Cyberscope

Audit Report

TokenVesting

October 2022

Github https://github.com/moonappxxx/moonapp-contracts

Commit 849ced7b7b96948529d46f9295717ec5a1620f4f

Audited by © cyberscope

Table of Contents

Introduction

The contract TokenVesting implements a vesting contract. The token vesting contract allows the users to release their vesting gradually. The contract provides four methods. It provides a release method to withdraw tokens gradually to the beneficiary. There are there more methods in order to monitor the vesting functionality.

Contract Review

Contract Name	TokenVesting
Compiler Version	v0.8.11+commit.d7f03943
Github	https://github.com/moonappxxx/moonapp-contracts
Commit	849ced7b7b96948529d46f9295717ec5a1620f4f
Testing Deploy	https://testnet.bscscan.com/token/0xa82DfCe9c53e528680653Ca2b9e4d7d2Ff87C6F4
Domain	https://moonapp.org

Audit Updates

Initial Audit	3rd October 2022 https://github.com/cyberscope-io/audits/blob/main/1-xxx/v1/tokenVesting.pdf
Corrected	7th October 2022

Source Files

Filename	SHA256
@openzeppelin/contracts/access/Ownable.sol	9353af89436556f7ba8abb3f37a6677249aa4df6024fbfaa94f79ab2f44f3231
@openzeppelin/contracts/token/ERC20/ERC20.sol	5031430cc2613c32736d598037d3075985a2a09e61592a013dbd09a5bc2041b8
@openzeppelin/contracts/token/ERC20/extensions/draft-IERC20Permit.sol	3e7aa0e0f69eec8f097ad664d525e7b3f0a3fda8dcdd97de5433ddb131db86ef
@openzeppelin/contracts/token/ERC20/extensions/ERC20Burnable.sol	0344809a1044e11ece2401b4f7288f414ea41fa9d1dad24143c84b737c9fc02e
@openzeppelin/contracts/token/ERC20/extensions/IERC20Metadata.sol	af5c8a77965cc82c33b7ff844deb9826166689e55dc037a7f2f790d057811990
@openzeppelin/contracts/token/ERC20/IERC20.sol	94f23e4af51a18c2269b355b8c7cf4db8003d075c9c541019eb8dcf4122864d5
@openzeppelin/contracts/token/ERC20/utils/SafeERC20.sol	fa36a21bd954262006d806b988e4495562e7b50420775e2aa0deecb596fd1902
@openzeppelin/contracts/utils/Address.sol	1e0922f6c0bf6b1b8b4d480dcabb691b1359195a297bde6dc5172e79f3a1f826

@openzeppelin/contracts/utils/Context.sol	1458c260d010a08e4c20a4a517882259a23a4baa0b5bd9add9fb6d6a1549814a
@openzeppelin/contracts/utils/math/Math.sol	929523c09910460ad708c75878d89b9fbed12b65cb5d8b670200c793131072f4
@openzeppelin/contracts/utils/math/SafeMath.sol	0dc33698a1661b22981abad8e5c6f5ebca0dfe5ec14916369a2935d888ff257a
contracts/Governed.sol	216f03644d4e517caba4b44b8f3b74c358462601918a7be264790ef1cc1bde4c
contracts/MoonappToken.sol	bc938fcfe911c7df6871209c77bf053a2f1b4b9bab19f7c6d45a4feeae03e9d6
contracts/TokenVesting.sol	66f193371f6346b5fa85acf98fbadcd29c4b5e7468728ab94d4f341d1e3c0fdc

Contract Diagnostics

Critical Medium Minor / Informative

Severity	Code	Description	Status
	VCL	Vesting Contract Logic	Unresolved
	L01	Public Function could be Declared External	Unresolved
	L13	Divide before Multiply Operation	Unresolved

VCL - Vesting Contract Logic

Criticality	minor / informative
Location	contracts/TokenVesting.sol
Status	Unresolved

Description

The contract is not operating as a vesting contract because the amount is not transferred and locked on the contract. As a result, the vesting state may be correct but there is no guarantee that the amount is vested. This contract is operating properly only if it is combined with the Seed contract.

```
constructor(
    address _beneficiary,
    uint256 _start,
    uint256 _cliff,
    uint256 _releaseRate,
    uint256 _releasedInitially
) {
    ...
}
```

Recommendation

The vesting period should start when the contract receive the corresponding vesting amount. For instance, the constructor could initiate a transfer from the Seed to the Vest contract.

L08 - Tautology or Contradiction

Criticality	minor / informative
Location	contracts/TokenVesting.sol#L39
Status	Unresolved

Description

Detects expressions that are tautologies or contradictions. For instance, an uint variable will always be greater than or equal to zero.

```
require(bool)(_releasedInitially >= 0)
```

Recommendation

Fix the incorrect comparison by changing the value type or the comparison.

