

expelee

Building the Futuristic Blockchain Ecosystem

SECURITY AUDIT REPORT



TALKING TOM CEO

TABLE OF CONTENTS

02	Table of Contents	—
03	Overview	—
04	Project Description	—
05	Social Media Profiles	—
06	Contract Details	—
07	Owner Privileges	—
08	Audit Methodology	—
09	Vulnerabilities Checklist	—
10	Risk Classification	—
11	Inheritance Trees & Risk Overview	—
12	Function Details	—
17	Test Net versions	—
19	Manual Review	—
20	Findings	—
23	About Expelee	—
24	Disclaimer	—

OVERVIEW

The Expelee team has performed a line-by-line manual analysis and automated review of the smart contract. The smart contract was analysed mainly for common smart contract vulnerabilities, exploits, and manipulation hacks. According to the smart contract audit:

Audit Result	Passed
KYC Verification	Done
Audit Date	19 May 2023

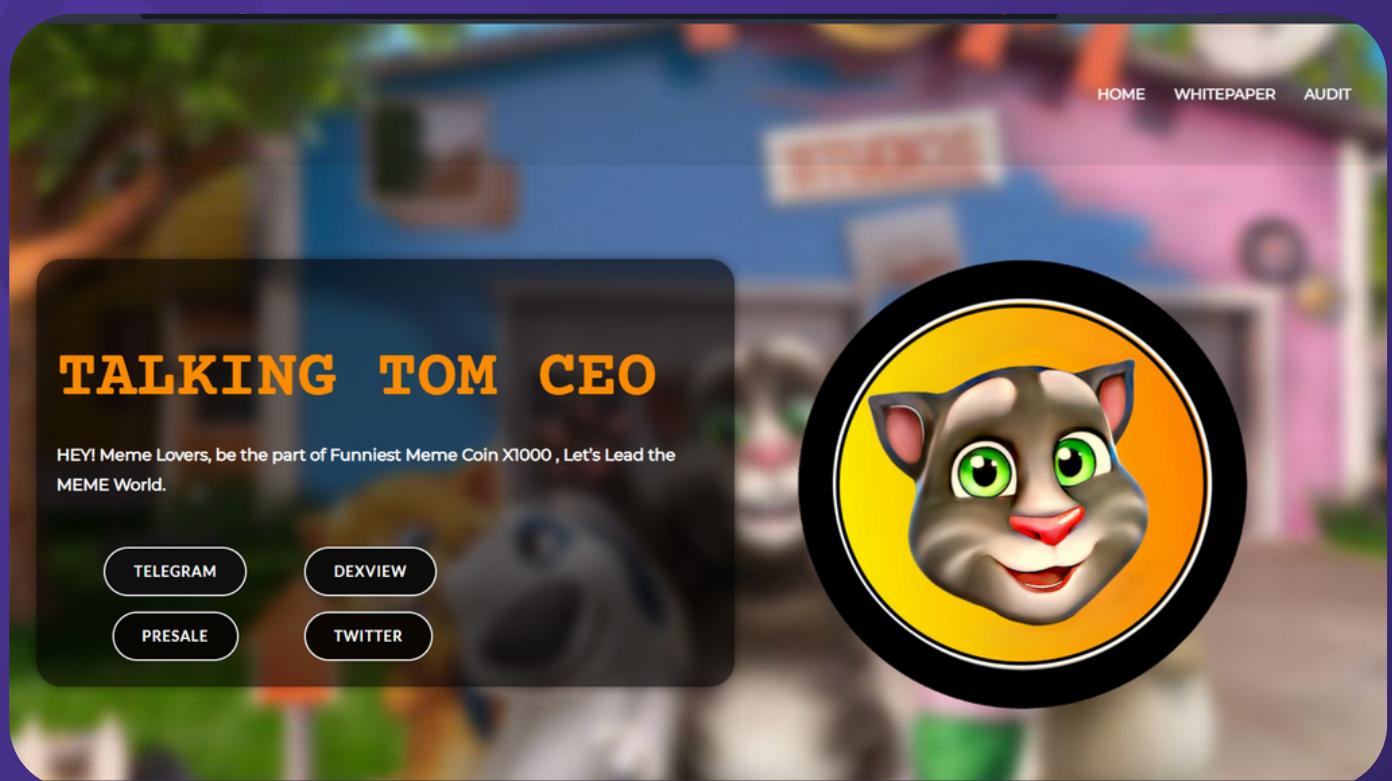
PROJECT DESCRIPTION

TALKING TOM CEO is one of the funniest Cat CEO entered to the MEME World to make meme revolution, holders of TOMCEO will receive BUSD as reward



SOCIAL MEDIA PROFILES

TALKING TOM CEO



<https://t.me/TalkingTomCEO>



<https://twitter.com/talkingtomceo>



<https://tomceo.org/>

It's always good to check the social profiles of the project, before making your investment.

