HackSafe

Smart Contract Security Audit Report

Octa Gold

December 2022

Security Status

★★★★☆

www.hacksafe.io

Audit Details

Audited project
Octa Gold

Deployer address
0xa8fa6fdcd031c4709c0497bcfd4fde6332c3e695

Client contacts
Octa Gold Team

Blockchain
Binance smart chain

Website
https://bsc.octax.finance/

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 Octa gold to perform an audit of smart contracts:

- https://bscscan.com/address/0x4F1498da0f50F94e97F900b7e6E13d8e5220aBE9#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 01.12.2022

Token Type	: DEFI
Contract name	: OctaGold
Contract address	: 0x4F1498da0f50F94e97F900b7e6E13d8e5220aBE9
Total supply	: 888,888
Token ticker	: OCTAG
Decimals	: 18
Token Holders	: 4,007
Transactions count	: 16,130
Compiler version	: v0.6.12+commit.27d51765
Contract deployer address	: 0xa8fa6fdcd031c4709c0497bcfd4fde6332c3e695
Owner address	: 0xa8fa6fdcd031c4709c0497bcfd4fde6332c3e695

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, 1 medium and 1 low.

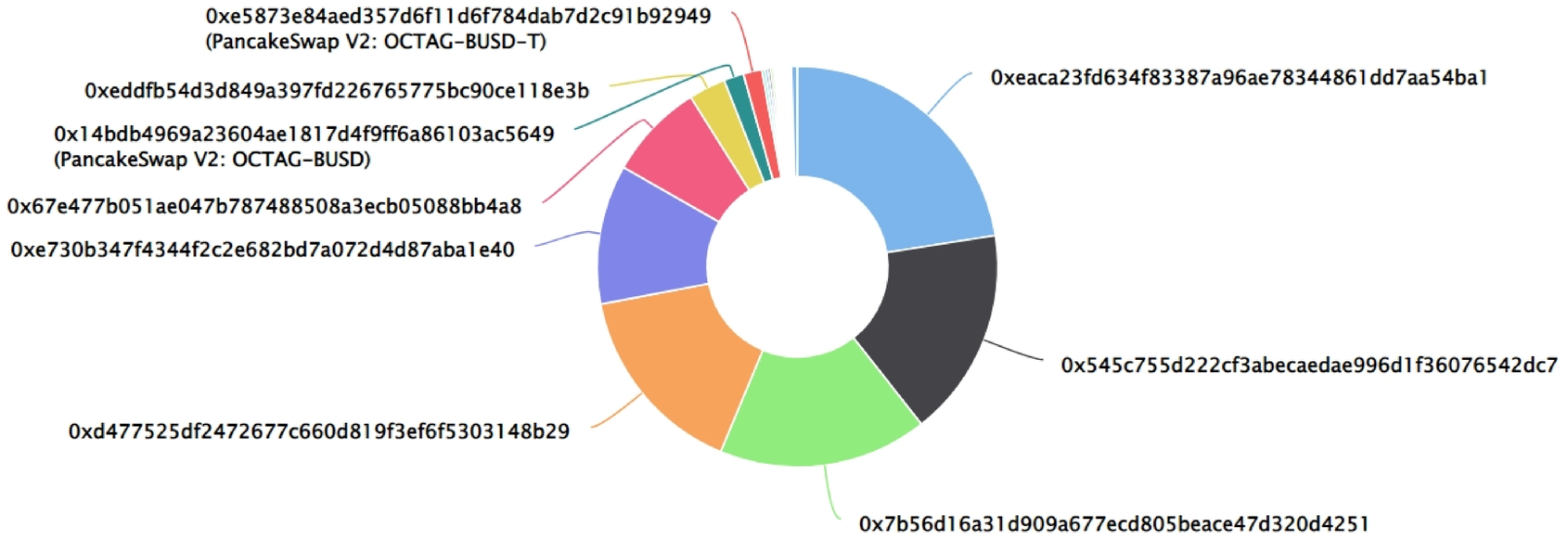
OctaGold Distribution

The top 100 holders collectively own 99.53% (884,700.19 Tokens) of Octa Gold

Token Total Supply: 888,888.00 Token | Total Token Holders: 4,007

Octa Gold Top 100 Token Holders

Source: BscScan.com



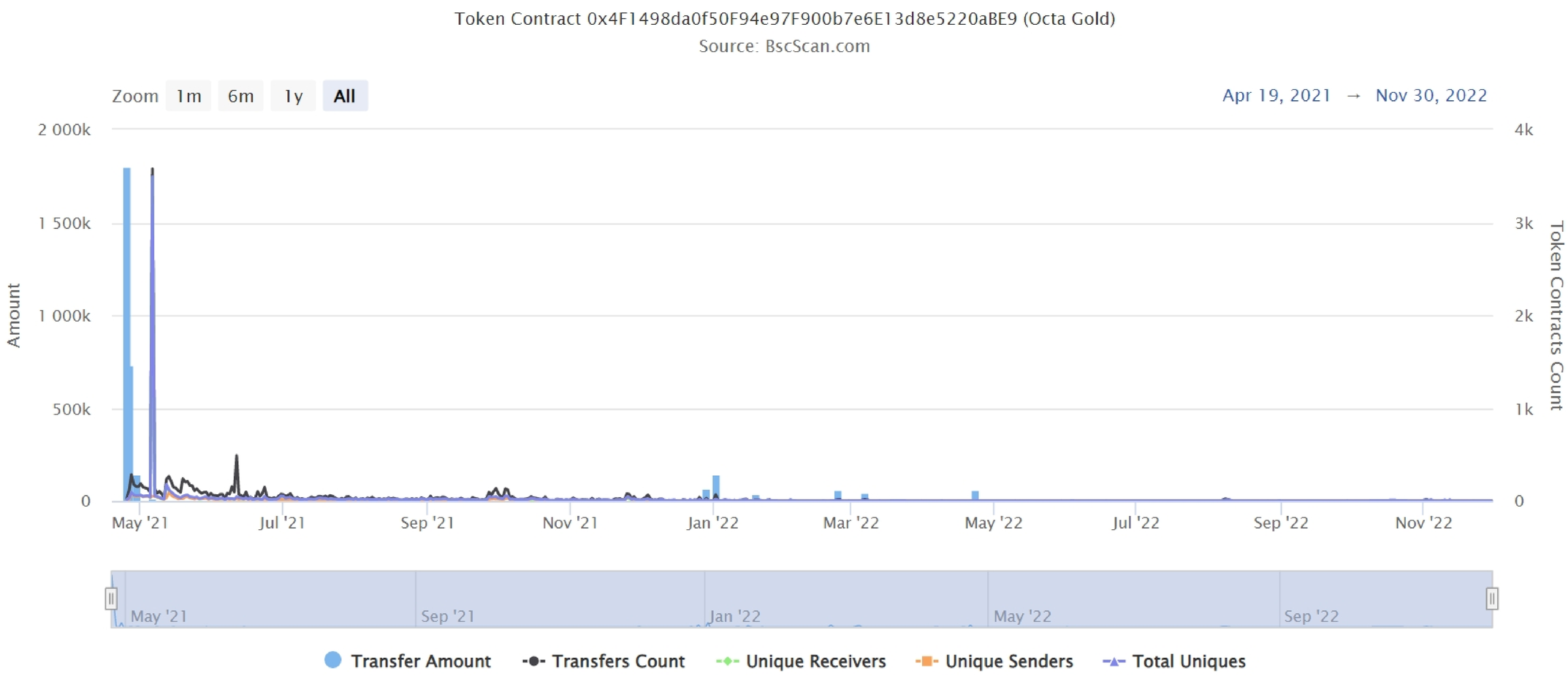
OctaGold Top 20 Token Holders

(A total of 884,700.19 tokens held by the top 100 accounts from the total supply of 888,888.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0xeaca23fd634f83387a96ae78344861dd7aa54ba1	200,171.822959213378676007	22.5194%
2	0x545c755d222cf3abecaedae996d1f36076542dc7	150,000	16.8750%
