Cyberscope

Audit Report

HealthFi Token

May 2022

Type	BEP20
Network	BSC
Address	0xFD626E4c00B59AFCAFd0F47F743051A58BCc4A62
Audited by	© cyberscope

Table of Contents

Contract Review

Contract Name	FirstToken
Compiler Version	v0.8.12+commit.f00d7308
Optimization	20 runs
Licence	MIT
Explorer	https://bscscan.com/token/0xFD626E4c00B59AFCAFd0F47F743051A58BCc4A62
Symbol	HEFI
Decimals	18
Total Supply	100,000,000
Domain	healthfi.app

Source Files

Filename	**SHA256**
contract.sol	46f5233e0eaddd0a4ce3d384abb068db5951dad86c931317054b6cdb4ee87557

Audit Updates

Initial Audit	23rd May 2022
Corrected	

Contract Analysis

Critical Medium Minor Pass

Severity	Code	Description
●	ST	Contract Owner is not able to stop or pause transactions
●	OCTD	Contract Owner is not able to transfer tokens from specific address
●	OTUT	Owner Transfer User's Tokens
●	ELFM	Contract Owner is not able to increase fees more than a reasonable percent (25%)
●	ULTW	Contract Owner is not able to increase the amount of liquidity taken by dev wallet more than a reasonable percent
●	MT	Contract Owner is not able to mint new tokens
●	BT	Contract Owner is not able to burn tokens from specific wallet
●	BC	Contract Owner is not able to blacklist wallets from selling

ELFM - Exceed Limit Fees Manipulation

Criticality	critical
Location	contract.sol#L1447

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 setFeeRate function with a high percentage value.

```
function setFeeRate(uint256 _sellFeeRate, uint256 _buyFeeRate)
        external
        onlyRole(FEE_CONTROL_ROLE)
    {
        require(_sellFeeRate > 0 && _sellFeeRate < 50, "sellFeeRate invalid");
        require(_buyFeeRate > 0 && _buyFeeRate < 50, "buyFeeRate invalid");

        sellFeeRate = _sellFeeRate;
        buyFeeRate = _buyFeeRate;

        emit UpdateTransferRate(sellFeeRate, buyFeeRate);
    }
```

Recommendation

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

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.

ULTW - Unlimited Liquidity to Team Wallet

Criticality	minor
Location	contract.sol#L1497, 1510

Description

The contract owner has the authority to transfer funds without limit to the team wallet. These funds have been accumulated from fees collected from the contract. The owner may take advantage of it by calling the `sweepTokenForBosses` functions.

```
function sweepTokenForBosses(uint256 tokenAmount)
        external
        onlyRole(SWEEPER_ROLE)
    {
        uint256 contractTokenBalance = balanceOf(address(this));
        if (tokenAmount > contractTokenBalance) {
            tokenAmount = contractTokenBalance;
        }
        if (contractTokenBalance >= tokenForBosses) {
            _swapTokensForEth(tokenAmount);
        }
    }
```

```
function sweepTokenForBosses() external onlyRole(SWEEPER_ROLE) {
        uint256 contractTokenBalance = balanceOf(address(this));
        if (contractTokenBalance >= tokenForBosses) {
            _swapTokensForEth(tokenForBosses);
        }
    }
```

Recommendation

The contract could embody a check for the maximum amount of funds that can be swapped. Since a huge amount may volatile the token's price.

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

Critical Medium Minor

Severity	Code	Description
	FSA	Fixed Swap Address
	L01	Public Function could be Declared External
	L02	State Variables could be Declared Constant
	L04	Conformance to Solidity Naming Conventions
	L09	Dead Code Elimination
	L14	Uninitialized Variables in Local Scope

FSA - Fixed Swap Address

Criticality	minor
Location	contract.sol#L1487

Description

The swap address is assigned once in the constructor and it can not be changed. The decentralized swaps sometimes create a new swap version or abandon the current. A contract that cannot change the swap address may not be able to catch-up the upgrade.

```
IUniswapV2Router02 _uniswapV2Router = IUniswapV2Router02(
            newRouter // address uniswap
        );
        uniswapV2Pair = IUniswapV2Factory(_uniswapV2Router.factory())
            .createPair(address(this), _uniswapV2Router.WETH());
        uniswapV2Router = _uniswapV2Router;
```

Recommendation

It could be better to allow the swap address mutation in case of future swap updates.

