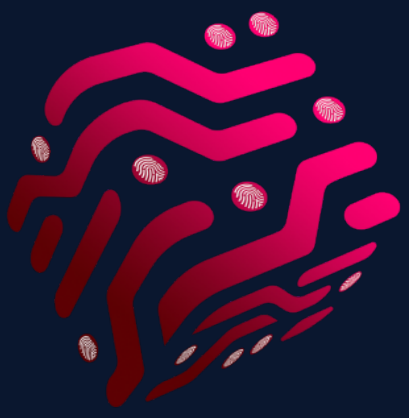
freshcoins

SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT



3N Tokens

$3NT

23/06/2024

TOKEN OVERVIEW

Fees

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

Fees privileges

- Can’t change fees

Ownership

- Owned

Minting

- No mint function

Max Tx Amount / Max Wallet Amount

- Can’t change max tx amount and / or max wallet amount

Blacklist

- Blacklist function not detected

Other privileges

- There are several improvements that should be implemented in the contract code to enhance safety and security

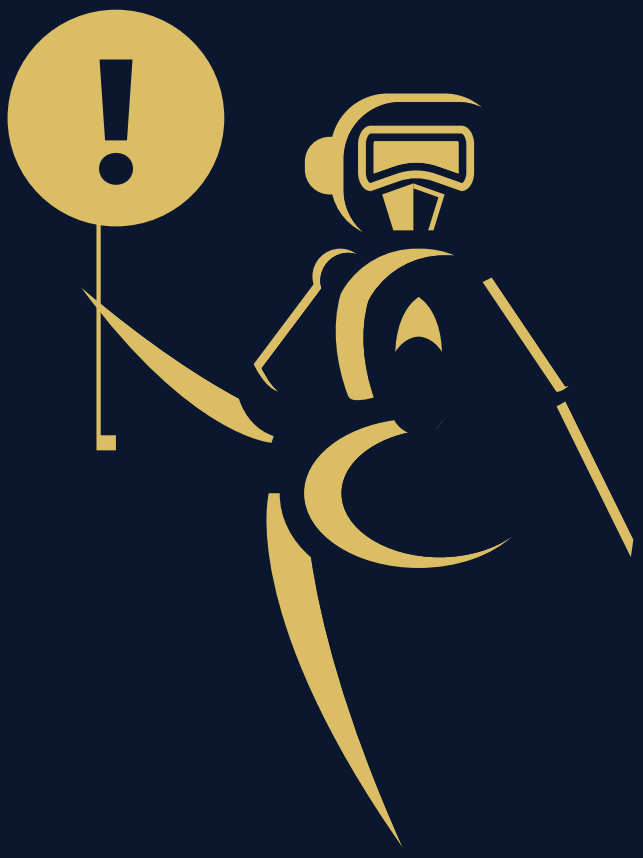
TABLE OF CONTENTS

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
3N Tokens (Customer) to conduct a Smart Contract Code Review and Security Analysis.

0x3c1EFced2Be78B0D0Bb2b217E768F815d4a68193

Network: Base Network (ETH)

This report presents the findings of the security assessment of Customer's smart contract and its code review conducted on 23/06/2024

WEBSITE DIAGNOSTIC

https://nnn.cloud


0-49


50-89


90-100

Performance

Accessibility

Best Practices

SEO

Progressive Web App

Socials


Twitter

https://twitter.com/nnn_onX


Telegram

https://t.me/join_nnn

AUDIT OVERVIEW

58

Security Score
HIGH RISK
Audit FAIL

93

Static Scan
Automatic scanning for common vulnerabilities

55

ERC Scan
Automatic checks for ERC's conformance

3	High
3	Medium
0	Low
0	Optimizations
0	Informational

No.	Issue description	Checking Status
1	Compiler Errors / Warnings	Passed
2	Reentrancy and Cross-function	Medium
3	Front running	Low
4	Timestamp dependence	Passed
5	Integer Overflow and Underflow	Passed
6	Reverted DoS	Passed
7	DoS with block gas limit	Low
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't exclude addresses from transactions

