Cyberscope

Audit Report

SpaceFalconX

June 2022

Table of Contents

Contract Review

Contract Name	SpaceFalconX
Compiler Version	v0.8.13+commit.abaa5c0e
Optimization	200 runs
Licence	MIT
Explorer	https://bscscan.com/token/0xc10dA9401f0a45aaAa4d6C5530Cd1511C45760DA
Symbol	$SFX
Decimals	18
Total Supply	1,000,000,000,000
Domain	spacefalconx.com

Source Files

Filename	**SHA256**
contract.sol	f86f026ba1f4eff0f6ee266c2be091cc01ab98154255bd72098c851c9485104c

Audit Updates

Initial Audit	6th June 2022
Corrected	14th June 2022

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

OCTD - Owner Contract Tokens Drain

Criticality	minor
Location	contract.sol#L763

Description

The contract owner has the authority to claim all the balance of the contract. The owner may take advantage of it by calling the `rescueStuckBNB` or `rescueBEP20` function.

```solidity
function rescueStuckBNB() external onlyAuthorized {
    uint256 bnbAmount = address(this).balance;
    payable(msg.sender).transfer(bnbAmount);
}

function rescueBEP20(address _token) external onlyAuthorized {
    uint256 tamt = IERC20(_token).balanceOf(address(this));
    IERC20(_token).transfer(msg.sender, tamt);
}
```

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

● Critical   ● Medium   ● Minor

Severity	Code	Description
●	CO	Code Optimization
●	L04	Conformance to Solidity Naming Conventions

CO - Code Optimization

Criticality	minor
Location	contract.sol#L747

Description

The `burnAmt` is already checked in the setter method (`planBurn()`). As a result, the `require(..)` expression will never yield false during the runtime.

```solidity
function doBurn(uint256 burnAmt) internal inburn {
    require(burnAmt <= 50 * TOTAL_SUPPLY / 1000, "burnAmount is limited to 5% in
single transaction");
    super._transfer(address(this), deadAddress, burnAmt);
    accumulatingForBurn = false;
}
```

Recommendation

Rewrite some code segments so the runtime will be more performant.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contract.sol#L19,82,66,110,112,114,116,117,118,200,201,210,212,224,530,605, 768,398,399,400

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.

```
deadAddress
_maxWalletToken
_maxTxAmount
_token
_minDistribution
_minPeriod
_tradeCooldown
dividendsPerShareAccuracyFactor
_uniswapV2Router
...
```

## Recommendation

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

Contract Functions

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
IUniswapV2Router	Interface			
	factory	External		-
	WETH	External		-
	addLiquidityETH	External	Payable	-
	swapExactTokensForTokensSupportingFeeOnTransferTokens	External	✓	-
	swapExactTokensForETHSupportingFeeOnTransferTokens	External	✓	-
	swapExactETHForTokensSupportingFeeOnTransferTokens	External	Payable	-
IUniswapV2Factory	Interface			
	createPair	External	✓	-
IDividendDistributor	Interface			
	setDistributionCriteria	External	✓	-
	setShare	External	✓	-
	deposit	External	Payable	-
	process	External	✓	-

Ownable	Implementation			
	<Constructor>	Public	✓	-
	owner	Public		-
	authorize	External	✓	onlyOwner
	renounceOwnership	External	✓	onlyOwner
	transferOwnership	External	✓	onlyOwner
ERC20	Implementation	IERC20		
	<Constructor>	Public	✓	-
	name	External		-
	symbol	External		-
	decimals	External		-
	totalSupply	External		-
	balanceOf	Public		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
	increaseAllowance	External	✓	-
	decreaseAllowance	External	✓	-
	_transfer	Internal	✓	
	_mint	Internal	✓	
	_approve	Internal	✓	
RDividendDistributor	Implementation	IDividendDistributor		
	<Constructor>	Public	✓	-
	setDistributionCriteria	External	✓	onlyToken
	setShare	External	✓	onlyToken
	deposit	External	Payable	-
	<Receive Ether>	External	Payable	-
	process	External	✓	-
	shouldDistribute	Internal		
	distributeDividend	Internal	✓	
	claimDividend	External	✓	-

	getUnpaidEarnings	Public		-
	getCumulativeDividends	Internal		
	addShareholder	Internal	✓	
	removeShareholder	Internal	✓	
SpaceFalconX	Implementation	ERC20, Ownable		
	\<Constructor\>	Public	✓	ERC20
	launch	External	✓	onlyOwner
	updateDividendDistributor	External	✓	onlyOwner
	updateUniswapV2Router	External	✓	onlyOwner
	setMinContractSells	External	✓	onlyAuthorized
	setMinTokenSells	External	✓	onlyAuthorized
	excludeFromFees	Public	✓	onlyOwner
	excludeFromDividends	Public	✓	onlyOwner
	setAutomatedMarketMakerPair	External	✓	onlyOwner
	_setAutomatedMarketMakerPair	Internal	✓	
	updateInternalAddresses	External	✓	onlyAuthorized
	updateGasForProcessing	External	✓	onlyOwner
	setDistributionCriteria	External	✓	onlyOwner
	getClaimWait	External		-
	getTotalDividendsDistributed	External		-
	claim	External	✓	-
	getNumberOfDividendTokenHolders	External		-
	setFees	External	✓	onlyOwner
	setTradeRestrictions	External	✓	onlyOwner
	setSwapTokensAtAmount	External	✓	onlyOwner
	checkValidTrade	Internal	✓	
	_transfer	Internal	✓	
	rewards	Internal	✓	
	takeFees	Internal	✓	
	rush	External	✓	onlyAuthorized
	calculateFee	Internal	✓	
	shouldBurn	Internal		
	planBurn	External	✓	onlyAuthorized
	doBurn	Internal	✓	inburn

