Cyberscope

Audit Report

Lanco - Decentralized Freelancing Platform

July 2023

Network	BSC
Address	0x270fdb771725e1718f9937ce4f79bc3405ae2614
Audited by	© cyberscope

Analysis

Critical Medium Minor / Informative Pass

Severity	Code	Description	Status
●	ST	Stops Transactions	Passed
●	OTUT	Transfers User's Tokens	Passed
●	ELFM	Exceeds Fees Limit	Passed
●	MT	Mints Tokens	Passed
●	BT	Burns Tokens	Passed
●	BC	Blacklists Addresses	Passed

Diagnostics

Critical Medium Minor / Informative

Severity	Code	Description	Status
	L13	Divide before Multiply Operation	Unresolved

Table of Contents

Review

Contract Name	Lanco
Compiler Version	v0.8.20+commit.a1b79de6
Optimization	200 runs
Explorer	https://bscscan.com/address/0x270fdb771725e1718f9937ce4f79bc3405ae2614
Address	0x270fdb771725e1718f9937ce4f79bc3405ae2614
Network	BSC
Symbol	$LANC
Decimals	18
Total Supply	1,000,000,000

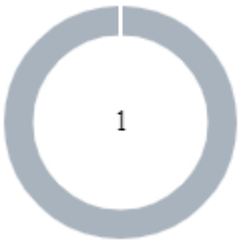
Audit Updates

Initial Audit	31 Jul 2023 https://github.com/cyberscope-io/audits/blob/main/lanc/v1/audit.pdf
Corrected Phase 2	07 Aug 2023

Source Files

Filename	SHA256
src/Vesting.sol	a212a9b7352682b53bdd1968d0fd0575426f32e3934bbeb95d34f2f52a869c3e
src/LancToken.sol	b50fff2f3fc82dc56af0f6d68749ce6fa03cbd193ecbac76bbfad80e72a32b89
@openzeppelin/contracts/utils/Context.sol	1458c260d010a08e4c20a4a517882259a23a4baa0b5bd9add9fb6d6a1549814a
@openzeppelin/contracts/utils/Address.sol	8b85a2463eda119c2f42c34fa3d942b61aee65df381f48ed436fe8edb3a7d602
@openzeppelin/contracts/token/ERC20/IERC20.sol	7ebde70853ccafcf1876900dad458f46eb9444d591d39bfc58e952e2582f5587
@openzeppelin/contracts/token/ERC20/ERC20.sol	d20d52b4be98738b8aa52b5bb0f88943f62128969b33d654fbca731539a7fe0a
@openzeppelin/contracts/token/ERC20/utils/SafeERC20.sol	c8309ed2c1c7edf52a23833798c94507702248debfc4ed1f645e571e3c230f8b
@openzeppelin/contracts/token/ERC20/extensions/IERC20Permit.sol	b7383c48331f3cc9901fc05e5d5830fcd533699a77f3ee1e756a98681bfbb2ee
@openzeppelin/contracts/token/ERC20/extensions/IERC20Metadata.sol	af5c8a77965cc82c33b7ff844deb9826166689e55dc037a7f2f790d057811990
@openzeppelin/contracts/finance/VestingWallet.sol	c9f8d2f9404b4c16465cf6db64cbdd9cdde5a7a1083a768bd9e5b94dcfadc5b0
@openzeppelin/contracts/access/Ownable.sol	a8e4e1ae19d9bd3e8b0a6d46577eec098c01fbaffd3ec1252fd20d799e73393b

Findings Breakdown



Critical	0
Medium	0
Minor / Informative	1

Severity	Unresolved	Acknowledged	Resolved	Other
Critical	0	0	0	0
Medium	0	0	0	0
Minor / Informative	1	0	0	0

L13 - Divide before Multiply Operation

Criticality	Minor / Informative
Location	src/Vesting.sol#L36,39
Status	Unresolved

Description

It is important to be aware of the order of operations when performing arithmetic calculations. This is especially important when working with large numbers, as the order of operations can affect the final result of the calculation. Performing divisions before multiplications may cause loss of prediction.

```
uint256 elapsedIntervel = (timestamp - start()) / intervel()
return
                (totalAllocation * elapsedIntervel) / (duration() /
intervel())
```

