ASSURE DEFI®
THE VERIFICATION GOLD STANDARD

Security Assessment:

Nodez TOKEN

September 26, 2024

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

NODEZ

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	30%
Sale Tax	40%
Cannot Buy	Pass
Cannot Sale	Pass
Max Tax	40%
Modify Tax	Yes
Fee Check	Pass
Is Honeypot?	Not Detected
Trading Cooldown	Not Detected
Can Pause Trade?	Pass
Pause Transfer?	Not-Detected
Max Tx?	Fail
Is Anti Whale?	Detected
Is Anti Bot?	Not-Detected

Contract Privilege	Description
Is Blacklist?	Not-Detected
Blacklist Check	Pass
is Whitelist?	Not 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?	Detected
Other?	Not Detected
Holders	120
Auditor Confidence	high
KYC Present	No
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	0x3B24ED67481A80609AF2F8913A45Da2049547CfD
Name	Nodez
Token Tracker	Nodez (NODE)
Decimals	18
Supply	100,000,000
Platform	ETHEREUM
compiler	v0.8.25+commit.b61c2a91
Contract Name	Nodez
Optimization	Yes with 200 runs
LicenseType	MIT
Language	Solidity
Codebase	https://etherscan.io/token/0x3B24ED67481A80609AF2F8913A45Da2049547CfD#code
Payment Tx	Corporate

Main Contract Assessed Contract Name

Name	Contract	Live
Nodez	0x3B24ED67481A80609AF2F8913A45Da2049547CfD	Yes

TestNet Contract Assessed Contract Name

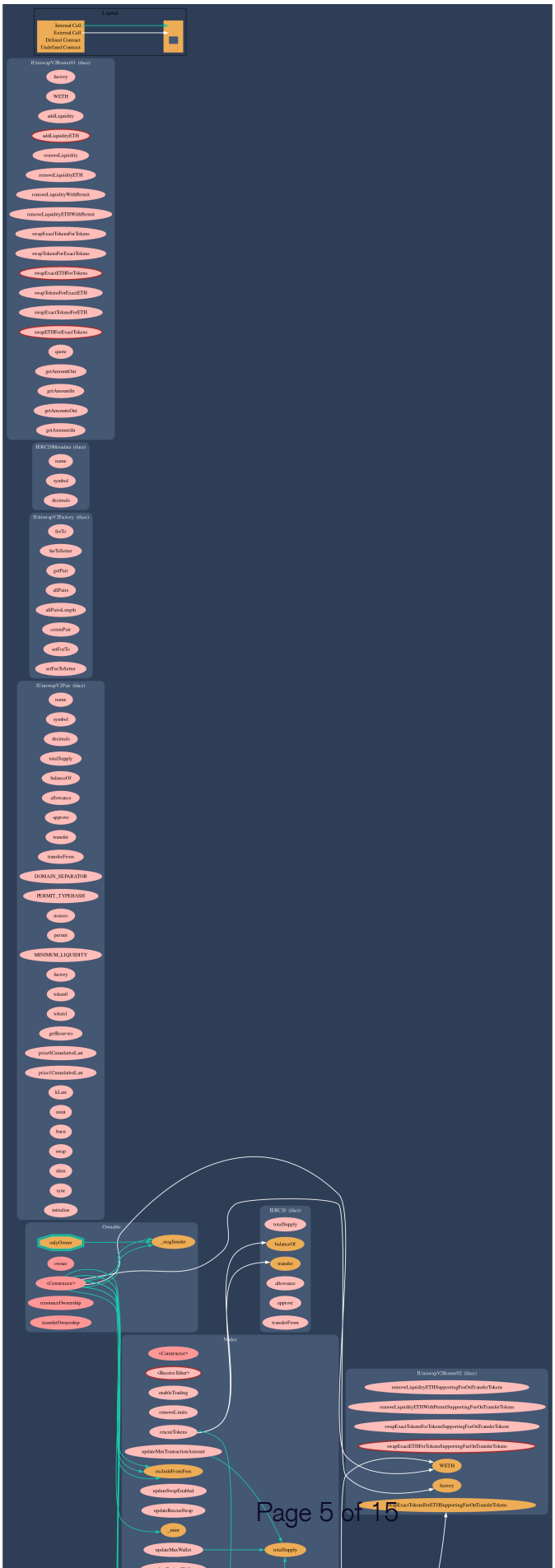
Name	Contract	Live
Nodez		Yes

Solidity Code Provided

SolID	File Sha-1	FileName
Nodez	9d205d9426b761267365f991582c56ca7ad8698c	Nodez.sol
Nodez		.sol
Nodez		.sol
Nodez		.sol
Nodez		.sol
Nodez		.sol