CONTRACT DETAILS

Token Name: TALKING TOM CEO

Symbol: TOMCEO

Network: Binance Smart Chain

Language: Solidity

Contract Address:

0xd205A31da8406162441523bBaA0e13c5EEE812C4

Total Supply: 1,000,000,000

Contract SHA-256 Checksum: -

e5cbcef14ab2f162a4ae3d0ad1cb7c580266ad56

Owner's Wallet:

0xD0c50CE78F4914F058272b6A86AC28323268D0A4

Deployer's Wallet:

0x428f2FF548Ce83c0c9ee7d1463775a4970014d57

Testnet:

<https://testnet.bscscan.com/token/0x4229b7d4fbec12e93399fc7de07ffe64ab806b83>

OWNER PRIVILEGES

- Contract owner can set marketing wallet address
- Sum of all fees can not exceed 25% (buy + sell + fee <= 25%)
- Contract owner can toggle swapping on and off
- Contract owner can whitelist or unwhitelist wallets
- Contract owner can not mint new tokens
- Contract owner can not disable trades
- Contract owner can not blacklist wallets
- Contract gives BUSD as rewards to investors

AUDIT METHODOLOGY

Audit Details

Our comprehensive audit report provides a full overview of the audited system's architecture, smart contract codebase, and details on any vulnerabilities found within the system.

Audit Goals

The audit goal is to ensure that the project is built to protect investors and users, preventing potentially catastrophic vulnerabilities after launch, that lead to scams and rugpulls.

Code Quality

Our analysis includes both automatic tests and manual code analysis for the following aspects:

- Exploits
- Back-doors
- Vulnerability
- Accuracy
- Readability

Tools

- DE
- Open Zeppelin
- Code Analyzer
- Solidity Code
- Compiler
- Hardhat

VULNERABILITY CHECKS

Design Logic	Passed
Compiler warnings	Passed
Private user data leaks	Passed
Timestamps dependence	Passed
Integer overflow and underflow	Passed
Race conditions & reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front Running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed

RISK CLASSIFICATION

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

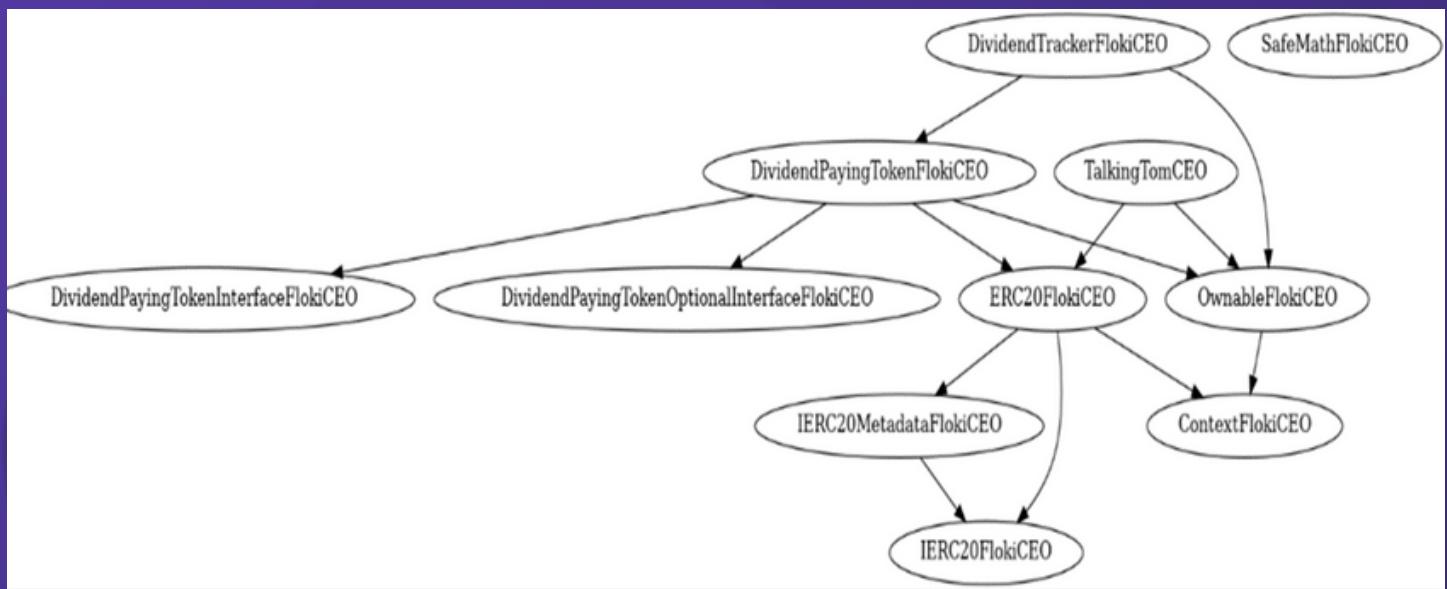
Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Issues on this level are minor details and warning that can remain unfixed.