L01 - Public Function could be Declared External

Criticality	minor
Location	contract.sol#L432,440,457,464,483,506,528,551,571,1115,1128,1146

Description

Public functions that are never called by the contract should be declared external to save gas.

```
renounceRole
revokeRole
grantRole
decreaseAllowance
increaseAllowance
transferFrom
approve
transfer
totalSupply
...
```

Recommendation

Use the external attribute for functions never called from the contract.

L02 - State Variables could be Declared Constant

Criticality	minor
Location	contract.sol#L1481

Description

Constant state variables should be declared constant to save gas.

```
maxSupply
```

Recommendation

Add the constant attribute to state variables that never change.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contract.sol#L1216,1397,1407,1420,1433,1447

Description

Solidity defines a naming convention that should be followed. Rule exceptions:

- Allow constant variable name/symbol/decimals to be lowercase.
- Allow _ at the beginning of the mixed_case match for private variables and unused parameters.

```
_buyFeeRate
_sellFeeRate
_tokenForBosses
_addressForBosses
_target
WETH
```

Recommendation

Follow the Solidity naming convention.
https://docs.soliditylang.org/en/v0.4.25/style-guide.html#naming-conventions

L09 - Dead Code Elimination

Criticality	minor
Location	contract.sol#L1179,650,887,862

Description

Functions that are not used in the contract, and make the code's size bigger.

```
toString
toHexString
_burn
_setRoleAdmin
```

Recommendation

Remove unused functions.

L14 - Uninitialized Variables in Local Scope

Criticality	minor
Location	contract.sol#L1539

Description

The are variables that are defined in the local scope and are not initialized.

```
transferFeeRate
```

Recommendation

All the local scoped variables should be initialized.

Contract Functions

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		
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
IERC20Metadata	Interface	IERC20		
	name	External		-
	symbol	External		-
	decimals	External		-

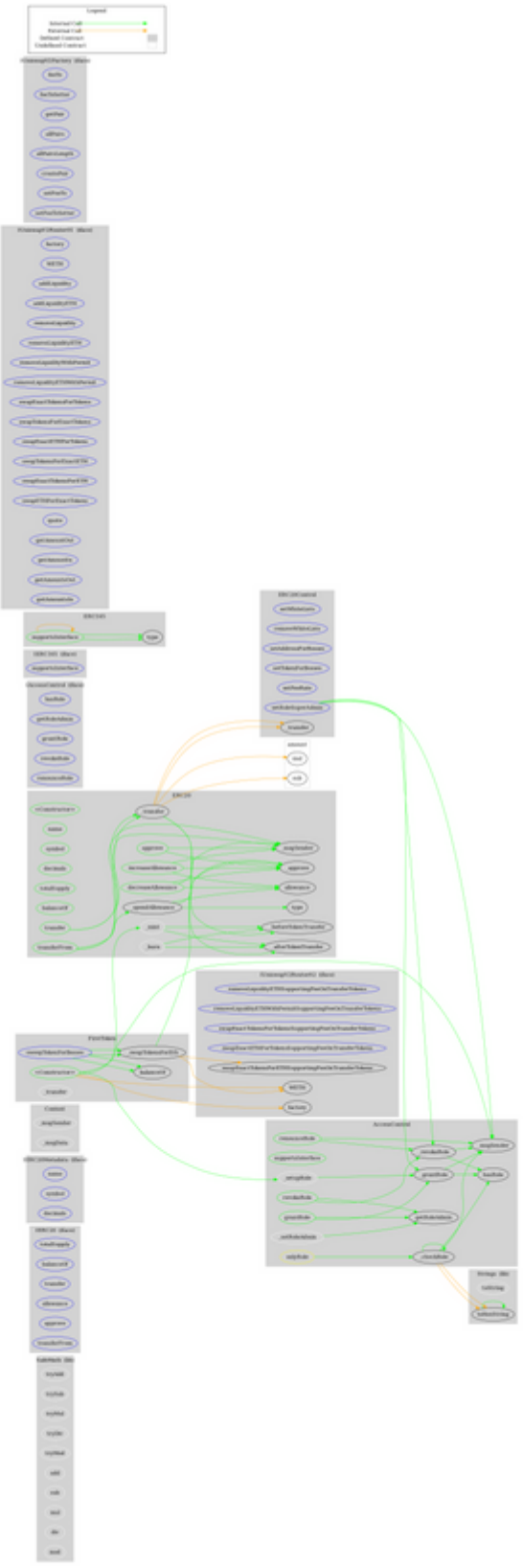
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
ERC20	Implementation	Context, IERC20, IERC20Metadata		
	<Constructor>	Public	✓	-
	name	Public		-
	symbol	Public		-
	decimals	Public		-
	totalSupply	Public		-
	balanceOf	Public		-
	transfer	Public	✓	-
	allowance	Public		-
	approve	Public	✓	-
	transferFrom	Public	✓	-
	increaseAllowance	Public	✓	-
	decreaseAllowance	Public	✓	-
	_transfer	Internal	✓	
	_mint	Internal	✓	
	_burn	Internal	✓	
	_approve	Internal	✓	
	_spendAllowance	Internal	✓	
	_beforeTokenTransfer	Internal	✓	
	_afterTokenTransfer	Internal	✓	
IAccessControl	Interface			
	hasRole	External		-
	getRoleAdmin	External		-
	grantRole	External	✓	-
	revokeRole	External	✓	-
	renounceRole	External	✓	-

