expelee

Building the Futuristic Blockchain Ecosystem

SECURITY AUDIT REPORT

YEE

expelee

TOKEN OVERVIEW

Risk Findings

Severity	Found
High	3
Medium	1
Low	0
Informational	0

Centralization Risks

Owner Privileges	Description
Can Owner Set Taxes >25% ?	Not Detected
Owner needs to enable trading ?	Not Detected
Can Owner Disable Trades ?	Detected
Can Owner Mint ?	Not Detected
Can Owner Blacklist ?	Not Detected
Can Owner set Max Wallet amount ?	Detected
Can Owner Set Max TX amount ?	Not Detected

HIGH RISK FINDING

Maximum buy/sell/transfer

Category: Centralization
Status: Open
Impact: High

Overview:
Owner is able to set maximum amount of buy/sell/transfer to zero.

```
function setMaxTxAmount(uint256 maxTxAmount) external onlyOwner {
  require(
    maxTxAmount <= (40 * 10 ** 6 * 10 ** 9),
    "Max wallet should be less or equal to 4% totalSupply"
  );
  _maxTxAmount = maxTxAmount;
}
```

Suggestion:
Put a lower bound for maximum amount of buy/sell/transfes.

```
function setMaxTxAmount(uint256 maxTxAmount) external onlyOwner {
  require(
    maxTxAmount >= totalSupply() / 1000,
    "Maximum Tx must be greater than 0.1% of total supply"
  );
  _maxTxAmount = maxTxAmount;
}
```

HIGH RISK FINDING

Updating router

Category: Centralization / Logical
Status: Open
Impact: High

Overview:
Contract owner is able to update dex router which is used by contract to perform internal swap.
Updating router to a malicious contract causes internal swaps to revert the transaction.

```
function changeRouterVersion(
  address newRouterAddress
) public onlyOwner returns (address newPairAddress) {
  IUniswapV2Router02 _uniswapV2Router = IUniswapV2Router02(
    newRouterAddress
  );
  newPairAddress = IUniswapV2Factory(_uniswapV2Router.factory()).getPair(
    address(this),
    _uniswapV2Router.WETH()
  );
  if (newPairAddress == address(0)) {
    newPairAddress = IUniswapV2Factory(_uniswapV2Router.factory())
      .createPair(address(this), _uniswapV2Router.WETH());
  }
  uniswapPair = newPairAddress;
  uniswapV2Router = _uniswapV2Router;
  isWalletLimitExempt[address(uniswapPair)] = true;
  isMarketPair[address(uniswapPair)] = true;
}
```

Suggestion:
Ensure that router address is immutable after deploying the contract and adding liquidity.

HIGH RISK FINDING

setting swap threshold to zero

Category: Logical
Status: Open
Impact: High

Overview:
Setting minimumTokensBeforeSwap to zero and enabling swapAndLiquifyByLimitOnly causes internal swaps to be reverted in an attempt for swapping 0 tokens to ETH.

```
function setNumTokensBeforeSwap(uint256 newLimit) external onlyOwner {
  minimumTokensBeforeSwap = newLimit;
}

function setSwapAndLiquifyByLimitOnly(bool newValue) public onlyOwner {
  swapAndLiquifyByLimitOnly = newValue;
}
```

Suggestion:
Ensure that minimumTokensBeforeSwap is always greater than 1 tokens.

```
function setNumTokensBeforeSwap(uint256 newLimit) external onlyOwner {
require(newLimit <= 10 ** decimals(), “swap threshold must be greater than 1 token’);
  minimumTokensBeforeSwap = newLimit;
}
```

expelee

TABLE OF CONTENTS

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 with high risk**
KYC Verification	**-**
Audit Date	**4 August 2023**

expelee

CONTRACT DETAILS

Token Name: Yeecoin

Symbol: YEE

Network: Ethereum mainnet

Language: Solidity

Contract Address:
0x009764D7Ab6BeFf7Cc8E61437c0879420E8E3f3B

Total Supply: 420,690,000,000,000

Owner's Wallet:
0x1c7919E6796f015ce216F46c5dEC62F813c90e1D

Deployer's Wallet:
0x3be96b568729B94cE91116bB9d53850316F21371

Testnet.
https://testnet.bscscan.com/token/0x2B17C5727d31454878
0156342547Ad7Cb5121c07

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 Zepplin module	Passed

RISK CLASSIFICATION

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and acces 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.

