CFG NINJA AUDITS

Security Assessment

Lunar Token

March 17, 2023

Audit Status: Pass

Audit Edition: Advance

POWERED BY
BLADE POOL

Table of Contents

Assessment Summary

This report has been prepared for Lunar Token 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.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders
- Thorough line-by-line manual review of the entire codebase by industry experts.

Project Overview

Token Summary

Parameter	Result
Address	0xc1A59a17F87ba6651Eb8E8F707db7672647c45bD
Name	Lunar
Token Tracker	Lunar (LNR)
Decimals	18
Supply	100000000
Platform	Binance Smart Chain
compiler	v0.8.17+commit.8df45f5f
Contract Name	Lunar
Optimization	Yes with 200 runs
LicenseType	MIT
Language	Solidity
Codebase	https://bscscan.com/address/0xc1A59a17F87ba6651Eb8E8F707db7672647c45bD#code
Payment Tx	Corporate

Project Overview

Risk Analysis Summary

Parameter	Result
Buy Tax	6%
Sale Tax	6%
Is honeypot?	Clean
Can edit tax?	Yes
Is anti whale?	Yes
Is blacklisted?	Yes
Is whitelisted?	Yes
Holders	39,127
Confidence Level	Trusted

The following quick summary it's added to the project overview; however, there are more details about the audit and its results. Please read every detail.

Project Overview

Simulation Summary

Parameter	Result
Transfer From Owner	Pass
Transfer From Holder	Pass
Add Liquidity	Pass
Buy from Owner	Pass
Buy from Holder	Pass
Remove Liquidity	Pass
SwapAndLiquify	Pass
RemoveLiquidity	Pass
LaunchPad	N/A

The following quick summary it's added to the project overview; however, there are more details about the audit and its results. Please read every detail.

Main Contract Assessed
Contract Name

Name	Contract	Live
Lunar	0xc1A59a17F87ba6651Eb8E8F707db7672647c45bD	Yes

TestNet Contract Assessed
Contract Name

Name	Contract	Live
Lunar	0xA8CA720d120870f9cb6F99C2d73707849DDD1f83	Yes

Solidity Code Provided

SolID	File Sha-1	FileName
LunarV2	01c07d6143dfd7c24f176630c2d68ef4340fc46c	LunarV2.sol
LunarV2		
LunarV2		

Mint Check

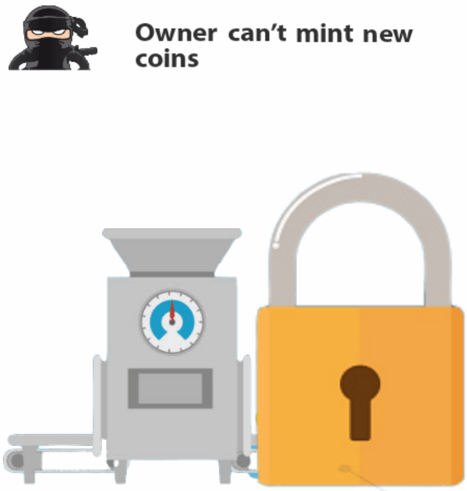
The project owners of Lunar do not have a mint function in the contract, owner cannot mint tokens after initial deploy.

The Project has a Total Supply of 100000000 and cannot mint any more than the Max Supply.

Mint Notes:

Auditor Notes: Customer has a mint compliance and cannot mint more than the total supply.

Project Owner Notes:



Fees Check

The project owners of Lunar do not have the ability to set fees higher than 25% .

The team May have fees defined; however, they can't set those fees higher than 25% or may not be able to configure the same.

Tax Fee Notes:

Auditor Notes: The contract currently has 6% buy and 6% sale taxes and total fees cannot be higher than 25%.

Project Owner Notes:

Fees can be changed up to a maximum of 25%

Blacklist Check

The project owners of Lunar have the ability to Blacklist holders from transferring their tokens.

We recommend the Team be careful with a blacklist function as this can prevent a holder from buying/ selling/transferring their assets. Malicious or compromised owners can trap contracts relying on tokens with a blacklist

Blacklist Notes:

Auditor Notes: Contract have a blacklist function presented, however this is done per wallet basis.

Project Owner Notes: Project Owner state the following 'We need to be able to ban people that are abusing the platform.'

MaxTx Check

The Project Owners of Lunar can set max tx amount.

The ability to set MaxTx can be used as bad actor, this can limit the ability of investors to sale their tokens at any given time if is set too low..