Call Graph

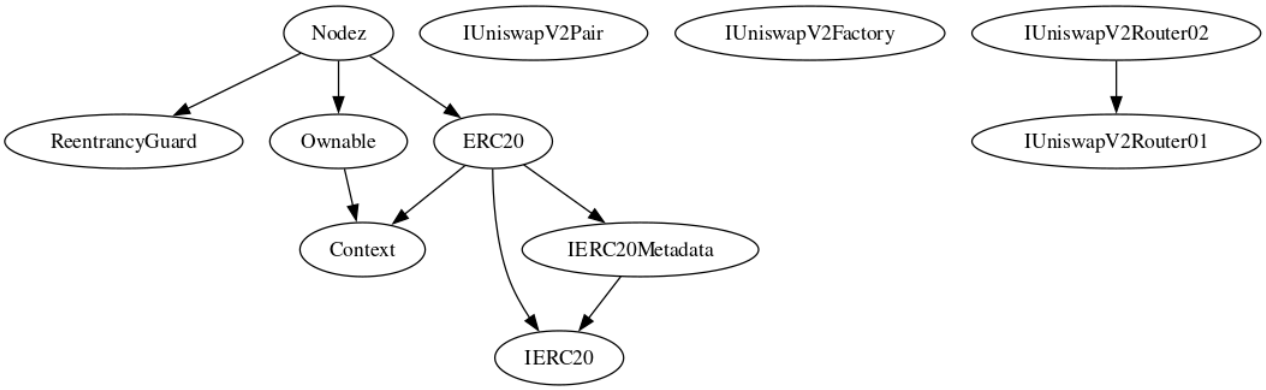
The contract for Nodez has the following call graph structure.



Inheritance

The contract for Nodez has the following inheritance structure.

The Project has a Total Supply of 100,000,000



NODE-03 | Lack of Input Validation.

Category	Severity	Location	Status
Volatile Code	Low	Nodez.sol: L: 545 C: 12, L: 559 C: 12, L: 579 C: 12, L: 585 C: 12, L: 591 C: 12, L: 596 C: 12, L: 611 C: 12, L: 616 C: 12, L: 0 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..

NODE-05 | Missing Event Emission.

Category	Severity	Location	Status
Volatile Code	Low	Nodez.sol: L: 601 C: 12, L: 809 C: 12, L: 816 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.

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	1
High	0	0	0
Medium	0	1	0
Low	2	2	0
Informational	0	0	0
Total	2	4	0

Social Media Checks

Social Media	URL	Result
Twitter	https://x.com/nodeztech	Pass
Other		N/A
Website	nodez.tech	Pass
Telegram	https://t.me/NodezTech	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	100/100
Auditor Score	80/100
Review by Section	**Score**
Manual Scan Score	28
Auto Scan Score	37
Advance Check Score	36

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 most 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:

- Reentrancy: Protected by ReentrancyGuard, but ensure all external calls are safe.ı
- Owner Privileges: Owner can modify fees, enable/disable trading, and rescue tokens. High risk if owner account is compromised.ı
- Fee Mechanism: Time-based fee adjustments could lead to unexpected behavior if not properly managed.ı
- External Interactions: Relies on Uniswap for liquidity and swaps. Ensure addresses and interactions are secure.ı
- High Initial Tax Rates: Up to 30% buy and 40% sell fees in the first 5 minutes. This could deter trading and liquidity provision if not communicated clearly to users.ı
- Dynamic Fee Adjustments: Time-based fee changes require precise timing and testing to ensure correct application and avoid user confusion.ı
- Trading Activation: Trading can be enabled only once. Ensure this is executed correctly to prevent locking the contract.ı
- Liquidity Management: swapBack function handles liquidity; potential for gas issues or incorrect execution.ı
- Limits and Exclusions: Ensure exclusions from fees and transaction limits are correctly applied and tested.ı
- Complex Functions: Functions like swapBack could be

optimized for gas usage.ı

- Recommendations:ı
- Owner Security: Implement multi-signature for owner functions to reduce risk.ı
- Testing: Thoroughly test all edge cases, especially around fee changes and liquidity functions.ı
- Monitoring: Set up alerts for unusual activities, particularly those involving owner functions.

Auditor Score =80
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

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 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 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.