CFG NINJA AUDITS

Security Assessment

CONFINAMENTO TOKEN Token

October 29, 2023

Audit Status: Pass

Audit Edition: Advance

Risk Analysis

Classifications of Manual Risk Results

Classification	Description
🔴 Critical	Danger or Potential Problems.
🟠 Major	Be Careful or Fail test.
🟢 Minor	Pass, Not-Detected or Safe Item.
ℹ️ Informational	Function Detected

Manual Code Review Risk Results

Contract Priviledge	Description
🟡 Buy Tax	25
🟡 Sale Tax	25
🟢 Cannot Buy	Pass
🟢 Cannot Sale	Pass
🟡 Max Tax	30
🟡 Modify Tax	Detected
🟢 Fee Check	Pass
🟢 Is Honeypot?	Not detected
🟢 Trading Cooldown	Not Detected
🟢 Can Pause Trade?	Pass
🟢 Pause Transfer?	Not-Detected

Contract Priviledge	Description
🟢 Max Tx?	Pass
🟢 Is Anti Whale?	Not Detected
🟢 Is Anti Bot?	Not Detected
🟢 Is Blacklist?	Not Detected
ℹ️ Blacklist Check	Pass
🟠 is Whitelist?	Detected
🟢 Can Mint?	Pass
🟢 Is Proxy?	Not Detected
🟢 Can Take Ownership?	Not detected
🟢 Hidden Owner?	Not detected
ℹ️ Owner	0x6D68A9d9c575255F45C5280b7B7EaaafdcBC009B
🟢 Self Destruct?	Not Detected
ℹ️ Other?	Not detected
🟢 Other?	Not detected
🟢 Holders	1
🟡 Auditor Confidence	Medium

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

Token Summary

Parameter	Result
Address	0x660e259C4f7F28BfDD8dAC5D5CdacE8BbF276FF4
Name	CONFINAMENTO TOKEN
Token Tracker	CONFINAMENTO TOKEN (CNT)
Decimals	18
Supply	1,000,000,000
Platform	Binance Smart Chain
compiler	v0.8.18+commit.87f61d96
Contract Name	CONFINAMENTOTOKEN
Optimization	Yes with 200 runs
LicenseType	MIT
Language	Solidity
Codebase	https://bscscan.com/address/0x660e259C4f7F28BfDD8dAC5D5CdacE8BbF276FF4#code
Payment Tx	0x4ac9bd7541f8fd4e46eee80015af08876cd4728072192f12b0210157f3a0eced

Main Contract Assessed
Contract Name

Name	Contract	Live
CONFINAMENTO TOKEN	0x660e259C4f7F28BfDD8dAC5D5CdacE8BbF276FF4	Yes

TestNet Contract Assessed
Contract Name

Name	Contract	Live
CONFINAMENTO TOKEN	0x892bd76544Cf54f679492b813B41BaCa0A30E1aB	Yes

Solidity Code Provided

SolID	File Sha-1	FileName
CONFINAMENTOTOKEN	e3778159b87047744d7ed581902913b539eb10ed	CONFINAMENTOTOKEN.sol
CONFINAMENTOTOKEN		
CONFINAMENTOTOKEN		
CONFINAMENTOTOKEN		

Call Graph

The contract for CONFINAMENTO TOKEN has the following call graph structure.
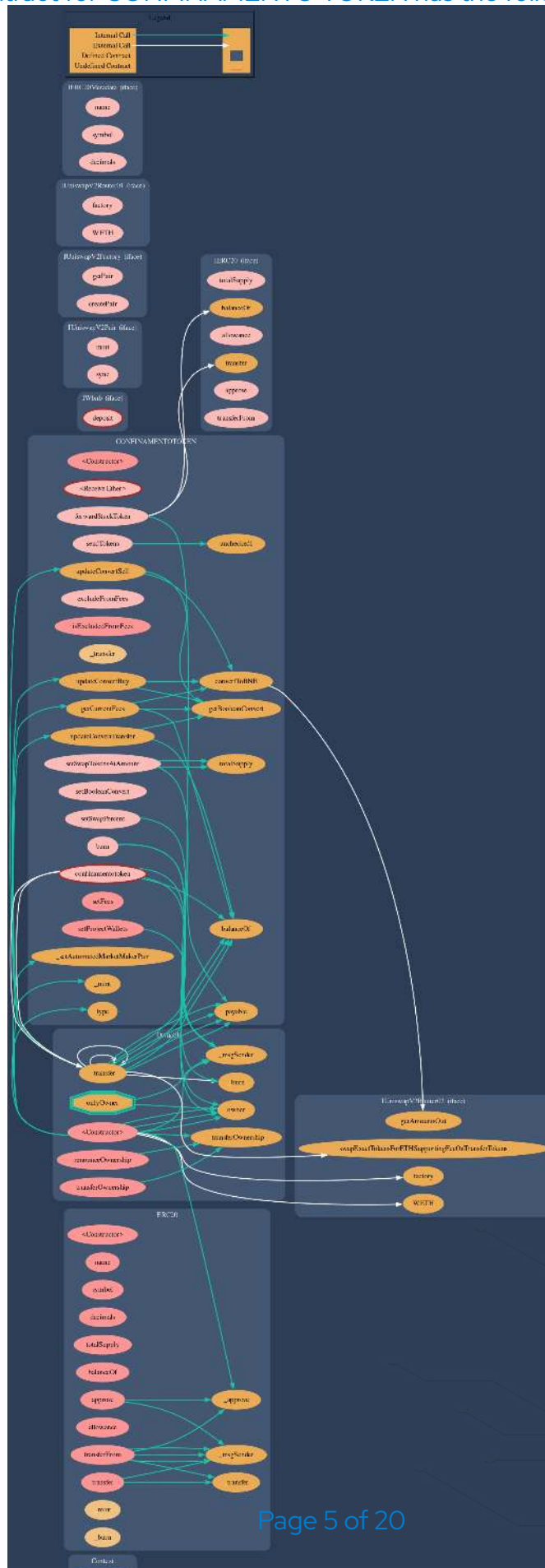
Smart Contract Vulnerability Checks

