



TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

August, 2021

Audit Details



Audited project

Nomen Finance



Deployer address

0x06bB16C0470282E328Df736e4dC2DDD79a831aaD



Client contacts:

Nomen Finance team



Blockchain

Ethereum



Project website:

<http://nomen.finance/>

Disclaimer

This is a limited report on our findings based on our analysis, in accordance with good industry practice as at the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the below disclaimer below – please make sure to read it in full.

DISCLAIMER: By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and TechRate and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (TechRate) owe no duty of care towards you or any other person, nor does TechRate make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and TechRate hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, TechRate hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against TechRate, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report.

The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed.

Background

TechRate was commissioned by Nomen Finance to perform an audit of smart contracts:

<https://etherscan.io/address/0xfe72971578bd3a18c87c653548bf0372567e4c28#code>

The purpose of the audit was to achieve the following:

- Ensure that the smart contract functions as intended.
- Identify potential security issues with the smart contract.

The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Contracts Details

Token contract details for 10.08.2021

Contract name	Nomen Finance
Contract address	0xfe72971578bd3a18c87c653548bf0372567e4c28
Total supply	10,000,000,000
Token ticker	NMN
Decimals	9
Token holders	39
Transactions count	72
Top 100 holders dominance	99.74%
Liquidity fee	0
Tax fee	3
Total fees	530026115047091223
Uniswap V2 pair	0x9514ccb3be524f8dabca7ac84bfc4b4a2dedc16
Contract deployer address	0x06bB16C0470282E328Df736e4dC2DDD79a831aaD
Contract's current owner address	0x06bB16C0470282E328Df736e4dC2DDD79a831aaD

Nomen Finance Token Distribution

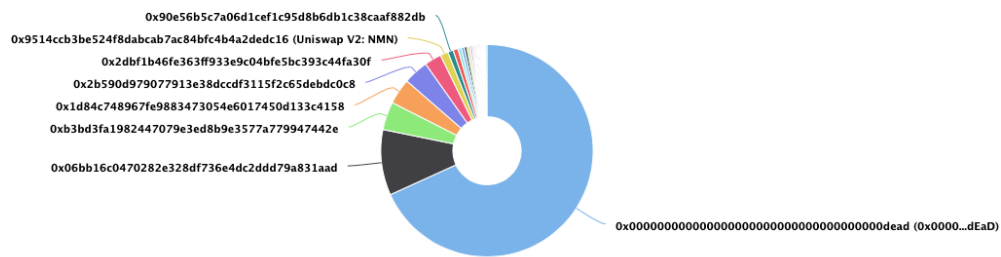
 The top 100 holders collectively own 99.74% (9,974,406,633.67 Tokens) of Nomen Finance

 Token Total Supply: 10,000,000,000.00 Token

|


Total Token Holders: 39

Nomen Finance Top 100 Token Holders
Source: Etherscan.io



(A total of 9,974,406,633.67 tokens held by the top 100 accounts from the total supply of 10,000,000,000.00 token)

