Audit Report

XRPNATION

January 2022

Type	BEP20
Network	BSC
Address	0xC07c894D01A8785CB289620C25878d3CdAb40552
Audited by	© coinscope

Table of Contents

Contract Review

Contract Name	XRPNATION
Compiler Version	v0.8.6+commit.11564f7e
Optimization	200 runs
Licence	Unlicense
Explorer	https://bscscan.com/token/0xC07c894D01A8785CB289620C25878d3CdAb40552
Symbol	XRPNATION
Decimals	9
Total Supply	100,000,000,000
Source	contract.sol
Domain	xrpnation.app

Audit Updates

Initial Audit	24th January 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

ST - Stop Transactions

Criticality	critical
Location	contract.sol#L433,L441,L447,L452

Description

The contract owner has the authority to stop the sales for all users excluding the owner. The owner may take advantage of it by:

Setting a high amount to the sell fees.

```
if(recipient == pair){
    sellFees();
}
```

Setting the `_maxSellTxAmount` to zero and disabling the `autoLimits` variable.

```
if(recipient == pair){
    require(amount <= _maxSellTxAmount || isTxLimitExempt[sender], "TX Limit
Exceeded");
}
```

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 `tradingOpen` to false.

```
if(!authorizations[sender] && !authorizations[recipient]){
    require(tradingOpen,"Trading not open yet");
}
```

Setting the `_maxWalletToken` to zero.

```
require((heldTokens + amount) <= _maxWalletToken,"Total Holding is currently
limited, you can not buy that much.");}
```

Recommendation

The contract could embody a check for not allowing setting the _maxTxAmount less than a reasonable amount. A suggested implementation could check that the maximum amount should be more than a fixed percentage of the total supply.

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.

ELFM - Exceed Limit Fees Manipulation

Criticality	critical
Location	contract.sol#L642

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 `setSellFees` function with a high percentage value.

```
function setSellFees(uint256 _liquidityFee, uint256 _reflectionFee, uint256
_marketingFee, uint256 _DevFee) external authorized {
    SellliquidityFee = _liquidityFee;
    SellreflectionFee = _reflectionFee;
    SellmarketingFee = _marketingFee;
    SellDevFee = _DevFee;
    SelltotalFee = _liquidityFee + (_reflectionFee) + (_marketingFee) +
(_DevFee);
}
```

Recommendation

The contract could embody a check for the maximum acceptable value.

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
	L01	Public Function could be Declared External
	L02	State Variables could be Declared Constant
	L05	Unused State Variable
	L04	Conformance to Solidity Naming Conventions
	L07	Missing Events Arithmetic

L01 - Public Function could be Declared External

Criticality	minor
Location	contract.sol#L711,L627,L57 and 2 more

Description

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

```
rescueToken
tradingStatus
transferOwnership
...
```

Recommendation

Use the external attribute for functions never called from the contract

L02 - State Variables could be Declared Constant

Criticality	minor
Location	contract.sol#L311,L306,L304 and 3 more

Description

Constant state variables should be declared constant to save gas.

```
_totalSupply
ZERO
WBNB
...
```

Recommendation

Add the constant attribute to state variables that never change.

L05 - Unused State Variable

Criticality	minor
Location	contract.sol#L306

Description

There are segments that contains unused state variable.

```
ZERO
```

Recommendation

Remove unused state variables.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contract.sol#L351,L346,L345 and 52 more

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.

```
DevFeeReceiver
_maxWalletToken
_maxSellTxAmount
...
```

Recommendation

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

L07 - Missing Events Arithmetic

Criticality	minor
Location	contract.sol#L705,L700,L695 and 4 more

Description

Detected missing events for critical arithmetic parameters. There are functions that have no event emitted, so it is difficult to track off-chain changes.

```
_maxSellTxAmount = _totalSupply / (1000) * (maxSellTXPercentage_base1000)
_maxBuyTxAmount = _totalSupply / (1000) * (maxBuyTXPercentage_base1000)
_maxWalletToken = _totalSupply / (1000) * (maxWallPercent_base1000)
...
```

Recommendation

Emit an event for critical parameter changes.