- Contract owner can update URLs from urls list

  Instead of using delete urls followed by a loop to push new URLs, it can be more gas-efficient to simply update the array in place if possible

```
function updateUrls(string[] calldata newUrls) external onlyOwner {
    require(
      block.timestamp < restrictionEndTime,
      "Cannot update URLs after restriction end time"
    );
    delete urls;
    for (uint256 i = 0; i < newUrls.length; i++) {
      urls.push(newUrls[i]);
    }
}
```

- Contract owner can update PriceFeeds

  Emitting an event after updating the price feeds can help in tracking these changes also deleting the array and then reinitializing it might not be the most gas-efficient approach

  It's generally a good practice to check for zero addresses to prevent setting invalid price feeds

```
function updatePriceFeeds(
    address[] calldata newPriceFeeds,
    address newPriceFeed
  ) external onlyOwner {
    delete priceFeeds;
    usePriceFeeds = newPriceFeeds.length > 0;
    for (uint256 i = 0; i < newPriceFeeds.length; i++) {
      priceFeeds.push(AggregatorV3Interface(newPriceFeeds[i]));
    }
    priceFeed = AggregatorV3Interface(newPriceFeed);
}
```

- Function commitPriceUpdate appears to work as intended

  Emitting an event after a price commit can help track changes

```
function commitPriceUpdate(bytes32 priceHash) external onlyOwner {
    priceCommits[msg.sender] = PriceCommit(priceHash, block.timestamp);
}
```

The revealPriceUpdate function requires improvements to ensure proper functionality and security

Emitting an event after a successful price update can help track changes

With Solidity 0.8+, you don't need to use SafeMath for addition since overflow checks are built-in

```
function revealPriceUpdate(
    int256 newPrice,
    string calldata secret
  ) external onlyOwner {
    PriceCommit memory commit = priceCommits[msg.sender];
    require(commit.timestamp > 0, "No committed price update");
    require(
      block.timestamp >= commit.timestamp.add(REVEAL_PERIOD),
      "Reveal period has not passed"
    );

    bytes32 hash = keccak256(abi.encodePacked(newPrice, secret));
    require(hash == commit.priceHash, "Invalid price or secret");

    // Update the latest price
    latestPrice = newPrice;
    _updatePriceHistory(newPrice);

    // Clear the commit
    delete priceCommits[msg.sender];
}
```

The calculateMedianPrice function requires multiple improvements

Bubble sort is not the most efficient sorting algorithm for large datasets. For better performance, consider using a more efficient algorithm like QuickSort

When calculating the median for an even number of elements, you should be aware that integer division in Solidity will truncate the result

```
function calculateMedianPrice(
    int256[] memory prices,
    uint256 count
  ) internal pure returns (int256) {
    int256[] memory sortedPrices = new int256[](count);
    for (uint256 i = 0; i < count; i++) {
      sortedPrices[i] = prices[i];
    }
    bubbleSort(sortedPrices, count);
    if (count % 2 == 1) {
      return sortedPrices[count / 2];
    } else {
      return
        (sortedPrices[(count / 2) - 1] + sortedPrices[count / 2]) / 2;
    }
}
```

Contract owner can set up the initial distribution of tokens to various addresses

The function ensures that the total supply of tokens is minted before initiating the distribution and calculates the distribution progress for each category

Function doesn't seem to make any external calls, it's generally a good practice to use a reentrancy guard on functions modifying the state extensively

Solidity 0.8 and above includes built-in overflow and underflow checks, so there's no need for explicit SafeMath library usage. Ensure your Solidity version is 0.8 or above (The / operator is used instead of div from the SafeMath library, assuming Solidity 0.8 or later, where overflow checks are implicit)

