KRONICLABZ
AUDITS

Security Assessment

ION Token

May 13, 2022

Table of Contents

Audit Summary

This report has been prepared for ION Token on the Ethereum network. KronicLabs and CFGNINJA provides both client-centered and user-centered examination of the smart contracts and their current status when applicable. This report represents the security assessment made to find issues and vulnerabilities on the source code along with the current liquidity and token holder statistics of the protocol.

A comprehensive examination has been performed, utilizing Cross Referencing, Static Analysis, In-House Security Tools, and line-by-line Manual Review.

The auditing process pays special attention to the following considerations:

- Testing the smart contracts against both common and uncommon attack vectors.

- Inspecting liquidity and holders statistics to inform the current status to both users and client when applicable.

- Assessing the codebase to ensure compliance with current best practices and industry standards.

- Verifying contract functions that allow trusted and/or untrusted actors to mint, lock, pause, and transfer assets.

Project Overview

Token Summary

Parameter	Result
Address	0x831dAA3B72576867cD66319259bf022AFB1D9211
Name	ION
Token Tracker	ION (ION)
Decimals	5
Supply	250,000
Platform	Ethereum
compiler	v0.8.11+commit.d7f03943
Contract Name	ION
Optimization	Yes with 200 runs
LicenseType	Unlicense
Language	Solidity
Codebase	https://bscscan.com/token/0x3C6cD7CD70B01E869A09A955683e5D9C91338c0e
Url	https://thehumanoids.co/

Main Contract Assessed
Contract Name

Name	Contract	Live
ION	0x831dAA3B72576867cD66319259bf022AFB1D9211	Yes

TestNet Contract Assessed
Contract Name

Name	Contract	Live
ION	0x50763663974d5603d8504968f79cd06c0d9b32d1	Yes

Solidity Code Provided

SolID	FileNameMD5	FileName
ION	5fe56db1650d35d1e542b2845e40e6a1f1d5b411	ION.sol

Smart Contract Vulnerability Checks

Vulnerability	Automatic Scan	Manual Scan	Result
Unencrypted Private Data On-Chain	Complete	Complete	Low / No Risk
Code With No Effects	Complete	Complete	Low / No Risk
Message call with hardcoded gas amount	Complete	Complete	Low / No Risk
Hash Collisions With Multiple Variable Length Arguments	Complete	Complete	Low / No Risk
Unexpected Ether balance	Complete	Complete	Low / No Risk
Presence of unused variables	Complete	Complete	Low / No Risk
Right-To-Left-Override control character (U+202E)	Complete	Complete	Low / No Risk
Typographical Error	Complete	Complete	Low / No Risk
DoS With Block Gas Limit	Complete	Complete	Low / No Risk
Arbitrary Jump with Function Type Variable	Complete	Complete	Low / No Risk
Insufficient Gas Griefing	Complete	Complete	Low / No Risk
Incorrect Inheritance Order	Complete	Complete	Low / No Risk
Write to Arbitrary Storage Location	Complete	Complete	Low / No Risk
Requirement Violation	Complete	Complete	Low / No Risk
Missing Protection against Signature Replay Attacks	Complete	Complete	Low / No Risk

Vulnerability	Automatic Scan	Manual Scan	Result
Weak Sources of Randomness from Chain Attributes	Complete	Complete	Low / No Risk

Mint Check

The Project Onwers of ION has the ability to Mint New Tokens.

We Recommend the team to create a new contract without a Mint Function.

Owner can mint new coins

Fees Check

The Project Owners of ION does not have the ability to set fees higher than 25% .

Team May have fees defined, however they dont have the ability to set those fees higher than 25%.

.

Fees can be changed up to a maximum of 25%

MaxTx Check

The Project Onwers of ION does not has the ability to set max tx amount

The Team allow any investors to swap, transfer or sale their total amount if needed.

Project Has No MaxTX

Pause Trade Check

The Project Onwers of ION Owner can pause trading but he can't move tokens (Owner can't pause trading)

The Team has done a great job to avoid stop trading, and investors has the ability to trade at any given time without any problems

Pause Trade Notes:

Auditor Notes:

Project Owner Notes: Project Owners Ack

Owner can't pause trading

Contract Ownership

The contract ownership of ION is not currently renounced. The ownership of the contract grants special powers to the protocol creators, making them the sole addresses that can call sensible ownable functions that may alter the state of the protocol.

