HackSafe

Smart Contract Security Audit Report

EXENO COIN

September 2022

Security Status

★★★★½

www.hacksafe.io

Audit Details

Audited project
EXENO COIN

Deployer address
0xa190D367c57F35Eb50327803599e5d139B98A045

Client contacts
EXENO COIN Team

Blockchain
Binance Smart Chain

Website
https://exeno.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 EXENO COIN to perform an audit of smart contracts:

- https://bscscan.com/address/0x0c9b3ab1bd0cf0745625381f5c3aa1cd9bbc7abb#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 13.09.2022

Token Type	: ERC20
Contract name	: ExenoToken_L2
Contract address	: 0x0c9b3aB1bd0CF0745625381F5C3Aa1CD9BBc7Abb
Compiler version	: v0.8.11+commit.d7f03943
Total supply	: 50,000,000
Token ticker	: EXN
Decimals	: 18
Token holders	: 103
Transactions count	: 133
Contract deployer address	: 0xa190D367c57F35Eb50327803599e5d139B98A045
Owner address	: 0xa190d367c57f35eb50327803599e5d139b98a045
Manager address	: 0xa190d367c57f35eb50327803599e5d139b98a045

Social profiles

Twitter profile:	: https://twitter.com/ExenoOfficial
Telegram profile	: https://t.me/exeno_com
LinkedIN Profile	: https://www.linkedin.com/company/exeno
Facebook profile	: https://www.facebook.com/exeno
Coinmarketcap profile	: https://coinmarketcap.com/currencies/exeno-coin/
Coingecko profile	: https://www.coingecko.com/en/coins/exeno/

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	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.

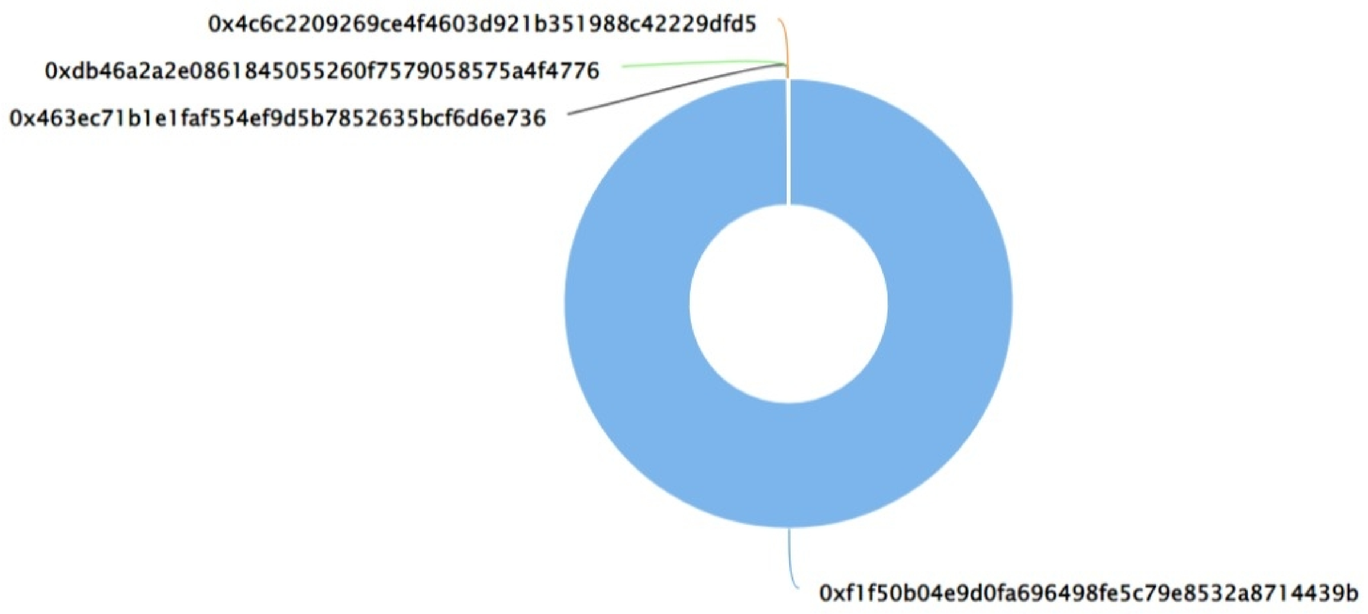
EXENO COIN Token Distribution

The top 100 holders collectively own 100.00% (49,999,989.00 Tokens) of EXENO COIN

