expelee

Building the Futuristic Blockchain Ecosystem

# SECURITY AUDIT REPORT

## SPX6900

# TOKEN OVERVIEW

## Risk Findings

| Severity | Found |
|---|---|
| High | 2 |
| 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** | **24 October 2023** |

expelee

# CONTRACT DETAILS

**Token Address:** 0xfAfd781B2E5E79c954ABCD9df60e227a7B5A2C6a

**Name:** SPX6900

**Symbol:** SPX

**Decimals:** 18

**Network:** BSC

**Token Type:** BEP20

**Owner:** 0x1Cd0cE334Ca8297D638Ead7C6105b11e4B7a7e86

**Deployer:** 0x1Cd0cE334Ca8297D638Ead7C6105b11e4B7a7e86

**Token Supply:** 420,000,000,000

**Checksum:**
cb2134035a08d9a9f0030b2f1bc77b3adcf0973d

**Testnet version:**
The tests conducted were performed on the contract deployed on the Binance Smart Chain (BSC) Testnet.
https://testnet.bscscan.com/token/0xf5765a48A7DBC2BC31632C720A7B18d3c35C4B82

# 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

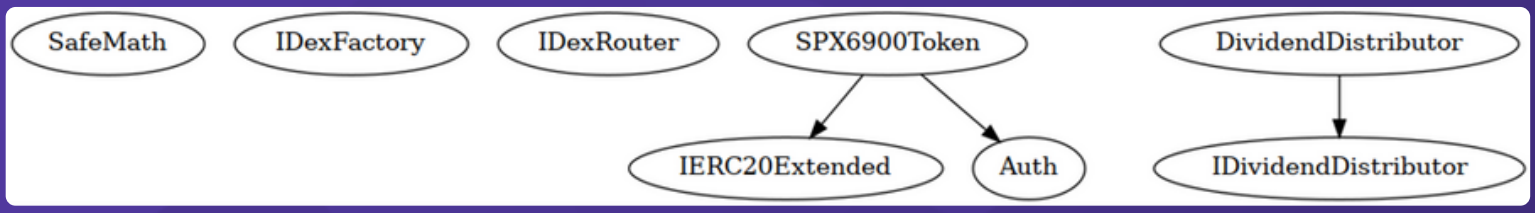
Issues on this level are minor details and warning that can remain unfixed.

## Informational

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

expelee

# INHERITANCE TREES



# FUNCTION DETAILS

| Contract | Type | Bases | | |
|---|---|---|---|---|
| └ | **Function Name** | **Visibility** | **Mutability** | **Modifiers** |
| **SafeMath** | Library | | | |
| └ | tryAdd | Internal 🔒 | | |
| └ | trySub | Internal 🔒 | | |
| └ | tryMul | Internal 🔒 | | |
| └ | tryDiv | Internal 🔒 | | |
| └ | tryMod | Internal 🔒 | | |
| └ | add | Internal 🔒 | | |
| └ | sub | Internal 🔒 | | |
| └ | mul | Internal 🔒 | | |
| └ | div | Internal 🔒 | | |
| └ | mod | Internal 🔒 | | |
| └ | sub | Internal 🔒 | | |
| └ | div | Internal 🔒 | | |
| └ | mod | Internal 🔒 | | |
| **IDexFactory** | Interface | | | |
| └ | createPair | External ❗ | 🛑 | NO ❗ |
| **IDexRouter** | Interface | | | |
| └ | factory | External ❗ | | NO ❗ |
| └ | WETH | External ❗ | | NO ❗ |
| └ | addLiquidityETH | External ❗ | 💵 | NO ❗ |
| └ | swapExactETHForTokensSupportingFeeOnTransferTokens | External ❗ | 💵 | NO ❗ |
| └ | swapExactTokensForETHSupportingFeeOnTransferTokens | External ❗ | 🛑 | NO ❗ |
| **IERC20Extended** | Interface | | | |
| └ | totalSupply | External ❗ | | NO ❗ |
| └ | decimals | External ❗ | | NO ❗ |
| └ | symbol | External ❗ | | NO ❗ |
| └ | name | External ❗ | | NO ❗ |
| └ | balanceOf | External ❗ | | NO ❗ |
| └ | transfer | External ❗ | 🛑 | NO ❗ |
| └ | allowance | External ❗ | | NO ❗ |
| └ | approve | External ❗ | 🛑 | NO ❗ |