The current owner is the address 0x80580d6c8950956fd624322664cbd5ee36171f50 which can be viewed from:
HERE

The owner wallet has the power to call the functions displayed on the priviliged functions chart below, if the owner wallet is compromised this privileges could be exploited.

We recommend the team to renounce ownership at the right timing if possible, or gradually migrate to a timelock with governing functionalities in respect of transparency and safety considerations.

We recommend the team to use a Multisignature Wallet if contract is not going to be renounced, this will give the ability to the team to have more control over the contract.

Liquidity Ownership

The token does not have liquity at the moment of the audit, block 14165614

KYC Information

The Project Owners of ION is not KYC. .

The owner wallet has the power to call the functions displayed on the priviliged functions chart below, if the owner wallet is compromised this privileges could be exploited.

We recommend the team to renounce ownership at the right timing if possible, or gradually migrate to a timelock with governing functionalities in respect of transparency and safety considerations.

KYC Information Notes:

Auditor Notes: Auditor asked project owner if there was any plans to KYC.

Project Owner Notes: Customer already KYC with Pinksale.

Mythx Security Summary Checks

ID	Severity	Name	File	location
SWC-100	Pass	Function .	ION.sol	L: 0 C: 0
SWC-101	Pass	Integer Overflow and Underflow.	ION.sol	L: 0 C: 0
SWC-102	Pass	Outdated Compiler Version file.	ION.sol	L: 0 C: 0
SWC-103	Low	A floating pragma is set.	ION.sol	L: 7 C: 0
SWC-104	Pass	Unchecked Call Return Value.	ION.sol	L: 0 C: 0
SWC-105	Pass	Unprotected Ether Withdrawal.	ION.sol	L: 0 C: 0
SWC-106	Pass	Unprotected SELFDESTRUCT Instruction	ION.sol	L: 0 C: 0
SWC-107	PASS	Read of persistent state following external call.	ION.sol	L: 0 C: 0
SWC-108	Pass	State variable visibility is not set..	ION.sol	L: 0 C: 0
SWC-109	Pass	Uninitialized Storage Pointer.	ION.sol	L: 0 C: 0
SWC-110	Pass	Assert Violation.	ION.sol	L: 0 C: 0
SWC-111	Pass	Use of Deprecated Solidity Functions.	ION.sol	L: 0 C: 0
SWC-112	Pass	Delegate Call to Untrusted Callee.	ION.sol	L: 0 C: 0
SWC-113	Pass	Multiple calls are executed in the same transaction.	ION.sol	L: 0 C: 0

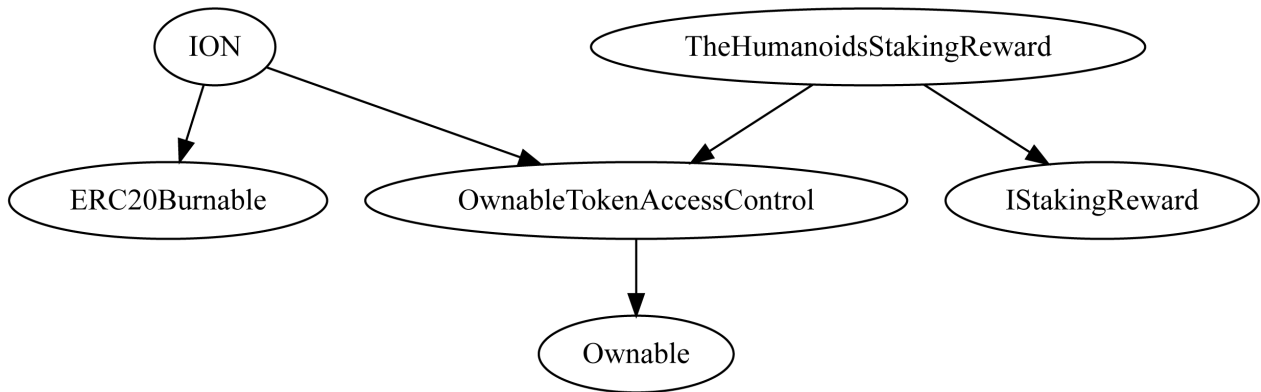| ID	Severity	Name	File	location
SWC-114	Pass	Transaction Order Dependence.	ION.sol	L: 0 C: 0
SWC-115	Pass	Authorization through tx.origin.	ION.sol	L: 474 C: 15
SWC-116	Pass	A control flow decision is made based on The block.timestamp environment variable.	ION.sol	L: 0 C: 0
SWC-117	Pass	Signature Malleability.	ION.sol	L: 0 C: 0
SWC-118	Pass	Incorrect Constructor Name.	ION.sol	L: 0 C: 0
SWC-119	Pass	Shadowing State Variables.	ION.sol	L: 0 C: 0
SWC-120	Pass	Potential use of block.number as source of randonmness.	ION.sol	L: 0 C: 0
SWC-121	Pass	Missing Protection against Signature Replay Attacks.	ION.sol	L: 0 C: 0
SWC-122	Pass	Lack of Proper Signature Verification.	ION.sol	L: 0 C: 0
SWC-123	Pass	Requirement Violation.	ION.sol	L: 0 C: 0
SWC-124	Pass	Write to Arbitrary Storage Location.	ION.sol	L: 0 C: 0
SWC-125	Pass	Incorrect Inheritance Order.	ION.sol	L: 0 C: 0
SWC-126	Pass	Insufficient Gas Griefing.	ION.sol	L: 0 C: 0
SWC-127	Pass	Arbitrary Jump with Function Type Variable.	ION.sol	L: 0 C: 0
SWC-128	Pass	DoS With Block Gas Limit.	ION.sol	L: 0 C: 0

