ASSURE DEFI®
THE VERIFICATION GOLD STANDARD

Security Assessment:

JEJE TOKEN

June 21, 2024

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

VERIFIED BY ASSURE DEFI®
INTEGRITY • TRUST • CREDIBILITY

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	25%
🟠 Sale Tax	25%
🟢 Cannot Buy	Pass
🟢 Cannot Sale	Pass
🟢 Max Tax	25%
ℹ 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	Pass
🟢 is Whitelist?	Detected
🟢 Can Mint?	Pass
🟢 Is Proxy?	Not Detected
🟢 Can Take Ownership?	Not Detected
🟢 Hidden Owner?	Not-Detected
ℹ Owner	No
🟢 Self Destruct?	Not Detected
🟢 External Call?	Not-Detected
🟢 Other?	Not Detected
🟢 Holders	4,377
🟡 Auditor Confidence	Medium
🟡 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	0x1FDD61eF9a5C31B9a2abC7D39c139c779e8412Af
Name	JEJE
Token Tracker	JEJE (JJ)
Decimals	18
Supply	420,690,000,000,000
Platform	ETHEREUM
compiler	v0.8.23+commit.f704f362
Contract Name	JJ
Optimization	Yes with 200 runs
LicenseType	MIT
Language	Solidity
Codebase	https://etherscan.io/address/0x1FDD61eF9a5C31B9a2abC7D39c139c779e8412Af#code
Payment Tx	Corporate

Main Contract Assessed
Contract Name

Name	Contract	Live
JEJE	0x1FDD61eF9a5C31B9a2abC7D39c139c779e8412Af	Yes

TestNet Contract Assessed
Contract Name

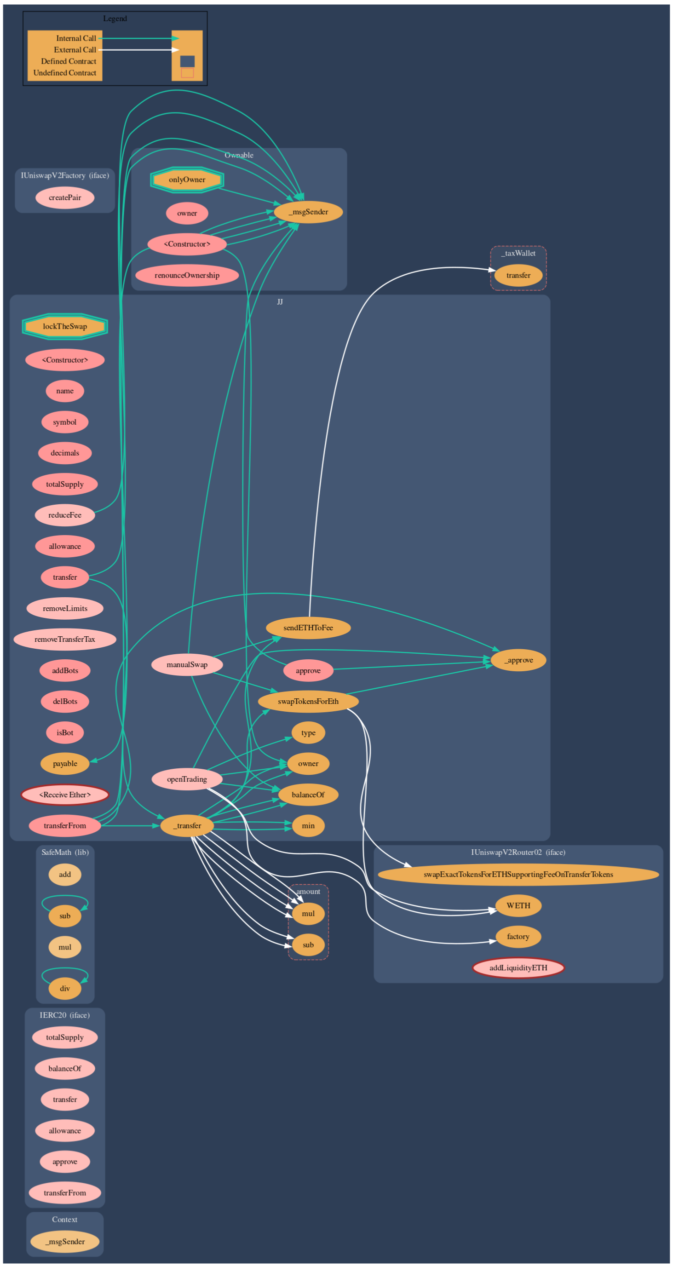
Name	Contract	Live
JEJE	0x7869B2D21B04881119849Bbe9aCB572d6619658D	Yes

Solidity Code Provided

SolID	File Sha-1	FileName
JEJE	b1aff8f4e7b4ce878784305df8ec4ddb57d6eb76	JEJE.sol
JEJE		
JEJE		
JEJE		
JEJE		
JEJE		

