KRONICLABZ AUDITS

Security Assessment

Super Dudes NFT

April 12, 2022

Table of Contents

Audit Summary

This report has been prepared for Super Dudes NFT on the Ethereum Mainnet 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	
Name	Super Dudes
Token Tracker	Super Dudes (CNG)
Decimals	0
Supply	12888
Platform	Ethereum Mainnet
compiler	v0.8.13+commit.abaa5c0e
Contract Name	SuperDudes
Optimization	Yes with 200 runs
LicenseType	MIT
Language	Solidity
Codebase	https://ropsten.etherscan.io/address/0x6aa731926df284b100c8c2a1696ff892bd049072
Url	

Main Contract Assessed Contract Name

Name	Contract	Live
Super Dudes		No

TestNet Contract Assessed Contract Name

Name	Contract	Live
Super Dudes	0x6aa731926df284b100c8c2a1696ff892bd049072	Yes

Solidity Code Provided

SolID	FileNameMD5	FileName
SuperDudes	64b96207fba5dd5f9c38f82809d924292f5b2cc6	SuperDudes.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
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

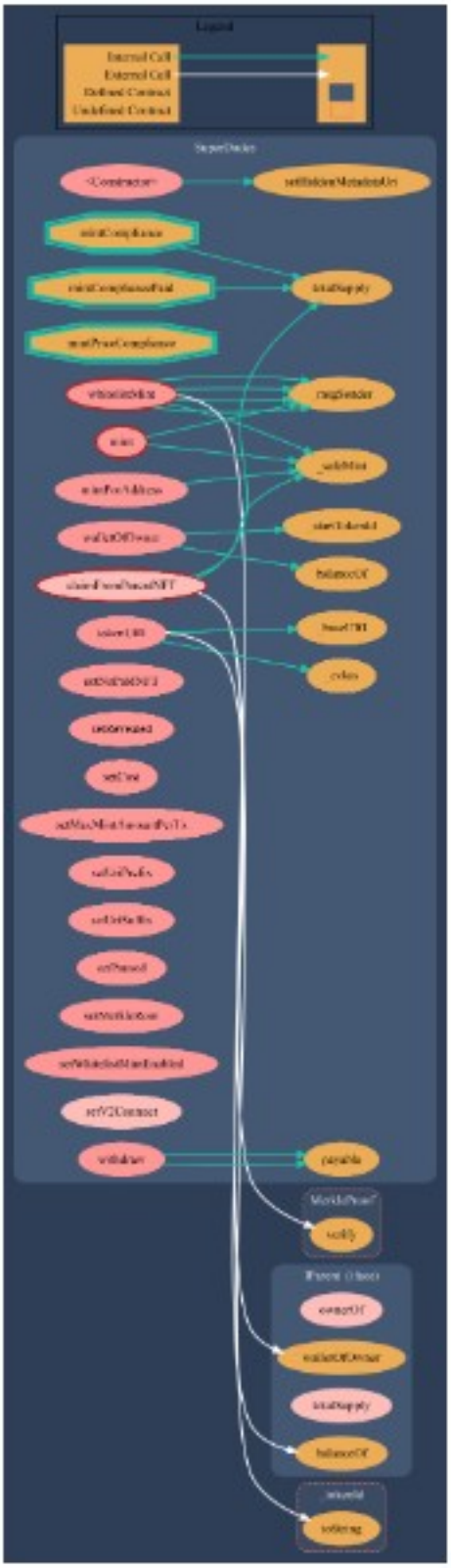
The Project Owners of Super Dudes has the ability to Mint New ERC 721 tokens.

Since this is an ERC 721 contract is expected to be able to mint new NFTs, so this will be considered a pass for the contract.

Call Graph and Inheritance

The contract for Super Dudes has the following call graph structure

The Project has a Total Supply of 12888 and has the following inheritance



Contract Ownership

The contract ownership of Super Dudes 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 0xB9A59DCa6ACfEad64391061Ff762957f579bba21 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 Super Dudes has provided KYC Documentation.

KYC Certificated 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: Team Lead Miles is currently Doxxed

Mythx Security Summary Checks

ID	Severity	Name	File	location
SWC-113	Medium	Multiple calls are executed in the same transaction.	IERC721.sol	L: 144 C: 2648
SWC-103	Low	A floating pragma is set.	IERC721.sol	L: 2 C: 1
SWC-107	Low	Read of persistent state following external call.	IERC721.sol	L: 144 C: 2712
SWC-107	Low	Write to persistent state following external call.	IERC721.sol	L: 61 C: 8

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

Security Check Information Notes:

Auditor Notes: No High Issues identified.

Project Owner Notes:

Priviliged Functions

Function Name	Parameters	Visibility
whitelistMint	mintCompliancePaid mintPriceCompliance	public
mint	mintCompliancePaid mintPriceCompliance	public
claimFromParentNFT	_numberOfTokens uint256	external
mintForAddress	mintCompliance	public
setNoPaidNFT	_newAmount uint256	external
setRevealed	_state bool	external
setCost	_state uint256	public
setMaxMintAmountPerTx	_maxMintAmountPerTx uint256	public
setHiddenMetadataUri	_hiddenMetadataUri string	public
setUriPrefix	_uriPrefix string	public
setUriSuffix	_uriPrefix string	public
setPaused	_state true	external
setWhitelistMintEnabled	_state bool	public
withdraw		public

Important Notes To The Users:

- The team lead is currently doxxed
- The contract is an ERC 721 and follow the development standards, the contract can mint new NFT and set price according to the same.
- No high-risk Exploits/Vulnerabilities Were Found in the Source Code.
- Customer currently do not have a website at the time of audit for the project, however we have conducted an audit of the source files and deployed to ropsten to test each functionality.
- Security scan did not identified mayor issues with code.
- Withdrawal functionality is defined as 4% to team and 96% to Project Owner.
- This audit has been performed by the CFG Ninja Team and Kroniclabz Team in a join venture.

Audit Passed

Social Media Checks

Social Media	URL	Result
Twitter	https://twitter.com/graveyardfalls	Pass
Instagram	https://www.instagram.com/	N/A
Website		N/A
Telegram		N/A

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.

CFG NINJA AUDITS