expelee

Building the Futuristic Blockchain Ecosystem

SECURITY AUDIT REPORT

Jungle

TOKEN OVERVIEW

Risk Findings

Severity	Found
High	1
Medium	0
Low	0
Informational	0

Centralization Risks

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

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	**21 June 2023**

CONTRACT DETAILS

Token Name: Jungle

Symbol: $JUNGLE

Network: Binance Smart Chain

Language: Solidity

Contract Address:
0xC70407b860C8C38adBF3c3C488706a4857Ac81De

Total Supply: 100,000,000,000

Owner's Wallet:
0x368ffBD1e34EAB57F8bCe0F94F47F02807019d77

Deployer's Wallet:
0x368ffBD1e34EAB57F8bCe0F94F47F02807019d77

Testnet.
https://testnet.bscscan.com/address/0x9246087965CD732021C7575C2617C9e536f6622F#code

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

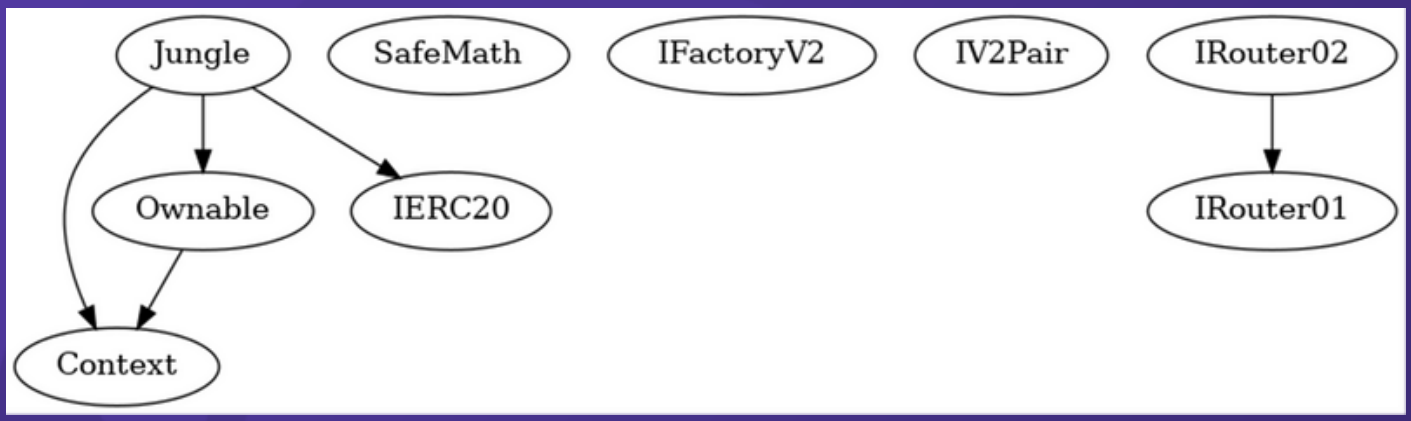
Issues on this level are minor details and warning that can remain unfixed.

Informational

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

expelee

INHERITANCE TREES



expelee

FUNCTION DETAILS

Contract	Type	Bases		
└	**Function Name**	**Visibility**	**Mutability**	**Modifiers**
Context	Implementation			
└	<Constructor>	Public ❗	🛑	NO ❗
└	_msgSender	Internal 🔒		
└	_msgData	Internal 🔒		
Ownable	Implementation	Context		
└	<Constructor>	Public ❗	🛑	NO ❗
└	owner	Public ❗		NO ❗
└	renounceOwnership	Public ❗	🛑	onlyOwner
└	transferOwnership	Public ❗	🛑	onlyOwner
└	_setOwner	Private 🔐	🛑	
SafeMath	Library			
└	add	Internal 🔒		
└	sub	Internal 🔒		
└	sub	Internal 🔒		
└	mul	Internal 🔒		
└	div	Internal 🔒		
└	div	Internal 🔒		
└	mod	Internal 🔒		
└	mod	Internal 🔒		
IFactoryV2	Interface			
└	getPair	External ❗		NO ❗
└	createPair	External ❗	🛑	NO ❗
IV2Pair	Interface			
└	factory	External ❗		NO ❗
└	getReserves	External ❗		NO ❗
└	sync	External ❗	🛑	NO ❗
IRouter01	Interface			
└	factory	External ❗		NO ❗
└	WETH	External ❗		NO ❗
└	addLiquidityETH	External ❗	💵	NO ❗
└	addLiquidity	External ❗	🛑	NO ❗
└	swapExactETHForTokens	External ❗	💵	NO ❗
└	getAmountsOut	External ❗		NO ❗
└	getAmountsIn	External ❗		NO ❗
IRouter02	Interface	IRouter01		
└	swapExactTokensForETHSupportingFeeOnTransferTokens	External ❗	🛑	NO ❗
└	swapExactETHForTokensSupportingFeeOnTransferTokens	External ❗	💵	NO ❗