Strings	Library			
	toString	Internal		
	toHexString	Internal		
	toHexString	Internal		
IERC165	Interface			
	supportsInterface	External		-
ERC165	Implementation	IERC165		
	supportsInterface	Public		-
AccessControl	Implementation	Context, IAccessControl, ERC165		
	supportsInterface	Public		-
	hasRole	Public		-
	_checkRole	Internal		
	_checkRole	Internal		
	getRoleAdmin	Public		-
	grantRole	Public	✓	onlyRole
	revokeRole	Public	✓	onlyRole
	renounceRole	Public	✓	-
	_setupRole	Internal	✓	
	_setRoleAdmin	Internal	✓	
	_grantRole	Internal	✓	
	_revokeRole	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	✓	-

ERC20Control	Implementation	AccessControl		
	setWhiteLists	External	✓	onlyRole
	removeWhiteLists	External	✓	onlyRole
	setAddressForBosses	External	✓	onlyRole
	setTokenForBosses	External	✓	onlyRole
	setFeeRate	External	✓	onlyRole
	setRoleSuperAdmin	External	✓	onlyRole
FirstToken	Implementation	ERC20, ERC20Control		
	<Constructor>	Public	✓	ERC20
	sweepTokenForBosses	External	✓	onlyRole
	sweepTokenForBosses	External	✓	onlyRole
	_swapTokensForEth	Private	✓	
	_transfer	Internal	✓	

Contract Flow



Domain Info

Domain Name	healthfi.app
Registry Domain ID	48E38B29B-APP
Creation Date	2022-05-03T12:10:51Z
Updated Date	2022-05-08T12:10:51Z
Registry Expiry Date	2024-05-03T12:10:51Z
Registrar WHOIS Server	whois.godaddy.com
Registrar URL	https://www.godaddy.com/
Registrar	GoDaddy.com, LLC
Registrar IANA ID	146

The domain has been created 20 days before the creation of the audit. It will expire in almost 2 years.

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

Summary

There are some functions that can be abused by the owner like manipulating fees and transferring funds to the team’s wallet. The maximum fee percentage that can be set is 49% 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.

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

About Cyberscope

Coinscope audit and K.Y.C. service has been rebranded to Cyberscope.

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.

Cyberscope and Coinscope are aiming to make crypto discoverable and efficient globally. They provide all the essential tools to assist users draw their own conclusions.

The Cyberscope team

https://www.cyberscope.io