Audit Report

Y-5 Finance

December 2021

Type	BEP20
Address	0x1E18eCd7DeCd05E360c8a2706688d80711E8BEdd
Audited by	© coinscope

Table of Contents

Contract Review

Contract Name	Y5Finance
Compiler Version	v0.8.5+commit.a4f2e591
Optimization	200 runs
Licence	MIT
Explorer	https://bscscan.com/token/0x1e18ecd7decd05e360c8a2706688d80711e8bedd
Symbol	Y-5
Decimals	18
Total Supply	1,000,000,000,000,000
Source	contract.sol
Domain	y-5.finance

Audit Updates

Initial Audit	22nd December 2021
Corrected	

Contract Analysis

Critical Medium Pass

Severity	Code	Description
	MT	Contract Owner is not able to mint new tokens
	BT	Contract Owner is not able to burn tokens from specific wallet
	ELFM	Contract Owner is not able to increase fees more than a reasonable percent (25%)
	ST	Contract Owner is not able to pause transactions for everyone else except him
	OCTD	Contract Owner is not able to transfer funds from specific address
	ULTW	Contract Owner is not able to increase the amount of liquidity taken by dev wallet more than a reasonable percent
	BC	Contract Owner is not able to blacklist wallets from selling

ELFM - Exceed Limit Fees Manipulation

Criticality	medium
Location	https://bscscan.com/address/0x1e18ecd7decd05e360c8a2706688d80711e8bedd#code#L890,L901,L912

Description

The contract owner has the authority to increase over the allowed limit of 25%. The owner may take advantage of it by calling the `setMarketingFee` function with a maximum upper limit of 30%.

```
    function setMarketingFee(uint256 marketingFee) external onlyOwner {
        uint256 taxFee = marketingFee.add(_reflectionFee).add(_buybackFee).add(
            _liquidityFee
        );
        require(taxFee <= TAX_UPPER_LIMIT, "Y-5: transfer tax exceeds limit");
        if (_marketingFee != marketingFee) {
            emit MarketingFeeUpdated(owner(), _marketingFee, marketingFee);
            _marketingFee = marketingFee;
        }
    }
```

Recommendation

The contract could embody a check for the maximum acceptable value to be lower than 25%.

We usually flag this warning as critical only if there are no limits to changing fees, the owner has implemented limits but they are 5% of our guidelines so we flag them as medium warning. Temporary locking the contract will eliminate the threat

ST - Stop Transactions

Criticality	medium
Location	https://bscscan.com/address/0x1e18ecd7decd05e360c8a2706688d80711e8bedd#code#L1115

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 low number. There is a limitation check to not allow the owner to set that variable to less than 1,000 tokens - but this is still a lot less than the total supply and will serve as a stopper in transactions.

```
    if (from != owner() && to != owner()) {
            require(
                amount <= _maxTxAmount,
                "Y-5: transfer amount exceeds the maxTxAmount."
            );
        }
```

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			
	decimals	External		-
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
Ownable	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	getUnlockTime	Public		-
	getTime	Public		-
	lock	Public	✓	onlyOwner
	unlock	Public	✓	-
SafeMath	Library			
	add	Internal		
	sub	Internal		
	sub	Internal		

