NCI6900 (NCI6900) Smart Contract Audit Report

Network: Ethereum (ERC20)
Contract Address: 0x21d846C3831Def0b85C492CbFA4831BA937dd78f
Total Supply: 1,000,000,000
Decimals: 9
Holders: 386

Audit Summary

The NCI6900 smart contract is based on OpenZeppelin ERC20 v5.4.0 with custom logic. The contract implements a fixed supply model with no owner privileges and no minting functions after deployment. Overall, the contract is relatively clean but includes non-standard logic that introduces moderate risk.

Key Findings

1. Infinite Allowance for Pair Address (Medium Risk)
The contract overrides the allowance logic so that any address marked as a pair automatically receives unlimited allowance from all holders. This allows the pair to transfer tokens without explicit user approval, which may be considered a hidden privilege and introduces trust risk.
2. Centralized Pair Privileges (Medium Risk)
The liquidity pair address is defined during deployment and granted special spending rights. While this cannot be changed later, the privilege itself is significant and should be clearly disclosed to users.
3. Non-Standard Decimals (Low Risk)
The token uses 9 decimals instead of the common 18. This does not affect security but may cause display or integration issues with some platforms.

Security Review

• No mint function after deployment
• No owner or admin privileges
• No blacklist or pause functionality
• Fixed total supply
• Custom allowance logic detected

Risk Assessment

Overall Risk Level: **Medium**
The primary concern is the infinite allowance granted to the pair address, which could theoretically be abused if the pair is compromised or behaves maliciously.

Trust Score

Trust & Security Score: 74%
This score reflects a solid ERC20 foundation with transparent supply mechanics, offset by non-standard logic that requires user trust and proper disclosure.

Final Verdict

NCI6900 is not identified as an outright malicious contract. However, it contains custom logic that deviates from the ERC20 standard and may pose moderate trust risks. Investors and users should be informed of the special allowance behavior before interacting with the token.