Contract Functions

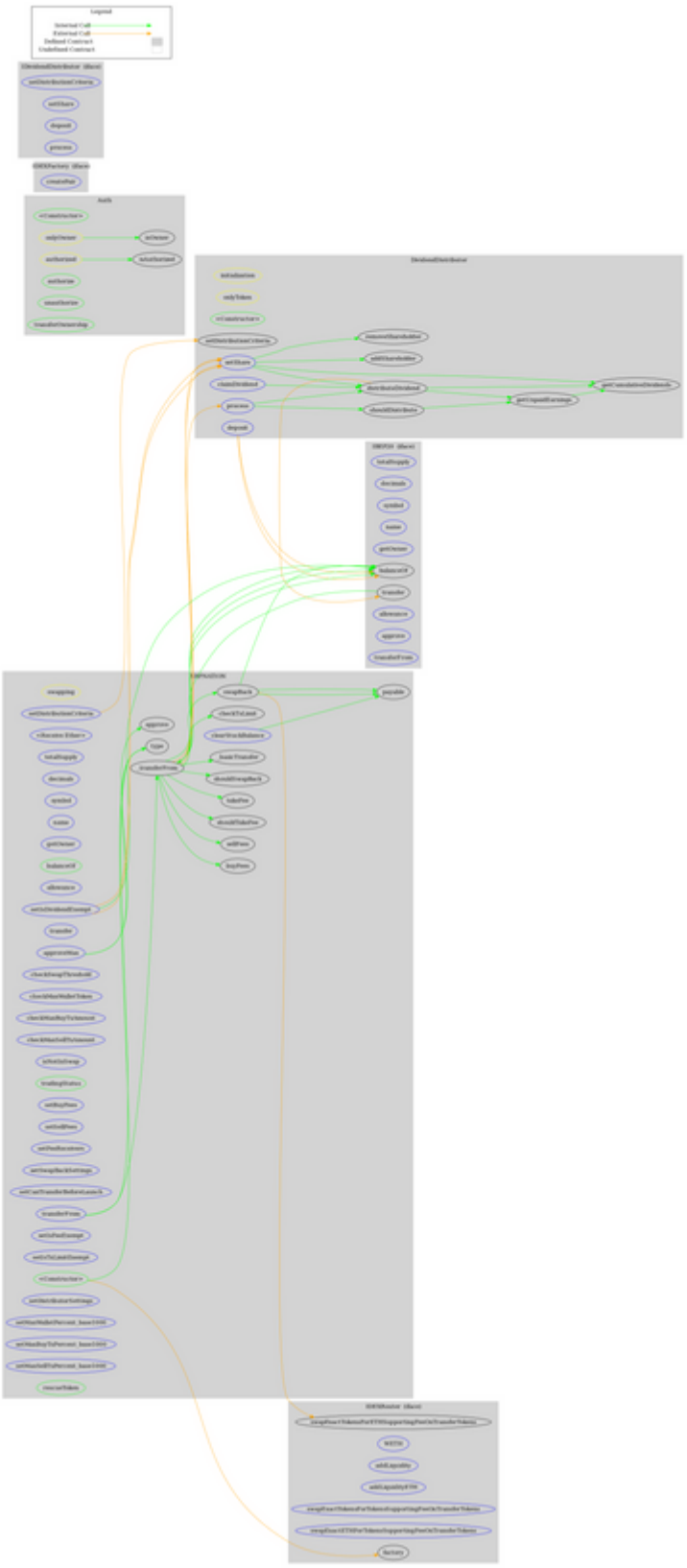
Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
IBEP20	Interface			
	totalSupply	External		-
	decimals	External		-
	symbol	External		-
	name	External		-
	getOwner	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
Auth	Implementation			
	<Constructor>	Public	✓	-
	authorize	Public	✓	onlyOwner
	unauthorize	Public	✓	onlyOwner
	isOwner	Public		-
	isAuthorized	Public		-
	transferOwnership	Public	✓	onlyOwner
IDEXFactory	Interface			
	createPair	External	✓	-
IDEXRouter	Interface			
	factory	External		-
	WETH	External		-
	addLiquidity	External	✓	-
	addLiquidityETH	External	Payable	-