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

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

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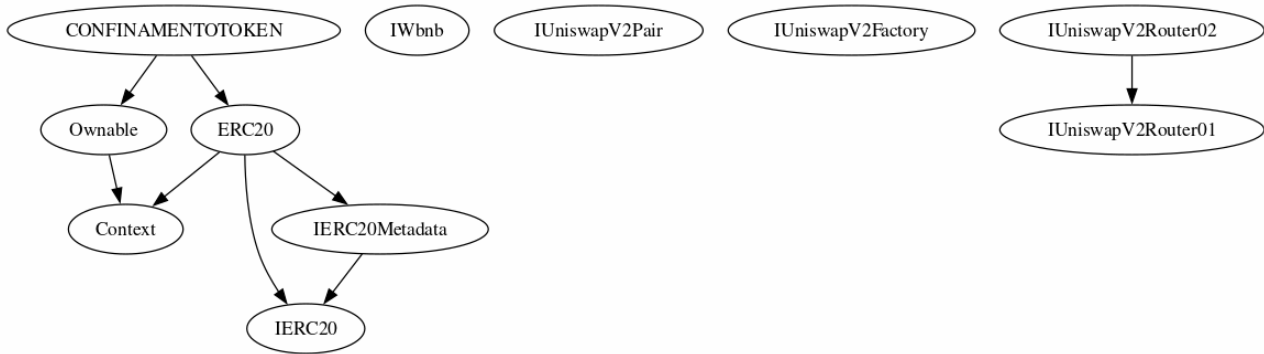
Smart Contract Advance Checks

ID	Severity	Name	Result	Status
CNT-01	Minor	Potential Sandwich Attacks.	Pass	Not-Found
CNT-02	Minor	Function Visibility Optimization	Pass	Not-Detected
CNT-03	Major	Lack of Input Validation.	Pass	Not-Detected
CNT-04	Major	Centralized Risk In addLiquidity.	Pass	Not-Detected
CNT-05	Major	Missing Event Emission.	Fail	Detected
CNT-06	Minor	Conformance with Solidity Naming Conventions.	Fail	Detected
CNT-07	Minor	State Variables could be Declared Constant.	Pass	Not-Found
CNT-08	Minor	Dead Code Elimination.	Pass	Not-Found
CNT-09	Major	Third Party Dependencies.	Pass	Not-Found
CNT-10	Major	Initial Token Distribution.	Pass	Not-Found
CNT-11	Medium	Multisend function found in code.	Fail	Detected
CNT-12	Major	Centralization Risks In The X Role	Pass	Not-Found
CNT-13	Informational	Extra Gas Cost For User..	Pass	Not-Found
CNT-6	Minor	Unnecessary Use Of SafeMath	Pass	Not-Detected
CNT-15	Medium	Symbol Length Limitation due to Solidity Naming Standards.	Pass	Not-Found

ID	Severity	Name	Result	Status
CNT-16	Meduium	Invalid collection of Taxes during Transfer.	Pass	Not-Detected
CNT-17	Informational	Conformance to numeric notation best practice.	Pass	Not-Found
CNT-18	Minor	Stop Transactions by using Enable Trade.	Pass	Not-Detected

CNT-05 | Missing Event Emission.

Category	Severity	Location	Status
Volatile Code	🟢 Major	CONFINAMENTOTOKEN.sol: 125, 14	🗎 Detected

Description

Detected missing events for critical arithmetic parameters. There are functions that have no event emitted, so it is difficult to track off-chain changes.The linked code does not create an event for the transfer.

Remediation

Emit an event for critical parameter changes. It is recommended emitting events for the sensitive functions that are controlled by centralization roles.

CNT-06 | Conformance with Solidity Naming Conventions.

Category	Severity	Location	Status
Coding Style	🟢 Minor	CONFINAMENTOTOKEN.s ol: 409,12	🗎 Detected

Description

Solidity defines a naming convention that should be followed. Rule exceptions: Allow constant variable name/symbol/decimals to be lowercase. Allow _ at the beginning of the mixed_case match for private variables and unused parameters.

setinb

Remediation

Follow the Solidity naming convention.

https://docs.soliditylang.org/en/v0.4.25/style-guide.html#naming-convention

CNT-11 | Multisend function found in code..

Category	Severity	Location	Status
Optimization	🟢 Medium	CONFINAMENTOTOKEN.sol: 305,14	🗒 Detected

Description

we recommend a multi send or airdrop to be performed separately from contract.

Remediation

Recommend to remove multisend from contract.

Project Action

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.
🔵 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	3	0	0
🔵 Informational	0	0	0
Total	3	0	0

Social Media Checks

Social Media	URL	Result
Twitter	https://twitter.com/Confinamentoken	Pass
Other	https://www.instagram.com/confinamentotoken/, https://www.tiktok.com/@confinamentotoken, https://www.facebook.com/confinamentotoken, https://k.kwai.com/p/C8IhxC2J, https://confinamento-token.gitbook.io/confinamento-token/lucro-por-cabeca	Pass
Website	https://confinamento-token.com/	Pass
Telegram	https://t.me/ConfinamentoTokenOficial	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	91/100
Auditor Score	84/100
Review by Section	Score
Manual Scan Score	36/53
SWC Scan Score	37 /37
Advance Check Score	18 /19

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:

- Owner can't set max tx amount.▊

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

Auditor Score =84
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.