# FUNCTION DETAILS

| └ | transferFrom | External ❗ | 🛑 |NO❗ |
|||||||
| **Auth** | Implementation | |||
| └ | <Constructor> | Public ❗ | 🛑 |NO❗ |
| └ | authorize | Public ❗ | 🛑 | onlyOwner |
| └ | unauthorize | Public ❗ | 🛑 | onlyOwner |
| └ | isOwner | Public ❗ | |NO❗ |
| └ | isAuthorized | Public ❗ | |NO❗ |
| └ | transferOwnership | Public ❗ | 🛑 | onlyOwner |
|||||||
| **IDividendDistributor** | Interface | |||
| └ | setDistributionCriteria | External ❗ | 🛑 |NO❗ |
| └ | setShare | External ❗ | 🛑 |NO❗ |
| └ | deposit | External ❗ | 🛑 |NO❗ |
| └ | process | External ❗ | 🛑 |NO❗ |
| └ | claimDividend | External ❗ | 🛑 |NO❗ |
| └ | getPaidEarnings | External ❗ | |NO❗ |
| └ | getUnpaidEarnings | External ❗ | |NO❗ |
| └ | totalDistributed | External ❗ | |NO❗ |
|||||||
| **DividendDistributor** | Implementation | IDividendDistributor |||
| └ | <Constructor> | Public ❗ | 🛑 |NO❗ |
| └ | setDistributionCriteria | External ❗ | 🛑 | onlyToken |
| └ | setShare | External ❗ | 🛑 | onlyToken |
| └ | deposit | External ❗ | 🛑 | onlyToken |
| └ | process | External ❗ | 🛑 | onlyToken |
| └ | shouldDistribute | Internal 🔒 | | |
| └ | distributeDividend | Internal 🔒 | 🛑 | |
| └ | claimDividend | External ❗ | 🛑 |NO❗ |
| └ | getPaidEarnings | Public ❗ | |NO❗ |
| └ | getUnpaidEarnings | Public ❗ | |NO❗ |
| └ | getCumulativeDividends | Internal 🔒 | | |
| └ | addShareholder | Internal 🔒 | 🛑 | |
| └ | removeShareholder | Internal 🔒 | 🛑 | |
|||||||
| **SPX6900Token** | Implementation | IERC20Extended, Auth |||
| └ | <Constructor> | Public ❗ | 🛑 | Auth |
| └ | <Receive Ether> | External ❗ | 💵 |NO❗ |
| └ | totalSupply | External ❗ | |NO❗ |
| └ | decimals | External ❗ | |NO❗ |
| └ | symbol | External ❗ | |NO❗ |
| └ | name | External ❗ | |NO❗ |
| └ | balanceOf | Public ❗ | |NO❗ |
| └ | allowance | External ❗ | |NO❗ |
| └ | approve | Public ❗ | 🛑 |NO❗ |
| └ | approveMax | External ❗ | 🛑 |NO❗ |

# FUNCTION DETAILS

| └ | transfer | External ❗ | 🛑 |NO ❗ |
| └ | transferFrom | External ❗ | 🛑 |NO ❗ |
| └ | _transferFrom | Internal 🔒 | 🛑 | |
| └ | _basicTransfer | Internal 🔒 | 🛑 | |
| └ | takeFee | Internal 🔒 | 🛑 | |
| └ | setBuyAccFee | Internal 🔒 | 🛑 | |
| └ | setSellAccFee | Internal 🔒 | 🛑 | |
| └ | shouldSwapBack | Internal 🔒 | | |
| └ | swapBack | Internal 🔒 | 🛑 | swapping |
| └ | enableTrading | External ❗ | 🛑 | authorized |
| └ | claimDividend | External ❗ | 🛑 |NO ❗ |
| └ | getPaidDividend | Public ❗ | |NO ❗ |
| └ | getUnpaidDividend | External ❗ | |NO ❗ |
| └ | getTotalDistributedDividend | External ❗ | |NO ❗ |
| └ | removeStuckBNB | External ❗ | 🛑 | authorized |
| └ | setIsDividendExempt | External ❗ | 🛑 | authorized |
| └ | setIsFeeExempt | External ❗ | 🛑 | authorized |
| └ | removeBots | External ❗ | 🛑 | onlyOwner |
| └ | setBuyFees | Public ❗ | 🛑 | authorized |
| └ | setSellFees | Public ❗ | 🛑 | authorized |
| └ | setFeeReceivers | External ❗ | 🛑 | authorized |
| └ | setSwapBackSettings | External ❗ | 🛑 | authorized |
| └ | setDistributionCriteria | External ❗ | 🛑 | authorized |
| └ | setDistributorSettings | External ❗ | 🛑 | authorized |

