HackSafe

Smart Contract Security Audit Report

Janus Network

October 2022

Security Status

★ ★ ★ ★ ⯪

www.hacksafe.io

Audit Details

Audited project
Janus Network

Deployer address
0xf56dB60DB4F4512A0C82F1316BF8F5a7A024aa8D

Client contacts
Janus Network Team

Blockchain
Avalanche

Website
https://janusnetwork.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 Janus Network to perform an audit of smart contract:

- https://snowtrace.io/address/0x7A023A408F51c23760Eb31190fc731bc12B52954#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 17.10.2022

Token Type	: ERC20
Contract name	: Janus
Contract address	: 0x7A023A408F51c23760Eb31190fc731bc12B52954
Total supply	: 8,000,000
Token ticker	: JNS
Decimals	: 18
Token holders	: 7,847
Transactions count	: 9,428
Compiler version	: v0.8.0+commit.c7dfd78e
Contract deployer address	: 0xf56dB60DB4F4512A0C82F1316BF8F5a7A024aa8D
Owner address	: 0xf56db60db4f4512a0c82f1316bf8f5a7a024aa8d

Social profiles

Twitter profile	: https://twitter.com/NetworkJanus
Telegram profile	: https://t.me/JanusOfficial
Coingecko profile	: https://www.coingecko.com/en/coins/janus-network/
Coinmarketcap profile	: https://coinmarketcap.com/currencies/janus-network/

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 

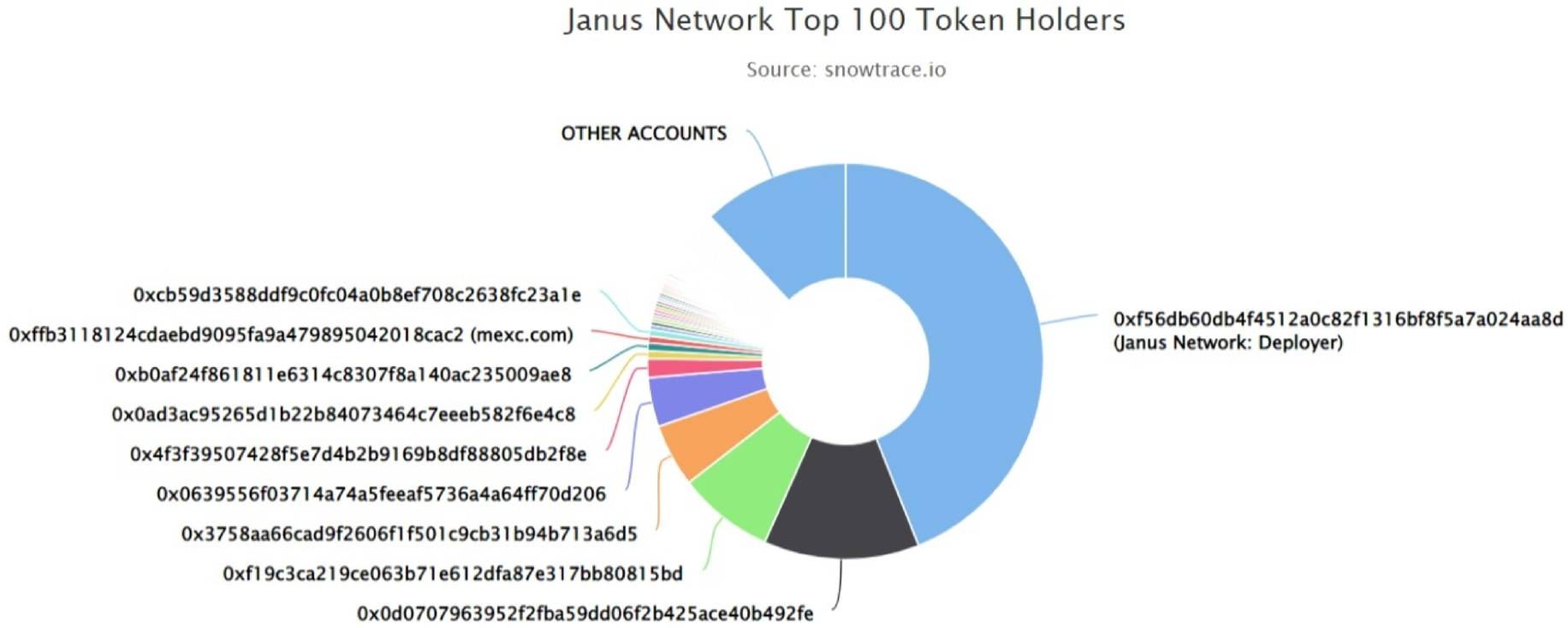
We used various tools like Slither, Mythril and Remix IDE. At the same time this finding is based on critical analysis of the manual audit. All issues found during automated analysis were manually reviewed and applicable vulnerabilities are presented in the issues checking status.

