CEG NINJA AUDITS

Security Assessment

KronicKatz.NFT NFT

April 14, 2022

Table of Contents

Audit Summary

This report has been prepared for KronicKatz.NFT NFT on the Etherum 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	0x19534c6bc37fd44c93f3a6506e44f32a99670f43
Name	KronicKatz.NFT
Token Tracker	KronicKatz.NFT (KRONIC)
Decimals	0
Supply	10000
Platform	Etherum
compiler	v0.8.10+commit.fc410830
Contract Name	KronicKatzNFT
Optimization	Yes with 200 runs
LicenseType	Unlicense
Language	Solidity
Codebase	https://etherscan.io/address/0x19534c6bc37fd44c93f3a6506e44f32a99670f43#code
Url	http://kronickatz.io

Main Contract Assessed Contract Name

Name	Contract	Live
KronicKatz.NFT	0x19534c6bc37fd44c93f3a6506e44f32a99670f43	Yes

TestNet Contract Assessed Contract Name

Name	Contract	Live
KronicKatz.NFT	0x1471d534a42ec12be2087dfc3e997636bfd0ab6b	Yes

Solidity Code Provided

SolID	FileName SHA-1	FileName
KronicKatzNFT	f1ceda6ca1e668540766ed9b8217a4ea7a7745db	KronicKatzNFT.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
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
Weak Sources of Randomness from Chain Attributes	Complete	Complete	Low / No Risk

Mint Check

The Project owner's of KronicKatz.NFT has the ability to Mint New NFTs as part of the project.

Since this is a NFT Contract is expected to have a mint function associated with it.

Contract Ownership

The contract ownership of KronicKatz.NFT 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 0x89c99aa9bf11f53d995f13a518d0de12bae7de38 which can be viewed from:
HERE

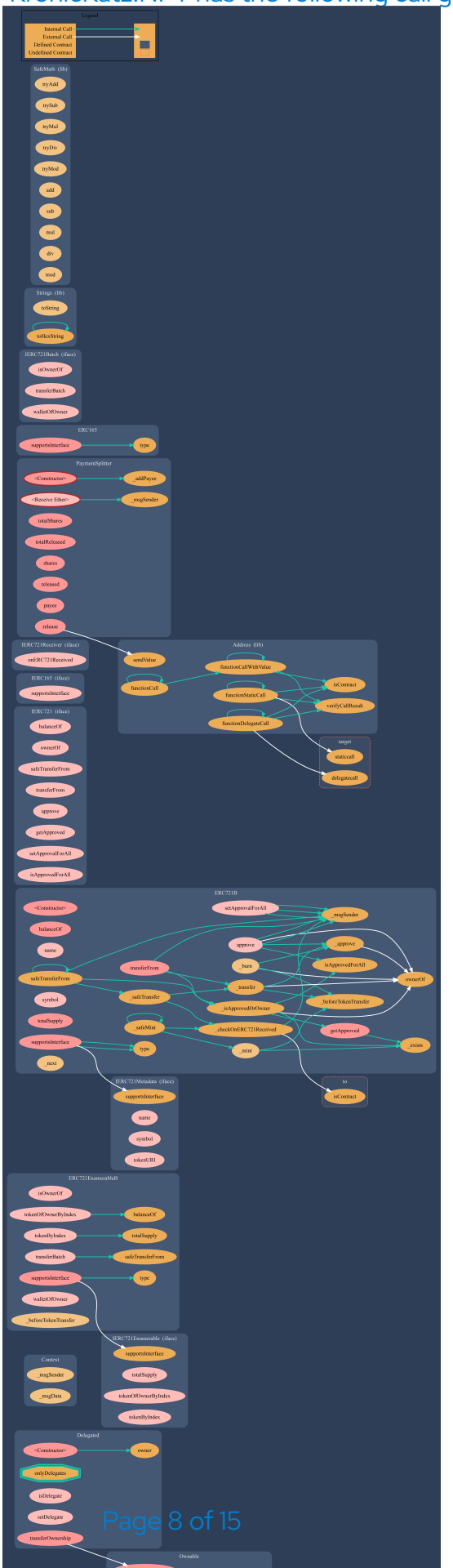
The owner wallet has the power to call the functions displayed on the priviliged functions chart below, if the owner wallet is compromised this privileges could be exploited.

