571.1349124	0.1528%
16	0x56f98a2f4ec898082cef152830aaf7e5a9669161	302,826	0.1514%
17	0x14bdac8f2c77b7611d1813a045ba124dc3fb5a84	300,032.8419	0.1500%
18	0xf0c4b4412d3684876abbd23d92391cd79580ac70	296,067.8	0.1480%
19	0x3e51ac0ee9a0341973f21f9570dae0375a3c4054	292,219.16235	0.1461%
20	0x0c23947f8cc5ffac51c39791ac280ca79ea0f58b	290,427.88694766507	0.1452%

TrueDeck Token Distribution

TrueDeck Contract Overview

Contract functions details

+ SafeMath
    -[Int] mul
    -[Int] div
    -[Int] sub
    -[Int] add

+ERC20
    -[Pub] totalSupply
    -[Pub] balanceOf
    -[Pub] allowance
    -[Pub] transfer
    -[Pub] approve
    -[Pub] transferFrom

+TrueDeckToken (ERC20)
    -[Pub] <constructor>
    -[Pub] totalSupply
    -[Pub] transfer #
    -[Pub] transferFrom #
    -[Pub] approve #
    -[Pub] allowance
    -[Pub] increaseApproval #
    -[Pub] decreaseApproval #
    -[Pub] balanceOf

($) = 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. 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.

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.