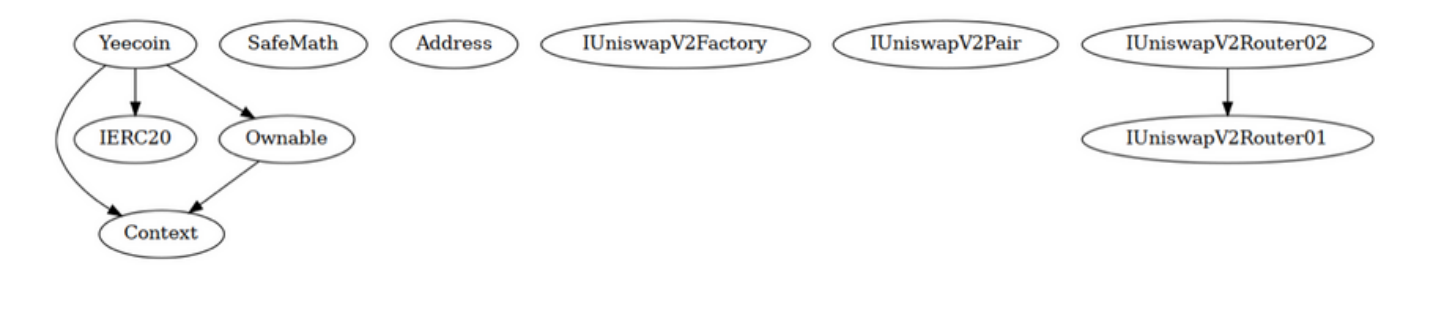
Low Risk

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		
	└	**Function Name**	**Visibility**	**Mutability**	**Modifiers**
Context	Implementation			
	└	_msgSender	Internal 🔒		
	└	_msgData	Internal 🔒		
IERC20	Interface			
	└	totalSupply	External ❗		NO ❗
	└	balanceOf	External ❗		NO ❗
	└	transfer	External ❗	🛑	NO ❗
	└	allowance	External ❗		NO ❗
	└	approve	External ❗	🛑	NO ❗
	└	transferFrom	External ❗	🛑	NO ❗
SafeMath	Library			
	└	add	Internal 🔒		
	└	sub	Internal 🔒		
	└	sub	Internal 🔒		
	└	mul	Internal 🔒		
	└	div	Internal 🔒		
	└	div	Internal 🔒		
	└	mod	Internal 🔒		
	└	mod	Internal 🔒		
Address	Library			
	└	isContract	Internal 🔒		
	└	sendValue	Internal 🔒	🛑	
	└	functionCall	Internal 🔒	🛑	
	└	functionCall	Internal 🔒	🛑	
	└	functionCallWithValue	Internal 🔒	🛑	
	└	functionCallWithValue	Internal 🔒	🛑	
	└	_functionCallWithValue	Private 🔐	🛑	
Ownable	Implementation	Context		
	└	<Constructor>	Public ❗	🛑	NO ❗
	└	owner	Public ❗		NO ❗
	└	waiveOwnership	Public ❗	🛑	onlyOwner

FUNCTION DETAILS

└	transferOwnership	Public ❗	🛑	onlyOwner
IUniswapV2Factory	Interface			
└	feeTo	External ❗		NO❗
└	feeToSetter	External ❗		NO❗
└	getPair	External ❗		NO❗
└	allPairs	External ❗		NO❗
└	allPairsLength	External ❗		NO❗
└	createPair	External ❗	🛑	NO❗
└	setFeeTo	External ❗	🛑	NO❗
└	setFeeToSetter	External ❗	🛑	NO❗
IUniswapV2Pair	Interface			
└	name	External ❗		NO❗
└	symbol	External ❗		NO❗
└	decimals	External ❗		NO❗
└	totalSupply	External ❗		NO❗
└	balanceOf	External ❗		NO❗
└	allowance	External ❗		NO❗
└	approve	External ❗	🛑	NO❗
└	transfer	External ❗	🛑	NO❗
└	transferFrom	External ❗	🛑	NO❗
└	DOMAIN_SEPARATOR	External ❗		NO❗
└	PERMIT_TYPEHASH	External ❗		NO❗
└	nonces	External ❗		NO❗
└	permit	External ❗	🛑	NO❗
└	MINIMUM_LIQUIDITY	External ❗		NO❗
└	factory	External ❗		NO❗
└	token0	External ❗		NO❗
└	token1	External ❗		NO❗
└	getReserves	External ❗		NO❗
└	price0CumulativeLast	External ❗		NO❗
└	price1CumulativeLast	External ❗		NO❗
└	kLast	External ❗		NO❗
└	burn	External ❗	🛑	NO❗
└	swap	External ❗	🛑	NO❗

