CFG NINJA AUDITS

Security Assessment

Ando (Rare Collection) NFT Stake

May 3, 2022

Table of Contents

Audit Summary

This report has been prepared for Ando (Rare Collection) NFT Stake on the Binance Smart Chain network. 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	0xc142Acb5dC56ee7C46f02E71e4DCb0B7d2f5295a
Name	Ando (Rare Collection)
Token Tracker	Ando (Rare Collection) ()
Decimals	0
Supply	0
Platform	Binance Smart Chain
compiler	v0.8.13+commit.abaa5c0e
Contract Name	AndoNFTStakeRare
Optimization	Yes with 200 runs
LicenseType	MIT
Language	Solidity
Codebase	https://bscscan.com/address/0xc142Acb5dC56ee7C46f02E71e4DCb0B7d2f5295a#code
Payment Tx	0x3bac61588e003c4591a5077562da3f1edc2d5d5f91d16ab7928fce15b2c37bb2

Main Contract Assessed Contract Name

Name	Contract	Live
Ando (Rare Collection)	0xc142Acb5dC56ee7C46f02E71e4DCb0B7d2f5295a	Yes

TestNet Contract was Not Assessed

Solidity Code Provided

SolID	FileNameMD5	FileName
AndoNFTStakeRare	89764a224851ed25b89c064f24a9060367e56c2e	AndoNFTStakeRare.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

Contract Ownership

The contract ownership of Ando (Rare Collection) 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 0x91df6835179f37fd11bd893a68d9d906e9ac7959 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.

KYC Information

The Project Onwers of Ando (Rare Collection) has provided KYC Documentation.

KYC Certificated can be found on the Following:
KYC Data

KYC Information Notes:

Auditor Notes: Team is doxxed.

Project Owner Notes: .

Mythx Security Summary Checks

ID	Severity	Name	File	location
SWC-100	Pass	Function .	AndoNFTStakeRare.sol	L: 0 C: 0
SWC-101	Pass	Integer Overflow and Underflow.	AndoNFTStakeRare.sol	L: 0 C: 0
SWC-102	Pass	Outdated Compiler Version file.	AndoNFTStakeRare.sol	L: 0 C: 0
SWC-103	Pass	A floating pragma is set.	AndoNFTStakeRare.sol	L: 1 C: 1
SWC-104	Pass	Unchecked Call Return Value.	AndoNFTStakeRare.sol	L: 0 C: 0
SWC-105	Pass	Unprotected Ether Withdrawal.	AndoNFTStakeRare.sol	L: 0 C: 0
SWC-106	Pass	Unprotected SELFDESTRUCT Instruction	AndoNFTStakeRare.sol	L: 0 C: 0
SWC-107	PASS	Read of persistent state following external call.	AndoNFTStakeRare.sol	L: 0 C: 0
SWC-108	Pass	State variable visibility is not set..	AndoNFTStakeRare.sol	L: 114 C: 30
SWC-108	Pass	State variable visibility is not set.	AndoNFTStakeRare.sol	L: 185 C: 9
SWC-108	Pass	State variable visibility is not set.	AndoNFTStakeRare.sol	L: 195 C: 14
SWC-109	Pass	Uninitialized Storage Pointer.	AndoNFTStakeRare.sol	L: 0 C: 0
SWC-110	Pass	Assert Violation.	AndoNFTStakeRare.sol	L: 0 C: 0

ID	Severity	Name	File	location
SWC-111	Pass	Use of Deprecated Solidity Functions.	AndoNFTStakeRare.sol	L: 0 C: 0
SWC-112	Pass	Delegate Call to Untrusted Callee.	AndoNFTStakeRare.sol	L: 0 C: 0
SWC-113	Pass	Multiple calls are executed in the same transaction.	AndoNFTStakeRare.sol	L: 1180 C: 8
SWC-114	Pass	Transaction Order Dependence.	AndoNFTStakeRare.sol	L: 0 C: 0
SWC-115	Pass	Authorization through tx.origin.	AndoNFTStakeRare.sol	L: 25 C: 4127
SWC-116	Low	A control flow decision is made based on The block.timestamp environment variable.	AndoNFTStakeRare.sol	L: 1205 C: 8
SWC-117	Pass	Signature Malleability.	AndoNFTStakeRare.sol	L: 0 C: 0
SWC-118	Pass	Incorrect Constructor Name.	AndoNFTStakeRare.sol	L: 0 C: 0
SWC-119	Pass	Shadowing State Variables.	AndoNFTStakeRare.sol	L: 0 C: 0
SWC-120	Pass	Potential use of block.number as source of randonmness.	AndoNFTStakeRare.sol	L: 608 C: 47
SWC-121	Pass	Missing Protection against Signature Replay Attacks.	AndoNFTStakeRare.sol	L: 0 C: 0
SWC-122	Pass	Lack of Proper Signature Verification.	AndoNFTStakeRare.sol	L: 0 C: 0
SWC-123	Pass	Requirement Violation.	AndoNFTStakeRare.sol	L: 0 C: 0
SWC-124	Pass	Write to Arbitrary Storage Location.	AndoNFTStakeRare.sol	L: 0 C: 0

