

Audit Report

PAF DAO Token

December 2021

Type	BEP20
Address	0x1EC8E66A4DdB61475e694e61a4657a65486c1A1D
Audited by	© coinscope

Table of Contents

Table of Contents 1
Contract Review 2
Audit Updates 2
Contract Analysis 3
ELFM - Exceed Limit Fees Manipulation 4
Description 4
Recommendation 4
ST - Stop Transactions 5
Description 5
Recommendation 5
Contract Diagnostics 6
Contract Functions 7
Contract Flow 17
Domain Info 18
Summary 19
Disclaimer 20
About Coinscope 21

Contract Review

Contract Name	PAFDAO
Compiler Version	v0.8.4+commit.c7e474f2
Optimization	200 runs
Licence	MIT
Explorer	https://bscscan.com/token/0x1EC8E66A4DdB61475e694e61a4657a65486c1A1D
Symbol	PAF
Decimals	9
Total Supply	100,000,000
Website	https://www.pafdao.com/

Audit Updates

Initial Audit	13th of December 2021
Corrected	

Contract Analysis

Pass	Description
✓	Contract Owner is not able to mint new tokens
✓	Contract Owner is not able to burn tokens from specific wallet
✗	Contract Owner is not able to increase fees more than a reasonable percent (10%)
✗	Contract Owner is not able to stop transactions
✓	Contract Owner is not able to transfer tokens from specific wallets
✓	Contract Owner is not able to increase the amount of liquidity taken by dev wallet more than a reasonable percent
✓	Contract Owner is not able to blacklist wallets from selling

ELFM - Exceed Limit Fees Manipulation

Criticality	high
Location	https://bscscan.com/address/0x1EC8E66A4DdB61475e694e61a4657a65486c1A1D#code#L1206,L1210,L1214,L1218

Description

The contract owner has the authority to increase fees to any amount without limitations. The owner may take advantage of it by calling the `setChartityFeePercent` function with a high percentage value.

```
function setChartityFeePercent(uint256 marketingFee) external onlyOwner() {
        _marketingFee = marketingFee;
    }
```

Recommendation

The contract's functions that can update fees should have limitations to what the fees can be up to a total of 10%.

The team should carefully manage the private keys of the owner's account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions. That risk can be prevented by temporarily locking the contract or renouncing ownership.

ST - Stop Transactions

Criticality	Medium
Location	https://bscscan.com/address/0x1EC8E66A4DdB61475e694e61a4657a65486c1A1D#code#L1226

Description

The contract owner has the authority to stop transactions for all users excluding the owner. The owner may take advantage of it by setting the `_maxTxAmount` to a very small number.

```
  function setMaxTxAmount(uint256 maxTxAmount, uint256 decimal) external
onlyOwner() {
        require(maxTxAmount > 0, "Cannot set transaction amount as zero");
        _maxTxAmount = maxTxAmount * 10**decimal;
    }
```

Recommendation

The team should carefully manage the private keys of the owner's account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions. That risk can be prevented by temporarily locking the contract or renouncing ownership.

Contract Diagnostics

Pass	Name
✓	Integer Underflow
✓	Parity Multisig Bug
✓	Callstack Depth Attack
✓	Transaction-Ordering Dependency
✓	Timestamp Dependency
✓	Re-Entrancy

Contract Functions

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
SafeMath	Library			
	add	Internal		
	sub	Internal		
	sub	Internal		
	mul	Internal		
	div	Internal		

	div	Internal		
	mod	Internal		
	mod	Internal		
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
Address	Library			
	isContract	Internal		
	sendValue	Internal	✓	
	functionCall	Internal	✓	
	functionCall	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionCallWithValue	Internal	✓	
	_functionCallWithValue	Private	✓	
Ownable	Implementation	Context		
		Public	✓	-

	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	geUnlockTime	Public		-
	lock	Public	✓	onlyOwner
	unlock	Public	✓	-
IUniswapV2Factory	Interface			
	feeTo	External		-
	feeToSetter	External		-
	getPair	External		-
	allPairs	External		-
	allPairsLength	External		-
	createPair	External	✓	-
	setFeeTo	External	✓	-
	setFeeToSetter	External	✓	-