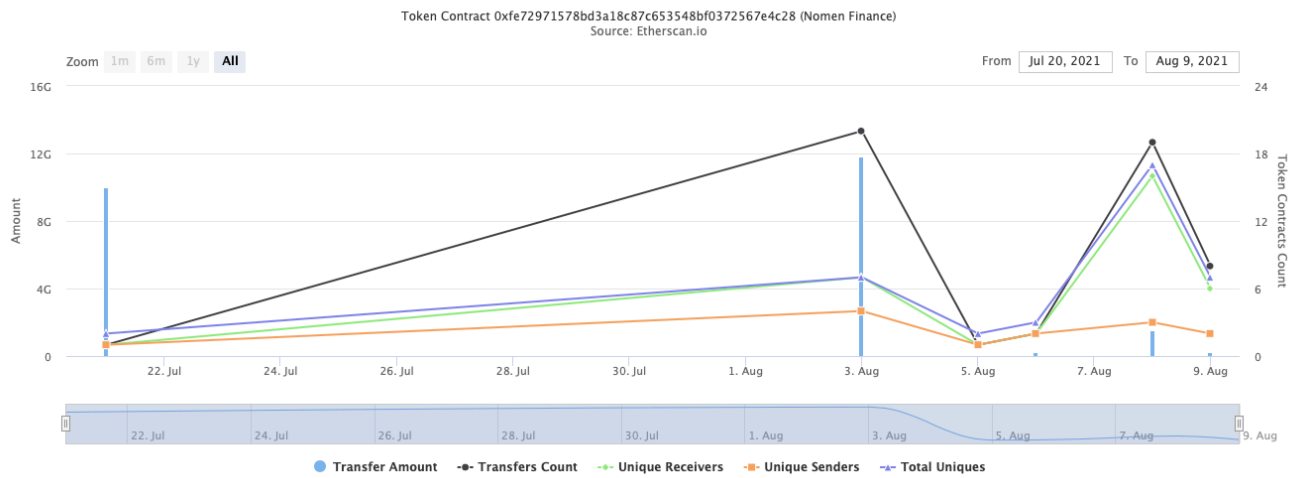
Nomen Finance Contract Interaction Details

Rank	Address	Quantity (Token)	Percentage
1	0x0000...dEaD	6,820,401,119.56514139	68.2040%
2	0x06bb16c0470282e328df736e4dc2ddd79a831aad	1,000,000,000	10.0000%
3	0xb3bd3fa1982447079e3ed8b9e3577a779947442e	428,165,167.108175805	4.2817%
4	0x1d84c748967fe9883473054e6017450d133c4158	391,229,226.23080124	3.9123%
5	0x2b590d979077913e38dcd3115f2c65debd0c8	380,079,861.623519922	3.8008%
6	0x2dbf1b46fe363ff933e9c04bfe5bc393c44fa30f	258,757,625.214486428	2.5876%
7	 Uniswap V2: NMN	121,183,727.59585125	1.2118%
8	0x90e56b5c7a06d1cef1c95d8b6db1c38caaf882db	83,827,832.956305342	0.8383%
9	0x2a29f4de367134b661d664a206adcc6704d38488	74,860,413.987764514	0.7486%
10	0x32fd35f33a82d443327fad4fb2f82138f809b223	50,040,289.038309565	0.5004%

Nomen Finance Top 10 Token Holders

Time Series: Token Contract Overview

Wed 21, Jul 2021 - Mon 9, Aug 2021



Contract functions details

+ Context

- [Int] _msgSender
- [Int] _msgData

+ [Int] IERC20

- [Ext] totalSupply
- [Ext] balanceOf
- [Ext] transfer #
- [Ext] allowance
- [Ext] approve #
- [Ext] transferFrom #

+ [Lib] SafeMath

- [Int] add
- [Int] sub
- [Int] sub
- [Int] mul
- [Int] div
- [Int] div
- [Int] mod
- [Int] mod

+ [Lib] Address

- [Int] isContract
- [Int] sendValue #
- [Int] functionCall #
- [Int] functionCall #
- [Int] functionCallWithValue #
- [Int] functionCallWithValue #
- [Prv] _functionCallWithValue #

+ Ownable (Context)

- [Pub] <Constructor> #
- [Pub] owner
- [Pub] renounceOwnership #
 - modifiers: onlyOwner
- [Pub] transferOwnership #
 - modifiers: onlyOwner
- [Pub] getUnlockTime
- [Pub] getTime
- [Pub] lock #
 - modifiers: onlyOwner
- [Pub] unlock #

+ [Int] IUniswapV2Factory

- [Ext] feeTo
- [Ext] feeToSetter
- [Ext] getPair
- [Ext] allPairs
- [Ext] allPairsLength
- [Ext] createPair #