ID	Severity	Name	File	location
SWC-129	Pass	Typographical Error.	ION.sol	L: 0 C: 0
SWC-130	Pass	Right-To-Left-Override control character (U +202E).	ION.sol	L: 0 C: 0
SWC-131	Pass	Presence of unused variables.	ION.sol	L: 0 C: 0
SWC-132	Pass	Unexpected Ether balance.	ION.sol	L: 0 C: 0
SWC-133	Pass	Hash Collisions with Multiple Variable Length Arguments.	ION.sol	L: 0 C: 0
SWC-134	Pass	Message call with hardcoded gas amount.	ION.sol	L: 0 C: 0
SWC-135	Pass	Code With No Effects (Irrelevant/Dead Code).	ION.sol	L: 0 C: 0
SWC-136	Pass	Unencrypted Private Data On-Chain.	ION.sol	L: 0 C: 0

We scan the contract for additional security issues using MYTHX and industry standard security scanning tool
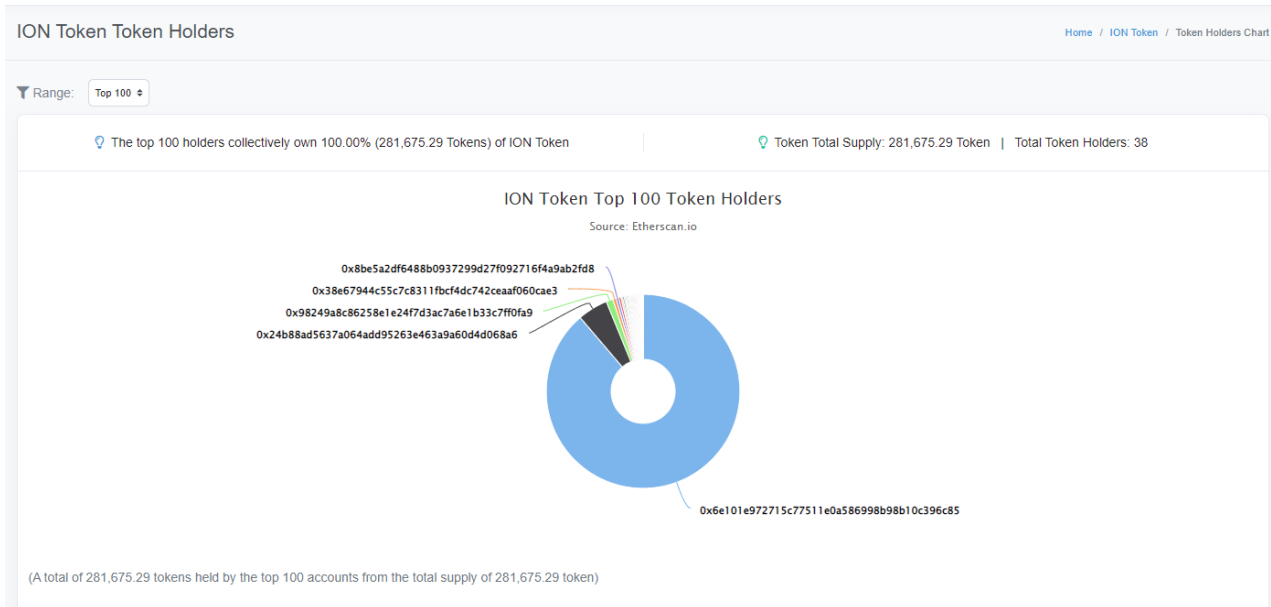
Call Graph and Inheritance