L13 - Divide before Multiply Operation

Criticality	minor / informative
Location	contracts/TokenVesting.sol#L94
Status	Unresolved

Description

Performing divisions before multiplications may cause lose of prediction.

```
monthsGone = (block.timestamp - cliff) / (60 * 60 * 24 * 30)
```

Recommendation

The multiplications should be prior to the divisions.

Contract Functions

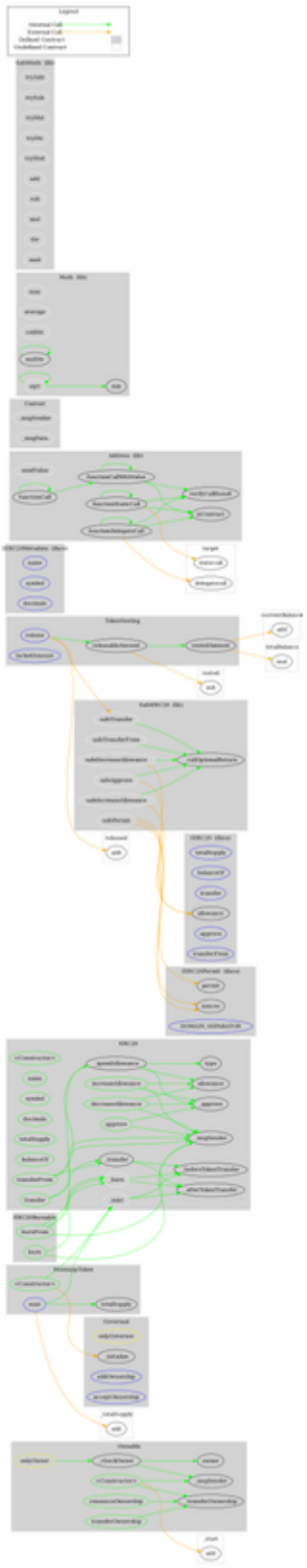
Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
Ownable	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	_checkOwner	Internal		
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	_transferOwnership	Internal	✓	
ERC20	Implementation	Context, 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	✓	
IERC20Permit	Interface			
	permit	External	✓	-
	nonces	External		-
	DOMAIN_SEPARATOR	External		-
ERC20Burnable	Implementation	Context, ERC20		
	burn	Public	✓	-
	burnFrom	Public	✓	-
IERC20Metadata	Interface	IERC20		
	name	External		-
	symbol	External		-
	decimals	External		-
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
SafeERC20	Library			
	safeTransfer	Internal	✓	
	safeTransferFrom	Internal	✓	
	safeApprove	Internal	✓	
	safeIncreaseAllowance	Internal	✓	
	safeDecreaseAllowance	Internal	✓	
	safePermit	Internal	✓	
	_callOptionalReturn	Private	✓	

Address	Library			
	isContract	Internal		
	sendValue	Internal	✓	
	functionCall	Internal	✓	
	functionCall	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionStaticCall	Internal		
	functionStaticCall	Internal		
	functionDelegateCall	Internal	✓	
	functionDelegateCall	Internal	✓	
	verifyCallResult	Internal		
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
Math	Library			
	max	Internal		
	min	Internal		
	average	Internal		
	ceilDiv	Internal		
	mulDiv	Internal		
	mulDiv	Internal		
	sqrt	Internal		
	sqrt	Internal		
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		
Governed	Implementation			
	_initialize	Internal	✓	
	addOwnership	External	✓	onlyGovernor
	acceptOwnership	External	✓	-
MoonappToken	Implementation	ERC20, ERC20Burnable, Governed		
	<Constructor>	Public	✓	ERC20
	burnFrom	Public	✓	onlyGovernor
	mint	External	✓	onlyGovernor
TokenVesting	Implementation	Ownable		
	<Constructor>	Public	✓	-
	release	External	✓	-
	releasableAmount	Public		-
	vestedAmount	Public		-
	lockedAmount	External		-

Contract Flow



Domain Info

Domain Name	moonapp.org
Registry Domain ID	ebf9cc2ae696406f89ddb496f15a1e47-LROR
Creation Date	2022-01-23T16:44:59Z
Updated Date	2022-03-25T03:49:23Z
Registry Expiry Date	2023-01-23T16:44:59Z
Registrar WHOIS Server	http://whois.reg.com
Registrar URL	http://www.reg.com
Registrar	Registrar of Domain Names REG.RU LLC
Registrar IANA ID	1606

The domain was created 8 months before the creation of the audit. It will expire in 4 months.

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

Summary

The TokenVesting contract operates as a vesting contract for the Moon App ecosystem. The Smart Contract analysis reported no compiler error or critical issues. This audit focused on investigating possible security issues and potential improvements.

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