



April 7, 2024

Express Audit Report for **ASPPIBRA [ASPPBR]**

DISCLAIMER: This is an automatically generated audit performed with De.Fi Scanner tool. De.Fi smart contract auditing tool is intended to assist in identifying potential vulnerabilities or malicious functions in smart contracts. While this is done to our best effort and knowledge, please notice that no tool can guarantee complete accuracy or comprehensiveness in detecting all possible vulnerabilities.



Project Summary

Project Name	BEP20Token
Address	0x0697ab2b003fd2cbaea2df1ef9b404e45be59d4c
Network	56

Issue ID	184
Severity	🔴 Optimization
Status	High
Description Code	<pre>function increaseAllowance(address spender, uint256 addedValue) public returns (bool) { _approve(_msgSender(), spender, _allowances[_msgSender()] [spender].add(addedValue)); return true; }</pre>
Location	<p>increaseAllowance(address,uint256) should be declared external:</p> <ul style="list-style-type: none">- BEP20Token.increaseAllowance(address,uint256) (BEP20Token.sol#474-477)

Issue ID	184
Severity	🎯 Optimization
Status	High
Description Code	<pre>function decreaseAllowance(address spender, uint256 subtractedValue) public returns (bool) { _approve(_msgSender(), spender, _allowances[_msgSender()] [spender].sub(subtractedValue, "BEP20: decreased allowance below zero")); return true; }</pre>
Location	<p>decreaseAllowance(address,uint256) should be declared external:</p> <ul style="list-style-type: none">- BEP20Token.decreaseAllowance(address,uint256) (BEP20Token.sol#493-496)

Issue ID	184
Severity	🔴 Optimization
Status	High
Description Code	<pre>function mint(uint256 amount) public onlyOwner returns (bool) { _mint(_msgSender(), amount); return true; }</pre>
Location	<p>mint(uint256) should be declared external:</p> <ul style="list-style-type: none">- BEP20Token.mint(uint256) (BEP20Token.sol#506-509)

Issue ID	186
Severity	🔴 Critical
Status	Medium
Description Code	function mint(uint256 amount) public onlyOwner returns (bool) { _mint(_msgSender(), amount); return true; }
Location	Mint function: BEP20Token.mint(uint256) (BEP20Token.sol#506-509) - in internal call: _mint(_msgSender(),amount) - In expression: _balances[account] = _balances[account].add(amount)

Issue ID	182
Severity	 Informational
Status	Medium
Description Code	<pre>constructor() public { _name = "ASPPIBRA"; _symbol = "ASPPBR"; _decimals = 18; _totalSupply = 21000000 * 10 ** 18; _balances[msg.sender] = _totalSupply; emit Transfer(address(0), msg.sender, _totalSupply); }</pre>
Location	<p>BEP20Token.constructor() (BEP20Token.sol#360-368) uses literals with too many digits:</p> <pre>- _totalSupply = 21000000 * 10 ** 18</pre> <p>(BEP20Token.sol#364)</p>