HackSafe

Smart Contract Security Audit Report

ZelusTestNFT

May **2022**

Security Status

★★★★☆

www.hacksafe.io

Audit Details

Audited project
ZelusTestNFT

Deployer address
0x8E03D316CB0a07dfd89C7586CFDDbf6542356281

Client contacts
ZelusTestNft team

Blockchain
Avalanche

Website
not provided by team

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 ZelusTestNft team to perform an audit of smart contract:

- https://snowtrace.io/address/0xDA635Ca13321b7cf2D57320Ca53A2f6695CC6D36#code

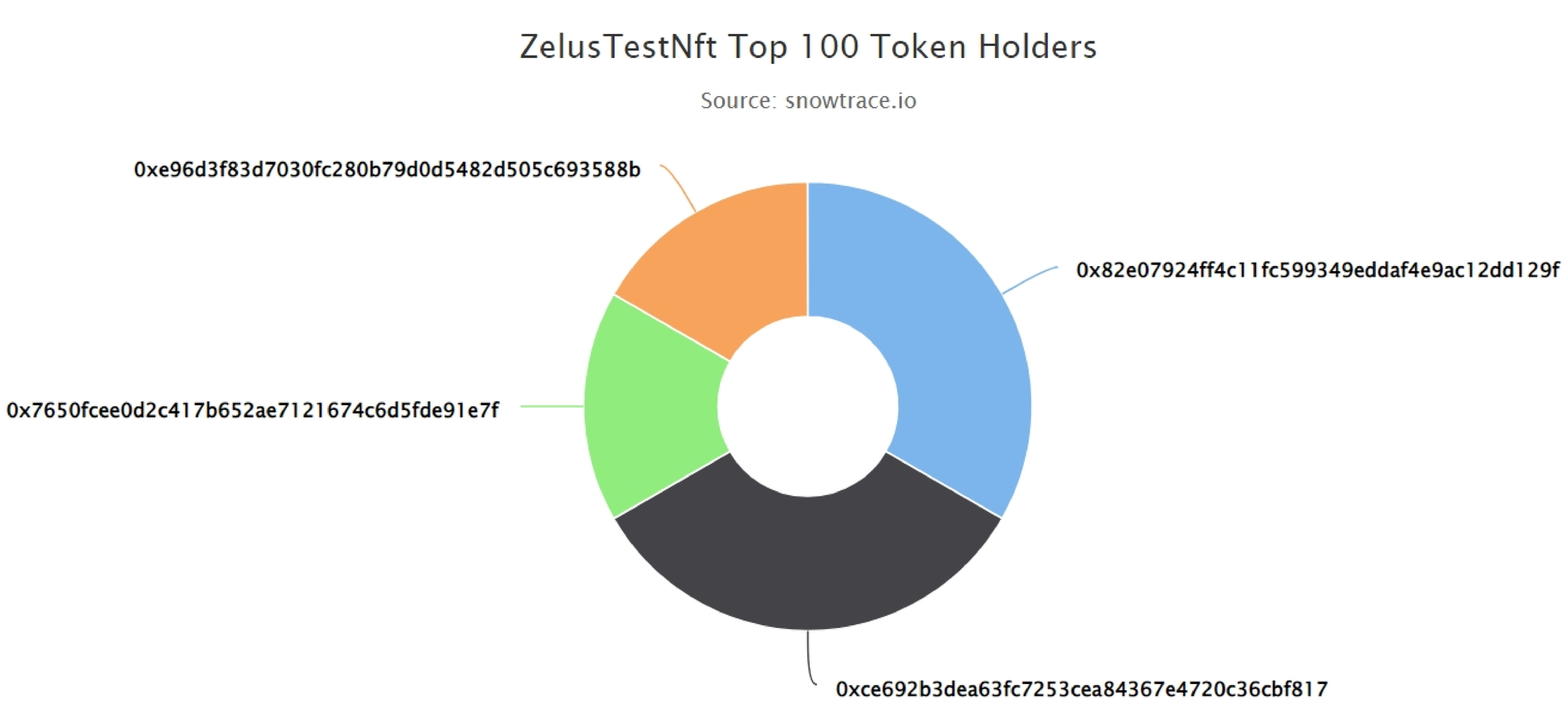
Contract Details

Token contract details for 27.05.2022

Contract name	: ZelusTestNft
Contract address	: 0xDA635Ca13321b7cf2D57320Ca53A2f6695CC6D36
Compiler version	: v0.8.1+commit.df193b15
Token Ticker	: ZTN
Token Type	: ERC1155Token
Token Holders	: 4
Transactions count	: 16
Contract deployer address	: 0x8E03D316CB0a07dfd89C7586CFDDbf6542356281
owner address	: 0x8E03D316CB0a07dfd89C7586CFDDbf6542356281

