freshcoins

SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT

AirJIT

$JIT

14/03/2025

TOKEN OVERVIEW

Fees

- Buy fees: 0%
- Sell fees: 0%

Fees privileges

- Can’t change / set fees

Ownership

- Owned

Minting

- No mint function

Max Tx Amount / Max Wallet Amount

- Can change max tx amount (without threshold)

Blacklist

- Blacklist function detected

Other privileges

- Contract owner can set the cooldown duration to very high value, locking tokens (transfer)

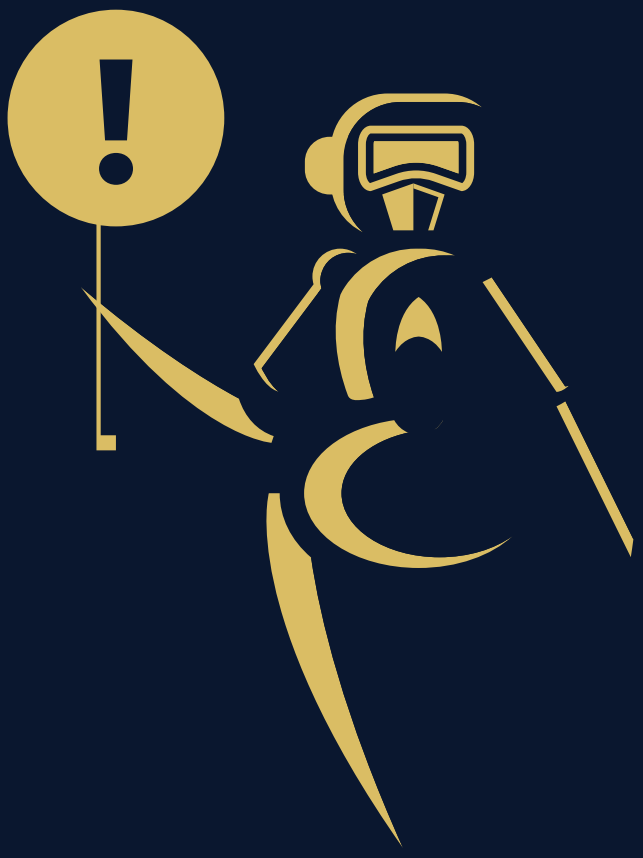
TABLE OF CONTENTS

DISCLAIMER

The information provided on this analysis document is only for general information and should not be used as a reason to invest.

FreshCoins Team will take no payment for manipulating the results of this audit.

The score and the result will stay on this project page information on our website https://freshcoins.io
FreshCoins Team does not guarantees that a project will not sell off team supply, or any other scam strategy (RUG or Honeypot etc)



INTRODUCTION

FreshCoins (Consultant) was contracted by AirJIT (Customer) to conduct a Smart Contract Code Review and Security Analysis.

0x087fECC62f2D7393191b3A4676ee66757C9e5cD1

Network: Binance Smart Chain (BSC)

This report presents the findings of the security assessment of Customer's smart contract and its code review conducted on 14/03/2025

WEBSITE DIAGNOSTIC

https://airjit.com/

0-49 50-89 90-100

Performance | Accessibility | Best Practices | SEO | Progressive Web App

Socials

X (Twitter)

https://x.com/AirJITGlobal

Telegram

https://t.me/AirJIT

AUDIT OVERVIEW

66

Security Score
HIGH RISK
Audit FAIL

93

Static Scan
Automatic scanning for common vulnerabilities

62

ERC Scan
Automatic checks for ERC's conformance

3	High
1	Medium
0	Low
0	Optimizations
0	Informational

No.	Issue description	Checking Status
1	Compiler Errors / Warnings	Passed
2	Reentrancy and Cross-function	Passed
3	Front running	Low
4	Timestamp dependence	Passed
5	Integer Overflow and Underflow	Passed
6	Reverted DoS	Passed
7	DoS with block gas limit	Passed
8	Methods execution permissions	Passed
9	Exchange rate impact	Passed
10	Malicious Event	Passed
11	Scoping and Declarations	Passed
12	Uninitialized storage pointers	Passed
13	Design Logic	Passed
14	Safe Zeppelin module	Passed

OWNER PRIVILEGES

- Contract owner can't mint tokens after initial contract deploy

- Contract owner can exclude addresses from transactions

```
function addBlacklist(
        address account
    ) external onlyRole(BLACKLIST_MANAGER_ROLE) {
        _blacklist[account] = true;
        emit Blacklisted(account);
}

function removeBlacklist(
        address account
    ) external onlyRole(BLACKLIST_MANAGER_ROLE) {
        _blacklist[account] = false;
        emit RemovedFromBlacklist(account);
}
```