We recommend the project to set MaxTx to Total Supply or simiar to avoid swap or transfer from failures

MaxTX Notes:

Auditor Notes: Project has AntiWhaleGuards for Max Wallet, Max Buy, Max Sale and Max Transfer

Project Owner Notes:

Pause Trade Check

The Project Owners of Lunar can stop or pause trading

We recommend the Team only allow Open Trade and never use Stop Trade, as this will be catastrophic for the Project and Investors.

We recommend the Team create a reconsider doing it without the stop trade function.

Pause Trade Notes:

Auditor Notes: There is a pause trade to allow the contract to update.

Project Owner Notes:

Owner can pause trading

Contract Ownership

The contract ownership of Lunar 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
0x8C1DF8d7BcBE1395Ef66508F76a8732EaB65FBeE
which can be viewed:
HERE

The owner wallet has the power to call the functions displayed on the privileged functions chart below, if the owner's wallet is compromised, they could exploit these privileges.

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

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

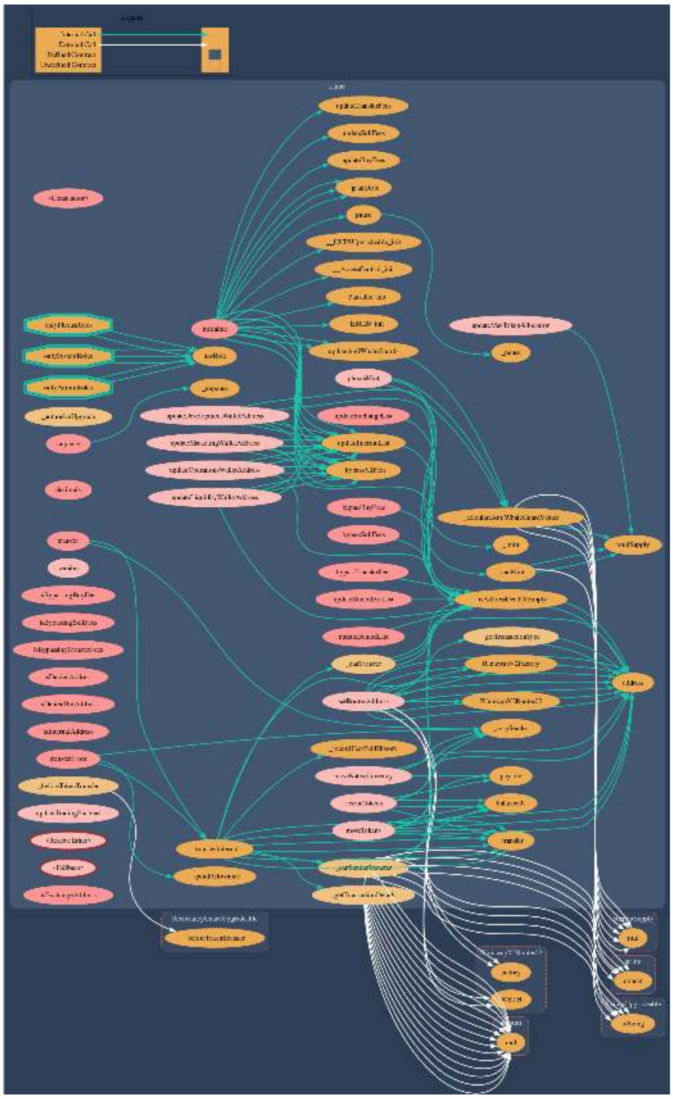
Liquidity Ownership

Most of the liquidity is currently locked; the lock can be seen here:

Liquidity Locker Link can be viewed from:
HERE

Call Graph

The contract for Lunar has the following call graph structure.



KYC Information

The Project Owners of Lunar have provided KYC Documentation.

KYC Certificated can be found on the Following: KYC Data

KYC Information Notes:

Auditor Notes: Customer is KYC by Dessert Finance

Project Owner Notes:

Smart Contract Vulnerability Checks

The Smart Contract Weakness Classification Registry (SWC Registry) is an implementation of the weakness classification scheme proposed in EIP-1470. It is loosely aligned to the terminologies and structure used in the Common Weakness Enumeration (CWE) while overlaying a wide range of weakness variants that are specific to smart contracts.