The contract for ION has the following call graph structure

The Project has a Total Supply of 250,000 and has the following inheritance

Top Token Holders

The contract for ION has the following top token holders

.

ION Token Token Holders

Range: Top 100

The top 100 holders collectively own 100.00% (281,675.29 Tokens) of ION Token

Token Total Supply: 281,675.29 Token | Total Token Holders: 38

ION Token Top 100 Token Holders

Source: Etherscan.io

0x8be5a2df6488b0937299d27f092716f4a9ab2fd8
0x38e67944c55c7c8311fbcf4dc742ceaaf060cae3
0x98249a8c86258e1e24f7d3ac7a6e1b33c7ff0fa9
0x24b88ad5637a064add95263e463a9a60d4d068a6

0x6e101e972715c77511e0a586998b98b10c396c85

(A total of 281,675.29 tokens held by the top 100 accounts from the total supply of 281,675.29 token)

Priviliged Functions (onlyOwner)

Function Name	Parameters	Visibility
renounceOwnership	none	public
transferOwnership	address newOwner	public
mint	to, amount	external
burnFrom	account, amount	public

Important Notes To The Users:

- The team has not provided a KYC Link during the time of assessment and can be found in the Audit.

- The team has the capability to mint new tokens, for the claimRewards() they will mint those tokens during the process.

- This Contract is part of the Staking Platform Reward System:

- https://etherscan.io/address/0xc08f2f8946593a8da611f70747b4360006b5b2c5#code

- Owner can't change fees up to 25%.

- Owner can't set max tx amount.

- Owner can't pause trading.

- No high-risk Exploits/Vulnerabilities Were Found in the Source Code.

- For transparency with the readers, the audit company also review the contract code and deployed to testnet.

Audit Passed

Social Media Checks

Social Media	URL	Result
Twitter	https://twitter.com/TheHumanoidsNFT	Pass
Instagram	https://www.instagram.com/ thehumanoidsnft/?hl=en	Pass
Website	https://thehumanoids.co/	Pass
Discord	https://discord.gg/hGNJwXPE2D	Pass

We recommend to have 3 or more social media sources including a completed working websites.

Social Media Information Notes:

Auditor Notes: undefined

Project Owner Notes:

Disclaimer

KronicLabs and CFGNINJA has conducted an independent audit to verify the integrity of and highlight any vulnerabilities or errors, intentional or unintentional, that may be present in the codes that were provided for the scope of this audit. This audit report does not constitute agreement, acceptance or advocation for the Project that was audited, and users relying on this audit report should not consider this as having any merit for financial advice in any shape, form or nature. The contracts audited do not account for any economic developments that may be pursued by the Project in question, and that the veracity of the findings thus presented in this report relate solely to the proficiency, competence, aptitude and discretion of our independent auditors, who make no guarantees nor assurance that the contracts are completely free of exploits, bugs, vulnerabilities or deprecation of technologies.

All information provided in this report does not constitute financial or investment advice, nor should it be used to signal that any persons reading this report should invest their funds without sufficient individual due diligence regardless of the findings presented in this report. Information is provided 'as is', and KronicLabs and CFGNINJA is under no covenant to the completeness, accuracy or solidity of the contracts audited. In no event will KronicLabs and CFGNINJA or its partners, employees, agents or parties related to the provision of this audit report be liable to any parties for, or lack thereof, decisions and/or actions with regards to the information provided in this audit report.

The assessment services provided by KronicLabs and CFGNINJA is subject to dependencies and under continuing development. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access, and depend upon, multiple layers of third-parties.