- [Ext] setFeeTo #
- [Ext] setFeeToSetter #

+ [Int] IUniswapV2Pair

- [Ext] name
- [Ext] symbol
- [Ext] decimals
- [Ext] totalSupply
- [Ext] balanceOf
- [Ext] allowance
- [Ext] approve #
- [Ext] transfer #
- [Ext] transferFrom #
- [Ext] DOMAIN_SEPARATOR
- [Ext] PERMIT_TYPEHASH
- [Ext] nonces
- [Ext] permit #
- [Ext] MINIMUM_LIQUIDITY
- [Ext] factory
- [Ext] token0
- [Ext] token1
- [Ext] getReserves
- [Ext] price0CumulativeLast
- [Ext] price1CumulativeLast
- [Ext] kLast
- [Ext] burn #
- [Ext] swap #
- [Ext] skim #
- [Ext] sync #
- [Ext] initialize #

+ [Int] IUniswapV2Router01

- [Ext] factory
- [Ext] WETH
- [Ext] addLiquidity #
- [Ext] addLiquidityETH (\$)
- [Ext] removeLiquidity #
- [Ext] removeLiquidityETH #
- [Ext] removeLiquidityWithPermit #
- [Ext] removeLiquidityETHWithPermit #
- [Ext] swapExactTokensForTokens #
- [Ext] swapTokensForExactTokens #
- [Ext] swapExactETHForTokens (\$)
- [Ext] swapTokensForExactETH #
- [Ext] swapExactTokensForETH #
- [Ext] swapETHForExactTokens (\$)
- [Ext] quote
- [Ext] getAmountOut
- [Ext] getAmountIn
- [Ext] getAmountsOut
- [Ext] getAmountsIn

+ [Int] IUniswapV2Router02 (IUniswapV2Router01)

- [Ext] removeLiquidityETHSupportingFeeOnTransferTokens #
- [Ext] removeLiquidityETHWithPermitSupportingFeeOnTransferTokens #

- [Ext] swapExactTokensForTokensSupportingFeeOnTransferTokens #
- [Ext] swapExactETHForTokensSupportingFeeOnTransferTokens (\$)
- [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #

+ nomenclature (Context, IERC20, Ownable)

- [Pub] <Constructor> #
- [Pub] name
- [Pub] symbol
- [Pub] decimals
- [Pub] totalSupply
- [Pub] balanceOf
- [Pub] transfer #
- [Pub] allowance
- [Pub] approve #
- [Pub] transferFrom #
- [Pub] recoverERC20 #
 - modifiers: onlyOwner
- [Pub] increaseAllowance #
- [Pub] decreaseAllowance #
- [Pub] isExcludedFromReward
- [Pub] totalFees
- [Pub] minimumTokensBeforeSwapAmount
- [Pub] buyBackUpperLimitAmount
- [Pub] deliver #
- [Pub] reflectionFromToken
- [Pub] tokenFromReflection
- [Pub] excludeFromReward #
 - modifiers: onlyOwner
- [Ext] includeInReward #
 - modifiers: onlyOwner
- [Prv] _approve #
- [Prv] _transfer #
- [Prv] swapTokens #
 - modifiers: lockTheSwap
- [Prv] buyBackTokens #
 - modifiers: lockTheSwap
- [Prv] swapTokensForEth #
- [Prv] swapETHForTokens #
- [Prv] addLiquidity #
- [Prv] _tokenTransfer #
- [Prv] _transferStandard #
- [Prv] _transferToExcluded #
- [Prv] _transferFromExcluded #
- [Prv] _transferBothExcluded #
- [Prv] _reflectFee #
- [Prv] _getValues
- [Prv] _getTValues
- [Prv] _getRValues
- [Prv] _getRate
- [Prv] _getCurrentSupply
- [Prv] _takeLiquidity #
- [Prv] calculateTaxFee
- [Prv] calculateLiquidityFee
- [Prv] removeAllFee #
- [Prv] restoreAllFee #