Call Graph

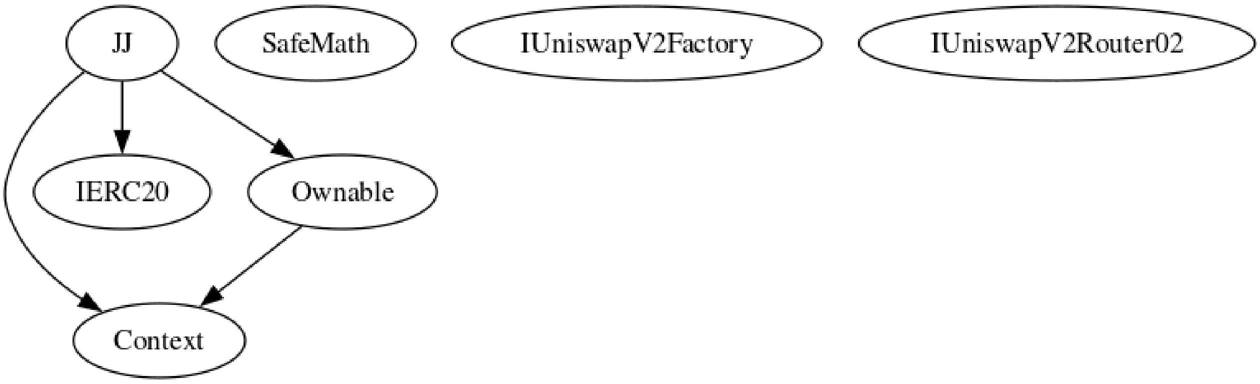
The contract for JEJE has the following call graph structure.



Inheritance

The contract for JEJE has the following inheritance structure.

The Project has a Total Supply of 420,690,000,000,000



Privileged Functions (onlyOwner)

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

Function Name	Parameters	Visibility
renounceOwnership		Public
removeLimits		External
removeTransferTax		External
addBots		Public
delBots		Public
openTrading		External

JJ-03 | Lack of Input Validation.

Category	Severity	Location	Status
Volatile Code	🟢 Low	JEJE.sol: L: 93 C: 14, L: 293 C: 14, L: 299 C: 14, L: 308 C: 14, L: 314 C: 14	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..

JJ-05 | Missing Event Emission.

Category	Severity	Location	Status
Volatile Code	🟢 Low	JEJE.sol: L: 308 C: 14, L: 314 C: 14, L: 325 C: 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.

JJ-14 | Unnecessary Use Of SafeMath

Category	Severity	Location	Status
Logical Issue	● Medium	JEJE.sol: L: 0 C: 0	Resolved

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

JJ-20 | Potential Reentrancy in transferToAddressETH.

Category	Severity	Location	Status
	🟢 Medium	JEJE.sol:	Resolved

Description

The function uses a call to transfer ETH which can be exploited for reentrancy.

Remediation

undefined

Project Action

JJ-22 | High Transfer Tax Rate.

Category	Severity	Location	Status
	● High	JEJE.sol:	Resolved

Description

The contract sets a high transfer tax rate of 70%, which can significantly reduce the amount of tokens transferred between users.

Remediation

undefined

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.
ℹ 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	1	0	1
🟡 Medium	1	0	1
🟢 Low	3	3	0
ℹ Informational	0	0	0
Total	5	0	5

Social Media Checks

Social Media	URL	Result
Twitter		Pass
Other		N/A
Website		Pass
Telegram		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:

ASSURE™
DEFI

OFFICIAL
PARTNER

Audit Result

Final Audit Score

Review	Score
Security Score	100
Auditor Score	85

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 85 Points for a higher standard, if a project does not attain 85% is an automatic failure. Read our notes and final assessment below.

Audit Fail

Assessment Results

Important Notes:

- Centralization Risks: Owner has significant control over contract parameters. Functions like removeLimits, removeTransferTax, addBots, delBots, openTrading are owner-restricted.ı
- Tax Wallet Control: _taxWallet has significant control over fees and manual swaps.ı
- Bot Management: Potential misuse of bot addition/removal functions, which could affect trading behavior.ı
- Sell Limitations: Only 3 sells per block, which could be manipulated or lead to trading restrictions.ı
- Fee Adjustment: _taxWallet can reduce fees (reduceFee), potentially impacting token economics.ı
- Reentrancy: Functions involving external calls (e.g., swapTokensForEth) should use reentrancy guards to prevent attacks.ı
- Initial High Taxes: Initial buy/sell taxes are high (25%), which could deter early investors.ı
- Trading Control: Tradin [illegible] d/closed by the owner, leading to potential ma [illegible]

VERIFIED BY ASSURE DEFI ™ INTEGRITY ★ TRUST ★ CREDIBILITY

Audit [illegible] e =85
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.

ASSURE DEFI™
THE VERIFICATION GOLD STANDARD