We found 0 critical, 0 high, 0 medium and 1 low and some very low-level issues

Janus Token Distribution

The top 100 holders collectively own 88.02% (7,041,779.47 Tokens) of Janus Network

Token Total Supply: 8,000,000.00 Token | Total Token Holders: 7,847



Janus Top 20 Token Holders

(A total of 7,041,779.47 tokens held by the top 100 accounts from the total supply of 8,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	Janus Network: Deployer	3,520,669.669679030829888974	44.0084%
2	0x0d0707963952f2fba59dd06f2b425ace40b492fe	1,015,540.24740601	12.6943%
3	0xf19c3ca219ce063b71e612dfa87e317bb80815bd	627,132.196732842439129749	7.8392%
4	0x3758aa66cad9f2606f1f501c9cb31b94b713a6d5	409,358.488496361884510721	5.1170%
5	0x0639556f03714a74a5feeaf5736a4a64ff70d206	321,807.96317235881	4.0226%
6	0x4f3f39507428f5e7d4b2b9169b8df88805db2f8e	121,941.473199344336949599	1.5243%
7	0x0ad3ac95265d1b22b84073464c7eeeb582f6e4c8	53,228.7	0.6654%
8	0xb0af24f861811e6314c8307f8a140ac235009ae8	50,000	0.6250%
9	mexc.com	44,129.36387411	0.5516%
10	0xcb59d3588ddf9c0fc04a0b8ef708c2638fc23a1e	43,168	0.5396%
11	0x40a64a462a742b40b414ed4d86d64f05ccd6abe7	26,813.68	0.3352%
12	0x689e21bce47cfe5bc2b67a601752aa6bf67cd4d9	23,597.869437716063197664	0.2950%
13	0x559347cd14bb7eccf4dbc1b882a421aabc40b196	23,527.79	0.2941%
14	0xca1a83aa4a865f3a50be27eb5bacc73ffd0a4458	20,089.97	0.2511%
15	0x62d7ee61153516a5a2b4d210527850fc25ae2141	20,049.47	0.2506%
16	0xcf4b9cd20c59b03965b85b6f1bd154014bae2ee7	19,794.24	0.2474%
17	0x0a18892ecb2bc0e42cc0d614a3afc48a3e5dec79	19,485.68	0.2436%
18	0x08b636606825883d4ab2c050f48e08d1b4b110e3	18,926.42209920517452	0.2366%
19	0x102225b01ae7f7ff4d3b4d51ccc42c7d86aafedc	18,700.06	0.2338%
20	0x95c318a011e381095dac7224599d128167a7841c	17,731.43	0.2216%

Contract functions details

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

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

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

+Janus (IERC20, Ownable)
  -<constructor>
  -[Pub] mint #
  -[Ext] setMinter #
    -modifiers: onlyOwner
  -[Ext] setTradingEnabled #
    -modifiers: onlyOwner
  -[Ext] burn #
  -[Ext] burnFrom #
  -[Ext] transfer #
  -[Ext] approve #
  -[Ext] transferFrom #
  -[Ext] increaseAllowance #
  -[Ext] decreaseAllowance #
  -[Ext] setFeePercentage #
    -modifiers: onlyOwner
  -[Ext] setBeneficiaryAddress #
  -[Ext] excludeFromFee #

Contract functions details

-modifiers: onlyOwner
-[Ext] totalSupply
-[Ext] balanceOf
-[Ext] allowance
-[Pvt] _transfer #
-[Int] _mint #
-[Pvt] _burn #
-[Pvt] _approve #

($) = 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 issues 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 0.8.0;

Centralization

Owner(vault/auth) Privileges :

- Janus Network Contract:
    - Owner can transfer and renounce ownership.
    - Owner can set minter.
    - Owner can set fee percentage.
    - Owner can enable trading bool variable.
    - Owner can set beneficiary address.

This smart contract has some functions which can be executed by the owner (Admin) only. If the admin wallet private key would be compromised, it would create trouble as smart contract ownership has not been renounced. Following are the only admin functions.

- Setfeepercentage
- Setbeneficiaryaddress
- Excludefromfee
- Renounceownership
- Transferownership
- Setminter
- Settradingenabled

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.