- Contract owner can change max tx amount limitation (without threshold)

Note that setting the value too low may prevent users from making purchase transactions

```
function setMaxTransactionAmount(
        uint256 amount
    ) external onlyRole(ANTIBOT_ROLE) {
        maxTransactionAmount = amount;
        emit MaxTransactionAmountUpdated(amount);
}
```

- Contract owner can set the cooldown duration

There's a risk the cooldown could be set to very high durations (or manipulated), effectively locking tokens for extended periods

```
function setCooldownDuration(
        uint256 duration
    ) external onlyRole(ANTIBOT_ROLE) {
        cooldownDuration = duration;
        emit CooldownDurationUpdated(duration);
}
```

Pausable contract

The Pausable contract is a security mechanism that allows certain functions in a smart contract to be paused or unpaused in emergencies. It provides modifiers (whenNotPaused, whenPaused) to restrict access based on the contract's state, helping prevent unwanted actions during critical situations.

For investors, the main risk with a Pausable contract is that the developer or admin can pause the contract at any time, potentially halting critical functions like transfers, withdrawals, or trading. If misused or controlled by a malicious actor, it could freeze user funds or limit access, undermining trust and liquidity.

Recommendation:

The team should carefully manage the private keys of the owner's account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions. The risk can be prevented by temporarily locking the contract or renouncing ownership.

CONCLUSION AND ANALYSIS

Smart Contracts within the scope were manually reviewed and analyzed with static tools.

Audit report overview contains all found security vulnerabilities and other issues in the reviewed code.

Found 3 HIGH issues during the first review.

TOKEN DETAILS

Details

Buy fees:	0%
Sell fees:	0%
Max TX:	100,000,000
Max Wallet:	N/A

Honeypot Risk

Ownership:	Owned
Blacklist:	Detected
Modify Max TX:	Detected
Modify Max Sell:	Detected
Disable Trading:	Not detected

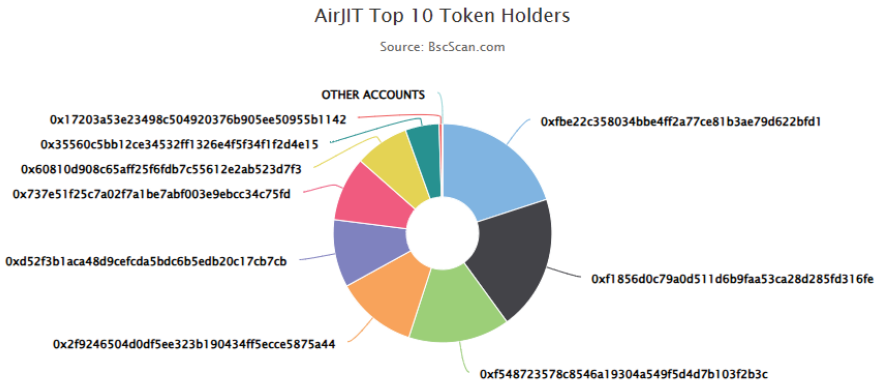
Rug Pull Risk

Liquidity:	N/A
Holders:	100% unlocked tokens

JIT TOKEN ANALYTICS & TOP 10 TOKEN HOLDERS

The top 10 holders collectively own 100.00% (100,000,000.00 Tokens) of AirJIT

Token Total Supply: 100,000,000.00 Token | Total Token Holders: 9



Rank	Address	Quantity (Token)	Percentage
1	0xfBE22c35...9d622BfD1	20,000,000	20.0000%
2	0xf1856D0c...85FD316fE	20,000,000	20.0000%
3	0xf5487235...b103F2b3C	15,000,000	15.0000%
4	0x2F924650...CE5875a44	12,000,000	12.0000%
5	0xd52f3b1a...0C17cb7cb	10,000,000	10.0000%
6	0x737E51F2...cC34C75FD	9,500,000	9.5000%
7	0x60810D90...ab523d7f3	8,000,000	8.0000%
8	0x35560c5B...f1f2D4e15	5,000,000	5.0000%
9	0x17203A53...0955b1142	500,000	0.5000%

TECHNICAL DISCLAIMER

Smart contracts are deployed and executed on the blockchain platform. The platform, its programming language, and other software related to the smart contract can have its vulnerabilities that can lead to hacks. The audit can't guarantee the explicit security of the audited project / smart contract.