ID	Severity	Name	File	location
SWC-100	Pass	Function Default Visibility	LunarV2.sol	L: 0 C: 0
SWC-101	Pass	Integer Overflow and Underflow.	LunarV2.sol	L: 0 C: 0
SWC-102	Pass	Outdated Compiler Version file.	LunarV2.sol	L: 0 C: 0
SWC-103	Pass	A floating pragma is set.	LunarV2.sol	L: 0 C: 0
SWC-104	Pass	Unchecked Call Return Value.	LunarV2.sol	L: 0 C: 0
SWC-105	Pass	Unprotected Ether Withdrawal.	LunarV2.sol	L: 0 C: 0
SWC-106	Pass	Unprotected SELFDESTRUCT Instruction	LunarV2.sol	L: 0 C: 0
SWC-107	Pass	Read of persistent state following external call.	LunarV2.sol	L: 0 C: 0
SWC-108	Pass	State variable visibility is not set..	LunarV2.sol	L: 0 C: 0
SWC-109	Pass	Uninitialized Storage Pointer.	LunarV2.sol	L: 0 C: 0
SWC-110	Pass	Assert Violation.	LunarV2.sol	L: 0 C: 0

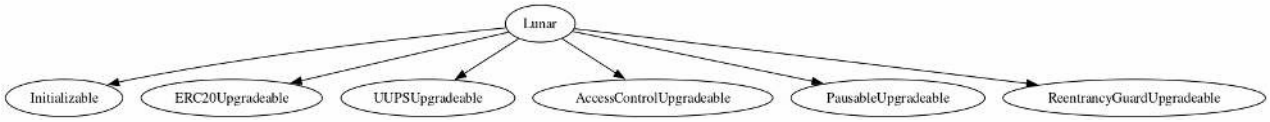
ID	Severity	Name	File	location
SWC-111	Pass	Use of Deprecated Solidity Functions.	LunarV2.sol	L: 0 C: 0
SWC-112	Pass	Delegate Call to Untrusted Callee.	LunarV2.sol	L: 0 C: 0
SWC-113	Pass	Multiple calls are executed in the same transaction.	LunarV2.sol	L: 0 C: 0
SWC-114	Pass	Transaction Order Dependence.	LunarV2.sol	L: 0 C: 0
SWC-115	Pass	Authorization through tx.origin.	LunarV2.sol	L: 0 C: 0
SWC-116	Pass	A control flow decision is made based on The block.timestamp environment variable.	LunarV2.sol	L: 0 C: 0
SWC-117	Pass	Signature Malleability.	LunarV2.sol	L: 0 C: 0
SWC-118	Pass	Incorrect Constructor Name.	LunarV2.sol	L: 0 C: 0
SWC-119	Pass	Shadowing State Variables.	LunarV2.sol	L: 0 C: 0
SWC-120	Pass	Potential use of block.number as source of randonmness.	LunarV2.sol	L: 0 C: 0
SWC-121	Pass	Missing Protection against Signature Replay Attacks.	LunarV2.sol	L: 0 C: 0
SWC-122	Pass	Lack of Proper Signature Verification.	LunarV2.sol	L: 0 C: 0
SWC-123	Pass	Requirement Violation.	LunarV2.sol	L: 0 C: 0
SWC-124	Pass	Write to Arbitrary Storage Location.	LunarV2.sol	L: 0 C: 0
SWC-125	Pass	Incorrect Inheritance Order.	LunarV2.sol	L: 0 C: 0

ID	Severity	Name	File	location
SWC-126	Pass	Insufficient Gas Griefing.	LunarV2.sol	L: 0 C: 0
SWC-127	Pass	Arbitrary Jump with Function Type Variable.	LunarV2.sol	L: 0 C: 0
SWC-128	Pass	DoS With Block Gas Limit.	LunarV2.sol	L: 0 C: 0
SWC-129	Pass	Typographical Error.	LunarV2.sol	L: 0 C: 0
SWC-130	Pass	Right-To-Left-Override control character (U +202E).	LunarV2.sol	L: 0 C: 0
SWC-131	Pass	Presence of unused variables.	LunarV2.sol	L: 0 C: 0
SWC-132	Pass	Unexpected Ether balance.	LunarV2.sol	L: 0 C: 0
SWC-133	Pass	Hash Collisions with Multiple Variable Length Arguments.	LunarV2.sol	L: 0 C: 0
SWC-134	Pass	Message call with hardcoded gas amount.	LunarV2.sol	L: 0 C: 0
SWC-135	Pass	Code With No Effects (Irrelevant/Dead Code).	LunarV2.sol	L: 0 C: 0
SWC-136	Pass	Unencrypted Private Data On-Chain.	LunarV2.sol	L: 0 C: 0

We scan the contract for additional security issues using MYTHX and industry-standard security scanning tools.