INHERITANCE TREES



FUNCTION DETAILS

Contract	Type	Bases			
L	**Function Name**	**Visibility**	**Mutability**	**Modifiers**	
ContextFlokiCEO Implementation					
L	_msgSender	Internal			
L	_msgData	Internal			
OwnableFlokiCEO Implementation ContextFlokiCEO					
L	<Constructor>	Public	!		NO !
L	owner	Public	!		NO !
L	renounceOwnership	Public	!		onlyOwner
L	transferOwnership	Public	!		onlyOwner
L	_transferOwnership	Internal			
SafeMathFlokiCEO Library					
L	add	Internal			
L	sub	Internal			
L	sub	Internal			
L	mul	Internal			
L	div	Internal			
L	div	Internal			
L	mod	Internal			
L	mod	Internal			
SafeMathIntFlokiCEO Library					
L	mul	Internal			
L	div	Internal			
L	sub	Internal			
L	add	Internal			
L	abs	Internal			
L	toUint256Safe	Internal			
SafeMathUintFlokiCEO Library					
L	toInt256Safe	Internal			
IterableMappingFlokiCEO Library					
L	get	Internal			
L	getIndexOfKey	Internal			
L	getKeyAtIndex	Internal			
L	size	Internal			
L	set	Internal			
L	remove	Internal			
IUniswapV2FactoryFlokiCEO Interface					
L	feeTo	External	!		NO !
L	feeToSetter	External	!		NO !

FUNCTION DETAILS

```

| L | getPair | External ! | NO ! | |
| L | allPairs | External ! | NO ! |
| L | allPairsLength | External ! | NO ! |
| L | createPair | External ! | ● | NO ! |
| L | setFeeTo | External ! | ● | NO ! |
| L | setFeeToSetter | External ! | ● | NO ! |
|||||
| **IUniswapV2PairFlokiCEO** | Interface | ||
| L | name | External ! | NO ! |
| L | symbol | External ! | NO ! |
| L | decimals | External ! | NO ! |
| L | totalSupply | External ! | NO ! |
| L | balanceOf | External ! | NO ! |
| L | allowance | External ! | NO ! |
| L | approve | External ! | ● | NO ! |
| L | transfer | External ! | ● | NO ! |
| L | transferFrom | External ! | ● | NO ! |
| L | DOMAIN_SEPARATOR | External ! | NO ! |
| L | PERMIT_TYPEHASH | External ! | NO ! |
| L | nonces | External ! | NO ! |
| L | permit | External ! | ● | NO ! |
| L | MINIMUM_LIQUIDITY | External ! | NO ! |
| L | factory | External ! | NO ! |
| L | token0 | External ! | NO ! |
| L | token1 | External ! | NO ! |
| L | getReserves | External ! | NO ! |
| L | price0CumulativeLast | External ! | NO ! |
| L | price1CumulativeLast | External ! | NO ! |
| L | kLast | External ! | NO ! |
| L | mint | External ! | ● | NO ! |
| L | burn | External ! | ● | NO ! |
| L | swap | External ! | ● | NO ! |
| L | skim | External ! | ● | NO ! |
| L | sync | External ! | ● | NO ! |
| L | initialize | External ! | ● | NO ! |
|||||
| **IUniswapV2Router01FlokiCEO** | Interface | ||
| L | factory | External ! | NO ! |
| L | WETH | External ! | NO ! |
| L | addLiquidity | External ! | ● | NO ! |
| L | addLiquidityETH | External ! | ● | NO ! |
| L | removeLiquidity | External ! | ● | NO ! |
| L | removeLiquidityETH | External ! | ● | NO ! |
| L | removeLiquidityWithPermit | External ! | ● | NO ! |
| L | removeLiquidityETHWithPermit | External ! | ● | NO ! |
| L | swapExactTokensForTokens | External ! | ● | NO ! |

