



TechRate
AUDIT COMPANY

Smart Contract Security Audit

TechRate

November, 2021

Audit Details



Audited project

MandoX



Deployer address

0xc21f548c1eaacef1a64462d9714801bcd61e508a



Client contacts:

MandoX team



Blockchain

Ethereum



Project website:

www.MadMandosNFT.com

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 MandoX to perform an audit of smart contracts:

<https://etherscan.io/address/0xAFbF03181833aB4E8DEc24D708a2a24c2bAaa4a4#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 18.11.2021

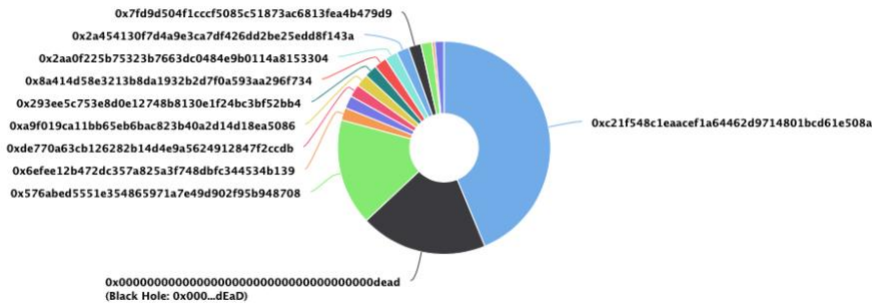
Contract name	MandoX
Contract address	0xAFbF03181833aB4E8DEc24D708a2a24c2bAaa4a4
Total supply	50,000,000,000,000,000
Token ticker	MANDOX
Decimals	9
Token holders	14
Transactions count	15
Top 100 holders dominance	98.61%
Contract deployer address	0xc21f548c1eaacef1a64462d9714801bcd61e508a
Contract's current owner address	0xc21f548c1eaacef1a64462d9714801bcd61e508a

MandoX Token Distribution

The top 100 holders collectively own 98.61% (49,304,844,588,733,400.00 Tokens) of MandoX


Token Total Supply: 50,000,000,000,000.00 Token | Total Token Holders: 14

MandoX Top 100 Token Holders
Source: Etherscan.io



(A total of 49,304,844,588,733,400.00 tokens held by the top 100 accounts from the total supply of 50,000,000,000,000.00 token)

MandoX Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	0xc21f548c1eaacef1a64462d9714801bcd61e508a	21,876,845,071,454,600.639850744	43.7537%
2	Black Hole: 0x000...dEaD	9,638,554,216,867,470.879518072	19.2771%
3	 0x576abed5551e354865971a7e49d902f95b948708	8,098,435,037,029,530.310433989	16.1969%
4	0x6efee12b472dc357a825a3f748dbfc344534b139	960,768,461,045,882.939009937	1.9215%
5	0xc0fec0cb111af730ab71ae17adc89174fa25f7dd	960,384,153,661,464.585834333	1.9208%
6	0xde770a63cb126282b14d4e9a5624912847f2ccdb	960,384,153,661,464.585834333	1.9208%
7	0xa9f019ca11bb65eb6bac823b40a2d14d18ea5086	960,384,153,661,464.585834333	1.9208%
8	0x293ee5c753e8d0e12748b8130e1f24bc3bf52bb4	960,384,153,661,464.585834333	1.9208%
9	0x8a414d58e3213b8da1932b2d7f0a593aa296f734	960,384,153,661,464.585834333	1.9208%
10	0x2aa0f225b75323b7663dc0484e9b0114a8153304	960,384,153,661,464.585834333	1.9208%

Contract functions details

- + Context
 - [Int] _msgSender
- + [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
- + Ownable (Context)
 - [Pub] <Constructor> #
 - [Pub] owner
 - [Pub] renounceOwnership #
 - modifiers: onlyOwner
- + [Int] IUniswapV2Factory
 - [Ext] createPair #
- + [Int] IUniswapV2Router02
 - [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #
 - [Ext] factory
 - [Ext] WETH
 - [Ext] addLiquidityETH (\$)
- + MandoX (Context, IERC20, Ownable)
 - [Pub] <Constructor> #
 - [Pub] name
 - [Pub] symbol
 - [Pub] decimals
 - [Pub] totalSupply
 - [Pub] balanceOf
 - [Pub] transfer #
 - [Pub] allowance
 - [Pub] approve #
 - [Pub] transferFrom #
 - [Ext] setCooldownEnabled #
 - modifiers: onlyOwner
 - [Prv] tokenFromReflection
 - [Prv] _approve #
 - [Prv] _transfer #
 - [Prv] swapTokensForEth #

- modifiers: lockTheSwap
- [Prv] sendETHToFee #
- [Ext] openTrading #
 - modifiers: onlyOwner
- [Pub] setBots #
 - modifiers: onlyOwner
- [Pub] delBot #
 - modifiers: onlyOwner
- [Prv] _tokenTransfer #
- [Prv] _transferStandard #
- [Prv] _takeTeam #
- [Prv] _reflectFee #
- [Ext] <Fallback> (\$)
- [Ext] manualswap #
- [Ext] manualsend #
- [Prv] _getValues
- [Prv] _getTValues
- [Prv] _getRValues
- [Prv] _getRate
- [Prv] _getCurrentSupply

(\$)= 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.	Passed
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

No low severity issues found.

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

- Owner can enable cooldown (user to user trading with time offset).

```
function setCooldownEnabled(bool onoff) external onlyOwner() {
    cooldownEnabled = onoff;
}
```

- Owner can open swap trading.

```
function openTrading() external onlyOwner() {
    require(!tradingOpen, "trading is already open");
    IUniswapV2Router02 _uniswapV2Router = IUniswapV2Router02(0x7a250d5630B4cF539739dF2C5dAcb4c659F2488D);
    _uniswapV2Router = _uniswapV2Router;
    _approve(address(this), address(_uniswapV2Router), _tTotal);
    _uniswapV2Pair = IUniswapV2Factory(_uniswapV2Router.factory()).createPair(address(this), _uniswapV2Router.WETH());
    _uniswapV2Router.addLiquidityETH(value: address(this).balance)(address(this), balanceOf(address(this)), 0, 0, owner(), block.timestamp);
    swapEnabled = true;
    cooldownEnabled = true;
    _maxTxAmount = 500000000000000 * 10**9;
    tradingOpen = true;
    IERC20(_uniswapV2Pair).approve(address(_uniswapV2Router), type(uint).max);
}
```

- Owner can add and remove bots (no transferring between this addresses).

```
function setBots(address[] memory bots_) public onlyOwner {
    for (uint i = 0; i < bots_.length; i++) {
        bots[bots_[i]] = true;
    }
}

function delBot(address notbot) public onlyOwner {
    bots[notbot] = false;
}
```

Conclusion

Smart contracts do not contain high severity issues! Liquidity pair contract's security is not checked due to out of scope.

Liquidity locking details are 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](#)