3	0x7b56d16a31d909a677ecd805beace47d320d4251	150,000	16.8750%
4	0xd477525df2472677c660d819f3ef6f5303148b29	140,000	15.7500%
5	0xe730b347f4344f2c2e682bd7a072d4d87aba1e40	100,000	11.2500%
6	0x67e477b051ae047b787488508a3ecb05088bb4a8	69,342.558828979841344944	7.8010%
7	0xeddfb54d3d849a397fd226765775bc90ce118e3b	26,471.27756019907940691	2.9780%
8	PancakeSwap V2: OCTAG-BUSD	14,166.289731844227694136	1.5937%
9	PancakeSwap V2: OCTAG-BUSD-T	13,314.193002127592837599	1.4978%
10	0x486d71107734b75be7fb1ace806a2db87645f04b	2,406.65811580159964596	0.2707%
11	PancakeSwap V2: OCTAX-OCTAG	2,180.376480543120823091	0.2453%
12	0xd711ee1274e3f6e910fc81c2cccd31bc2f98aec9	1,890.636576460777593083	0.2127%
13	0x1c13e40ca0175449090975f054bb5942a4edb137	1,729.235051925847405102	0.1945%
14	0xec8c1c24cc027f106fc15dbe584c3acc3bad8c4e	1,113.491733333015596375	0.1253%
15	0xf4f9ad5f3a001aba56bfb73d0c91c7b65cc145ca	1,059.837881378713100231	0.1192%
16	0x576c1549152570d1088d572a6addb3d7dd9295ab	918.659664814605916272	0.1033%
17	0xc8a6788c23fb07ea1cb5a73310329514a6937ef9	850.91752045451808696	0.0957%
18	0x1273790c41414f1c58112868751abdd52cad11f8	775.722819490998307068	0.0873%
19	0x76598e90df66d33518ee5be01fd548f9e96ff40f	758.129453660064585827	0.0853%
20	0x1698c7e8aca65e28a0dc41c0e32b068d615f491a	638.894607721722571603	0.0719%

OctaGold Distribution

OctaGold Overview



Contract functions details

OctaGold.sol
+OctaGold (BEP20)
  -[Pub] mint #
    -modifiers: onlyOwner
  -[Ext] delegates
  -[Ext] delegate
  -[Ext] delegateBySig
  -[Ext] getCurrentVotes
  -[Ext] getPriorVotes
  -[Int] _delegate
  -[Int] _moveDelegates
  -[Int] _writeCheckpoint
  -[Int] safe32
  -[Int] getChainId

BEP20.sol
+BEP20 (Context, IBEP20, Ownable)
