Nero: Security Audit Report

DogScan Security Team

July 21st, 2025

Contents

DogScan Security Audit Report

Project	Nero
Chain	Ethereum (ID 1)
Contract Address	NERO
Contract Type	ERC20 Token Contract
Audit Date	July 21st, 2025
Report Version	1.1

1. Executive Summary

We conducted a comprehensive security audit of the `NERO` token contract deployed on the Ethereum network. This contract is a standard ERC20 token built on OpenZeppelin libraries with minting, pausing, and burning capabilities. The audit results revealed **some design characteristics that require attention**, primarily related to centralized governance structure.

This analysis identified some design characteristics that require attention, mainly related to centralized governance structure. The contract is built on standard OpenZeppelin libraries with a solid technical foundation, and users need to understand the characteristics of its governance model.

Overall Risk Rating: Low

We recommend that users fully understand the contract's governance mechanism before participating.

2. Audit Scope

The audit scope covers the `NERO` token contract deployed on Ethereum:

Contract Information:

- Contract Address: `0x0169043c91be299445826619d492a2ecab487282`
- Contract Type: ERC20 Token Contract
- Token Name: NERO
- Token Symbol: NERO
- Decimals: 18

- Maximum Supply: 10,000,000,000 NERO
- Owner Address: `0xa86E8486DAc0c475c85060135C5374cb11614352`

Key Audit Areas:

- ERC20 standard implementation and security
- Minter role management mechanism
- Pause functionality implementation
- Ownership transfer mechanism
- Token burning functionality
- Centralized governance structure

3. Audit Methodology

This audit employed a multi-agent AI security analysis framework specifically designed for smart contract security assessment:

1. Specialized Analysis Modules:

- **Access Control Expert**: Evaluates upgrade mechanisms and administrative privileges
- **Core Logic Analyst**: Reviews token transfer and business logic implementation
- **Honeypot Detection Expert**: Checks for potential selling restriction mechanisms
- **Liquidity Risk Analyst**: Assesses liquidity manipulation risks
- **Reentrancy Expert**: Analyzes external call patterns and state management
- **Supply Economics Expert**: Evaluates token supply dynamics and economic models
- **User Privilege Analyst**: Assesses user token operation restrictions
- **DeFi Mathematics Expert**: Reviews arithmetic operations and mathematical security

2. Advanced Research Team:

- Advanced attack vector pattern recognition
- Cross-contract interaction analysis
- Systemic risk assessment

3. Comprehensive Analysis:

- Lead Security Strategist integrates all findings
- Risk prioritization and impact assessment
- Comprehensive reporting and recommendation development

4. Remediation Status Update

v1.1 Update Record (July 21st, 2025):

The project team has remediated the minting permission management issue in I-01:

- **Contract Address Update**: Updated from `0x39Dd9bC4db89423F926CD29892B3363B62520d19` to `0x0169043c91be299445826619d492a2ecab487282`
- **Supply Cap Implementation**: Added maximum supply limit (10,000,000,000 NERO)
- **Minting Restrictions**: Minting function is now subject to supply cap checks and cannot exceed the maximum supply
- **Status Change**: I-01 issue status updated from "User Notice" to "Partially Fixed"

Remaining Risks: Pause functionality is still controlled by a single owner, further decentralized governance is recommended.

5. Findings Summary

ID	Title	Severity	Status
I-01	Centralized Governance Structure Risk	**Information**	**Partially Fixed**

6. Detailed Findings

[I-01] Centralized Governance Structure Risk (Information)

Severity: Information

Description This contract adopts a centralized management model controlled by a single Externally Owned Account (EOA) owner with multiple critical functions. The owner address `0xa86E8486DAc0c475c85060135C5374cb11614352` possesses the following privileges:

1. **Minting Permission Management**: The owner can unilaterally grant "minter" roles to any address. **[FIXED]** Now implements maximum supply limit (10,000,000,000 NERO), minting function cannot exceed this cap
2. **Global Pause Control**: The owner can pause all token transfers, approvals, minting, and burning functions by calling the `pause` function

Impact This centralized governance structure means:

- **[IMPROVED]** Token supply is now limited by maximum supply cap (10,000,000,000 NERO), cannot be infinitely increased
- The owner can freeze all user funds and token functionality at any time
- Contract security depends on the trustworthiness of a single owner
- Users need to fully understand the risks of this governance model

Technical Details The contract uses OpenZeppelin's `Ownable` pattern to restrict key functions to owner-only calls:

Fix Details: Added supply cap, minting function now limited by maximum supply

```
uint256 private _maxSupply = 10_000_000_000 * (10 ** _decimals);

function addMinter(address account) external onlyOwner {
    _minters.add(account);
    emit MinterRegistered(account);
}

function mint(address to, uint256 amount) external onlyMinter {
    if(super.totalSupply() + amount > _maxSupply) {
        revert SupplyExceedsCap();
    }
    _mint(to, amount);
}

function pause() external onlyOwner {
    _pause();
}

function unpause() external onlyOwner {
    _unpause();
}
```

User Notice Users should understand before participating in this token:

1. This is a centrally managed token contract with all key functions controlled by a single owner
2. **[IMPROVED]** Token supply is now limited by maximum supply cap (10,000,000,000 NERO), cannot be infinitely increased
3. The owner can pause all token functionality at any time
4. Users should evaluate the project team's credibility and governance transparency
5. It is recommended to pay attention to the project's governance mechanism and multi-signature management

Recommendations

- Consider migrating control to a multi-signature wallet or decentralized governance mechanism (such as a DAO)
- **[IMPLEMENTED]** Maximum supply limit implemented (original requirement: implement supply caps and minting restrictions)
- Add time-lock mechanisms for critical functions
- Improve governance transparency and community participation

7. Architecture and Design Assessment

Design Strengths

1. **Use of Standard Libraries**: Contract is built on battle-tested OpenZeppelin contracts
2. **Correct ERC20 Implementation**: Basic token functionality complies with standards
3. **Secure Mathematical Operations**: Uses Solidity 0.8+ providing default overflow/underflow protection
4. **Reentrancy Protection**: Correctly follows Checks-Effects-Interactions (CEI) pattern

Key Architectural Issues

1. **Centralized Governance Structure**: Single EOA owner controls multiple key functions
2. **Supply Management Mechanism**: **[IMPROVED]** Now implements hardcoded supply cap (10,000,000,000 NERO)
3. **User Permission Control**: Owner can pause all token functionality

Systemic Risks

This contract adopts a centralized management model with the following systemic characteristics:

1. **Centralized Governance Structure**: The single EOA owner at `0xa86E8486DAc0c475c85060135C5374` controls multiple key functions, including minting permission management and global pause control. This design may be suitable for specific scenarios requiring centralized management.
2. **Supply Management Mechanism**: **[IMPROVED]** Now implements hardcoded supply cap (10,000,000,000 NERO), token supply cannot exceed this limit. This improvement enhances the predictability of the token economic model.

3. **User Permission Control**: The owner can pause all token functionality at any time, including transfers, approvals, minting, and burning. This design provides emergency control mechanisms but also means user funds may be frozen.

Recommendations for Improvement

1. **Decentralized Governance**: Consider migrating control to multi-signature wallets or DAOs
2. **Limit Minting Capability**: **[IMPLEMENTED]** Maximum supply limit implemented (original requirement: implement supply caps)
3. **Time-lock Mechanisms**: Add time delays for critical functions

8. Conclusion

This security audit identified **some design characteristics that require attention** in the `NERO` token contract. The contract is built on standard OpenZeppelin libraries with a solid technical foundation, and users need to understand the characteristics of its governance model.

Key Findings Summary:

- **Centralized Governance Structure**: Single owner EOA controls key functions, including minting permission management and global pause control
- **Supply Management Mechanism**: **[IMPROVED]** Now implements hardcoded supply cap (10,000,000,000 NERO), enhancing the predictability of the token economic model
- **User Permission Control**: Owner can pause all token functionality at any time, providing emergency control mechanisms

Overall Risk Rating: Low

The current implementation has certain centralized governance characteristics, and contract security depends on the owner's credibility. While the technical implementation is based on secure libraries, users need to understand the characteristics of this governance model.

Recommendations for Improvement:

1. Consider migrating control to multi-signature wallets or decentralized governance mechanisms (such as DAOs)
2. **[IMPLEMENTED]** Maximum supply limit implemented (10,000,000,000 NERO) (original requirement: implement supply caps and minting restrictions)
3. Add time-lock mechanisms for critical functions

We recommend that users fully understand the contract's governance mechanism and characteristics before participating.

Disclaimer

This audit report is provided for informational purposes only and does not constitute investment advice. The analysis is based on smart contract source code provided at a specific point in time and does not constitute an endorsement of the project or a guarantee of its security. Smart contracts carry inherent risks, including potential undiscovered vulnerabilities. Users should conduct their own research and exercise caution when interacting with any smart contract. The findings in this report are an assessment of risk based on known attack vectors and best practices.