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.

Call Graph

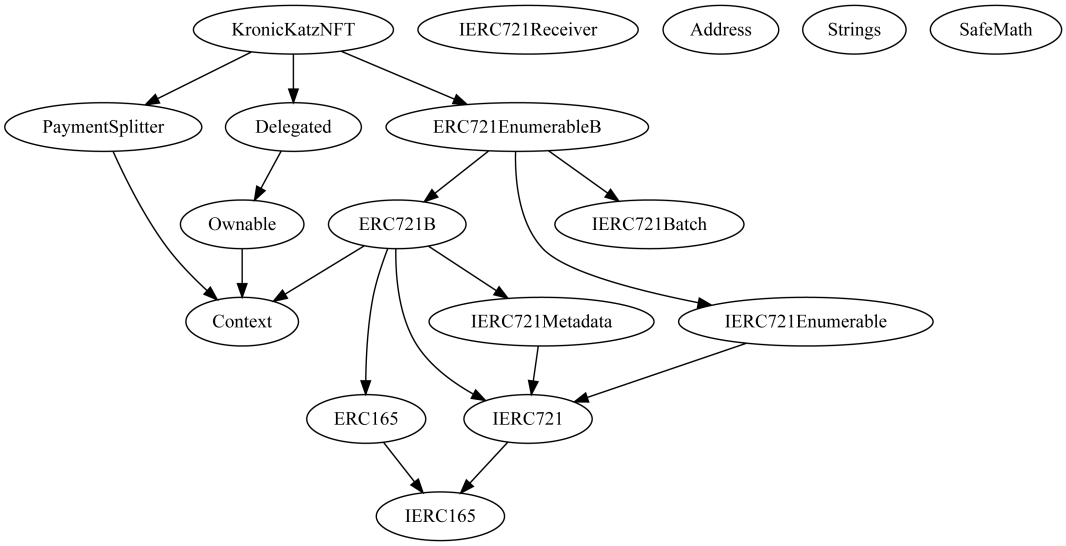
The contract for KronicKatz.NFT has the following call graph structure



Inheritance

The contract for KronicKatz.NFT has the following call graph structure

The Project has a Total Supply of 10000 and has the following inheritance



KYC Information

The Project Onwers of KronicKatz.NFT has provided KYC Documentation.

KYC Certification can be found on the Following:
KYC Data

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-103	Low	A floating pragma is set.	IERC721.sol	L: 3 C: 0
SWC-108	Low	State variable visibility is not set..	IERC721.sol	L: 31 C: 8

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

Priviliged Functions (onlyOwner)

Function Name	Parameters	Visibility
mint	payable quantity	external
mintTo	payable quantity recipient	external
setActive	isMainsaleActive_ (bool) isPresaleActive_ (bool)	external
setBaseURI	_newBaseURI (string) _newSuffix (string)	external
setFreline	freline (uint256)	external
setMaxOrder	maxOrder (uint256) maxSupply (uint256) maxWallet (uint256) presaleWallet (uint256)	external
setPresale	accounts (address[]) allowed (bool)	external
setPrice	mainsalePrice (uint256) presalePrice (uint256)	external
transferOwnership	newOwner (address)	external

Important Notes To The Users:

- The team has been confirmed with KYC and CFG Ninja is has noted them as safe
- Since this is an ERC 721 contract that can a mint, this is needed to generate new NFT. However it has been hardcoded not to go over 10,000 NFTs and the Current Supply is 2,871.
- The customer has an NFT Profile and can be found on http://opensea.io/kronickatz
- The customer has a function to pay four wallets currently, there is no option to update these wallet addresses. This can be a risk if one of the wallets gets compromised as there is no way to change the wallets from the contract.
- No high-risk Exploits/Vulnerabilities Were Found in the Source Code.
- The overall project is solid, we have reviewed the code in testnet and found no problems with the code as is currently set other than the major found on the wallets configuration and project owner acknowledged the risk.

Audit Passed

Social Media Checks

Social Media	URL	Result
Twitter	http://twitter.com/kronickatz	Pass
Instagram	http://instagram.com/kronickatz	Pass
Website	http://kronickatz.io	Pass
Telegram	http://discord.gg/kronickatz	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

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.