- [Pub] isExcludedFromFee
- [Pub] excludeFromFee #
 - modifiers: onlyOwner
- [Pub] includeInFee #
 - modifiers: onlyOwner
- [Ext] setTaxFeePercent #
 - modifiers: onlyOwner
- [Ext] setLiquidityFeePercent #
 - modifiers: onlyOwner
- [Ext] setMaxTxAmount #
 - modifiers: onlyOwner
- [Ext] setMarketingDivisor #
 - modifiers: onlyOwner
- [Ext] setNumTokensSellToAddToLiquidity #
 - modifiers: onlyOwner
- [Ext] setBuybackUpperLimit #
 - modifiers: onlyOwner
- [Ext] setMarketingAddress #
 - modifiers: onlyOwner
- [Pub] setSwapAndLiquifyEnabled #
 - modifiers: onlyOwner
- [Pub] setBuyBackEnabled #
 - modifiers: onlyOwner
- [Ext] prepareForPreSale #
 - modifiers: onlyOwner
- [Ext] afterPreSale #
 - modifiers: onlyOwner
- [Prv] transferToAddressETH #
- [Ext] <Fallback> (\$)

(\$)= payable function

= non-constant function

Issues Checking Status

Issue description		Checking status
1.	Compiler errors.	Passed
2.	Race conditions and Reentrancy. Cross-function race conditions.	Passed
3.	Possible delays in data delivery.	Passed
4.	Oracle calls.	Passed
5.	Front running.	Passed
6.	Timestamp dependence.	Passed
7.	Integer Overflow and Underflow.	Passed
8.	DoS with Revert.	Passed
9.	DoS with block gas limit.	Low issues
10.	Methods execution permissions.	Passed
11.	Economy model of the contract.	Passed
12.	The impact of the exchange rate on the logic.	Passed
13.	Private user data leaks.	Passed
14.	Malicious Event log.	Passed
15.	Scoping and Declarations.	Passed
16.	Uninitialized storage pointers.	Passed
17.	Arithmetic accuracy.	Passed
18.	Design Logic.	Passed
19.	Cross-function race conditions.	Passed
20.	Safe Open Zeppelin contracts implementation and usage.	Passed
21.	Fallback function security.	Passed

Security Issues

✓ High Severity Issues

No high severity issues found.

✓ Medium Severity Issues

No medium severity issues found.

✓ Low Severity Issues

1. Out of gas

Issue:

- The function `includeInReward()` uses the loop to find and remove addresses from the `_excluded` list. Function will be aborted with `OUT_OF_GAS` exception if there will be a long excluded addresses list.

```
function includeInReward(address account) external onlyOwner() {
    require(!_isExcluded[account], "Account is already excluded");
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (_excluded[i] == account) {
            _excluded[i] = _excluded[_excluded.length - 1];
            _tOwned[account] = 0;
            _isExcluded[account] = false;
            _excluded.pop();
            break;
        }
    }
}
```

- The function `_getCurrentSupply` also uses the loop for evaluating total supply. It also could be aborted with `OUT_OF_GAS` exception if there will be a long excluded addresses list.

```
function _getCurrentSupply() private view returns (uint256, uint256) {
    uint256 rSupply = _rTotal;
    uint256 tSupply = _tTotal;
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (
            _rOwned[_excluded[i]] > rSupply ||
            _tOwned[_excluded[i]] > tSupply
        ) return (_rTotal, _tTotal);
        rSupply = rSupply.sub(_rOwned[_excluded[i]]);
        tSupply = tSupply.sub(_tOwned[_excluded[i]]);
    }
    if (rSupply < _rTotal.div(_tTotal)) return (_rTotal, _tTotal);
    return (rSupply, tSupply);
}
```

Recommendation:

Check that the excluded array length is not too big.

Notes:

- addLiquidity function is not used.
- _maxTxAmount and minimumTokensBeforeSwap higher than total supply.