ZTN Token Distribution

Token Total Supply: 0.00 Token | Total Token Holders: 4



ZTN Top 4 Token Holders

(A total of 6.00 tokens held by the top 100 accounts from the total supply of 0.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0x82e07924ff4c11fc599349eddaf4e9ac12dd129f	2	-
2	0xce692b3dea63fc7253cea84367e4720c36cbf817	2	-
3	0x7650fcee0d2c417b652ae7121674c6d5fde91e7f	1	-
4	0xe96d3f83d7030fc280b79d0d5482d505c693588b	1	-

Contract functions details

ZelusTestNft.sol
+ ZelusTestNft (ERC1155, Ownable)
    -[Pub] <constructor> #
    -[Pub] setURI
      -modifier: onlyOwner
    -[Pub] mint #
      -modifier: onlyOwner
    -[Pub] mint #
      -modifier: onlyOwner

ERC1155.sol
+ ERC1155 (Context, ERC165, IERC1155, IERC1155MetadataURI)
    -<constructor> #
    - [Pub] supportsInterface
    - [Pub] uri
    -[Pub] balanceOf
    -[Pub] balanceOfBatch
    -[Pub] setApprovalForAll #
    -[Pub] isApprovedForAll #
    -[Pub] safeTransferFrom #
    -[Pub] safeBatchTransferFrom #
    -[Int] _safeTransferFrom #
    - [Int] _safeBatchTransferFrom #
    -[Int] _setURI #
    -[Int] _mint #
    -[Int] _mintBatch #
    -[Int] _burn #
    -[Int] _burnBatch #
    -[Int] _setApprovalForAll #
    -[Int] _beforeTokenTransfer #
    -[Int] _afterTokenTransfer #
    -[Pvt] _doSafeTransferAcceptanceCheck #
    -[Pvt] _doSafeBatchTransferAcceptanceCheck #
    -[Pvt] _asSingletonArray #

Contract functions details

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

IERC1155.sol
+[Int] IERC1155 (IERC165)
    -[Ext] balanceOf
    -[Ext] balanceOfBatch
    -[Ext] setApprovalForAll #
    -[Ext] isApprovedForAll #
    -[Ext] safeTransferFrom #
    -[Ext] safeBatchTransferFrom #

IERC1155Receiver.sol
+[Int] IERC1155Receiver (IERC165)
    -[Ext] onERC1155Received
    -[Ext] onERC1155BatchReceived #

IERC1155MetadataURI.sol
+ [Int] IERC1155MetadataURI (IERC1155)
    -[Ext] uri

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

Contract functions details

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

ERC165.sol
+ ERC165 (IERC165)
    -[Pub] supportsInterface #

IERC165.sol
+ [Int] IERC165
    -[Ext] supportsInterface

($) = 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.	Low issue
15.	Uninitialized storage pointers.	Passed
16.	Arithmetic accuracy.	Passed
17.	Design Logic.	Passed
18.	Safe Open Zeppelin contracts implementation and usage.	Low issue
19.	Incorrect Naming State Variable	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

Three 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 ^0.8.1 the contract should contain the following line:

  pragma solidity 0.8.1;

2. Scoping and Declarations.

Unused function.

- **Description**

  The sendValue, functionCall, functionCallWithValue, _functionCallWithValue, functionDelegateCall, functionStaticCall do nothing In the contract.

- **Location:**

  Adress.sol -> sendValue, functionCall, functionCallWithValue, _functionCallWithValue, functionDelegateCall, functionStaticCall functions.

- **Recommendation:**

  We advise to remove the mentioned function which can help you to develop clean coding style and save some computational gas too.

3. Safe Open Zeppelin contracts implementation and usage.

Import openzeppelin contract

- **Description**

  In ZelusTestNft.sol has imported openzeppelin contracts direct which is not recommended.

- **Location:**

  ZelusTestNft.sol

- **Recommendation:**

  We advise you to remove openzeppelin import line from ZelusTestNft.sol as any changes in openzeppelin cotnracts or github repository may cost your contract a big loss.

Owner Privileges

Owner Privileges (in the period when the owner is not renounced) :

- ZelusTestNFT CHAIN Contract:
    - owner can set URI.
    - Owner can mint tokens.
    - Owner can renounce ownership.
    - owner can transfer ownership.

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.