Audit Report

Christmas Token

December 2021

Type	BEP20
Address	0xa1629e42f86680592DCcdAe47B51e8f17c42aD71
Audited by	© coinscope

Table of Contents

Contract Review

Contract Name	XMAS
Compiler Version	v0.6.12+commit.27d51765
Optimization	200 runs
Licence	MIT
Explorer	https://bscscan.com/token/0xa1629e42f86680592DCcdAe47B51e8f17c42aD71
Symbol	XMAS
Decimals	18
Total Supply	1,000,000,000
Website	https://christmastoken.finance/

Audit Updates

Initial Audit	9th 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 or pause transactions
✓	Contract Owner is not able to transfer tokens from specific address
✗	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/0xa1629e42f86680592DCcdAe47B51e8f17c42aD71#code#L1478,L1484,L1490

Description

The contract owner has the authority to increase fees to the maximum value of MAX_FEE_RATE that is 25%. The owner may take advantage of it by calling the `updateMarketingFee` function with a high percentage value like 25.

```
function updateMarketingFee(uint8 newFee) external onlyOwner {
    require(newFee <= MAX_FEE_RATE, "wrong");
    marketingFee = newFee;
    totalFees = BNBRewardsFee.add(marketingFee).add(liquidityFee);
}
```

Recommendation

The contract could decrease the value of MAX_FEE_RATE to a value less than 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.

LTW - Liquidity to Team Wallet

Criticality	high
Location	https://bscscan.com/address/0xa1629e42f86680592DCcdAe47B51e8f17c42aD71#code#L1616

Description

The contract owner has the authority to transfer funds to the team wallet. These funds have been swapped from the swap & liquify feature. The owner may take advantage of it by setting a high fee to the marketingFee variable.

```
contractTokenBalance * (marketingFee/totalFees) =
contractTokenBalance * (25/100) =
contractTokenBalance * 0.25
```

```
uint256 swapMarketingTokens = contractTokenBalance
    .mul(marketingFee)
    .div(totalFees);
swapAndSendMarketingBNB(swapMarketingTokens);
```

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

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	✓	-
IERC20Metadata	Interface	IERC20		
	name	External		-
	symbol	External		-
	decimals	External		-
Context	Implementation			

	_msgSender	Internal		
	_msgData	Internal		
Ownable	Implementation	Context		
		Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
SafeMath	Library			
	add	Internal		
	sub	Internal		
	sub	Internal		
	mul	Internal		
	div	Internal		
	div	Internal		
	mod	Internal		
	mod	Internal		

IterableMapping	Library			
	get	Public		-
	getIndexOfKey	Public		-
	getKeyAtIndex	Public		-
	size	Public		-
	set	Public	✓	-
	remove	Public	✓	-
SafeMathUint	Library			
	toInt256Safe	Internal		
SafeMathInt	Library			
	mul	Internal		
	div	Internal		
	sub	Internal		
	add	Internal		
	abs	Internal		
	toUint256Safe	Internal		

DividendPaying TokenInterface	Interface			
	dividendOf	External		-
	distributeDividends	External	Payable	-
	withdrawDividend	External	✓	-
DividendPaying TokenOptionalIn terface	Interface			
	withdrawableDividendOf	External		-
	withdrawnDividendOf	External		-
	accumulativeDividendOf	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		-
	mint	External	✓	-
	burn	External	✓	-
	swap	External	✓	-
	skim	External	✓	-
	sync	External	✓	-

	initialize	External	✓	-
IUniswapV2Factory	Interface			
	feeTo	External		-
	feeToSetter	External		-
	getPair	External		-
	allPairs	External		-
	allPairsLength	External		-
	createPair	External	✓	-
	setFeeTo	External	✓	-
	setFeeToSetter	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	✓	-
ERC20	Implementation	Context, IERC20, IERC20Metadata		
		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	✓	
	_beforeTokenTransfer	Internal	✓	
DividendPaying Token	Implementation	ERC20, DividendPayingTokenInterface, DividendPayingTokenOptionalInterface		
		Public	✓	ERC20
		External	Payable	-
	distributeDividends	Public	Payable	-
	withdrawDividend	Public	✓	-
	_withdrawDividendOfUser	Internal	✓	
	dividendOf	Public		-
	withdrawableDividendOf	Public		-
	withdrawnDividendOf	Public		-
	accumulativeDividendOf	Public		-