```

FUNCTION DETAILS

```

| L | swapTokensForExactTokens | External ! | ● | NO ! |
| L | swapExactETHForTokens | External ! | ■ | NO ! |
| L | swapTokensForExactETH | External ! | ● | NO ! |
| L | swapExactTokensForETH | External ! | ● | NO ! |
| L | swapETHForExactTokens | External ! | ■ | NO ! |
| L | quote | External ! | | NO ! |
| L | getAmountOut | External ! | | NO ! |
| L | getAmountIn | External ! | | NO ! |
| L | getAmountsOut | External ! | | NO ! |
| L | getAmountsIn | External ! | | NO ! |
|||||
| **IUniswapV2Router02FlokiCEO** | Interface | IUniswapV2Router01FlokiCEO ||
| L | removeLiquidityETHSupportingFeeOnTransferTokens | External ! | ● | NO ! |
| L | removeLiquidityETHWithPermitSupportingFeeOnTransferTokens | External ! | ● | NO ! |
| L | swapExactTokensForTokensSupportingFeeOnTransferTokens | External ! | ● | NO ! |
| L | swapExactETHForTokensSupportingFeeOnTransferTokens | External ! | ■ | NO ! |
| L | swapExactTokensForETHSupportingFeeOnTransferTokens | External ! | ● | NO ! |
|||||
| **IERC20FlokiCEO** | Interface | ||
| L | totalSupply | External ! | | NO ! |
| L | balanceOf | External ! | | NO ! |
| L | allowance | External ! | | NO ! |
| L | transfer | External ! | ● | NO ! |
| L | approve | External ! | ● | NO ! |
| L | transferFrom | External ! | ● | NO ! |
|||||
| **IERC20MetadataFlokiCEO** | Interface | IERC20FlokiCEO ||
| L | name | External ! | | NO ! |
| L | symbol | External ! | | NO ! |
| L | decimals | External ! | | NO ! |
|||||
| **ERC20FlokiCEO** | Implementation | ContextFlokiCEO, IERC20FlokiCEO,
IERC20MetadataFlokiCEO ||
| L | <Constructor> | Public ! | ● | NO ! |
| L | name | Public ! | | NO ! |
| L | symbol | Public ! | | NO ! |
| L | decimals | Public ! | | NO ! |
| L | totalSupply | Public ! | | NO ! |
| L | balanceOf | Public ! | | NO ! |
| L | transfer | Public ! | ● | NO ! |
| L | allowance | Public ! | | NO ! |
| L | approve | Public ! | ● | NO ! |
| L | transferFrom | Public ! | ● | NO ! |
| L | increaseAllowance | Public ! | ● | NO ! |
| L | decreaseAllowance | Public ! | ● | NO !

```

FUNCTION DETAILS

```

| L | _transfer | Internal 🔒 | ● ||

| L | _mint | Internal 🔒 | ● ||

| L | _burn | Internal 🔒 | ● ||

| L | _approve | Internal 🔒 | ● ||

| L | _beforeTokenTransfer | Internal 🔒 | ● ||

||||||

| **DividendPayingTokenInterfaceFlokiCEO** | Interface | ||

| L | dividendOf | External ! | |NO ! |

| L | withdrawDividend | External ! | ● |NO ! |

||||||

| **DividendPayingTokenOptionalInterfaceFlokiCEO** | Interface | ||

| L | withdrawableDividendOf | External ! | |NO ! |

| L | withdrawnDividendOf | External ! | |NO ! |

| L | accumulativeDividendOf | External ! | |NO ! |

||||||

| **DividendPayingTokenFlokiCEO** | Implementation | ERC20FlokiCEO, OwnableFlokiCEO,
DividendPayingTokenInterfaceFlokiCEO, DividendPayingTokenOptionalInterfaceFlokiCEO ||

| L | <Constructor> | Public ! | ● | ERC20FlokiCEO |

| L | distributeDividends | Public ! | ● | onlyOwner |

| L | withdrawDividend | Public ! | ● |NO ! |

| L | _withdrawDividendOfUser | Internal 🔒 | ● ||

| L | dividendOf | Public ! | |NO ! |

| L | withdrawableDividendOf | Public ! | |NO ! |

| L | withdrawnDividendOf | Public ! | |NO ! |

| L | accumulativeDividendOf | Public ! | |NO ! |

| L | _transfer | Internal 🔒 | ● ||

| L | _mint | Internal 🔒 | ● ||

| L | _burn | Internal 🔒 | ● ||

| L | _setBalance | Internal 🔒 | ● ||

||||||

| **DividendTrackerFlokiCEO** | Implementation | OwnableFlokiCEO,
DividendPayingTokenFlokiCEO ||

| L | <Constructor> | Public ! | ● | DividendPayingTokenFlokiCEO |

| L | _transfer | Internal 🔒 | ||

| L | withdrawDividend | Public ! | |NO ! |

| L | updateMinimumTokenBalanceForDividends | External ! | ● | onlyOwner |

| L | excludeFromDividends | External ! | ● | onlyOwner |

| L | updateClaimWait | External ! | ● | onlyOwner |

| L | setLastProcessedIndex | External ! | ● | onlyOwner |

| L | getLastProcessedIndex | External ! | |NO ! |

| L | getNumberOfTokenHolders | External ! | |NO ! |

| L | getAccount | Public ! | |NO ! |

| L | getAccountAtIndex | Public ! | |NO ! |

| L | canAutoClaim | Private 🔒 | ||

| L | setBalance | External ! | ● | onlyOwner |

| L | process | Public ! | ● |NO ! |