	shouldSwap	Internal		
	rescueStuckBNB	External	✓	onlyAuthorized
	rescueBEP20	External	✓	onlyAuthorized
	swapTokens	Internal	✓	inSwap
	swapTokensForEth	Internal	✓	
	addLiquidity	Internal	✓	
	buybackStuckBNB	External	✓	onlyAuthorized
	<Receive Ether>	External	Payable	-

Contract Flow
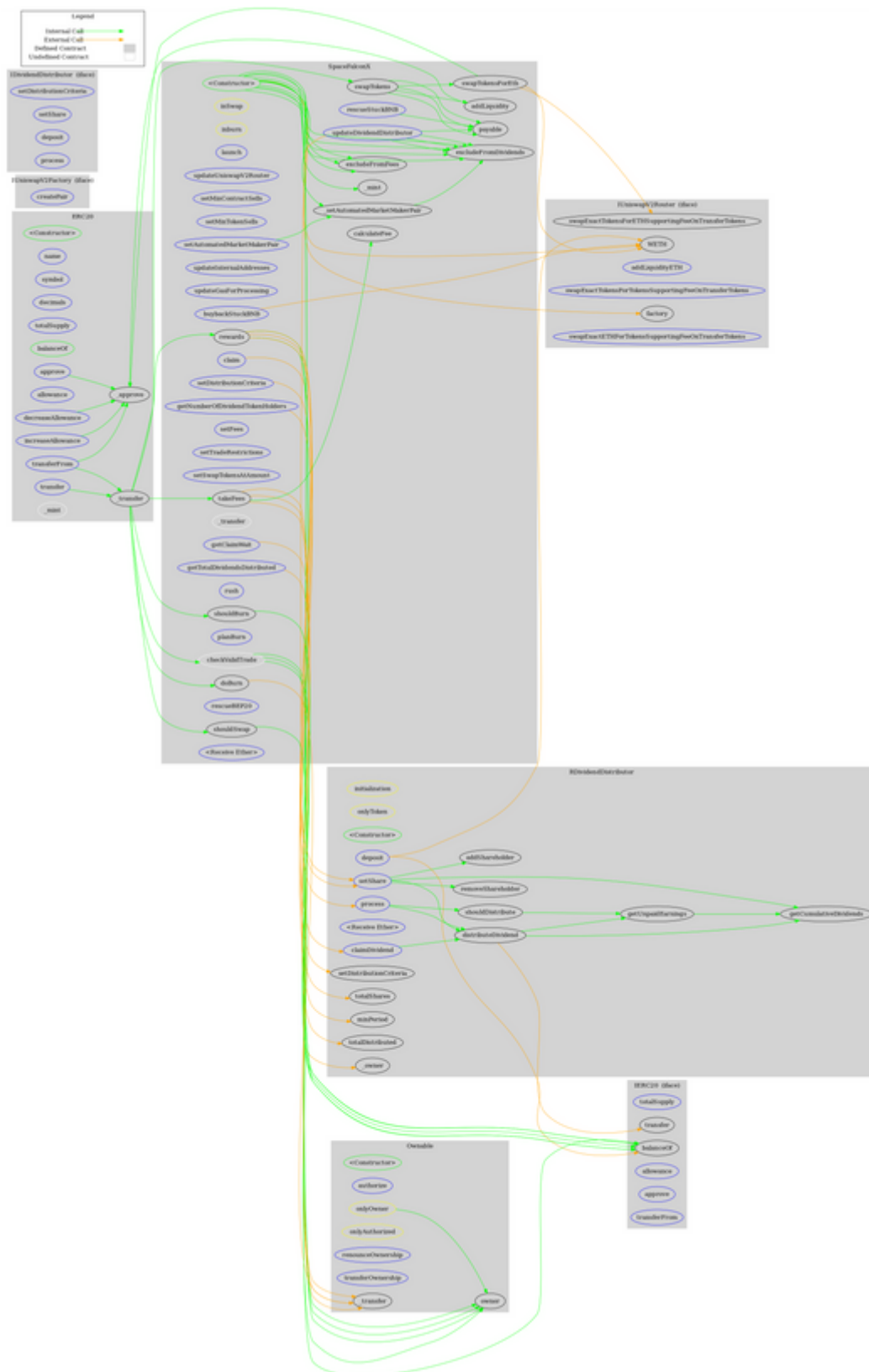
Domain Info

Domain Name	spacefalconx.com
Registry Domain ID	2701686615_DOMAIN_COM-VRSN
Creation Date	2022-06-06T02:52:56Z
Updated Date	2022-06-06T02:52:58Z
Registry Expiry Date	2023-06-06T02:52:56Z
Registrar WHOIS Server	whois.hostinger.com
Registrar URL	https://www.hostinger.com
Registrar	Hostinger, UAB
Registrar IANA ID	1636

The domain has been created about 9 hours before the creation of the audit. It will expire in 12 months.

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 misusing the contract configuration and manipulating fees. 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