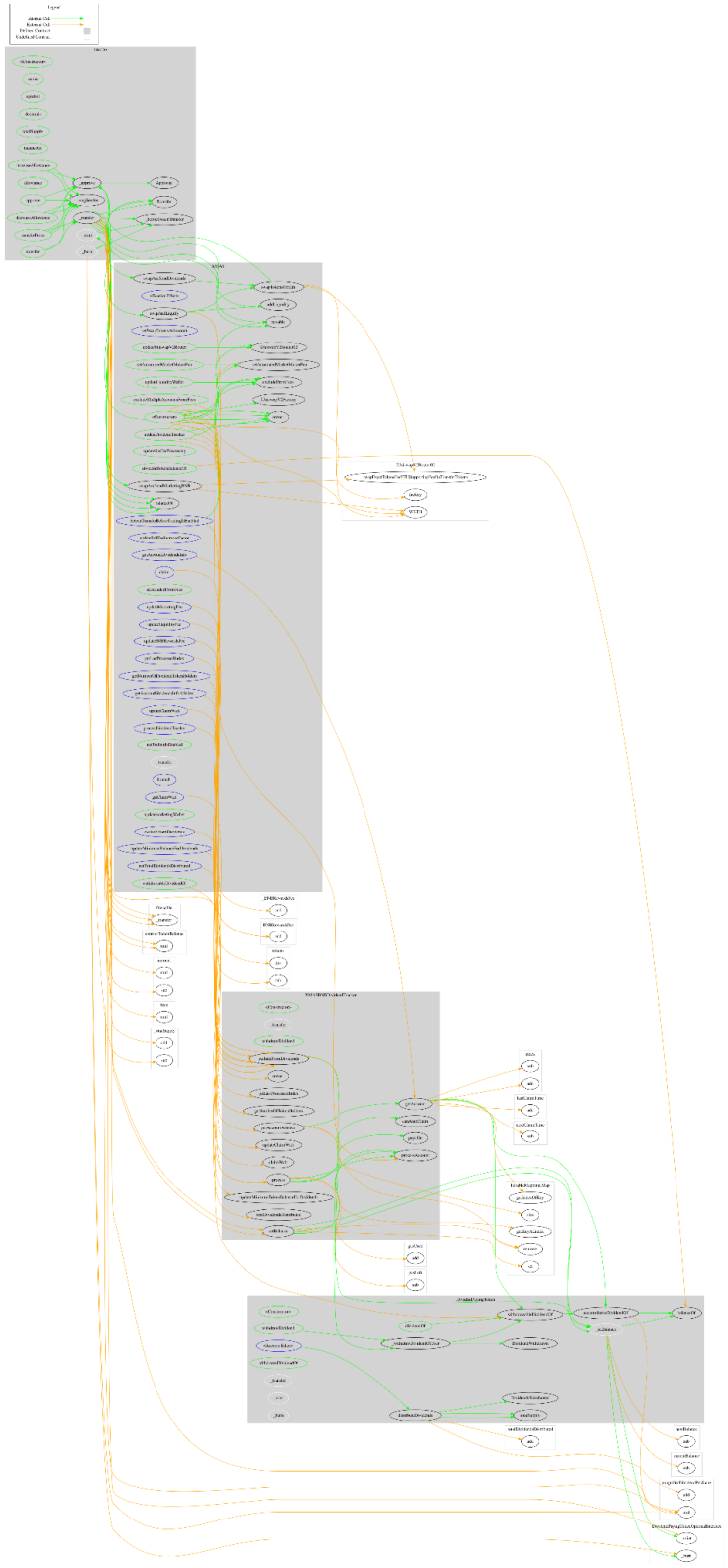
	_transfer	Internal	✓	
	_mint	Internal	✓	
	_burn	Internal	✓	
	_setBalance	Internal	✓	
XMAS	Implementation	ERC20, Ownable		
		Public	✓	ERC20
		External	Payable	-
	updateDividendTracker	Public	✓	onlyOwner
	setSwapTokensAtAmount	External	✓	onlyOwner
	updateMinimumBalanceForDividends	External	✓	onlyOwner
	updateUniswapV2Router	Public	✓	onlyOwner
	excludeFromDividends	External	✓	onlyOwner
	excludeFromFees	Public	✓	onlyOwner
	excludeMultipleAccountsFromFees	Public	✓	onlyOwner
	setAutomatedMarketMakerPair	Public	✓	onlyOwner
	_setAutomatedMarketMakerPair	Private	✓	
	updateLiquidityWallet	Public	✓	onlyOwner