```

FUNCTION DETAILS

```

| L | processAccount | Public ! | ● | onlyOwner |
|||||
| **TalkingTomCEO** | Implementation | ERC20FlokiCEO, OwnableFlokiCEO ||
| L | <Constructor> | Public ! | ฿ | ERC20FlokiCEO |
| L | <Receive Ether> | External ! | ฿ | NO !
| L | claimStuckTokens | External ! | ● | onlyOwner | |
| L | isContract | Internal 🔒 | |||
| L | sendBNB | Internal 🔒 | ● | |
| L | _setAutomatedMarketMakerPair | Private 🔒 | ● | |
| L | excludeFromFees | External ! | ● | onlyOwner |
| L | isExcludedFromFees | Public ! | |NO ! |
| L | updateFees | External ! | ● | onlyOwner |
| L | changeMarketingWallet | External ! | ● | onlyOwner |
| L | _transfer | Internal 🔒 | ● | |
| L | swapAndSendDividends | Private 🔒 | ● | |
| L | setMinimumTokenLeft | Public ! | ● | onlyOwner |
| L | setSwapTokensAtAmount | External ! | ● | onlyOwner |
| L | updateGasForProcessing | Public ! | ● | onlyOwner |
| L | updateMinimumBalanceForDividends | External ! | ● | onlyOwner |
| L | updateClaimWait | External ! | ● | onlyOwner |
| L | getClaimWait | External ! | |NO ! |
| L | getTotalDividendsDistributed | External ! | |NO ! |
| L | withdrawableDividendOf | Public ! | |NO ! |
| L | dividendTokenBalanceOf | Public ! | |NO ! |
| L | totalRewardsEarned | Public ! | |NO ! |
| L | excludeFromDividends | External ! | ● | onlyOwner |
| L | getAccountDividendsInfo | External ! | |NO ! |
| L | getAccountDividendsInfoAtIndex | External ! | |NO ! |
| L | processDividendTracker | External ! | ● | |NO ! |
| L | claim | External ! | ● | |NO ! |
| L | claimAddress | External ! | ● | onlyOwner |
| L | getLastProcessedIndex | External ! | |NO ! |
| L | setLastProcessedIndex | External ! | ● | onlyOwner |
| L | getNumberOfDividendTokenHolders | External ! | |NO ! |
| L | setAntisniperLimit | External ! | ● | onlyOwner |

```

Legend

Symbol	Meaning
-----	-----
●	Function can modify state
฿	Function is payable

TEST VERSION

Adding Liquidity ✓

Tx:

<https://testnet.bscscan.com/tx/0xd3c6a0b6549f3cf27feefe228ea98515c39c9d0eba89beed650a7184efd29b52>

Buying from a fee excluded wallet ✓

Tx (0% tax):

<https://testnet.bscscan.com/tx/0x386a177d52605c589cfb04b912508c7388e244c2cfb14120da6c2efdd7e50556>

Selling from a fee excluded wallet ✓

Tx (0% tax):

<https://testnet.bscscan.com/tx/0x66b73d33dd83a331122b710373727b69e50041b9441ecf4ce08eea0de95cd909>

Transferring using a fee excluded wallet ✓

Tx (0% tax):

