HackSafe

Smart Contract Security Audit Report

NDFT

September 2022

Security Status

★★★★½

www.hacksafe.io

Audit Details

Audited project
NDFT

Deployer address
0x7aB35F18eDC4db56B5ceC7499c727fb6BB5f80D5

Client contacts
NDFT Team

Blockchain
Binance smart chain

Website
https://ndft.io/

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 NDFT to perform an audit of smart contracts:

- https://bscscan.com/address/0x33c6e531a1e8b46cc1263ecba412877053d1a766#code

The purpose of the audit was to achieve the following:

- 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 26.09.2022

Token Type	: BEP20
Contract name	: NDFT
Contract address	: 0x33C6E531A1e8B46cc1263ECBA412877053d1a766
Total supply	: 21,000,000
Token ticker	: NDFT
Decimals	: 8
Token holders	: 845
Transactions count	: 4,469
Compiler version	: v0.8.9+commit.e5eed63a
Contract deployer address	: 0x7aB35F18eDC4db56B5ceC7499c727fb6BB5f80D5
Owner address	: 0x7ab35f18edc4db56b5cec7499c727fb6bb5f80d5

Social profiles

Twitter Profile	: https://twitter.com/Ndft_Official
Facebook profile	: https://www.facebook.com/NDFT_Official-104147148716016
Telegram profile	: https://t.me/ndftofficialchannel

Claimed Smart Contract Features

Claimed Feature Detail

Tokenomics :

- **Name** : NDFT
- **Symbol** : NDFT
- **Decimals** : 8
- **Protocol** : BEP20
- **Total supply** : 21,000,000
- **Contract address** : 0x33C6E531A1e8B46cc1263ECBA412877053d1a766

Our Observation

YES, this is valid.

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 

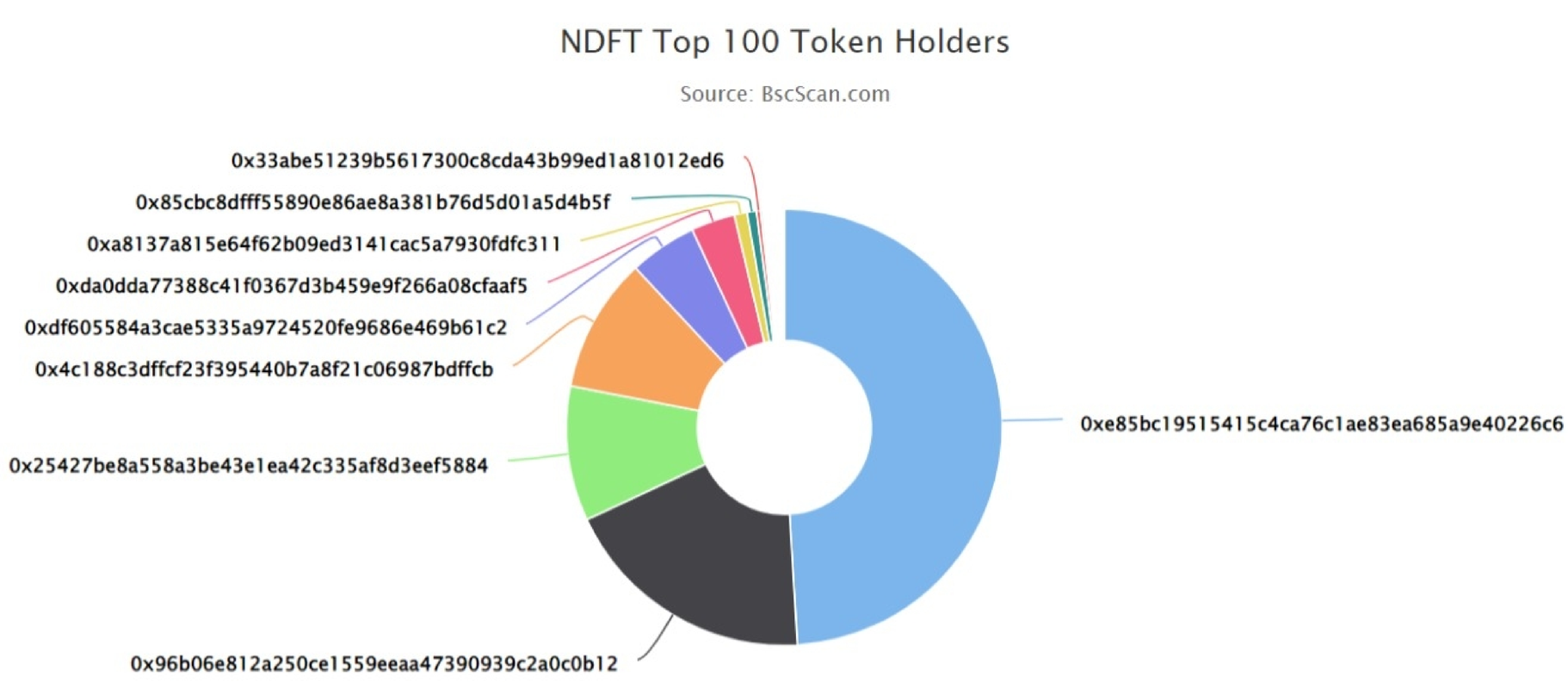
We used various tools like Slither, Mythril and Remix IDE. At the same time this finding is based on critical analysis of the manual audit. All issues found during automated analysis were manually reviewed and applicable vulnerabilities are presented in the issues checking status.