	updateGasForProcessing	Public	✓	onlyOwner
	updateClaimWait	External	✓	onlyOwner
	updateBNBRewardsFee	External	✓	onlyOwner
	updateMarketingFee	External	✓	onlyOwner
	updateLiquidityFee	External	✓	onlyOwner
	updateSellFeeIncreaseFactor	External	✓	onlyOwner
	getClaimWait	External		-
	getTotalDividendsDistributed	External		-
	isExcludedFromFees	Public		-
	withdrawableDividendOf	Public		-
	dividendTokenBalanceOf	Public		-
	getAccountDividendsInfo	External		-
	getAccountDividendsInfoAtIndex	External		-
	processDividendTracker	External	✓	-
	claim	External	✓	-
	getLastProcessedIndex	External		-
	getNumberOfDividendTokenHolders	External		-
	getTradingIsEnabled	Public		-
	_transfer	Internal	✓	

	Launch	External	✓	onlyOwner
	SetcanTransferBeforeTradingIsEnabled	External	✓	onlyOwner
	updatemarketingWallet	Public	✓	onlyOwner
	swapAndLiquify	Private	✓	
	swapTokensForEth	Private	✓	
	swapAndSendMarketingBNB	Private	✓	
	addLiquidity	Private	✓	
	swapAndSendDividends	Private	✓	
XMASBNBDividendTracker	Implementation	DividendPayingToken, Ownable		
		Public	✓	DividendPayingToken
	_transfer	Internal	✓	
	withdrawDividend	Public	✓	-
	updateMinimumTokenBalanceForDividends	External	✓	onlyOwner
	excludeFromDividends	External	✓	onlyOwner
	updateClaimWait	External	✓	onlyOwner
	getLastProcessedIndex	External		-

	getNumberOfTokenHolders	External		-
	getAccount	Public		-
	getAccountAtIndex	Public		-
	canAutoClaim	Private		
	setBalance	External	✓	onlyOwner
	process	Public	✓	-
	processAccount	Public	✓	onlyOwner

Contract Flow



Domain Info

Domain Name	christmastoken.finance
Registry Domain ID	ecb935cc2c7f48cc9345359831b6975c-DONUTS
Registrar WHOIS Server	whois.name.com
Registrar URL	http://www.name.com
Updated Date	2021-12-05T02:32:36Z
Creation Date	2021-12-05T02:31:13Z
Registry Expiry Date	2022-12-05T02:31:13Z
Registrar	Name.com, Inc.
Registrar IANA ID	625

The domain has been created one month before the creation of the audit. It will expire in one year.

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

Summary

Christmas tokens is a seasonal token that is aiming to give Christmas gifts for kids in orphanages from the charity wallet. The token has a friendly and growing community. 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 25%. A multi-wallet signing pattern or renouncing the 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