Inheritance

The contract for Lunar has the following inheritance structure.



Privileged Functions (onlyOwner)

Please Note if the contract is Renounced none of this functions can be executed.

Function Name	Parameters	Visibility
updateTransferFees	uint256 liquidityFee...	public
updateTradingEnabled	bool enableTradesFlag	external
updateSellFees	uint256 liquidityFee...	public
updateAntiWhaleGuards	uint256 maxWalletPercent..	public
updateBuyFees	uint256 liquidityFee..	public
setRouterAddress	address newRouterAddress	external
updateOperationsWalletAddress	address newWalletAddress	external
updateMarketingWalletAddress	address newWalletAddress	external
updateLiquidityWalletAddress	address newWalletAddress	external

Function Name	Parameters	Visibility
updateInternalList	address account, bool active	public
updateDeniedList	address account, bool active	public
updateDeniedBotList	address account, bool active	public
updateMaxTokenAllocation	uint256 maxAllocation	external
pause	none	public
plexusMint	none	public
updateExchangeList	address account, bool active	public
updateDevelopmentWalletAddress	address newWalletAddress	external
moveTokens	none	External
rescueToken	address fromAddress	External
moveNativeCurrency	uint256 amount	External

Function Name	Parameters	Visibility
bypassTransferFees	address account, bool bypassing	External
bypassSellFees	address account, bool bypassing	External
bypassBuyFees	address account, bool bypassing	External

Smart Contract Advance Checks

ID	Severity	Name	Result	Status
LNR-01	Minor	Potential Sandwich Attacks.	Pass	Not-Found
LNR-02	Minor	Function Visibility Optimization	Fail	Pending
LNR-03	Minor	Lack of Input Validation.	Pass	Not-Found
LNR-04	Major	Centralized Risk In addLiquidity.	Pass	Not-Found
LNR-05	Major	Missing Event Emission.	Pass	Not-Found
LNR-06	Minor	Conformance with Solidity Naming Conventions.	Pass	Not-Found
LNR-07	Minor	State Variables could be Declared Constant.	Pass	Not-Found
LNR-08	Major	Dead Code Elimination.	Pass	Not-Found
LNR-09	Major	Third Party Dependencies.	Pass	Not-Found
LNR-10	Major	Initial Token Distribution.	Pass	Not-Found
LNR-11	Critical	Initialization don't validate parameters.	Pass	Not-Found
LNR-12	Major	Centralization Risks In The X Role	Pass	Not-Found
LNR-13	Informational	Extra Gas Cost For User..	Pass	Not-Found
LNR-14	Medium	Unnecessary Use Of SafeMath	Pass	Not-Found
LNR-15	Medium	Symbol Length Limitation due to Solidity Naming Standards.	Pass	Not-Found

ID	Severity	Name	Result	Status
LNR-16	Medium	Invalid collection of Taxes during Transfer.	Pass	Not-Found

LNR-02 | Function Visibility Optimization.

Category	Severity	Location	Status
Gas Optimization	● Minor	LunarV2.sol: L: 1332 C: 13	Pending

Description

The following functions are declared as public and are not invoked in any of the contracts contained within the projects scope:

Function Name	Parameters	Visibility
bypassBuyFees		public
bypassSellFees		public
bypassTransferFees		public
updateBuyFees		public
updateAntiWhaleGuards		public
updateDeniedBotList		public
updateDeniedList		public
updateInternalList	address account, bool active	public
updateSellFees		public
updateTransferFees		public
updateExchangeList		public

The functions that are never called internally within the contract should have external visibility

Remediation

We advise that the function's visibility specifiers are set to external, and the array-based arguments change their data location from memory to calldata, optimizing the gas cost of the function.

References:

external vs public best practices.

Technical Findings Summary

Classification of Risk

Severity	Description
🔴 Critical	Risks are those that impact the safe functioning of a platform and must be addressed before launch. Users should not invest in any project with outstanding critical risks.
🟠 Major	Risks can include centralization issues and logical errors. Under specific circumstances, these major risks can lead to loss of funds and/or control of the project.
🟡 Medium	Risks may not pose a direct risk to users' funds, but they can affect the overall functioning of a platform
🟢 Minor	Risks can be any of the above but on a smaller scale. They generally do not compromise the overall integrity of the Project, but they may be less efficient than other solutions.
ℹ️ Informational	Errors are often recommended to improve the code's style or certain operations to fall within industry best practices. They usually do not affect the overall functioning of the code.