	swapExactTokensForTokensSupportingFeeOnTransferTokens	External	✓	-
	swapExactETHForTokensSupportingFeeOnTransferTokens	External	Payable	-
	swapExactTokensForETHSupportingFeeOnTransferTokens	External	✓	-
IDividendDistributor	Interface			
	setDistributionCriteria	External	✓	-
	setShare	External	✓	-
	deposit	External	Payable	-
	process	External	✓	-
DividendDistributor	Implementation	IDividendDistributor		
	<Constructor>	Public	✓	-
	setDistributionCriteria	External	✓	onlyToken
	setShare	External	✓	onlyToken
	deposit	External	Payable	onlyToken
	process	External	✓	onlyToken
	shouldDistribute	Internal		
	distributeDividend	Internal	✓	
	claimDividend	External	✓	-
	getUnpaidEarnings	Public		-
	getCumulativeDividends	Internal		
	addShareholder	Internal	✓	
	removeShareholder	Internal	✓	
XRPNATION	Implementation	IBEP20, Auth		
	<Constructor>	Public	✓	Auth
	<Receive Ether>	External	Payable	-
	totalSupply	External		-
	decimals	External		-
	symbol	External		-
	name	External		-

	getOwner	External		-
	balanceOf	Public		-
	allowance	External		-
	approve	Public	✓	-
	approveMax	External	✓	-
	transfer	External	✓	-
	transferFrom	External	✓	-
	_transferFrom	Internal	✓	
	_basicTransfer	Internal	✓	
	checkTxLimit	Internal	✓	
	buyFees	Internal	✓	
	sellFees	Internal	✓	
	shouldTakeFee	Internal		
	takeFee	Internal	✓	
	shouldSwapBack	Internal		
	swapBack	Internal	✓	swapping
	checkSwapThreshold	External		-
	checkMaxWalletToken	External		-
	checkMaxBuyTxAmount	External		-
	checkMaxSellTxAmount	External		-
	isNotInSwap	External		-
	tradingStatus	Public	✓	authorized
	setBuyFees	External	✓	authorized
	setSellFees	External	✓	authorized
	setFeeReceivers	External	✓	authorized
	setSwapBackSettings	External	✓	authorized
	setCanTransferBeforeLaunch	External	✓	authorized
	setIsDividendExempt	External	✓	authorized
	setIsFeeExempt	External	✓	authorized
	setIsTxLimitExempt	External	✓	authorized
	setDistributionCriteria	External	✓	authorized
	setDistributorSettings	External	✓	authorized
	setMaxWalletPercent_base1000	External	✓	onlyOwner
	setMaxBuyTxPercent_base1000	External	✓	onlyOwner
	setMaxSellTxPercent_base1000	External	✓	onlyOwner

	rescueToken	Public	✓	onlyOwner
	clearStuckBalance	External	✓	authorized

Contract Flow



Domain Info

Domain Name	xrpnation.app
Registry Domain ID	4858E696C-APP
Creation Date	2022-01-15T17:46:36Z
Updated Date	2022-01-20T17:46:36Z
Registry Expiry Date	2023-01-15T17:46:36Z
Registrar WHOIS Server	whois.nic.google
Registrar URL	http://www.tldregistrarsolutions.com/
Registrar	TLD Registrar Solutions Ltd
Registrar IANA ID	1564

The domain has been created 9 days 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

The XRPNATION token rewards our holders with passive income in XRP with every transaction being made. There are some functions that can be abused by the owner, like manipulating fees, stopping transactions and stopping the sales. 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