expelee

FUNCTION DETAILS

└	swapExactTokensForTokensSupportingFeeOnTransferTokens	External ❗	🔴	NO ❗
└	swapExactTokensForTokens	External ❗	🔴	NO ❗
IERC20	Interface			
└	totalSupply	External ❗		NO ❗
└	decimals	External ❗		NO ❗
└	symbol	External ❗		NO ❗
└	name	External ❗		NO ❗
└	getOwner	External ❗		NO ❗
└	balanceOf	External ❗		NO ❗
└	transfer	External ❗	🔴	NO ❗
└	allowance	External ❗		NO ❗
└	approve	External ❗	🔴	NO ❗
└	transferFrom	External ❗	🔴	NO ❗
Jungle	Implementation	Context, Ownable, IERC20		
└	<Receive Ether>	External ❗	💶	NO ❗
└	<Constructor>	Public ❗	🔴	NO ❗
└	totalSupply	External ❗		NO ❗
└	decimals	External ❗		NO ❗
└	symbol	External ❗		NO ❗
└	name	External ❗		NO ❗
└	getOwner	External ❗		NO ❗
└	allowance	External ❗		NO ❗
└	balanceOf	Public ❗		NO ❗
└	transferFrom	External ❗	🔴	NO ❗
└	transfer	Public ❗	🔴	NO ❗
└	_transfer	Internal 🔒	🔴	
└	checkCommunityWallet	Internal 🔒	🔴	inTxWinnerFlag
└	internalSwap	Public ❗	🔴	NO ❗
└	swapTokensForEth	Internal 🔒	🔴	inSwapFlag
└	takeTaxes	Internal 🔒	🔴	
└	approve	External ❗	🔴	NO ❗
└	_approve	Internal 🔒	🔴	
└	isBuy	Internal 🔒		
└	isSell	Internal 🔒		
└	isTransfer	Internal 🔒		
└	addLpPair	External ❗	🔴	onlyOwner
└	isExcludedFromFee	External ❗		NO ❗
└	increaseCommunityPrize	Public ❗	🔴	NO ❗
└	setIsExcludedFromFee	Public ❗	🔴	onlyOwner
└	setMarketingFee	Public ❗	🔴	onlyOwner
└	setCommunityFee	Public ❗	🔴	onlyOwner
└	setCommunityMinimumSeconds	Public ❗	🔴	onlyOwner
└	setSwapThreshold	Public ❗	🔴	onlyOwner
└	getCommunityInfo	Public ❗		NO ❗

FUNCTION DETAILS

└	getLastCommunityWinner	Public ❗		NO ❗
└	rescueStuckBEP20	Public ❗	🔴	onlyOwner
└	rescueStuckETH	Public ❗	🔴	onlyOwner
└	getTotalBurned	Public ❗		NO ❗
└	enableTrading	External ❗	🔴	onlyOwner

Legend

Symbol	Meaning
🔴	Function can modify state
💵	Function is payable

TESTNET VERSION

Adding Liquidity ✅
Tx:
https://testnet.bscscan.com/tx/0x4499b99644ee54c258c082462f25051664d146b106f6cc8949f1fb96771d1008

==========

Buying from a fee excluded wallet ✅
Tx (0% tax):
https://testnet.bscscan.com/tx/0x4e1fe63dac43c000660ba836a3bea5ea55dd04063adfaa4a2e69c84e49229694

==========

Selling from a fee excluded wallet ✅
Tx (0% tax):
https://testnet.bscscan.com/tx/0x3f16790eea7ec16f7ffd6fb303a5b563116d38385122bf7c946f506119fe32c3

==========

Transferring using a fee excluded wallet ✅
Tx (0% tax):
https://testnet.bscscan.com/tx/0x692a89ad8d9d0fc46533190886c4a973211ad24c54f2222b8181d53ed2131902

==========

Buying from a regular wallet ✅
Tx (0-8% tax):
https://testnet.bscscan.com/tx/0xa98a8f306f2e86577fb47eca053b8ac7d599dbafcaeabb27f49010d70993cb56

TESTNET VERSION

Selling from a regular wallet ✅
Tx (0-8% tax):
https://testnet.bscscan.com/tx/0x5bd6a96ff8cb3e23a91a02cfdc47b7a37ec3191cf677ca4372527c1147fc5b79

==========

Transferring from a regular wallet ✅
Tx (0-8%):
https://testnet.bscscan.com/tx/0xf4d9566311d6d554b006d960e1335a960c6e6eb0d46c465cfaf3f5ebadd9020d

==========

Internal swap (Marketing BNB) ✅
Tx:
https://testnet.bscscan.com/address/0x368ffbd1e34eab57f8bce0f94f47f02807019d77#tokentxns

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

Enabling trades is not guaranteed

Category: Centralization
Status: Partially Resolved
Severity: High

Overview:

Owner must enable trades for investors manually. If trades remain disabled, holders wont be able to trade their tokens.

Trades will be enabled automatically after 10 days after creation of the contract. Impact of this issue still depends on starting and ending date of the presale or launch.

```
  function enableTrading() external onlyOwner {
require(!isTradingEnabled, "Trading already enabled");
      isTradingEnabled = true;
      emit TradingEnabled();
  }
```

HIGH RISK FINDING

Enabling trades is not guaranteed

Suggestion:

There are multiple ways to resolve this issue:

•Enable trades prior to launch or presale : this ensurs that trades are already enabled forver and can not be disabled later. However, this completely negates the need for enableTrading function.

•Transfer Ownership of the contract to a trusted 3rd party: You can transfer ownership of the contract to a trusted 3rd party e.g a certified pinksale safu developer

•Create a time lock contract for enabling trades: this contract can enable trades after a fixed period of time. (Applied)

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

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 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.