We found 0 critical, 0 high, 0 medium and 0 low and some very low-level issues. These issues are not critical ones.

NDFT Token Distribution

The top 100 holders collectively own 99.95% (20,989,886.09 Tokens) of NDFT

Token Total Supply: 21,000,000.00 Token | Total Token Holders: 845

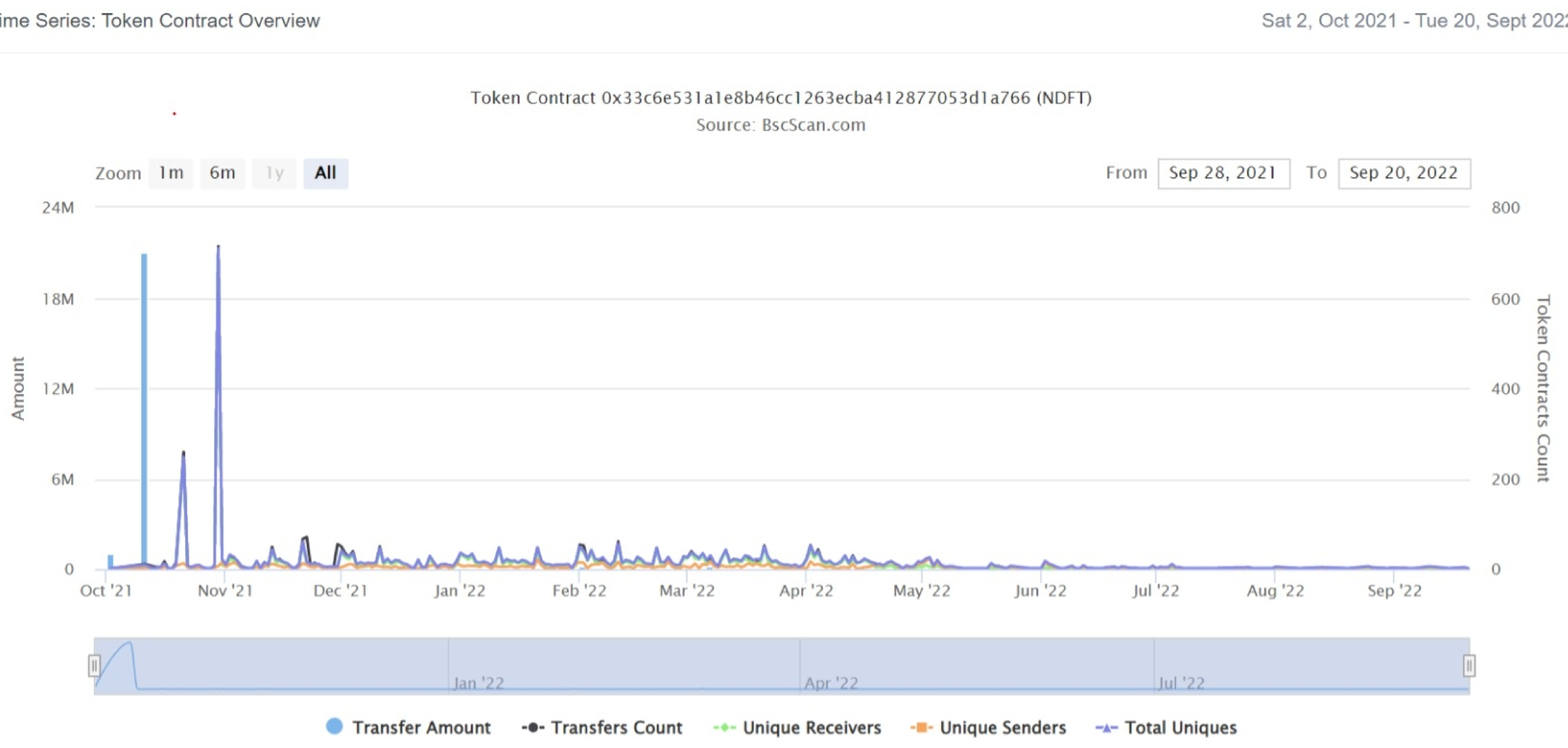


NDFT Top 20 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	0xe85bc19515415c4ca76c1ae83ea685a9e40226c6	10,300,000.105	49.0476%
2	0x96b06e812a250ce1559eeaa47390939c2a0c0b12	3,990,000	19.0000%
3	0x25427be8a558a3be43e1ea42c335af8d3eef5884	2,100,000	10.0000%
4	0x4c188c3dffcf23f395440b7a8f21c06987bdffcb	2,100,000	10.0000%
5	0xdf605584a3cae5335a9724520fe9686e469b61c2	1,050,000	5.0000%
6	0xda0dda77388c41f0367d3b459e9f266a08cfaaf5	687,219.58262559	3.2725%
7	0xa8137a815e64f62b09ed3141cac5a7930fdfc311	198,749	0.9464%
8	0x85cbc8dfff55890e86ae8a381b76d5d01a5d4b5f	145,819.91	0.6944%
9	0x33abe51239b5617300c8cda43b99ed1a81012ed6	61,050.13	0.2907%
10	0xa0f66086c32c692033b664a775cb3484c62c2c9e	37,965.01062603	0.1808%
11	0xada9e22315f63c1b8f0da051667f24ad34db6e34	29,872.28172072	0.1422%
12	0x49c3c24e49c5cd8ce60bc3b1f3f786177f7477ca	29,299	0.1395%
13	0x8e4872e8242463d183f155d3a92d54cb82f1bbe4	26,369.1	0.1256%
14	0x5c49f7589a5c4d740ebea088ca66639dbf49d11f	25,300	0.1205%
15	0x4ac73013b50dbf160285d17e793c0fedc2081bb4	24,000.30174564	0.1143%
16	0xc8ec449d1265346a38e49cc9e838ebf6df882a5b	20,312.29681856	0.0967%
17	0xcb258e8921cf8bf691e08a20b159ba8db51ded9f	18,264.06048946	0.0870%
18	0x5a16b0f85cb5454f5eed9898768705420676be56	15,000	0.0714%
19	0x41ccf905fd18770549f9ecd932a616170eb994dc	12,242	0.0583%
20	0x0aaba6dbbe056f007e9ece6cbe89256364bedcef	9,646.6203495	0.0459%

NDFT Token Distribution

NDFT Contract overview



Contract functions details

