HackSafe

Smart Contract Security Audit Report

LegendHeroNFT

July 2022

Security Status

★★★★½

www.hacksafe.io

Audit Details

Audited project
LegendHeroNFT

Deployer address
0x5e2F9cFD19BcFc4b48963c4fC76954657C31Ea92

Client contacts
LegendHeroNFT team

Blockchain
Binance Smart Chain

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 LegendHeroNFT to perform an audit of smart contracts:

- https://bscscan.com/address/0x054eddf9af1bff80286b2c27c64baa0c8e94ce08#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 29.07.2022

Token Type	: BEP-721
Contract name	: HeroNftToken
Contract address	: 0x054eDDF9Af1Bff80286B2c27c64bAa0C8E94ce08
Compiler version	: v0.8.7+commit.e28d00a7
Token Ticker	: LegendHeroNFT
Token Holders	: 3,767
Transactions count	: 9,383
Contract deployer address	: 0x5e2f9cfd19bcfc4b48963c4fc76954657c31ea92
Owner address	: 0x5e2f9cfd19bcfc4b48963c4fc76954657c31ea92

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

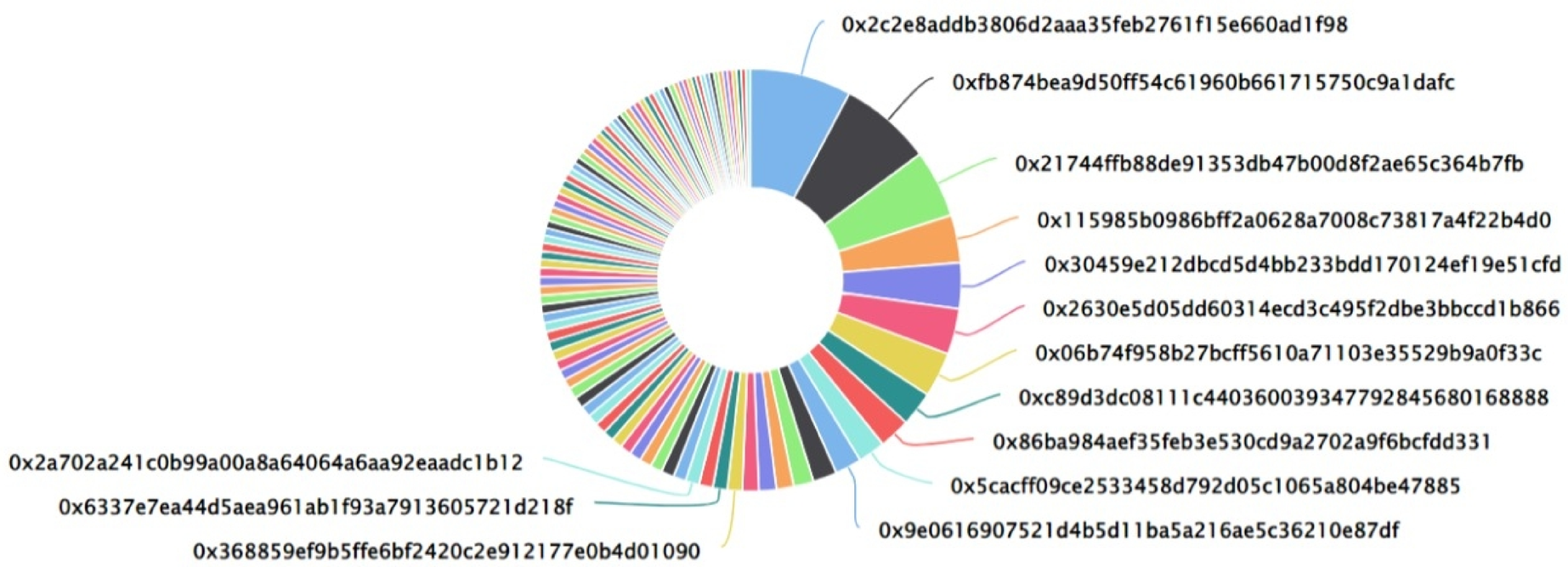
You are here 

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.