IUniswapV2Pair	Interface			
	name	External		-
	symbol	External		-
	decimals	External		-
	totalSupply	External		-
	balanceOf	External		-
	allowance	External		-
	approve	External	✓	-
	transfer	External	✓	-
	transferFrom	External	✓	-
	DOMAIN_SEPARATOR	External		-
	PERMIT_TYPEHASH	External		-
	nonces	External		-
	permit	External	✓	-
	MINIMUM_LIQUIDITY	External		-
	factory	External		-
	token0	External		-
	token1	External		-
	getReserves	External		-

	price0CumulativeLast	External		-
	price1CumulativeLast	External		-
	kLast	External		-
	burn	External	✓	-
	swap	External	✓	-
	skim	External	✓	-
	sync	External	✓	-
	initialize	External	✓	-
IUniswapV2Router01	Interface			
	factory	External		-
	WETH	External		-
	addLiquidity	External	✓	-
	addLiquidityETH	External	Payable	-
	removeLiquidity	External	✓	-
	removeLiquidityETH	External	✓	-
	removeLiquidityWithPermit	External	✓	-
	removeLiquidityETHWithPermit	External	✓	-
	swapExactTokensForTokens	External	✓	-

	swapTokensForExactTokens	External	✓	-
	swapExactETHForTokens	External	Payable	-
	swapTokensForExactETH	External	✓	-
	swapExactTokensForETH	External	✓	-
	swapETHForExactTokens	External	Payable	-
	quote	External		-
	getAmountOut	External		-
	getAmountIn	External		-
	getAmountsOut	External		-
	getAmountsIn	External		-
IUniswapV2Router02	Interface	IUniswapV2Router01		
	removeLiquidityETHSupportingFeeOnTransferTokens	External	✓	-
	removeLiquidityETHWithPermitSupportingFeeOnTransferTokens	External	✓	-
	swapExactTokensForTokensSupportingFeeOnTransferTokens	External	✓	-
	swapExactETHForTokensSupportingFeeOnTransferTokens	External	Payable	-

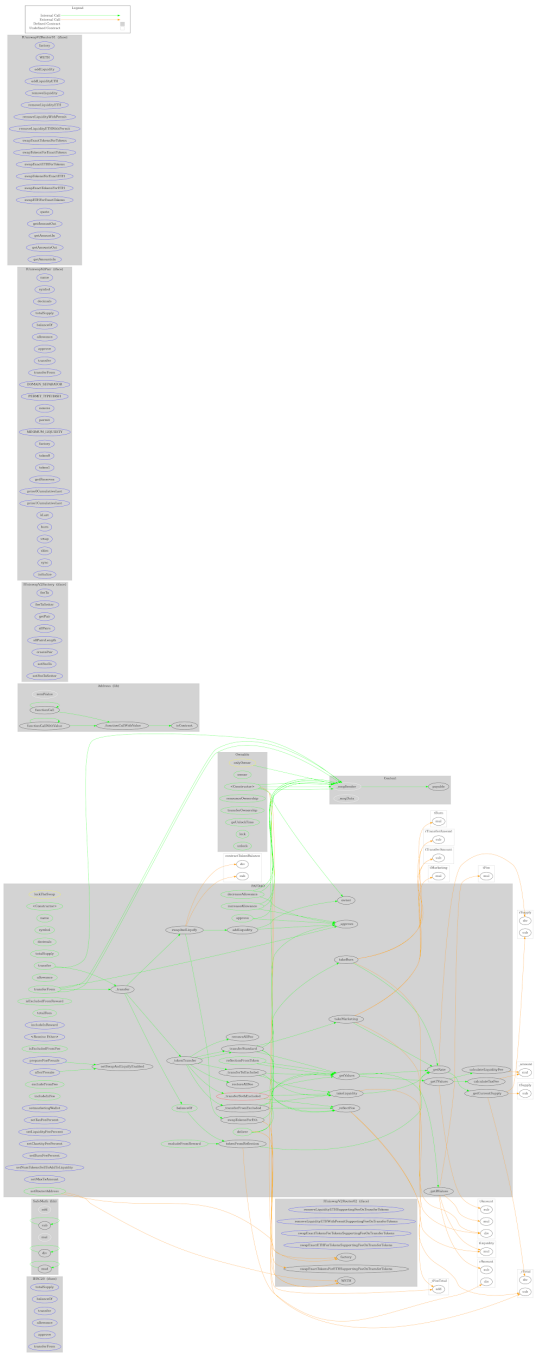
	swapExactTokensForETHSupportingFeeOnTransferTokens	External	✓	-
PAFDAO	Implementation	Context, IERC20, Ownable		
		Public	✓	-
	name	Public		-
	symbol	Public		-
	decimals	Public		-
	totalSupply	Public		-
	balanceOf	Public		-
	transfer	Public	✓	-
	allowance	Public		-
	approve	Public	✓	-
	transferFrom	Public	✓	-
	increaseAllowance	Public	✓	-
	decreaseAllowance	Public	✓	-
	isExcludedFromReward	Public		-
	totalFees	Public		-
	deliver	Public	✓	-