+Context

-[Int] _msgSender

-[Int] _msgData

+ Ownable (Context)

-< constructor>

-[Pub] owner

-[Pub] renounceOwnership #

-modifiers: onlyOwner

-[Pub] transferOwnership #

-modifiers: onlyOwner

+ [Int] IBEP20

-[Ext] name

-[Ext] symbol

-[Ext] decimals

-[Ext] totalSupply

-[Ext] balanceOf

-[Ext] getOwner

-[Ext] transfer

-[Ext] transferFrom

-[Ext] approve

-[Ext] allowance

+BEP20 (Ownable, IBEP20)

-<constructor>

-[Pub] name

-[Pub] symbol

-[Pub] decimals

-[Pub] totalSupply

-[Pub] balanceOf

-[Pub] getOwner

-[Pub] transfer #

-[Pub] transferFrom #

-[Pub] approve #

-[Pub] allowance

-[Pub] increaseAllowance #

-[Pub] decreaseAllowance #

Contract functions details

-[Int] _transfer #
-[Int] _mint #
-[Int] _burn #
-[Int] _approve #
-[Int] _setupDecimals #
-[Int] _beforeTokenTransfer #

+BEP20Capped (BEP20)
-<constructor>
-[Pub] cap
-[Int] _mint #

+BEP20Mintable (BEP20)
-[Pub] mintingFinished
-[Pub] mint #
-modifiers: canMint
-[Int] _finishMinting

+BEP20Burnable (BEP20)
-[Pub] burn #
-[Pub] burnFrom #

+NDFT (BEP20Capped, BEP20Mintable, BEP20Burnable)
-<constructor>
-[Int] _mint #
-modifiers: onlyOwner
-[Int] _finishMinting #
-modifiers: onlyOwner

($) = 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.	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 issues found.

Medium Severity Issues

No medium severity issues found.

Low Severity Issues

No low severity issue found.

Centralization

Owner Privileges :

- NDFT Contract:
    - Owner can remove and transfer ownership.
    - Owner can mint new tokens.
    - Owner can finish minting.

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
- Renounceownership
- _Mint
- _Finishminting

Conclusion

Smart contract contains no 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.