<https://testnet.bscscan.com/tx/0x64e061cacc06b09552235f97dea0cc813909c10d20d242db2fc848d6aa5f0564>

Buying from a regular wallet ✓

Tx (0-25% tax):

<https://testnet.bscscan.com/tx/0xf5f6d44c87d26f9feab45f5f20f91771af6932af12ba52a6143a2ee666000f2b>

Selling from a regular wallet ✓

Tx (0-25% tax):

<https://testnet.bscscan.com/tx/0xa3fae0cf487b78c762dd00c0944712317c2151062b78f3ac90c0819020b32766>

TEST VERSION

Transferring a regular wallet ✓

Tx (0-25%):

<https://testnet.bscscan.com/tx/0x028d4ca58a6c78a3e4ec988d96869f25801e668861559ce9147ca5b8ef05cc50>

Internal swap (marketing bnb + rewards distribution) ✓

Tx:

<https://testnet.bscscan.com/tx/0xa3fae0cf487b78c762dd00c0944712317c2151062b78f3ac90c0819020b32766>

MANUAL REVIEW

Severity Criteria

Expelee assesses the severity of disclosed vulnerabilities according to methodology based on OWASP standarts.

Vulnerabilities are divided into three primary risk categories:

High

Medium

Low

High-level considerations for vulnerabilities span the following key areas when conducting assessments:

- Malicious input handling
- Escalation of privileges
- Arithmetic
- Gas use

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
Likelihood				

FINDINGS

Findings	Severity	Found
High Risk	● High	1
Medium Risk	● Medium	0
Low Risk	● Low	1
Suggestion & discussion	● Informational	0
Gas Optimizations	● Gas Opt.	0

HIGH RISK FINDING

Setting minimum amount

Severity : High

Overview

if minimumTokenLeft is set to 0.1% of total supply, any transfer/buy/sell bigger than this amount will be reverted due to an underflow error.

```
function setMinimumTokenLeft(uint256 amount) public onlyOwner {
    require(amount != minimumTokenLeft, "Minimum token left is that value");
    require(
        amount <= ((totalSupply() * 1) / 1000),
        "Maximum token left is 0.1%"
    );
    minimumTokenLeft = amount;
    emit UpdateMinimumTokenLeft(amount);
}

if (
    !swapping &&
    !automatedMarketMakerPairs[from] &&
    (minimumTokenLeft > 0) &&
    !_isExcludedFromFees[from] &&
    (balanceOf(from) - amount < minimumTokenLeft)
) {
    super._transfer(from, to, (amount - minimumTokenLeft));
```

LOW RISK FINDING

Centralized control over swap threshold

Severity : Low

Overview

The contract owner is able to set swap thersholt to an arbitrary number more than 0.001% of supply.

A high swap threshold can increase slippage on trades

```
function setSwapTokensAtAmount(uint256 newAmount) external
onlyOwner {
    require(
        newAmount > totalSupply() / 100_000,
        "SwapTokensAtAmount must be greater than 0.001% of total supply"
    );
    swapTokensAtAmount = newAmount;
}
```

Suggestion:

|Ensure that swap threshold is less than a reasonable amount (1% of supply is suggested value)

ABOUT EXPELEE

Expelee is a product-based aspirational Web3 start-up. Coping up with numerous solutions for blockchain security and constructing a Web3 ecosystem from deal making platform to developer hosting open platform, while also developing our own commercial and sustainable blockchain.



www.expelee.com



[expeleeofficial](#)



[Expelee](#)



[expelee_official](#)



[expelee](#)



[expelee](#)



[expelee-co](#)

expelee

Building the Futuristic **Blockchain Ecosystem**

DISCLAIMER

All the content provided in this document is for general information only and should not be used as financial advice or a reason to buy any investment. Team provides no guarantees against the sale of team tokens or the removal of liquidity by the project audited in this document.

Always do your own research and protect yourselves from being scammed. The Expelee team has audited this project for general information and only expresses their opinion based on similar projects and checks from popular diagnostic tools.

Under no circumstances did Expelee receive a payment to manipulate those results or change the awarding badge that we will be adding in our website. Always do your own research and protect yourselves from scams.

This document should not be presented as a reason to buy or not buy any particular token. The Expelee team disclaims any liability for the resulting losses.

The logo consists of the word "expelee" in a lowercase, sans-serif font. The letter "e" is white, while the rest of the letters are orange. The "e" is slightly taller than the others and has a small upward-pointing arrow above its top-left corner.

Building the Futuristic **Blockchain Ecosystem**