Emitting events for critical actions is a good practice for better tracking and debugging

```
function startInitialDistribution(
        DistributionAddresses calldata _addresses
    ) external onlyOwner {
        require(
            totalSupply() == TOTAL_SUPPLY,
            "Total supply must be minted first"
        );

        nexusSpriteAddresses = _addresses.nexusSpriteAddresses;
        ...
        nodeRewardsAddresses = _addresses.nodeRewardsAddresses;

        // Initialize distribution progress
        nexusSpriteProgress = DistributionProgress(
            0,
            NEXUS_SPRITE_SUPPLY.div(_addresses.nexusSpriteAddresses.length)
        );
        ...
        liquidityPoolsProgress = DistributionProgress(
            0,
            LIQUIDITY_POOLS_SUPPLY.div(
                _addresses.liquidityPoolsAddresses.length
            )
        );
        nodeRewardsProgress = DistributionProgress(
            0,
            NODE_REWARDS_SUPPLY.div(_addresses.nodeRewardsAddresses.length)
        );
    }
```

The _transfer function appears to include the necessary logic for enforcing sale limits on founding team addresses and dynamically adjusting the allowed transfer percentage

Since you're using Solidity 0.8 or later, overflow and underflow checks are built-in. However, if you prefer explicit safety, you can continue using SafeMath (Although Solidity 0.8+ includes overflow checks, SafeMath usage is retained for explicit safety)

Emitting events for critical actions can help with tracking and debugging

Ensure that the isFoundingTeamAddress mapping is necessary to update for the recipient in every transfer

```
function _transfer(
        address sender,
        address recipient,
        uint256 amount
    ) internal override {
        uint256 currentTimestamp = block.timestamp;

        // Dynamic adjustment of allowed percentage based on market conditions
        uint256 allowedPercentage = getDynamicAllowedPercentage();

        // Apply sale limits for founding team addresses post 90 days
        if (
            currentTimestamp >= restrictionEndTime &&
            isFoundingTeamAddress[sender]
        ) {
            uint256 allowedAmount = (allowedPercentage.mul(balanceOf(sender)))
                .div(100);
            require(
                foundingTeamSoldAmount[sender].add(amount) <= allowedAmount,
                "Transfer amount exceeds the allowed limit for founding team addresses"
            );

            foundingTeamSoldAmount[sender] = foundingTeamSoldAmount[sender].add(
                amount
            );
            lastFoundingTeamSaleTimestamp[sender] = currentTimestamp;

            // Mark recipient as restricted if the sender is a founding team member
            isFoundingTeamAddress[recipient] = true;
        }

        super._transfer(sender, recipient, amount);
    }
```

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:	N/A
Max Wallet:	N/A

Honeypot Risk

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

Rug Pull Risk

Liquidity:	N/A
Holders:	100% unlocked tokens

3NT TOKEN ANALYTICS & TOP 10 TOKEN HOLDERS

The top 10 holders collectively own 99.24% (1,091,641,000.00 Tokens) of 3N Tokens

Token Total Supply: 1,100,000,000.00 Token | Total Token Holders: 18

(A total of 1,091,641,000.00 tokens held by the top 10 accounts from the total supply of 1,100,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0x1757d696...f60Aa5aEC	170,000,000	15.4545%
2	0xF9B83faC...171C311dC	162,000,000	14.7273%
3	0x9b2D3B7F...5F0c6bd0f	150,001,000	13.6365%
4	0x2d44fba5...8A1B09c7e	150,000,000	13.6364%
5	0x4eE6cc7C...F87C511e2	140,000,000	12.7273%
6	0x477a1AF9...F5B2c84Bd	89,640,000	8.1491%
7	0xcBe2AD7B...E32057c0F	75,000,000	6.8182%
8	0xF5E04c22...CfADAcF41	70,000,000	6.3636%
9	0x83f3de1F...A172c4D4D	60,000,000	5.4545%
10	0xEa84ACAd...853d4A5d5	25,000,000	2.2727%

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.