

Security Assessment: **OcNest AI TOKEN**

February 5, 2025

- Audit Status: **Pass**
- Audit Edition: **Advance**
































Risk Analysis

Classifications of Manual Risk Results

Classification	Description
 Critical	Danger or Potential Problems.
 High	Be Careful or Fail test.
 Medium	Pass, Not-Detected or Safe Item.
 Low	Function Detected

Manual Code Review Risk Results

Contract Privilege	Description
 Buy Tax	5%
 Sale Tax	5%
 Cannot Buy	Pass
 Cannot Sale	Pass
 Max Tax	20%
 Modify Tax	Yes
 Fee Check	Pass
 Is Honeypot?	Not Detected
 Trading Cooldown	Not-Detected
 Can Pause Trade?	Pass
 Pause Transfer?	Not-Detected
 Max Tx?	Pass
 Is Anti Whale?	Detected
 Is Anti Bot?	Not-Detected

Contract Privilege	Description
 Is Blacklist?	Detected
 Blacklist Check	Fail
 is Whitelist?	Detected
 Can Mint?	Pass
 Is Proxy?	Not Detected
 Can Take Ownership?	Not Detected
 Hidden Owner?	Not-Detected
 Owner	No
 Self Destruct?	Not Detected
 External Call?	Not-Detected
 Other?	Not Detected
 Holders	354
 Auditor Confidence	Medium
 KYC Present	Yes
 KYC URL	

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	0xE0396Ef787F8B0385F0e73D30Acf8b922B1761F1
Name	OcNest AI
Token Tracker	OcNest AI (OCAI)
Decimals	9
Supply	10,000,000
Platform	ETHEREUM
compiler	v0.8.19+commit.7dd6d404
Contract Name	OCAI
Optimization	Yes with 200 runs
LicenseType	MIT
Language	Solidity
Codebase	https://etherscan.io/address/0xE0396Ef787F8B0385F0e73D30Acf8b922B1761F1#code
Payment Tx	Corporate