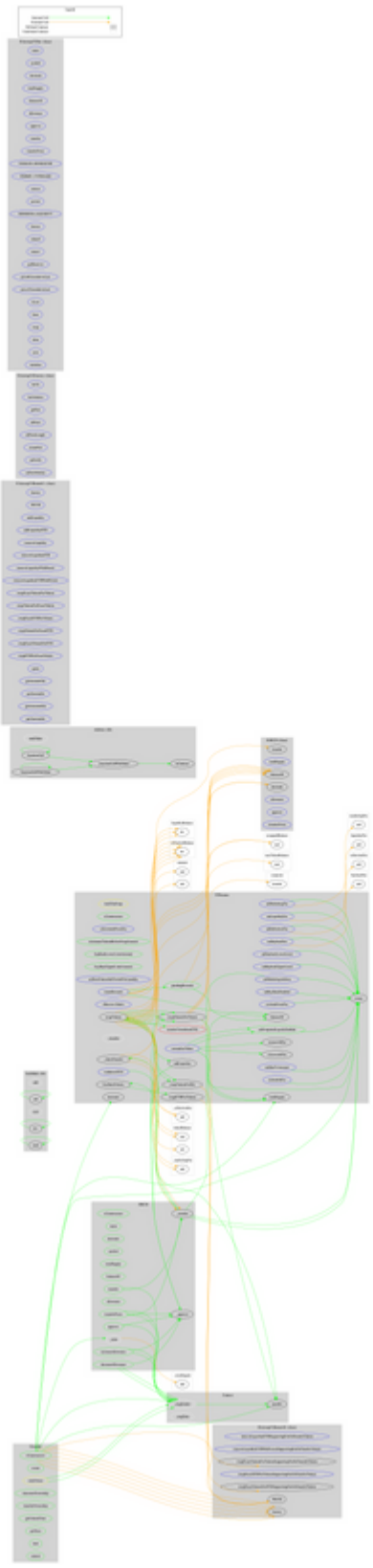
	mul	Internal		
	div	Internal		
	div	Internal		
	mod	Internal		
	mod	Internal		
Address	Library			
	isContract	Internal		
	sendValue	Internal	✓	
	functionCall	Internal	✓	
	functionCall	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionCallWithValue	Internal	✓	
	_functionCallWithValue	Private	✓	
ERC20	Implementation	Context, IERC20, Ownable		
	<Constructor>	Public	✓	-
	name	Public		-
	decimals	Public		-
	symbol	Public		-
	totalSupply	Public		-
	balanceOf	Public		-
	transfer	Public	✓	-
	allowance	Public		-
	approve	Public	✓	-
	transferFrom	Public	✓	-
	increaseAllowance	Public	✓	-
	decreaseAllowance	Public	✓	-
	_transfer	Internal	✓	
	_approve	Internal	✓	
	_mint	Internal	✓	
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	✓	-
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	✓	-
Y5Finance	Implementation	ERC20		

	<Constructor>	Public	✓	-
	isExcludedFromFee	External		-
	excludeFromFee	External	✓	onlyOwner
	includeInFee	External	✓	onlyOwner
	setReflectionFee	External	✓	onlyOwner
	setBuybackFee	External	✓	onlyOwner
	setMarketingFee	External	✓	onlyOwner
	setLiquidityFee	External	✓	onlyOwner
	setMaxTxAmount	External	✓	onlyOwner
	minimumTokensBeforeSwapAmount	Public		-
	buyBackLowerLimitAmount	Public		-
	buyBackUpperLimitAmount	Public		-
	setNumTokensSellToAddToLiquidity	External	✓	onlyOwner
	setBuybackLowerLimit	External	✓	onlyOwner
	setBuybackUpperLimit	External	✓	onlyOwner
	setMarketingAddress	External	✓	onlyOwner
	setSwapAndLiquifyEnabled	Public	✓	onlyOwner
	setBuyBackEnabled	External	✓	onlyOwner
	removeAllFee	Private	✓	
	restoreAllFee	Private	✓	
	normalizeToken	External	✓	onlyOwner
	transferToAddressETH	Private	✓	
	withdrawETH	External	✓	onlyOwner
	<Receive Ether>	External	Payable	-
	pendingRewards	Public		-
	claimRewards	External	✓	-
	_transfer	Internal	✓	
	swapTokens	Private	✓	lockTheSwap
	buyBackTokens	Private	✓	lockTheSwap
	swapTokensForEth	Private	✓	
	swapTokensForTokens	Private	✓	
	swapETHForTokens	Private	✓	
	addLiquidity	Private	✓	
	_tokenTransfer	Private	✓	

Contract Flow



Domain Info

Domain Name	y-5.finance
Registry Domain ID	a7d855f7875344f384b190727749f86e-DONUTS
Creation Date	2021-11-26T12:07:29Z
Updated Date	2021-12-13T17:26:08Z
Registry Expiry Date	2022-11-26T12:07:29Z
Registrar WHOIS Server	whois.tucows.com
Registrar URL	http://www.tucows.com
Registrar	Tucows Domains Inc.
Registrar IANA ID	69

The domain has been created 26 days before the creation of the audit. It will expire in 11 months.

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

Summary

Y-5 finance is a very interesting and innovative project. According to their website, holders will receive 13% of each transaction in Crypter, Evergrow, Reflecto, Rematic and BUSD. The token has a friendly and growing community. The Smart Contract analysis reported no major and only 2 medium-low threat issues. The Contract Owner can change fees up to a total of 30%. He is also able to stop transactions for everyone else apart from the owner by exploiting the anti-whale mechanism. A multi-wallet signing pattern will provide security against potential hacks. Temporarily locking the contract or renouncing ownership will eliminate all the contract threats.

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