ASSURE DEFI®
THE VERIFICATION GOLD STANDARD

Security Assessment:

Zydio AI TOKEN

May 13, 2024

- Audit Status: **Pass**
- Audit Edition: **Standard**

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	5%
Sale Tax	5%
Cannot Buy	Pass
Cannot Sale	Pass
Max Tax	10%
Modify Tax	Yes
Fee Check	Pass
Is Honeypot?	Not Detected
Trading Cooldown	Detected
Can Pause Trade?	Pass
Pause Transfer?	Detected
Max Tx?	Fail
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
Owner	no
Self Destruct?	Not Detected
External Call?	Not Detected
Other?	Not Detected
Holders	678
Auditor Confidence	Medium
KYC Present	No
KYC URL	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.

Project Overview

Token Summary

Parameter	Result
Address	0x8B683C400457ef31F3c27c90ACB6AB69304D1B77
Name	Zydio AI
Token Tracker	Zydio AI ($ZDAI)
Decimals	9
Supply	100,000,000
Platform	ETHEREUM
compiler	v0.8.20+commit.a1b79de6
Contract Name	ZydioaAI
Optimization	Yes with 200 runs
LicenseType	MIT
Language	Solidity
Codebase	https://etherscan.io/address/0x8b683c400457ef31f3c27c90acb6ab69304d1b77#code
Payment Tx	Corporate

Main Contract Assessed Contract Name

Name	Contract	Live
Zydio AI	0x8B683C400457ef31F3c27c90ACB6AB69304D1B77	Yes

TestNet Contract Assessed Contract Name

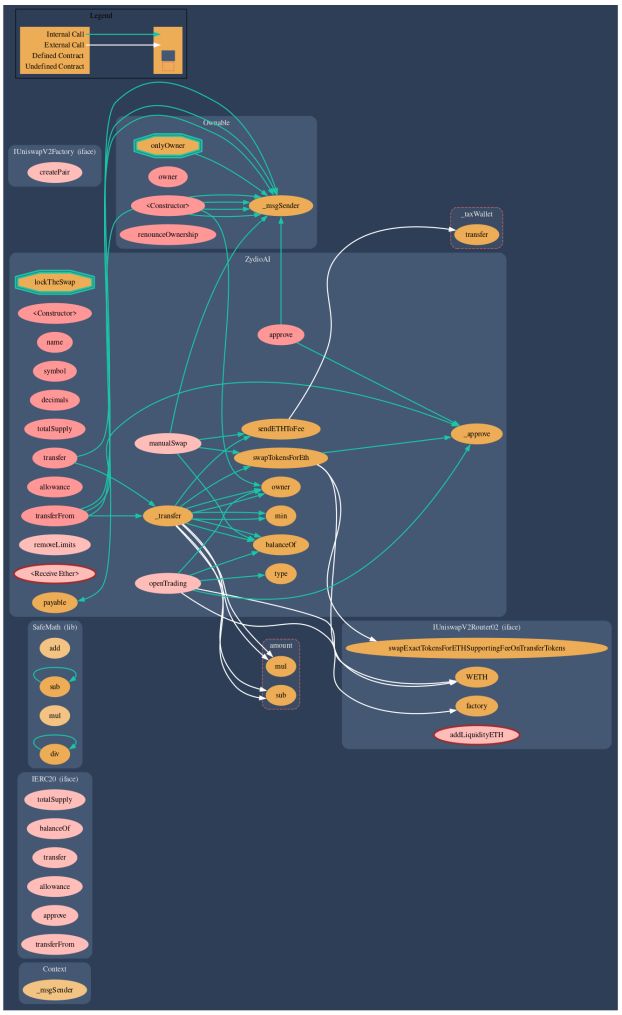
Name	Contract	Live
Zydio AI	https://testnet.bscscan.com/address/0x09e7999095aabEdE6802423F52ccCB16B83B836c	Yes

Solidity Code Provided

SolID	File Sha-1	FileName
Zydio AI	07f075b77c25c164cd8d65e65c6d1fa8cb93ef7d	ZDAI.sol
Zydio AI		
Zydio AI		
Zydio AI		
Zydio AI		
Zydio AI		