FUNCTION DETAILS

└	skim	External ❗	🛑	NO❗
└	sync	External ❗	🛑	NO❗
└	initialize	External ❗	🛑	NO❗
IUniswapV2Router01	Interface			
└	factory	External ❗		NO❗
└	WETH	External ❗		NO❗
└	addLiquidity	External ❗	🛑	NO❗
└	addLiquidityETH	External ❗	💵	NO❗
└	removeLiquidity	External ❗	🛑	NO❗
└	removeLiquidityETH	External ❗	🛑	NO❗
└	removeLiquidityWithPermit	External ❗	🛑	NO❗
└	removeLiquidityETHWithPermit	External ❗	🛑	NO❗
└	swapExactTokensForTokens	External ❗	🛑	NO❗
└	swapTokensForExactTokens	External ❗	🛑	NO❗
└	swapExactETHForTokens	External ❗	💵	NO❗
└	swapTokensForExactETH	External ❗	🛑	NO❗
└	swapExactTokensForETH	External ❗	🛑	NO❗
└	swapETHForExactTokens	External ❗	💵	NO❗
└	quote	External ❗		NO❗
└	getAmountOut	External ❗		NO❗
└	getAmountIn	External ❗		NO❗
└	getAmountsOut	External ❗		NO❗
└	getAmountsIn	External ❗		NO❗
IUniswapV2Router02	Interface	IUniswapV2Router01		
└	removeLiquidityETHSupportingFeeOnTransferTokens	External ❗	🛑	NO❗
└	removeLiquidityETHWithPermitSupportingFeeOnTransferTokens	External ❗	🛑	NO❗
└	swapExactTokensForTokensSupportingFeeOnTransferTokens	External ❗	🛑	NO❗
└	swapExactETHForTokensSupportingFeeOnTransferTokens	External ❗	💵	NO❗
└	swapExactTokensForETHSupportingFeeOnTransferTokens	External ❗	🛑	NO❗
Yeecoin	Implementation	Context, IERC20, Ownable		
└	<Constructor>	Public ❗	🛑	NO❗
└	name	Public ❗		NO❗
└	symbol	Public ❗		NO❗

FUNCTION DETAILS

└	decimals	Public ❗		NO ❗
└	totalSupply	Public ❗		NO ❗
└	balanceOf	Public ❗		NO ❗
└	allowance	Public ❗		NO ❗
└	increaseAllowance	Public ❗	🛑	NO ❗
└	decreaseAllowance	Public ❗	🛑	NO ❗
└	approve	Public ❗	🛑	NO ❗
└	_approve	Private 🔐	🛑		
└	addMarketPair	Public ❗	🛑	onlyOwner
└	setIsTxLimitExempt	External ❗	🛑	onlyOwner
└	setIsExcludedFromFee	Public ❗	🛑	onlyOwner
└	setMaxTxAmount	External ❗	🛑	onlyOwner
└	setIsWalletLimitExempt	External ❗	🛑	onlyOwner
└	setNumTokensBeforeSwap	External ❗	🛑	onlyOwner
└	setSwapAndLiquifyEnabled	Public ❗	🛑	onlyOwner
└	setSwapAndLiquifyByLimitOnly	Public ❗	🛑	onlyOwner
└	getCirculatingSupply	Public ❗		NO ❗
└	transferToAddressETH	Private 🔐	🛑		
└	changeRouterVersion	Public ❗	🛑	onlyOwner
└	<Receive Ether>	External ❗	💵	NO ❗
└	transfer	Public ❗	🛑	NO ❗
└	transferFrom	Public ❗	🛑	NO ❗
└	_transfer	Private 🔐	🛑		
└	_basicTransfer	Internal 🔒	🛑		
└	swapAndLiquify	Private 🔐	🛑	lockTheSwap
└	swapTokensForEth	Private 🔐	🛑		
└	addLiquidity	Private 🔐	🛑		
└	takeFee	Internal 🔒	🛑		

Legend

Symbol	Meaning
🛑	Function can modify state
💵	Function is payable

TESTNET VERSION

Adding Liquidity ✅
Tx:
https://testnet.bscscan.com/tx/0xc66a3a58ed21da9e9cb814fc3d30f17892756c193a5a80bebdc7cab9d0549680

==========

Buying when excluded from fees ✅
Tx (0% tax):
https://testnet.bscscan.com/tx/0xd177f2e7b2b740719f2ae1a8d4182af9b5bddebe777aa9a2d20be28873d57879

==========

Selling when excluded from fees ✅
Tx (0% tax):
https://testnet.bscscan.com/tx/0xa0ec588140c521ea0d3ed97542a3e6f7f710b414828ba3b69025b9bdf4a4343e

==========

Transferring when excluded from fees ✅
Tx(0% tax):
https://testnet.bscscan.com/tx/0x9e81192b55cf85b960d530c1ae6c3dc19a0184b76b101c1b8712a840199ba1ea

==========

Buying ✅
Tx(2% tax):
https://testnet.bscscan.com/tx/0xba2909063e3f88077abf1dc27a7c36f3088feb718e1065381e9fcf9801e79129