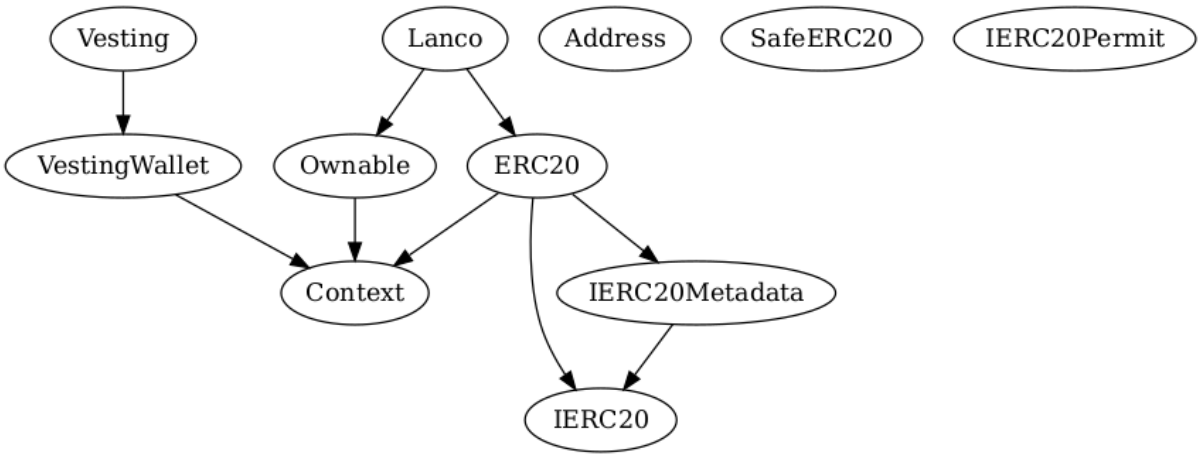
Recommendation

To avoid this issue, it is recommended to carefully consider the order of operations when performing arithmetic calculations in Solidity. It's generally a good idea to use parentheses to specify the order of operations. The basic rule is that the multiplications should be prior to the divisions.