	reflectionFromToken	Public		-
	tokenFromReflection	Public		-
	excludeFromReward	Public	✓	onlyOwner
	includeInReward	External	✓	onlyOwner
	_transferBothExcluded	Private	✓	
		External	Payable	-
	_reflectFee	Private	✓	
	_getValues	Private		
	_getTValues	Private		
	_getRValues	Private		
	_getRate	Private		
	_getCurrentSupply	Private		
	_takeLiquidity	Private	✓	
	calculateTaxFee	Private		
	calculateLiquidityFee	Private		
	removeAllFee	Private	✓	
	restoreAllFee	Private	✓	
	isExcludedFromFee	Public		-

	_approve	Private	✓	
	_transfer	Private	✓	
	swapAndLiquify	Private	✓	lockTheSwap
	swapTokensForEth	Private	✓	
	addLiquidity	Private	✓	
	_tokenTransfer	Private	✓	
	_transferStandard	Private	✓	
	takeBurn	Private	✓	
	takeMarketing	Private	✓	
	_transferToExcluded	Private	✓	
	_transferFromExcluded	Private	✓	
	prepareFoePresale	External	✓	onlyOwner
	afterPresale	External	✓	onlyOwner
	excludeFromFee	Public	✓	onlyOwner
	includeInFee	Public	✓	onlyOwner
	setmarketingWallet	External	✓	onlyOwner

	setTaxFeePercent	External	✓	onlyOwner
	setLiquidityFeePercent	External	✓	onlyOwner
	setChartityFeePercent	External	✓	onlyOwner
	setBurnFeePercent	External	✓	onlyOwner
	setNumTokensSellToAddToLiquidity	External	✓	onlyOwner
	setMaxTxAmount	External	✓	onlyOwner
	setRouterAddress	Public	✓	onlyOwner
	setSwapAndLiquifyEnabled	Public	✓	onlyOwner

Contract Flow



Domain Info

Domain Name	pafdao.com
Registry Domain ID	2658699011_DOMAIN_COM-VRSN
Registrar WHOIS Server	whois.namecheap.com
Registrar URL	http://www.namecheap.com
Updated Date	0001-01-01T00:00:00.00Z
Creation Date	2021-12-01T06:41:05.00Z
Registry Expiry Date	2022-12-01T06:41:05.00Z
Registrar	NAMECHEAP INC
Registrar IANA ID	1068

The domain has been created almost 20 days before the analysis of the audit. It is set for expiration in one year.

There is no public billing information, the creator is protected by the privacy settings.

Summary

PAF DAO is the outcome of 2 decentralised projects merging into a new one. The team aims to launch staking features for their previous and new token as well as Airdrops. The smart contract analysis showed no compiler errors. There are some functions that can be abused by the owner, like manipulating fees without any limitation. The owner can also set the max transaction amount to any number. A multi-wallet signing pattern, locking or renouncing the ownership of the contract will eliminate all the threats mentioned above.

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.

Coinscope 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 Coinscope 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 Coinscope 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 Coinscope team disclaims any liability for the resulting losses.

About Coinscope

Coinscope is the leading early coin listing, voting and auditing authority firm. The audit process is analyzing and monitoring many aspects of the project. That way, it gives the community a good sense of security using an informative report and a generic score.

Coinscope is aiming to make crypto discoverable and efficient globally. It provides all the essential tools to assist users draw their own conclusions.



The Coinscope.co team

https://www.coinscope.co