LegendHeroNFT Token Distribution

Token Total Supply: 0.00 Token | Total Token Holders: 3,767



LegendHeroNFT Top 20 Token Holders

(A total of 1,426.00 tokens held by the top 100 accounts from the total supply of 0.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0x2c2e8addb3806d2aaa35feb2761f15e660ad1f98	111	-
2	0xfb874bea9d50ff54c61960b661715750c9a1dafc	101	-
3	0x21744ffb88de91353db47b00d8f2ae65c364b7fb	74	-
4	0x115985b0986bff2a0628a7008c73817a4f22b4d0	52	-
5	0x30459e212dbcd5d4bb233bdd170124ef19e51cfd	50	-
6	0x2630e5d05dd60314ecd3c495f2dbe3bbccd1b866	50	-
7	0x06b74f958b27bcff5610a71103e35529b9a0f33c	49	-
8	0xc89d3dc08111c4403600393477928456801688888	38	-
9	0x86ba984aef35feb3e530cd9a2702a9f6bcfdd331	34	-
10	0x5cacff09ce2533458d792d05c1065a804be47885	30	-
11	0x9e0616907521d4b5d11ba5a216ae5c36210e87df	29	-
12	0xed6a79ca81d0b69b820dddf474126fe602e9d295	26	-
13	0xee1924b0c9c62be53e76cac427f9a142d474b50c	22	-
14	0x3253dca4a14a343adfeb3bc460312ed7c531610e	19	-
15	0x2f4e0fa9a06b12e3f960db2d3a145e9cbbb93e6f	19	-
16	0x197c0f9d24f5f237429d20631d81c55ef5e5f073	18	-
17	0x368859ef9b5ffe6bf2420c2e912177e0b4d01090	16	-
18	0x6337e7ea44d5aea961ab1f93a7913605721d218f	16	-
19	0x947de4df890e35a938dcff001adb8913ffe5f0d4	15	-
20	0x2a702a241c0b99a00a8a64064a6aa92eaadc1b12	15	-

Contract functions details

+ [Int] IERC721Token
    -[Ext] mintHeroNft
    -[Ext] mintHeroNfts
    -[Ext] transferHero

+[Lib] Counters
    -[Int] current
    -[Int] increment
    -[Int] decrement
    -[Int] reset

+[Lib] Strings
    -[Int] toString
    -[Int] toHexString
    -[Int] toHexString

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

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

+ [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

+ [Int] IERC721Token
    -[Ext] onERC721Received

+[Int] IERC165
    -[Ext] supportsInterface

+ ERC165 (IERC165)
    -[Pub] supportsInterface

+ [Int] IERC721 (IERC165)
    -[Ext] balanceOf
    -[Ext] ownerOf
    -[Ext] safeTransferFrom
    -[Ext] transferFrom
    -[Ext] approve
    -[Ext] getApproved
    -[Ext] setApprovalForAll
    -[Ext] isApprovedForAll
    -[Ext] safeTransferFrom

+[Int] IERC721Metadata (IERC721)
    -[Ext] name
    -[Ext] symbol
    -[Ext] tokenURI

+ ERC721 (Context, ERC165, IERC721, IERC721Metadata)
    -<constructor>
    -[Pub] supportsInterface
    -[Pub] balanceOf
    -[Pub] ownerOf
    -[Pub] name
    -[Pub] symbol
    -[Pub] tokenURI
    -[Int] _baseURI
    -[Pub] approve #
    -[Pub] getApproved
    -[Pub] setApprovalForAll #
    -[Pub] isApprovedForAll
    -[Pub] transferFrom #
    -[Pub] safeTransferFrom #
    -[Pub] safeTransferFrom #
    -[Int] _safeTransfer #

Contract functions details

-[Int] _exists #
-[Int] _isApprovedOrOwner #
-[Int] _safeMint #
-[Int] _safeMint #
-[Int] _mint #
-[Int] _burn #
-[Int] _transfer#
-[Int] _approve #
-[Int] _setApprovalForAll #
-[Pvt] _checkOnERC721Received #
-[Int] _beforeTokenTransfer
-[Int] _afterTokenTransfer

+ ERC721URIStorage (ERC721)
-[Pub] tokenURI
-[Int] _setTokenURI #
-[Int] _burn #

+ HeroNftToken (ERC721, ERC721URIStorage, IERC721Token, Ownable)
-<constructor>
-[Pub] setFeeTradeSwitch #
-modifiers: onlyOwner
-[Pub] addOperators #
-modifiers: onlyOwner
-[Pub] setBaseURI#
-modifiers: onlyOwner
-[Int] _setTokenURI #
-[Int] _baseURI #
-[Int] _burn #
-[Pub] tokenURI
-[Pub] transferHero #
-[Pub] mintHeroNfts #
-[Pub] mintHeroNft #
-[Pub] safeTransferFrom #
-[Pub] transferFrom #
-[Pub] safeTransferFrom #

($) = 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.	Low 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	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. DoS with block gas limit.

Out of gas

- **Description**

  The function mintHeroNfts has loop to mint the bunch of nfts. The function might be aborted with the out of gas exception if there will be long nftcounts.

- **Recommendation**

It is advisable to check the length of nftcounts variable, it should be short.

Centralization

Owner privileges:

- LegendHeroNFT Contract:
    - Owner can transfer and renounce ownership.
    - Owner can set fee for trade.
    - Owner can add operators.
    - Owner can set Base URI.

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
- Setfeetradeswitch
- Addoperators
- Setbaseuri

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.