Main Contract Assessed Contract Name

Name	Contract	Live
OcNest AI	0xE0396Ef787F8B0385F0e73D30Acf8b922B1761F1	Yes

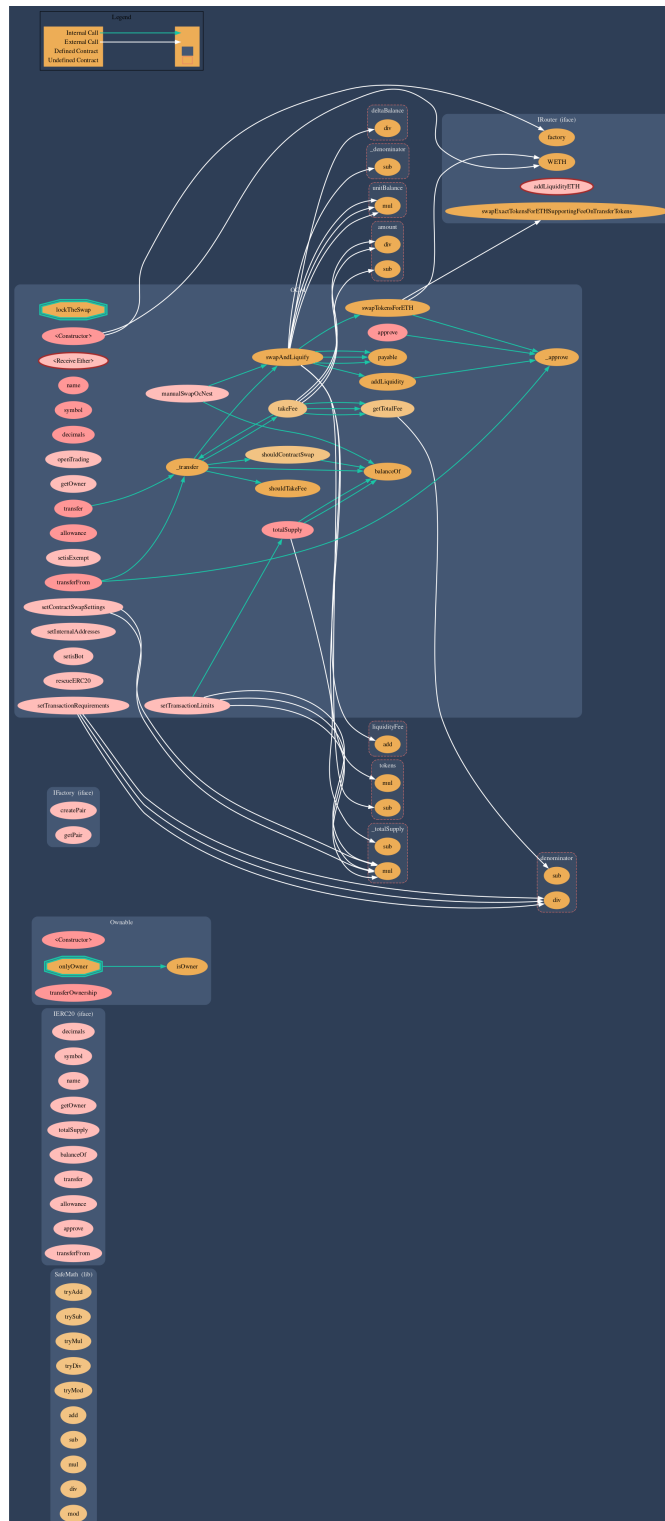
TestNet Contract was Not Assessed

Solidity Code Provided

SolidID	File Sha-1	FileName
OCAI	d7b5e6b176a136f2aa33ec2cb20a7073e368cce9	OCAI.sol
OCAI		.sol
OCAI		.sol
OCAI		.sol
OCAI		.sol
OCAI		.sol

Call Graph

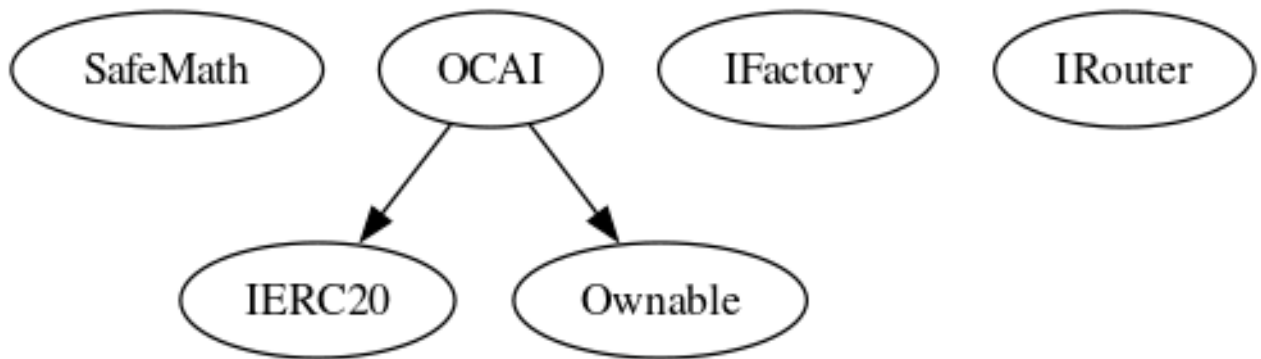
The contract for OcNest AI has the following call graph structure.





Inheritance

The contract for OcNest AI has the following inheritance structure.

The Project has a Total Supply of 10,000,000



OCAI-03 | Lack of Input Validation.

Category	Severity	Location	Status
Volatile Code	 Low	OCAI.sol: L: 129 C: 12, L: 218 C: 12, L: 223 C: 12, L: 233 C: 12, L: 250 C: 12, L: 255 C: 12, L: 260 C: 12, L: 266 C: 12	 Detected

Description

The given input is missing the check for the non-zero address.

The given input is missing the check for the onlyOwners need to be revisited for require..



