ERC20-NOVASTRO Audit Report

January 22, 2025

PVE001: Improved Vesting Schedule Creation Logic in TokenVesting

```
function createVestingSchedule( ...
) external onlyOwner {
    require(_beneficiary != address(0), "Beneficiary address cannot be 0");
    require(_totalAmount > 0, "Total amount must be greater than 0");
    require(!vestingSchedules[_beneficiary].initialized, "Vesting schedule already exists");

    uint256 tgeAmount = (_totalAmount * _tgePercentage) / 1000; // Divide by 1000 since percentage i
    uint256 cliffDuration = _cliffMonths * 30 days;
    uint256 vestingDuration = _vestingMonths * 30 days;

    vestingSchedules[_beneficiary] = VestingSchedule({
        totalAmount: _totalAmount,
        tgeAmount: tgeAmount,
        cliffDuration: cliffDuration,
        vestingDuration: vestingDuration,
        startTime: block.timestamp,
        released: 0,
        initialized: true
    });

    // Transfer TGE tokens immediately if any
    if (tgeAmount > 0) {
        require(token.transfer(_beneficiary, tgeAmount), "Token transfer failed");
        vestingSchedules[_beneficiary].released = tgeAmount;
    }

    emit VestingScheduleCreated(_beneficiary, _totalAmount);
```

tgeAmount,

remove

PVE002: Trust on Admin Keys

- Owner is privileged to guard/coordinate token-wide operations
  - Create new vesting schedules for assigned beneficiaries

```
}

function createVestingSchedule(
    address _beneficiary,
    uint256 _totalAmount,
    uint256 _tgePercentage, // Percentage * 10 (e.g., 225 for 22.5%)
    uint256 _cliffMonths,
    uint256 _vestingMonths
) external onlyOwner {
    require(_beneficiary != address(0), "Beneficiary address cannot
    require(_totalAmount > 0, "Total amount must be greater than 0")
    require(!vestingSchedules[_beneficiary].initialized, "Vesting sc
    require(_tgePercentage < 1000);
    uint256 tgeAmount = (_totalAmount * _tgePercentage) / 1000; // D
    uint256 cliffDuration = _cliffMonths * 30 days;
```

N1: Suggested Immutable Storage State When Assigned Only in Constru

```
contract TokenVesting is Ownable {
    struct VestingSchedule {
        uint256 totalAmount;
        uint256 tgeAmount;
        uint256 cliffDuration;
        uint256 vestingDuration;
        uint256 startTime;
        uint256 released;
        bool initialized;
    }

    IERC20 public token;

    // Mapping from beneficiary address to vesting schedule
    mapping(address => VestingSchedule) public vestingSchedules;

    event TokensReleased(address beneficiary, uint256 amount);
    event VestingScheduleCreated(address beneficiary, uint256 totalAmount);

    constructor(address _token) Ownable(msg.sender) {
        require(_token != address(0), "Token address cannot be 0");
        token = IERC20(_token);
    }
```

immutable