CFG NINJA
AUDITS

Security Assessment

LUNCX Token

July 17, 2022

Table of Contents

Audit Summary

This report has been prepared for LUNCX Token on the Binance 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	0x96CEaf0Eb83C28690C46E4F059e2D83f0A6190f4
Name	LUNCX
Token Tracker	LUNCX (LUNCX)
Decimals	18
Supply	100,000,000,000
Platform	Binance
compiler	v0.8.15+commit.e14f2714
Contract Name	LuncxToken
Optimization	Yes with 200 runs
LicenseType	Unlicensed
Language	Solidity
Codebase	https://bscscan.com/address/0x96CEaf0Eb83C28690C46E4F059e2D83f0A6190f4#code
Payment Tx	0x1aafedf9482f1238fe1e2347fc6881e3fb352cbc8b3d450899bb1b340b9261ea

Project Overview

Risk Analysis Summary

Parameter	Result
Buy Tax	9%
Sale Tax	9%
Is honeypot?	Clean
Can edit tax?	Yes
Is anti whale?	No
Is blacklisted?	Yes
Is whitelisted?	No
Holders	Clean
Security Score	95/100
Auditor Score	95/100
Confidence Level	Medium

The following quick summary has been added to the project overview, however there are more details about the audit and their results please read every details.

Main Contract Assessed
Contract Name

Name	Contract	Live
LUNCX	0x96CEaf0Eb83C28690C46E4F059e2D83f0A6190f4	Yes

TestNet Contract Assessed
Contract Name

Name	Contract	Live
LUNCX	0xFE33Ca9eE7B85A046E5093D3C76342266459D8da	Yes

Solidity Code Provided

SolID	File Sha-1	FileName
Luncx	70f00f8771ae418884cff00a189885b0dfeb11fc	Luncx.sol
Luncx		
Luncx		

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

CFG NINJA

Mint Check

The Project Owners of LUNCX does not have a mint function in the contract, owner cannot mint tokens after initial deploy
. .

The Project has a Total Supply of 100,000,000,000 and cannot mint any more than the Max Supply.

.

Mint Notes:

Auditor Notes:

Project Owner Notes:

Owner can't mint new coins

CFG NINJA

Fees Check

The Project Owners of LUNCX 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%.

.

Tax Fee Notes:

Auditor Notes: Project team has a function to limit MaxTax to 25%

Project Owner Notes: .

Fees can be changed up to a maximum of 25%

CFG NINJA

MaxTx Check

The Project Onwers of LUNCX 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.

MaxTX Notes:

Auditor Notes: Contract taxes cannot be higher than 25% and is currently set like this in the contract

Project Owner Notes:

Project Has No MaxTX

CFG NINJA

Pause Trade Check

The Project Onwers of LUNCX 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: test

Project Owner Notes:

Owner can't pause trading

CFG NINJA

Contract Ownership

The contract ownership of LUNCX 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 0xdb70a0771a1d070fedfe781f8f156b09ca3feea6 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 liquidity at the moment of the audit, block 19525371

CFG NINJA

KYC Information

The Project Onwers of LUNCX has provided KYC Documentation.

KYC Certificated can be found on the Following:
KYC Data

KYC Information Notes:

Auditor Notes: Asked project owner about KYC or Doxxed

Project Owner Notes: Project Owner has KYC with Cyberscope

CFG NINJA

Mythx Security Summary Checks

ID	Severity	Name	File	location
SWC-100	Pass	Function Default Visibility	Luncx.sol	L: 0 C: 0
SWC-101	Pass	Integer Overflow and Underflow.	Luncx.sol	L: 0 C: 0
SWC-102	Pass	Outdated Compiler Version file.	Luncx.sol	L: 0 C: 0
SWC-103	Low	A floating pragma is set.	Luncx.sol	L: 5 C: 0
SWC-104	Pass	Unchecked Call Return Value.	Luncx.sol	L: 0 C: 0
SWC-105	Pass	Unprotected Ether Withdrawal.	Luncx.sol	L: 0 C: 0
SWC-106	Pass	Unprotected SELFDESTRUCT Instruction	Luncx.sol	L: 0 C: 0
SWC-107	Pass	Read of persistent state following external call.	Luncx.sol	L: 0 C: 0
SWC-108	Pass	State variable visibility is not set..	Luncx.sol	L: 0 C: 0
SWC-109	Pass	Uninitialized Storage Pointer.	Luncx.sol	L: 0 C: 0
SWC-110	Pass	Assert Violation.	Luncx.sol	L: 0 C: 0
SWC-111	Pass	Use of Deprecated Solidity Functions.	Luncx.sol	L: 0 C: 0
SWC-112	Pass	Delegate Call to Untrusted Callee.	Luncx.sol	L: 0 C: 0
SWC-113	Pass	Multiple calls are executed in the same transaction.	Luncx.sol	L: 0 C: 0

CFG NINJA

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

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

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

Security Check Details Page

SWC-103 - Floating Pragma.