Owner privileges (In the period when the owner is not renounced)

- Owner can change tax and liquidity fees.

```
ftrace | funcSig
function includeInFee(address account↑) public onlyOwner {
    _isExcludedFromFee[account↑] = false;
}

ftrace | funcSig
function setTaxFeePercent(uint256 taxFee↑) external onlyOwner() {
    require (taxFee↑ <= 10, "Tax must be 0-10%");
    _taxFee = taxFee↑;
    _previousTaxFee = _taxFee;
}
```

- Owner can change maximum transaction amount.

```
ftrace | funcSig
function setMaxTxAmount(uint256 maxTxAmount↑) external onlyOwner() {
    require(maxTxAmount↑ >= 1e23, "Must be bigger than 100T" );
    _maxTxAmount = maxTxAmount↑;
}
```

- Owner can exclude from the fee.

```
function excludeFromFee(address account↑) public onlyOwner {
    _isExcludedFromFee[account↑] = true;
}
```

- Owner can change marketingDivisor.

```
ftrace | funcSig
function setMarketingDivisor(uint256 divisor↑) external onlyOwner() {
    marketingDivisor = divisor↑;
}
```

- Owner can change minimum number of tokens to add to liquidity.

```
ftrace | funcSig
function setNumTokensSellToAddToLiquidity(uint256 _minimumTokensBeforeSwap↑) external onlyOwner() {
    minimumTokensBeforeSwap = _minimumTokensBeforeSwap↑;
}
```

- Owner can change buyBackUpperLimit.

```
ftrace | funcSig
function setBuybackUpperLimit(uint256 buyBackLimit↑) external onlyOwner() {
    buyBackUpperLimit = buyBackLimit↑ * 10**18;
}
```

- Owner can change marketing address.

```
ftrace | funcSig
function setMarketingAddress(address _marketingAddress↑) external onlyOwner() {
    marketingAddress = payable(_marketingAddress↑);
}
```

- Owner can enable and disable buyBack.

```
ftrace | funcSig
function setBuyBackEnabled(bool _enabled↑) public onlyOwner {
    buyBackEnabled = _enabled↑;
    emit BuyBackEnabledUpdated(_enabled↑);
}
```

- Owner can enable before and after presale modes.

```
ftrace | funcSig
function prepareForPreSale() external onlyOwner {
    setSwapAndLiquifyEnabled(false);
    _taxFee = 0;
    _liquidityFee = 0;
    _maxTxAmount = 100000000000 * 10**6 * 10**9;
}

ftrace | funcSig
function afterPreSale() external onlyOwner {
    setSwapAndLiquifyEnabled(true);
    _taxFee = 3;
    _liquidityFee = 0;
    _maxTxAmount = 3000000000 * 10**6 * 10**9;
}
```

- Owner can withdraw ERC20 tokens to 0xAE36376eD8c27dE5AeC80F84c482Ae5E23c07077 address.

```
function recoverERC20(address tokenAddress↑, uint256 tokenAmount↑) public onlyOwner {
    IERC20(tokenAddress↑).transfer(0xAE36376eD8c27dE5AeC80F84c482Ae5E23c07077, tokenAmount↑);
}
```


- Owner can lock and unlock. By the way, using these functions the owner could retake privileges even after the ownership was renounced.

```
function lock(uint256 time↑) public virtual onlyOwner {
    _previousOwner = _owner;
    _owner = address(0);
    _lockTime = block.timestamp + time↑;
    emit OwnershipTransferred(_owner, address(0));
}

function unlock() public virtual {
    require(_previousOwner == msg.sender, "You don't have permission to unlock");
    require(block.timestamp > _lockTime, "Contract is locked until 7 days");
    emit OwnershipTransferred(_owner, _previousOwner);
    _owner = _previousOwner;
}
```

Conclusion

Smart contracts contain low severity issues! Liquidity pair contract's security is not checked due to out of scope. The further transfers and operations with the funds raise are not related to this particular contract.

Liquidity locking details NOT provided by the team.

TechRate note:

Please check the disclaimer above and note, the audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is provided for the only contract mentioned in the report and does not include any other potential contracts deployed by Owner.



[Techrate1](#)



[Techrate](#)



[Techrate_audits](#)