### Legend

|Symbol | Meaning|
|:--------:|-----------|
| 🛑 | Function can modify state |
| 💵 | Function is payable |

# TESTNET VERSION

**Adding Liquidity ✅**
**Tx:**
https://testnet.bscscan.com/tx/0xd9419257561b9fd2c39440925ff5f1324e21211fa49bb101e32eab92527cc171

==========

**Buying from a fee excluded wallet ✅**
**Tx (0% tax):**
https://testnet.bscscan.com/tx/0x76ea731b7cc4e4b011eb8503063e60813e01f3476674bdfb9e1267815b430836

==========

**Selling from a fee excluded wallet ✅**
**Tx (0% tax):**
https://testnet.bscscan.com/tx/0xc4097993d4253d7a408a8886a07e9c85fb05640354f539e19860ddbde08192e2

==========

**Transferring using a fee excluded wallet ✅**
**Tx (0% tax):**
https://testnet.bscscan.com/tx/0xc86839af9ef0a6dae653a3a4ebd5171b15b5d06f49a1ef6cfd2cbb2000e00033

==========

**Buying from a regular wallet ✅**
**Tx (0-25% tax):**
https://testnet.bscscan.com/tx/0x825e8c3d26ce630306540cd9b15e5a265a1a6488a79188c5bde2c190719e2e9c

# TESTNET VERSION

**Selling from a regular wallet ✅**
**Tx (0-25% tax):**
https://testnet.bscscan.com/tx/0xb45436bc1e92b0a081dc6b4baaac2adb476bfe9445d0e2e7010a0e2c2b5d1892

==========

**Transferring from a regular wallet ✅**
**Tx (0% tax):**
https://testnet.bscscan.com/tx/0x02c1bf8d9b56e1d6d224c1aabd7028e80e2fa841eea905e7b8d923b78cda05ae

==========

**Internal swap (Reward distribution / Marketing wallet received BNB) ✅**
**Tx:**
https://testnet.bscscan.com/tx/0xb45436bc1e92b0a081dc6b4baaac2adb476bfe9445d0e2e7010a0e2c2b5d1892

# 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

**Category: Logical**
**Subject: Sell transactions would be reverted because of reward distributor**
**Status: Open**
**Impact: High**

**Overview:**
The linked reward distributor is distributing self tokens (SPX tokens), hence, _transfer will be called by dividend tracker each time a share holder is rewarded. This issue reverts sell transactions because contract tries to perform internal swap each time.

Mitigation:
Add below condition in _transfer function to make sure that dividend distributor is not calling additional functions.

```
if (inSwap || sender == address(distributor)) {
    return _basicTransfer(sender, recipient, amount);
}
```

# HIGH RISK FINDING

**Category: Centralization**
**Subject: Trades are disabled by default**
**Status: Open**
**Impact: High**

**Overview:**
The contract has been structured such that all trading is disabled by default, necessitating the contract owner's manual intervention to enable trading. This can lead to a situation where, if trades remain disabled, token holders won't be able to buy, sell, or trade their tokens, causing a severe impact on the token's usability and market liquidity.

```
function enableTrading() external authorized {
    require(!trading, " already enabled");
    trading = true;
    swapEnabled = true;
    launchedAt = block.timestamp;
}
```

**Suggestion:**
To mitigate this risk, it is recommended that trading be enabled before the token presale. This can be achieved by invoking the "enableTrading" function or by transferring ownership of the contract to a third-party that has established trust with the community, such as a Certified SAFU developer. This reduces the concentration of power and the potential for malicious actions, thereby promoting a more decentralized and fair environment for all participants.

# 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.