Token Total Supply: 50,000,000.00 Token | Total Token Holders: 103

EXENO COIN Top 100 Token Holders

Source: BscScan.com



EXENO COIN Top 20 Token Holders

(A total of 49,999,989.00 tokens held by the top 100 accounts from the total supply of 50,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0xf1f50b04e9d0fa696498fe5c79e8532a8714439b	49,953,200.115533308179802282	99.9064%
2	0x463ec71b1e1faf554ef9d5b7852635bcf6d6e736	11,000	0.0220%
3	0xdb46a2a2e0861845055260f7579058575a4f4776	7,145.4512857	0.0143%
4	0x4c6c2209269ce4f4603d921b351988c42229dfd5	6,000.01537771357820957	0.0120%
5	0x858a91969eaad5c0b22923d00bd44d50f28f8dd2	2,750.000000000000000627	0.0055%
6	0x0574bb013dcc2bb72ff735965a79d6bf3967a452	850.000000000000001369	0.0017%
7	0xf85f3dd5e5426cfc967d494b237eea77fcdd00a0	731.000000000000000705	0.0015%
8	0xdb6266a05ef66d6bd810d6bb7162e6fa80872874	700.000000000000000613	0.0014%
9	0xd15bcae2308ebc0804659f1796449da32c8a67ab	600.000000000000001225	0.0012%
10	0xb65b86a997c5ee2ea12047f3903af812b1fd947b	571.4285714	0.0011%
11	0x12a7c1f5dea764f9dd3184a94246734d2591fea9	517.1428571	0.0010%
12	0x49149dc170b75451b5d4d4a95d3f9fbd76cab747	451.4285714	0.0009%
13	0x2165cf00b1e4a6b16242814675ab93749e49c720	428.5714286	0.0009%
14	0x33038fa42da48320aaf3ef973a573eedd18c55f7	385.7142857	0.0008%
15	0xe5499877349ac499427d3843745900449658a7c3	348.5714286	0.0007%
16	0xa6c13315d5ff7c544326be3198061a2beb75df5e	342.8571429	0.0007%
17	0x70a3f83cad7242eb8c3578e02b02fc777bdb04ec	298.5714286	0.0006%
18	0x4a4891a3de18f8dda99e60299e93dd55601f5e11	292.8571429	0.0006%
19	0xdb2f0f4e5c4e85f4f02f369dadff4a89da72f041	291.4285714	0.0006%
20	0x362d614d2cf2f34afa94563882f60e45ab4a8a4d	285.7142857	0.0006%

Contract functions details

+[Int] IERC1363Spender
  -[Ext] onApprovalReceived

+[Int] IERC1363Receiver
  -[Ext] onTransferReceived

+[Int] IERC165
  -[Ext] supportsInterface

+ ERC165 (IERC165)
  -[Pub] supportsInterface

+[Lib] Address
  -[Int] isContract
  -[Int] sendValue
  -[Int] functionCall
  -[Int] functionCall
  -[Int] functionCallWithValue
  -[Int] functionCallWithValue
  -[Int] functionStaticCall
  -[Int] functionStaticCall
  -[Int] functionDelegateCall
  -[Int] functionDelegateCall
  -[Int] verifyCallResult

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

+[Int] IERC1363 (IERC20, IERC165)
  -[Ext] transferAndCall
  -[Ext] transferAndCall
  -[Ext] transferFromAndCall
  -[Ext] transferFromAndCall
  -[Ext] approveAndCall
  -[Ext] approveAndCall

Contract functions details

+[Int] IERC20Metadata (IERC20)
- -[Ext] name
- -[Ext] symbol
- -[Ext] decimals

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

+ERC20 (Context, IERC20, IERC20Metadata)
- -<constructor>
- -[Pub] name
- -[Pub] symbol
- -[Pub] decimals
- -[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] _spendAllowance #
- -[Int] _beforeTokenTransfer #
- -[Int] _afterTokenTransfer #

+ERC1363 (ERC20, IERC1363, ERC165)
- -[Pub] supportsInterface
- -[Pub] transferAndCall
- -[Pub] transferAndCall
- -[Pub] transferFromAndCall
- -[Pub] transferFromAndCall
- -[Pub] approveAndCall
- -[Pub] approveAndCall

Contract functions details

-[Int] _checkAndCallTransfer
-[Int] _checkAndCallApprove

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

+ ExenoToken_L2 (Ownable, ERC1363)
-<constructor>
-[Ext] setManager #
-modifiers: onlyOwner
-[Ext] mint #
-modifiers: onlyManager
-[Ext] burn #
-modifiers: onlyManager

($) = payable function
= non-constant function

Issues Checking Status

No.	Title	Status
1.	Unlocked Compiler Version	Low issue
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

One low severity issue found.

1. Unlocked Compiler Version.

- **Description**

  The contract utilizes an unlocked compiler version. An unlocked compiler version in the contract's source code permits the user to compile it at or above a particular version. This, in turn, leads to differences in the generated bytecode between compilations due to differing compiler version numbers. This can lead to ambiguity when debugging as compiler-specific bugs may occur in the codebase that would be difficult to identify over a span of multiple compiler versions rather than a specific one.

- **Recommendation**

  It is advisable that the compiler version is alternatively locked at the lowest version possible so that the contract can be compiled. For example, for version ^0.8.0 the contract should contain the following line:

  pragma solidity 0.8.11;

Centralization

Owner Privileges :

- EXENO COIN Contract:
    - Owner can renounce and transfer ownership.
    - Owner can change manager address .
    - Manager can mint and burn 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 functions:

- Transferownership
- Renounceownership
- Mint
- Burn
- Setmanager

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.