Call Graph

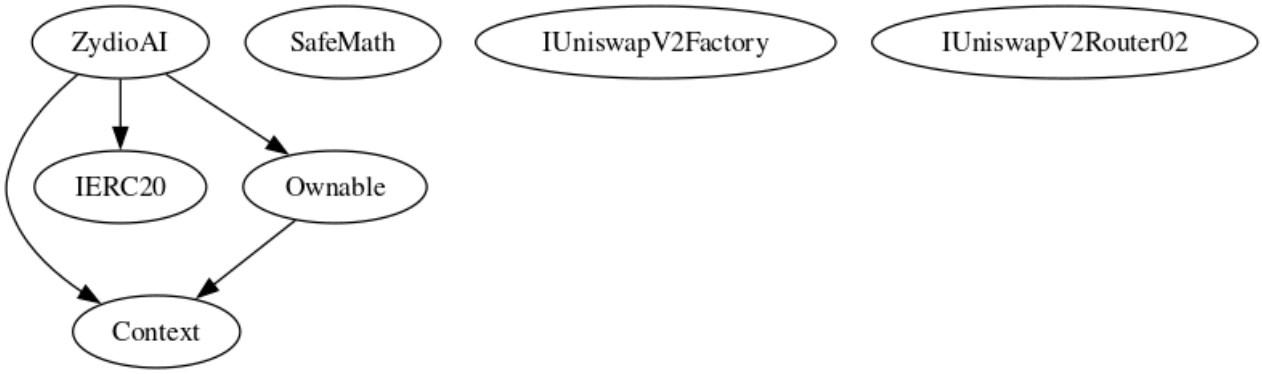
The contract for Zydio AI has the following call graph structure.



Inheritance

The contract for Zydio AI has the following inheritance structure.

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



$ZDAI-03 | Lack of Input Validation.

Category	Severity	Location	Status
Volatile Code	Low	ZDAI.sol: L: 289 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..

$ZDAI-05 | Missing Event Emission.

Category	Severity	Location	Status
Volatile Code	Low	ZDAI.sol: L: 301 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.

$ZDAI-14 | Unnecessary Use Of SafeMath

Category	Severity	Location	Status
Logical Issue	Medium	ZDAI.sol: L: 36 C: 9	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

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	1	0	1
Low	2	0	2
Informational	0	0	0
Total	3	0	3

Social Media Checks

Social Media	URL	Result
Twitter	https://x.com/ZydioAI	Pass
Other	https://www.youtube.com/channel/UCjgNEhlgAZx4CZxGn06urgg , https://www.tiktok.com/@zydio.ai	Pass
Website	https://zydio.ai/	Pass
Telegram	https://t.me/ZydioAI	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

Assessment Results

Score Results

Review	Score
Overall Score	100/100
Auditor Score	90/100
Review by Section	**Score**
Manual Scan Score	37
Auto Scan Score	37
Advance Check Score	29

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:

- High Initial Tax: Initial buy/sell tax is set at 40%, which is extremely high. This could deter potential users.
- Owner Privileges: The owner has significant control over the contract, including disabling transfer delay and setting max transaction and wallet sizes to the total supply.
- No Timelock on Ownership Transfer: The renounceOwnership function does not have a delay, which could be risky if used hastily.
- Transfer Delay: Enforces a one-block delay between transfers to prevent bots, but could also hinder regular users.
- Swap Mechanism: The contract swaps tokens for ETH if certain conditions are met, which could impact the token price if not managed properly.
- Manual Swap Function: The manualSwap function allows the tax wallet to swap tokens for ETH, which could be used to drain the contract.
- Hardcoded Router Address: The Uniswap router address is hardcoded, which could be problematic if the router changes.
- Liquidity Additions: The openTrading function adds liquidity once and enables trading, which could be gamed by the owner.
- No Reentrancy Guard: External calls could potentially be exploited without reentrancy protection.

- Use of tx.origin: The use of tx.origin for transfer delay checks can be problematic and is not recommended.ı
- No Burn Mechanism: There is no function to burn tokens and reduce the total supply.ı
- Lack of Events: Some functions, like manualSwap, could benefit from emitting events for transparency.ı
- Code Readability: Some functions are complex and could be broken down for better readability and maintainability.ı
- Compliance: Ensure the contract complies with the ERC20 standard and check for any deviations.ı
- Testing: Extensive testing is needed to ensure all functions behave as expected under various conditions.ı
- Gas Optimization: Some functions could be optimized for gas usage.ı
- Commenting: Inline comments are sparse, making it harder to understand the purpose of complex functions.ı
- No Multisig Wallet: The tax wallet is a single point of failure; a multisig wallet could improve security.ı
- Version: The contract uses Solidity 0.8.20, which is relatively recent, but always check for the latest stable version.ı
- These notes should be addressed to enhance the security and functionality of the contract before deployment.ı
- The contract is renounced.

Auditor Score =90

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