



Audit Report

XENOVERSE

December 2021

Type BEP20

Address 0xcb9fD3784e9F369C4AD3BD4CB0d3a21aCbF23a51

Audited by © coinscope

Table of Contents

Table of Contents	1
Contract Review	2
Audit Updates	2
ELFM - Exceed Limit Fees Manipulation	3
Description	4
Recommendation	4
LTW - Liquidity to Team Wallet	4
Description	5
Recommendation	5
OCTD - Owner Contract Tokens Drain	6
Description	6
Recommendation	6
Contract Diagnostics	7
Contract Functions	8
Contract Flow	17
Domain Info	19
Summary	20
Disclaimer	21
About Coinscope	22

Contract Review

Contract Name	xenoX
Compiler Version	v0.8.6+commit.11564f7e
Optimization	No with 200 runs
Licence	MIT
Explorer	https://bscscan.com/token/0xcb9fD3784e9F369C4AD3BD4CB0d3a21aCbF23a51
Symbol	xenoX
Decimals	9
Total Supply	100,000,000
Website	https://xenoversecrypto.com/

Audit Updates

Initial Audit	19th of 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 (10%)
●	ST	Contract Owner is not able to stop or pause transactions
●	OCTD	Contract Owner is not able to transfer tokens 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	high
Location	https://bscscan.com/address/0xcb9fd3784e9f369c4ad3bd4cb0d3a21acbf23a51#code#L1083,L1087,L1091,L1095,L1099,L1103

Description

The contract owner has the authority to increase fees to any value without limitations. This can be used in a malicious way and disturb the holders' transactions.

```
function setSelldevFeePercent(uint256 devFee) external onlyOwner() {  
    _selldevFee = devFee;  
}
```

Recommendation

The contract could have a limitation to require the fees to not exceed a value more 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/0xcb9fd3784e9f369c4ad3bd4cb0d3a21acbf23a51#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.

```
// dev Portion
uint256 devBalance = newBalance.div(totalLiqFee).mul(_devFee);
uint256 devPortion = otherHalf.div(totalLiqFee).mul(_devFee);

uint256 finalBalance = newBalance.sub(devBalance);
uint256 finalHalf = otherHalf.sub(devPortion);

(bool sent,) = _devAddress.call{value: devBalance}("");

if (sent) {
    _tokenTransfer(address(this), _devAddress, devPortion, false);
} else {
    addLiquidity(devPortion, devBalance, _devAddress);
}
```

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.

OCTD - Owner Contract Tokens Drain

Criticality	high
Location	https://bscscan.com/address/0xcb9fd3784e9f369c4ad3bd4cb0d3a21acbf23a51#code#L1116

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 `transferTokens` function.

```
function transferTokens(address receipient, uint256 amount) public onlyOwner {  
    require(balanceOf(address(this)) >= amount, "Attempt to transfer a  
greater amount than allowed");  
    token.transfer(receipient, amount);  
}
```

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
IPancakeRouter01	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		-
IPancakeRouter02	Interface	IPancakeRouter01		
	removeLiquidityETHSupportingFeeOnTransferTokens	External	✓	-
	removeLiquidityETHWithPermitSupportingFeeOnTransferTokens	External	✓	-
	swapExactTokensForTokensSupportingFeeOnTransferTokens	External	✓	-
	swapExactETHForTokensSupportingFeeOnTransferTokens	External	Payable	-
	swapExactTokensForETHSupportingFeeOnTransferTokens	External	✓	-
IPancakeFactory	Interface			
	feeTo	External		-

	feeToSetter	External		-
	getPair	External		-
	allPairs	External		-
	allPairsLength	External		-
	createPair	External	✓	-
	setFeeTo	External	✓	-
	setFeeToSetter	External	✓	-
IPancakePair	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	✓	-
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		
Address	Library			
	isContract	Internal		
	sendValue	Internal	✓	
	functionCall	Internal	✓	
	functionCall	Internal	✓	

	functionCallWithValue	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionStaticCall	Internal		
	functionStaticCall	Internal		
	functionDelegateCall	Internal	✓	
	functionDelegateCall	Internal	✓	
	verifyCallResult	Internal		
IBEP20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	transferFrom	External	✓	-
	approve	External	✓	-
	allowance	External		-
Ownable	Implementation			
	_msgSender	Internal		
	_msgData	Internal		