TESTNET VERSION

Selling ✅
Tx (0-2% tax):
https://testnet.bscscan.com/tx/0x94d996be708a52e1eaf2e58768a0bf74b25cbf67e6c7d07f1fb7890432844d35

==========

Transferring ✅
Tx(0% tax):
https://testnet.bscscan.com/tx/0x26853a1fa5d964b48617a56e2a9b5db67fb3b0190b80d94373b67a63157e4f67

==========

Internal swap (BNB to marketing wallet | reward token to dividend tracker | reward distribution) ✅
Tx:
https://testnet.bscscan.com/tx/0x88d9d55f4a7ec3c0e4f00eedeadbe13a53967d6da752e55e17004f6b42615703

MANUAL REVIEW

Severity Criteria

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

Vulnerabilities are dividend into three primary risk categroies:
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			

HIGH RISK FINDING

Maximum buy/sell/transfer

Category: Centralization
Status: Open
Impact: High

Overview:
Owner is able to set maximum amount of buy/sell/transfer to zero.

```
function setMaxTxAmount(uint256 maxTxAmount) external onlyOwner {
  require(
    maxTxAmount <= (40 * 10 ** 6 * 10 ** 9),
    "Max wallet should be less or equal to 4% totalSupply"
  );
  _maxTxAmount = maxTxAmount;
}
```

Suggestion:
Put a lower bound for maximum amount of buy/sell/transfes.

```
function setMaxTxAmount(uint256 maxTxAmount) external onlyOwner {
  require(
    maxTxAmount >= totalSupply() / 1000,
    "Maximum Tx must be greater than 0.1% of total supply"
  );
  _maxTxAmount = maxTxAmount;
}
```

HIGH RISK FINDING

Updating router

Category: Centralization / Logical
Status: Open
Impact: High

Overview:
Contract owner is able to update dex router which is used by contract to perform internal swap.
Updating router to a malicious contract causes internal swaps to revert the transaction.

```
function changeRouterVersion(
  address newRouterAddress
) public onlyOwner returns (address newPairAddress) {
  IUniswapV2Router02 _uniswapV2Router = IUniswapV2Router02(
    newRouterAddress
  );
  newPairAddress = IUniswapV2Factory(_uniswapV2Router.factory()).getPair(
    address(this),
    _uniswapV2Router.WETH()
  );
  if (newPairAddress == address(0)) {
    newPairAddress = IUniswapV2Factory(_uniswapV2Router.factory())
      .createPair(address(this), _uniswapV2Router.WETH());
  }
  uniswapPair = newPairAddress;
  uniswapV2Router = _uniswapV2Router;
  isWalletLimitExempt[address(uniswapPair)] = true;
  isMarketPair[address(uniswapPair)] = true;
}
```

Suggestion:
Ensure that router address is immutable after deploying the contract and adding liquidity.

HIGH RISK FINDING

setting swap threshold to zero

Category: Logical
Status: Open
Impact: High

Overview:
Setting minimumTokensBeforeSwap to zero and enabling swapAndLiquifyByLimitOnly causes internal swaps to be reverted in an attempt for swapping 0 tokens to ETH.

```
function setNumTokensBeforeSwap(uint256 newLimit) external onlyOwner {
  minimumTokensBeforeSwap = newLimit;
}

function setSwapAndLiquifyByLimitOnly(bool newValue) public onlyOwner {
  swapAndLiquifyByLimitOnly = newValue;
}
```

Suggestion:
Ensure that minimumTokensBeforeSwap is always greater than 1 tokens.

```
function setNumTokensBeforeSwap(uint256 newLimit) external onlyOwner {
require(newLimit <= 10 ** decimals(), “swap threshold must be greater than 1 token’);
  minimumTokensBeforeSwap = newLimit;
}
```

MEDIUM RISK FINDING

EOA receiving LP tokens

Category: Logical
Status: Open
Impact: Medium

Overview:
an EOA is receiving LP tokens which are generated from auto-liquidity, this causes more centralization power over liquidity pool overtime.

```
function addLiquidity(uint256 tokenAmount, uint256 ethAmount) private {
  _approve(address(this), address(uniswapV2Router), tokenAmount);
  uniswapV2Router.addLiquidityETH{value: ethAmount}(
    address(this),
    tokenAmount,
    0,
    0,
    owner(),
    block.timestamp
  );
}
```

Suggestion:
its suggested to burn or lock new LP tokens.

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

expelee

expelee_official

expelee-co

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 guarantess against the sale of team tokens or the removal of liquidity by the project audited in this document.

Always do your own research and project 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. Alway 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.

Building the Futuristic Blockchain Ecosystem