Remediation

We advise the client to add the check for the passed-in values to prevent unexpected errors as below:

```
...
require(receiver != address(0), "Receiver is the zero address");
...
...
require(value X limitation, "Your not able to do this function");
...
```

We also recommend customer to review the following function that is missing a required validation. onlyOwners need to be revisited for require..

OCAI-05 | Missing Event Emission.

Category	Severity	Location	Status
Volatile Code	 Low	OCAI.sol: L: 129 C: 12, L: 218 C: 12, L: 223 C: 12, L: 233 C: 12, L: 238 C: 12, L: 243 C: 12, L: 250 C: 12, L: 255 C: 12, L: 260 C: 12, L: 266 C: 12	 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.

OCAI-14 | Unnecessary Use Of SafeMath

Category	Severity	Location	Status
Logical Issue	 Medium	OCAI.sol: L: 0 C: 0	 Detected

Description

The SafeMath library is used unnecessarily. With Solidity compiler versions 0.8.0 or newer, arithmetic operations

will automatically revert in case of integer overflow or underflow.

library SafeMath {

An implementation of SafeMath library is found.

using SafeMath for uint256;

SafeMath library is used for uint256 type in contract.



Remediation

We advise removing the usage of SafeMath library and using the built-in arithmetic operations provided by the

Solidity programming language

Project Action

OCAI-19 | Centralization Privileges of.

Category	Severity	Location	Status
	 Medium	OCAI.sol: L: 0 C: 14	 Detected

Description

Centralized Privileges are found on the following functions.






Remediation

Inheriting from Ownable and calling its constructor on yours ensures that the address deploying your contract is registered as the owner. The onlyOwner modifier makes a function revert if not called by the address registered as the owner.






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.
 High	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
 Low	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
 High	0	0	0
 Medium	2	2	0
 Low	2	2	0
 Informational	0	0	0
Total	4	4	0

Social Media Checks

Social Media	URL	Result
Twitter	https://x.com/OcNestAi	Pass
Other	https://link3.to/ocnestai	Pass
Website	https://www.ocnest.ai	Pass
Telegram	https://t.me/OcNestAI	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	85/100
Auditor Score	88/100
Review by Section	Score
Manual Scan Score	28
Auto Scan Score	37
Advance Check Score	20

The Following Score System Has been Added to this page to help understand the value of the audit, the maximum score is 100, however to attain that value the project must pass and provide all the data needed for the assessment. Our Passing Score has been changed to 84 Points for a higher standard, if a project does not attain 85% is an automatic failure. Read our notes and final assessment below.

Audit Passed



Assessment Results

Important Notes:

- Ownership: Ownership is renounced, meaning no further changes can be made by the original owner. Libraries and Interfaces: Uses SafeMath for arithmetic operations, ensuring overflow protection. Implements IERC20 interface correctly.
- Fee Structure: Multiple fees: liquidity, marketing, operations, treasury, and burn. Fees are adjustable but capped at 20%.
- Trading Controls: Trading can be enabled/disabled by the owner. Maximum transaction and wallet limits are in place.
- Swap and Liquify: Automatic liquidity provision and fee distribution. Swapping is controlled by thresholds and limits.
- Security Considerations: Uses require statements for input validation. onlyOwner modifier ensures restricted access to critical functions.
- Potential Risks: Bot protection mechanism in place. Ensure swap thresholds and limits are set appropriately to avoid excessive gas usage.



Appendix

Finding Categories

Centralization / Privilege

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

Gas Optimization

Gas Optimization findings do not affect the functionality of the code but generate different, more optimal EVM 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 how `block.timestamp` works.

Control Flow

Control Flow findings concern the access control imposed on functions, such as owner-only functions being 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 may result in a vulnerability.

Coding Style

Coding Style findings usually do not affect the generated byte-code but rather comment on how to make the 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 requirements on the input variables than a setter function.

Coding Best Practices

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

Disclaimer

Assure Defi 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 advocacy 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 Assure Defi is under no covenant to audited completeness, accuracy, or solidity of the contracts. In no event will Assure Defi 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 Assure Defi 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.