CWE-664: Improper Control of a Resource Through its Lifetime.

Description:

Contracts should be deployed with the same compiler version and flags that they have been tested with thoroughly. Locking the pragma helps to ensure that contracts do not accidentally get deployed using, for example, an outdated compiler version that might introduce bugs that affect the contract system negatively.

Remediation:

Lock the pragma version and also consider known bugs (https://github.com/ethereum/solidity/releases) for the compiler version that is chosen.

Pragma statements can be allowed to float when a contract is intended for consumption by other developers, as in the case with contracts in a library or EthPM package. Otherwise, the developer would need to manually update the pragma in order to compile locally.

References:

Ethereum Smart Contract Best Practices - Lock pragmas to specific compiler version.
SWC-115 - Authorization through tx.origin

CWE-477: Use of Obsolete Function

Description:

tx.origin is a global variable in Solidity which returns the address of the account that sent the transaction. Using the variable for authorization could make a contract vulnerable if an authorized account calls into a malicious contract. A call could be made to the vulnerable contract that passes the authorization check since tx.origin returns the original sender of the transaction which in this case is the authorized account.

Remediation:

tx.origin should not be used for authorization. Use msg.sender instead.

CFG NINJA

References:

Solidity Documentation – tx.origin

Ethereum Smart Contract Best Practices – Avoid using tx.origin

SigmaPrime – Visibility.

SWC Information Notes:

Auditor Notes: No Vulnerabilities where found during the security scan, however we did notice they used an older compiler version instead of latest of 0.8.14. Important to read about the bugs associated with 0.7.6 https://docs.soliditylang.org/en/v0.7.6/bugs.html#
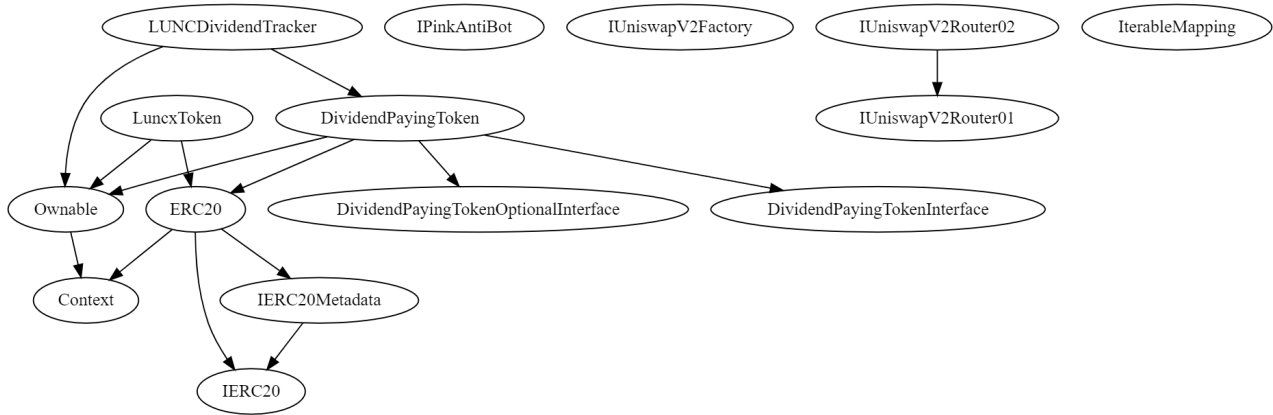
Project Owner Notes:

Call Graph and Inheritance

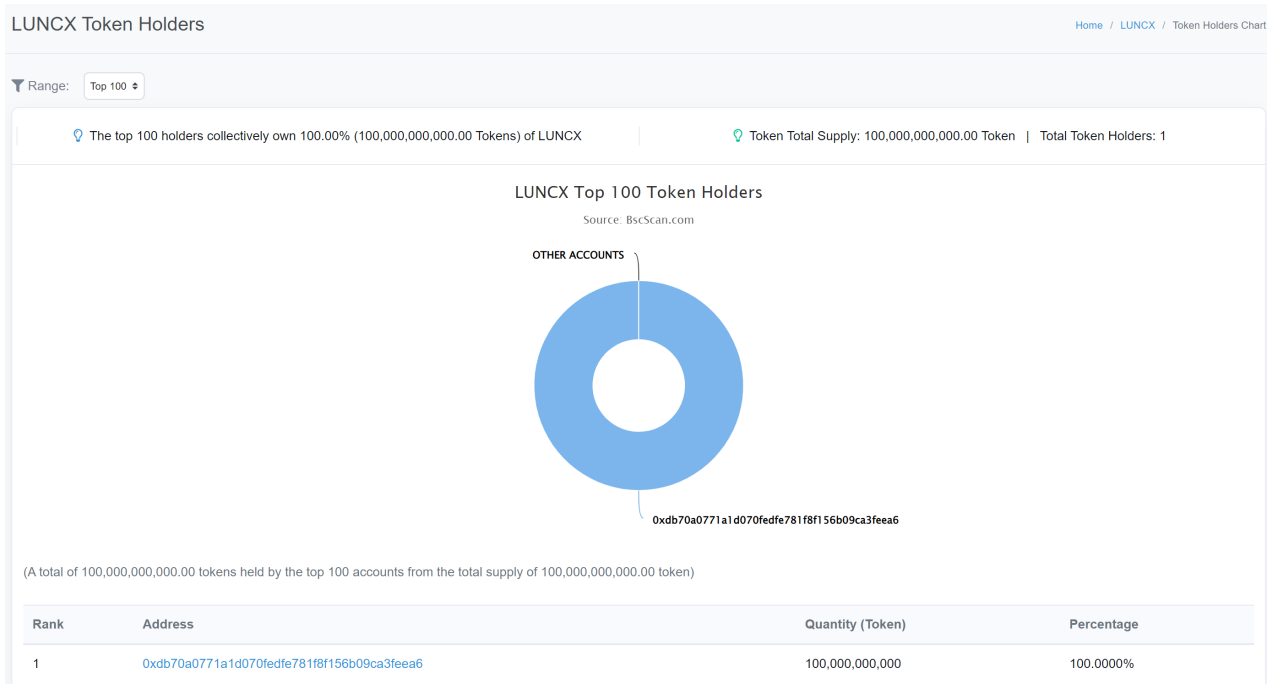The contract for LUNCX has the following call graph structure

The Project has a Total Supply of 100,000,000,000 and has the following inheritance

CFG NINJA

Top Token Holders

The contract for LUNCX has the following top token holders

.

LUNCX Token Holders

Range: Top 100 ⇅

The top 100 holders collectively own 100.00% (100,000,000,000.00 Tokens) of LUNCX

Token Total Supply: 100,000,000,000.00 Token | Total Token Holders: 1

LUNCX Top 100 Token Holders

Source: BscScan.com

OTHER ACCOUNTS

0xdb70a0771a1d070fedfe781f8f156b09ca3feea6

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

Rank	Address	Quantity (Token)	Percentage
1	0xdb70a0771a1d070fedfe781f8f156b09ca3feea6	100,000,000,000	100.0000%

CFG NINJA

Priviliged Functions (onlyOwner)

Function Name	Parameters	Visibility
renounceOwnership		Public
transferOwnership	address newOwner	Public
distributeDividends	uint256 amount	Public
excludeFromDividends	address account	External
updateClaimWait	uint256 newClaimWait	External
setBalance	address account, uint256 newBalance	External
processAccount	address account, bool automatic	Public
setFees	uint256 _burn, uint256 _reward, uint256 _marketing	External
setMarketingWallet	address _marketingWallet	External
updateDividendTracker	address newAddress	Public
updateUniswapV2Router	address newAddress	Public
excludeFromFees	address account, bool excluded	Public
excludeMultipleAccountsFromFees	address[] calldata accounts, bool excluded	Public
blacklistAddress	address account, bool value	External
updateGasForProcessing	uint256 newValue	External

CFG NINJA

Function Name	Parameters	Visibility
updateClaimWait	uint256 claimWait	External
excludeFromDividends	address account	External
startAntiDump		External

CFG NINJA

Important Notes To The Users:

- Owner can't set fees more than 25%.

- Owner can't set max tx amount.

- Owner can't pause trading.

- Owner has function for anti-dump

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

Audit Passed

Social Media Checks

Social Media	URL	Result
Twitter	https://twitter.com/official_luncx	Pass
Reddit		Fail
Website	Https://www.luncx.co	Pass
Telegram	https://t.me/luncx_official	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:

CFG NINJA

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.

CFG NINJA AUDITS

CFG NINJA