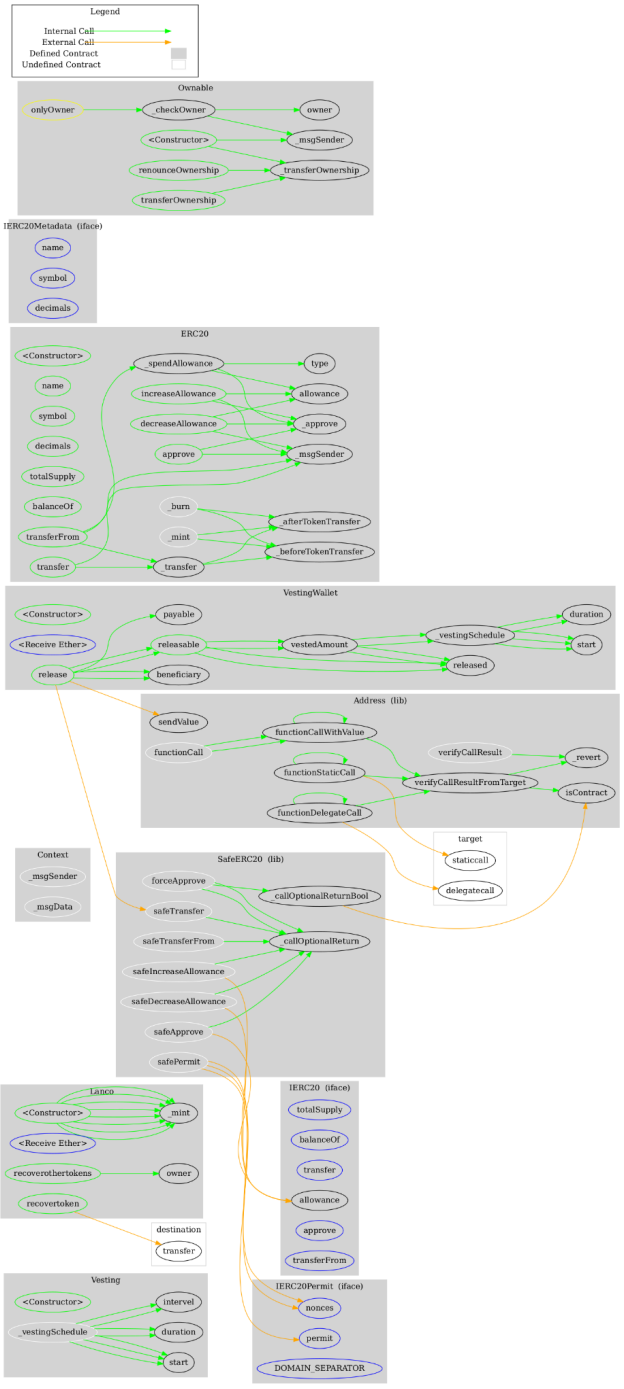
Functions Analysis

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
Vesting	Implementation	VestingWallet		
		Public	Payable	VestingWallet
	intervel	Public		-
	_vestingSchedule	Internal		
Lanco	Implementation	ERC20, Ownable		
		Public	✓	-
		External	Payable	-
	recoverothertokens	Public	✓	onlyOwner
	recovertoken	Public	✓	onlyOwner

Inheritance Graph



Flow Graph


Legend
Internal Call
External Call
Defined Contract
Undefined Contract
Ownable
onlyOwner
checkOwner
owner
<Constructor>
_msgSender
renounceOwnership
transferOwnership
transferOwnership
IERC20Metadata (iface)
name
symbol
decimals
ERC20
<Constructor>
name
symbol
decimals
totalSupply
balanceOf
transferFrom
transfer
spendAllowance
increaseAllowance
decreaseAllowance
approve
type
allowance
_approve
_msgSender
_burn
_mint
transfer
_afterTokenTransfer
_beforeTokenTransfer
VestingWallet
<Constructor>
<Receive Ether>
release
payable
releasable
beneficiary
vestedAmount
vestingSchedule
released
duration
start
Address (lib)
sendValue
functionCall
functionCallWithValue
functionStaticCall
functionDelegateCall
verifyCallResult
verifyCallResultFromTarget
_revert
isContract
target
staticcall
delegatecall
Context
_msgSender
_msgData
SafeERC20 (lib)
forceApprove
safeTransfer
safeTransferFrom
safeIncreaseAllowance
safeDecreaseAllowance
safeApprove
safePermit
_callOptionalReturnBool
_callOptionalReturn
Lanco
<Constructor>
<Receive Ether>
recoverothertokens
recovertoken
_mint
owner
destination
transfer
IERC20 (iface)
totalSupply
balanceOf
transfer
allowance
approve
transferFrom
Vesting
<Constructor>
_vestingSchedule
intervel
duration
start
IERC20Permit (iface)
nonces
permit
DOMAIN_SEPARATOR

Summary

Lanco - Decentralized Freelancing Platform. contract implements a token mechanism. This audit investigates security issues, business logic concerns, and potential improvements. Lanco - Decentralized Freelancing Platform. is an interesting project that has a friendly and growing community. The Smart Contract analysis reported no compiler errors or critical issues. The Contract Owner can access some admin functions that can not be used in a malicious way to disturb the users' transactions.

Disclaimer

The information provided in this report does not constitute investment, financial or trading advice and you should not treat any of the document's content as such. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes nor may copies be delivered to any other person other than the Company without Cyberscope's prior written consent. This report is not nor should be considered an "endorsement" or "disapproval" of any particular project or team. This report is not nor should be regarded as an indication of the economics or value of any "product" or "asset" created by any team or project that contracts Cyberscope to perform a security assessment. This document does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors' business, business model or legal compliance. This report should not be used in any way to make decisions around investment or involvement with any particular project. This report represents an extensive assessment process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk Cyberscope's position is that each company and individual are responsible for their own due diligence and continuous security Cyberscope's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies and in no way claims any guarantee of security or functionality of the technology we agree to analyze. The assessment services provided by Cyberscope are subject to dependencies and are under continuing development. You agree that your access and/or use including but not limited to any services reports and materials will be at your sole risk on an as-is where-is and as-available basis Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives false negatives and other unpredictable results. The services may access and depend upon multiple layers of third parties.

About Cyberscope

Cyberscope is a blockchain cybersecurity company that was founded with the vision to make web3.0 a safer place for investors and developers. Since its launch, it has worked with thousands of projects and is estimated to have secured tens of millions of investors' funds.

Cyberscope is one of the leading smart contract audit firms in the crypto space and has built a high-profile network of clients and partners.

The Cyberscope team

https://www.cyberscope.io