Findings

Severity	Found	Pending	Resolved
🔴 Critical	0	0	0
🟠 Major	0	0	0
🟡 Medium	0	0	0
🟢 Minor	0	0	0
ℹ️ Informational	1	0	0
Total	1	0	0

Social Media Checks

Social Media	URL	Result
Twitter	https://twitter.com/LNRDAO	Pass
Other	https://discord.gg/lnr	Pass
Website	https://lunar.io/	Pass
Telegram	https://t.me/LNRDAO	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:

Assessment Results

Score Results

Review	Score
Overall Score	96/100
Auditor Score	100/100
Review by Section	**Score**
Manual Scan Score	44/50
SWC Scan Score	37 /37
Advance Check Score	15 /16

The Following Score System Has been Added to this page to help understand the value of the audit, the maximun score is 100, however to attain that value the project most pass and provide all the data needed for the assessment. Our Passing Score has been changed to 80 Points, if a project does not attain 80% is an automatic failure. Read our notes and final assessment below.

Audit Passed

Assessment Results

Important Notes:

- The contract is a Proxy Contract and its implementation is under 0xb8448630a74ad7E871265ae661b8c3e470F7b5a4
- Lunar has been a very successful project, while this contract is proxy and can be upgraded the project team has ensured its safety.
- Lunar Development team is committed to the safety and evolution of its product, every revision and upgrade to the contract is done to almost perfection.
- When choosing a proxy contract like this, a team of professionals only guarantees its success in the long term.
- Bladepool has performed a peer review, build test cases and validated the code parameters for this audit. When auditing a proxy contract is not just about the functionality of the code, When there are new vulnerabilities or exploits released, the Lunar team will be capable of detecting them and improving their code to ensure holder safety.

- This is the first project that has earned a 100 score, which is the result of many factors, including their ability to code Solidity, their ability to properly document all functions, and the overall project goals
- Finally not every proxy contract out there will be as transparent in its coding as Lunar, is important for investors to always review projects behind any proxy contract implementation before investing.

Auditor Score =100
Audit Passed

Appendix

Finding Categories

Centralization / Privilege

Centralization / Privilege findings refer to either feature logic or implementation of components that actagainst the nature of decentralization, such as explicit ownership or specialized access roles incombination with a mechanism to relocate funds.

Gas Optimization

Gas Optimization findings do not affect the functionality of the code but generate different, more optimalEVM opcodes resulting in a reduction on the total gas cost of a transaction.

Logical Issue

Logical Issue findings detail a fault in the logic of the linked code, such as an incorrect notion on howblock.timestamp works.

Control Flow

Control Flow findings concern the access control imposed on functions, such as owner-only functionsbeing invoke-able by anyone under certain circumstances.

Volatile Code

Volatile Code findings refer to segments of code that behave unexpectedly on certain edge cases that mayresult in a vulnerability.

Coding Style

Coding Style findings usually do not affect the generated byte-code but rather comment on how to makethe codebase more legible and, as a result, easily maintainable.

Inconsistency

Inconsistency findings refer to functions that should seemingly behave similarly yet contain different code,such as a constructor assignment imposing different require statements on the input variables than a setterfunction.

Coding Best Practices

ERC 20 Conding Standards are a set of rules that each developer should follow to ensure the code meet a set of creterias and is readable by all the developers.

Disclaimer

CFGNINJA has conducted an independent security assessment to verify the integrity of and highlight any vulnerabilities or errors, intentional or unintentional, that may be present in the reviewed code for the scope of this assessment. This report does not constitute agreement, acceptance, or advocation for the Project, and users relying on this 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 the Project in question may pursue, and 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 entirely 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. Information is provided ‘as is, and CFGNINJA is under no covenant to audited completeness, accuracy, or solidity of the contracts. 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 or actions with regards to the information provided in this audit report.

The assessment services provided by CFGNINJA are subject to dependencies and are under continuing development. You agree that your access 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 with high levels of technical risk and uncertainty. The assessment reports could include false positives, negatives, and unpredictable results. The services may access, and depend upon, multiple layers of third parties.