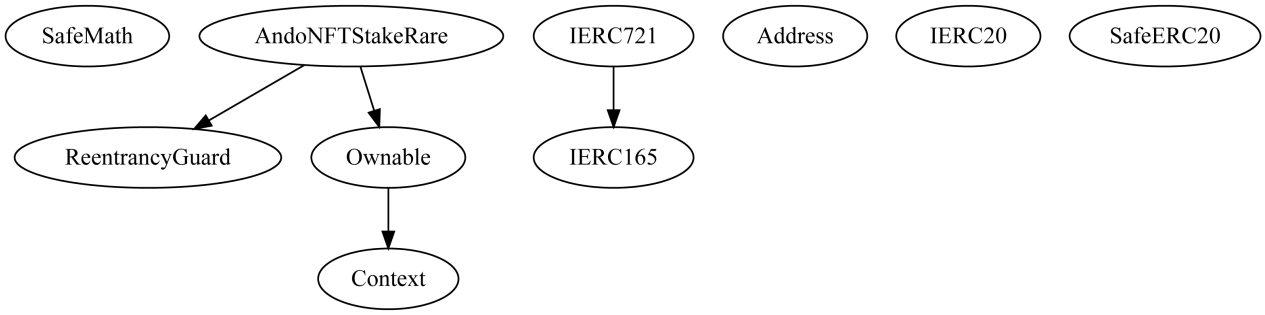
ID	Severity	Name	File	location
SWC-125	Pass	Incorrect Inheritance Order.	AndoNFTStakeRare.sol	L: 0 C: 0
SWC-126	Pass	Insufficient Gas Griefing.	AndoNFTStakeRare.sol	L: 0 C: 0
SWC-127	Pass	Arbitrary Jump with Function Type Variable.	AndoNFTStakeRare.sol	L: 0 C: 0
SWC-128	Pass	DoS With Block Gas Limit.	AndoNFTStakeRare.sol	L: 0 C: 0
SWC-129	Pass	Typographical Error.	AndoNFTStakeRare.sol	L: 0 C: 0
SWC-130	Pass	Right-To-Left-Override control character (U +202E).	AndoNFTStakeRare.sol	L: 0 C: 0
SWC-131	Pass	Presence of unused variables.	AndoNFTStakeRare.sol	L: 0 C: 0
SWC-132	Pass	Unexpected Ether balance.	AndoNFTStakeRare.sol	L: 0 C: 0
SWC-133	Pass	Hash Collisions with Multiple Variable Length Arguments.	AndoNFTStakeRare.sol	L: 0 C: 0
SWC-134	Pass	Message call with hardcoded gas amount.	AndoNFTStakeRare.sol	L: 0 C: 0
SWC-135	Pass	Code With No Effects (Irrelevant/Dead Code).	AndoNFTStakeRare.sol	L: 0 C: 0
SWC-136	Pass	Unencrypted Private Data On-Chain.	AndoNFTStakeRare.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 Ando (Rare Collection) has the following call graph structure

The Project has a Total Supply of 0 and has the following inheritance



Priviliged Functions (onlyOwner)

Function Name	Parameters	Visibility
renounceOwnership	none	public
transferOwnership	address newOwner	public
setRewardsPerHour		public
setNftCollection	address nftcollection	public
setRewardsToken	address rewardtoken	public
setTeamAddress	address teamwallet	public
addRewardTreasure		public
recoverTreasure		public
recoverETHfromContract		public
recoverRewardTokensFromContract		public
recoverRewardTokensFromContract		public
setApprovedTokenid		public

Important Notes To The Users:

- Ando Team is KYC with Pinksale.
- Contract did not show any issues on their code, or any concerns of hidden information or functions.
- We tested the dapp on a extensively and did not encounter any issues.
- No high-risk Exploits/Vulnerabilities Were Found in the Source Code.

Audit Passed

Social Media Checks

Social Media	URL	Result
Twitter	https://twitter.com/andotoken	Pass
Instagram	https://www.instagram.com/andotoken/	Pass
Website	https://www.andotoken.com/	Pass
Telegram	https://t.me/andotoken	Pass

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

Social Media Information Notes:

Auditor Notes:

Project Owner Notes:

Disclaimer

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 CFGNINJA is under no covenant to the completeness, accuracy or solidity of the contracts audited. In no event will 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 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.