HackSafe

Smart Contract Security Audit Report

Talent

January 2023

Security Status

★★★★☆

www.hacksafe.io

Audit Details

Audited project
Talent

Deployer address
0x7790a6dae3174a60e171a25a040f913b5d6054d4

Client contacts
Talent Team

Blockchain
Ethereum

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 Talent to perform an audit of smart contracts:

- https://etherscan.io/token/0x6692de64716a177c15360d8d010bc522bbc530a0#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 06.01.2023

Token Type	: DEFI
Contract name	: Talent
Contract address	: 0x6692De64716a177c15360D8d010BC522bBc530a0
Total supply	: 1,000,000,000
Token ticker	: TNT
Decimals	: 18
Token Holders	: 456
Transactions count	: 505
Compiler version	: v0.5.8+commit.23d335f2
Contract deployer address	: 0x7790a6dae3174a60e171a25a040f913b5d6054d4
Owner address	: 0xc6de650182e065fa7272DB0974409CFa0c244BFc

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.

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 1 low.

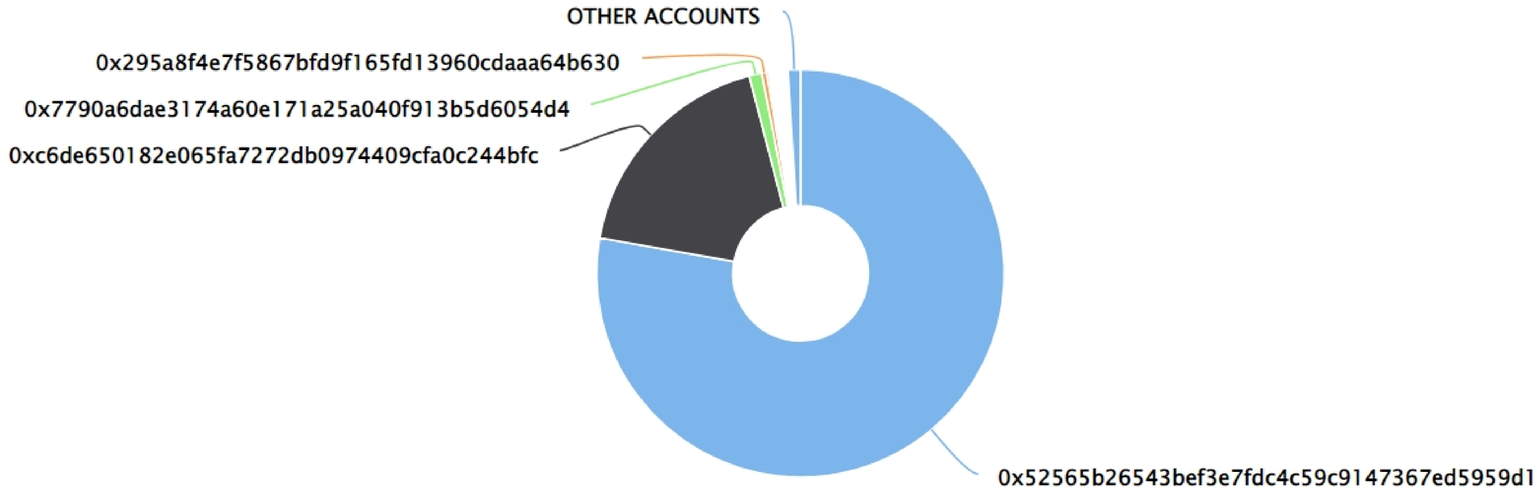
Talent Token Distribution

The top 100 holders collectively own 99.01% (990,101,511.51 Tokens) of Talent

Token Total Supply: 1,000,000,000.00 Token | Total Token Holders: 456

Talent Top 100 Token Holders

Source: Etherscan.io



Talent Top 20 Token Holders

(A total of 990,101,511.51 tokens held by the top 100 accounts from the total supply of 1,000,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0x52565b26543bef3e7fdc4c59c9147367ed5959d1	777,975,085.727099	77.7975%
2	0xc6de650182e065fa7272db0974409cfa0c244bfc	181,570,918.18600339317	18.1571%
3	0x7790a6dae3174a60e171a25a040f913b5d6054d4	10,000,000	1.0000%
4	0x295a8f4e7f5867bfd9f165fd13960cdaaa64b630	3,900,000	0.3900%
5	0x6404fbdff0eb353f00704cd4423fb38f694b3a1f	1,982,210.3403	0.1982%
6	0xfcff5d87c7ebacb5e92b19117fdb5ebdb27d6419	1,319,412.141784	0.1319%
7	0x59d56b0c2233eddf1fca901c42b29fcfc6ff836a	870,827.285441219	0.0871%
8	0xee93ede57fadba712ba9d4fe17269435c67a6864	829,440.3436	0.0829%
9	0x9ebe58c4d47a5272b62d1ac6eb33451e9c74c24a	794,828	0.0795%
10	0xbd5e9495abfb4fa0452abc455a8290b0600a1514	702,102.993001	0.0702%
11	0xd9754c9961cdcbc6175a205341236e5215f71ada	628,374.455	0.0628%
12	0xfdbbdf6852656c007bdf85919fd7d17a0d424eee	550,000	0.0550%
13	0xb9d982c4dd88bac623afe979f31cb4a32147de07	522,496.372	0.0522%
14	0x9272bb93a904f997f402de8ba339e358d9ee5916	520,000	0.0520%
15	0x04f1ba517ad83188ebd896c7a48c5e86d6d1c04b	520,000	0.0520%
16	0x5135025604fd318a98f7fb083481d1f101a48b46	493,468.795516691	0.0493%
17	0x120051a72966950b8ce12eb5496b5d1eeec1541b	488,553.6597	0.0489%
18	0x3f23ce0899ab5c087358d022b1e124038b7f9c45	401,728	0.0402%
19	0xf9907c892159c44802617d18bafea2ad5648daa5	300,000	0.0300%
20	0x07c3c9c5c5240a67467a652293a7afa1187a0c54	220,308	0.0220%

Talent Token Distribution

Talent Contract Overview

Contract functions details

+[Int] IcERC20
    -[Ext] totalSupply
    -[Ext] balanceOf
    -[Ext] transfer
    -[Ext] allowance
    -[Ext] approve

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

+ERC20 (IERC20)
    -[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] _burnFrom #

+Talent (ERC20)
    -[Pub] < constructor>
    -[Pub] transferOwnership #
      -modifiers: onlyOwner
    -[Int] _transferOwnership #
    -[Pub] transfer #
    -[Pub] transferFrom #
    -[Pub] burn #
      -modifiers: onlyOwner
    -[Pub] balanceOf
    -[Int] releaseLock #

Contract functions details

-[Pub] lockCount
-[Pub] lockState
-[Pub] lock #
  -modifiers: onlyOwner
-[Pub] unlock #
  -modifiers: onlyOwner
-[Pub] transferWithLock #
  -modifiers: onlyOwner

($) = 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 Issue
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

One medium severity issue found.

1. Out of gas limit

- **Description**

  The function balanceOf (), releaseLock() uses the loop to add locked balance. Function will be aborted with OUT_OF_GAS exception if there will be a long length of lockInfo mapping .

- **Recommendation**

  Use EnumerableSet instead of array or do not use long arrays.

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 :

- Talent Contract:

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
- burn
- lock
- unlock
- transferWithLock

Conclusion

Smart contract contains low and 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.