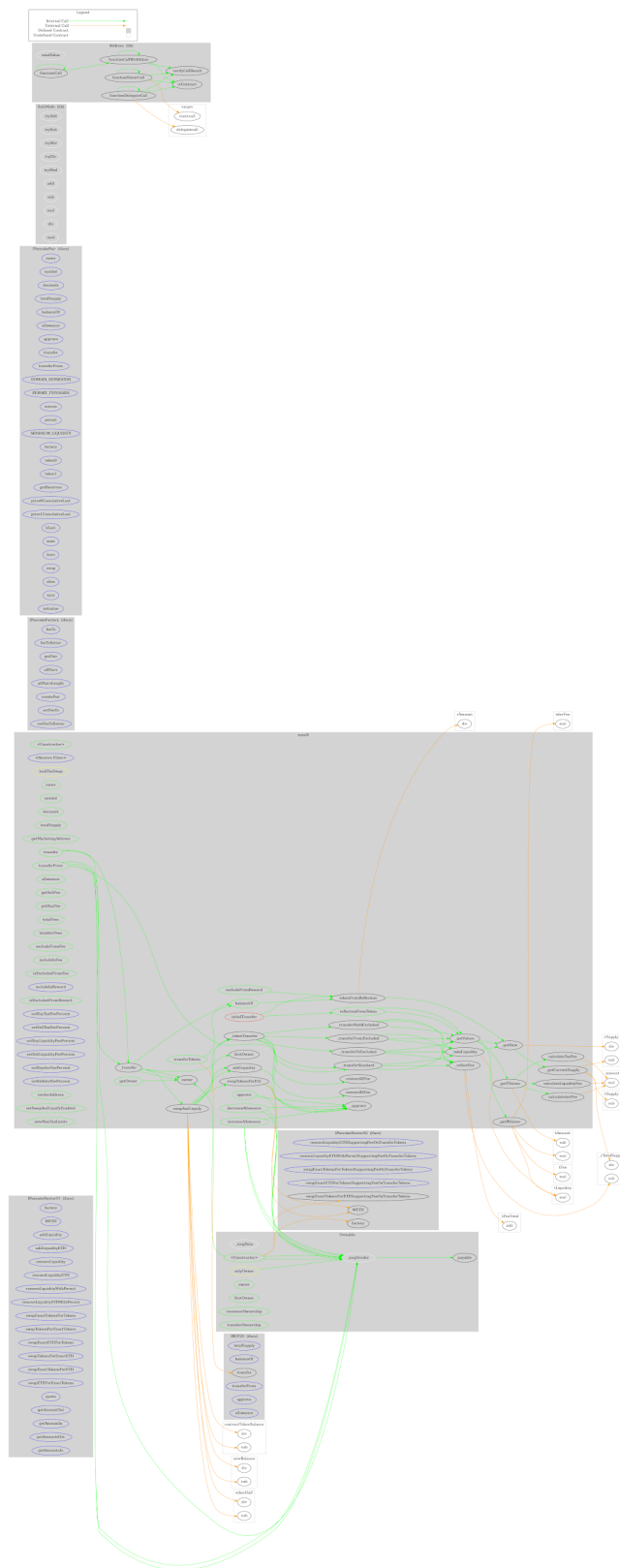
		Public	✓	-
	owner	Public		-
	firstOwner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
xenoX	Implementation	IBEP20, Ownable		
		Public	✓	-
		External	Payable	-
	name	Public		-
	symbol	Public		-
	decimals	Public		-
	totalSupply	Public		-
	balanceOf	Public		-
	getOwner	Public		-
	getMarketingAddress	Public		-
	transfer	Public	✓	-

	transferFrom	Public	✓	-
	approve	Public	✓	-
	allowance	Public		-
	increaseAllowance	Public	✓	-
	decreaseAllowance	Public	✓	-
	getSellFee	Public		-
	getBuyFee	Public		-
	totalFees	Public		-
	totaldevFees	Public		-
	excludeFromFee	Public	✓	onlyOwner
	includeInFee	Public	✓	onlyOwner
	isExcludedFromFee	Public		-
	excludeFromReward	Public	✓	onlyOwner
	includeInReward	External	✓	onlyOwner
	isExcludedFromReward	Public		-
	setBuyTaxFeePercent	External	✓	onlyOwner
	setSellTaxFeePercent	External	✓	onlyOwner

	setBuyLiquidityFeePercent	External	✓	onlyOwner
	setSellLiquidityFeePercent	External	✓	onlyOwner
	setBuydevFeePercent	External	✓	onlyOwner
	setSelldevFeePercent	External	✓	onlyOwner
	setdevAddress	Public	✓	onlyOwner
	setSwapAndLiquifyEnabled	Public	✓	onlyOwner
	transferTokens	Public	✓	onlyOwner
	newMaxTxnLimits	Public	✓	onlyOwner
	reflectionFromToken	Public		-
	tokenFromReflection	Public		-
	_transfer	Private	✓	
	_approve	Private	✓	
	_getValues	Private		
	_getTValues	Private		
	_getRValues	Private		
	_getRate	Private		

	_getCurrentSupply	Private		
	calculateTaxFee	Private		
	calculateLiquidityFee	Private		
	calculatedevFee	Private		
	swapAndLiquify	Private	✓	lockTheSwap
	swapTokensForEth	Private	✓	
	_tokenTransfer	Private	✓	
	addLiquidity	Private	✓	
	removeAllFee	Private	✓	
	restoreAllFee	Private	✓	
	_transferStandard	Private	✓	
	_transferToExcluded	Private	✓	
	_transferFromExcluded	Private	✓	
	_transferBothExcluded	Private	✓	
	_takeLiquidity	Private	✓	
	_reflectFee	Private	✓	
	initialTransfer	Private	✓	

Contract Flow



Domain Info

Domain Name	xenoversecrypto.com
Registry Domain ID	2661107191_DOMAIN_COM-VRSN
Registrar WHOIS Server	whois.google.com
Registrar URL	http://www.google.com
Updated Date	2021-12-12T10:13:49Z
Creation Date	2021-12-12T10:13:47Z
Registry Expiry Date	2022-12-12T10:13:47Z
Registrar	Google LLC
Registrar IANA ID	895

The domain has been created almost 10 days before the analysis of the audit. It is set for expiration in one year.

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

Summary

Project Xenoverse \$XENOX aims to integrate into GameFi and Metaverse. The team is building a game using Unreal Engine 5 according to their website. The token has a friendly and growing community. There are some functions that can be abused by the owner, like manipulating fees to any amount without limitations, and also changing the amount of liquidity taken by the Dev team. 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>