  -[Pub] <constructor>
  -[Ext] getOwner
  -[Pub] name
  -[Pub] symbol
  -[Pub] decimals
  -[Pub] totalSupply
  -[Pub] balanceOf
  -[Pub] transfer #
  -[Pub] allowance
  -[Pub] approve #
  -[Pub] transferFrom #
  -[Pub] increaseAllowance #
  -[Pub] decreaseAllowance #
  -[Pub] mint #
    -modifiers: onlyOwner
  -[Int] _transfer #
  -[Int] _mint #
  -[Int] _burn #
  -[Int] _approve #
  -[Int] _burnFrom #

Contract functions details

IBEP20.sol
+[Int] IERC20
-[Ext] totalSupply
-[Ext] decimals
-[Ext] symbol
-[Ext] name
-[Ext] getOwner
-[Ext] balanceOf
-[Ext] transfer
-[Ext] allowance
-[Ext] approve
-[Ext] transferFrom

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

SafeMath.sol
+[Lib] SafeMath
-[Int] tryAdd
-[Int] trySub
-[Int] tryMul
-[Int] tryDiv
-[Int] tryMod
-[Int] add
-[Int] sub
-[Int] mul
-[Int] div
-[Int] mod
-[Int] sub
-[Int] div
-[Int] mod

Contract functions details

Context.sol
+Context
-[Int] _msgSender
-[Int] _msgData

($) = 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.	Medium issue
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. Safe Open Zeppelin contracts implementation and usage.

- **Description**

  The contract file BEP20.sol has direct imported openzeppelin contract as any changes in that repository can affect this smart contract too.

- **Recommendation**

  It is advisable to not direct import any file from any sources.

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 :

- Octa Gold Contract:
    - Owner can renounce and transfer 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:

- renounceOwnership
- transferOwnership
- mint

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.