Cyberscope

Audit Report

MoonLabs Token

April 2023

SHA256 503131e4c5848e3a6d6bed7c1c0cd113cf6b1327f41250916f1c7e2e52f42c4e

Audited by © cyberscope

Table of Contents

Review

Contract Name	MoonLabs
Testing Deploy	https://testnet.bscscan.com/address/0x3e1673aa20c037f9ffd9ca37a40ee5a1615ac5c1
Symbol	MLAB
Decimals	18
Total Supply	100.000.000

Audit Updates

Initial Audit	24 Mar 2023 https://github.com/cyberscope-io/audits/blob/main/moonlabsd/v1/token.pdf
Corrected Phase 2	06 Apr 2023

Source Files

Filename	SHA256
MoonLabs.sol	503131e4c5848e3a6d6bed7c1c0cd113cf6b1327f41250916f1c7e2e52f42c4e

Analysis

Critical Medium Minor / Informative Pass

Severity	Code	Description	Status
●	ST	Stops Transactions	Passed
●	OCTD	Transfers Contract's Tokens	Passed
●	OTUT	Transfers User's Tokens	Passed
●	ELFM	Exceeds Fees Limit	Passed
●	ULTW	Transfers Liquidity to Team Wallet	Passed
●	MT	Mints Tokens	Passed
●	BT	Burns Tokens	Passed
●	BC	Blacklists Addresses	Passed

Diagnostics

Critical Medium Minor / Informative

Severity	Code	Description	Status
●	RAV	Reentrancy Attack Vulnerability	Unresolved
●	RMC	Redundant Method Calls	Unresolved
●	MMSI	Max Mint Supply Inconsistency	Unresolved
●	DDP	Decimal Division Precision	Unresolved
●	MSC	Missing Sanity Check	Unresolved
●	RCS	Redundant Code Statement	Unresolved
●	L04	Conformance to Solidity Naming Conventions	Unresolved
●	L07	Missing Events Arithmetic	Unresolved
●	L14	Uninitialized Variables in Local Scope	Unresolved
●	L16	Validate Variable Setters	Unresolved

RAV - Reentrancy Attack Vulnerability

Criticality	Minor / Informative
Location	MoonLabs.sol#L246
Status	Unresolved

Description

The contract is vulnerable to a reentrancy attack, which can occur if a buyer initiates a trade using a contract address as the seller or by initiating a crypto trade from a contract. For instance,

A user tries to transfer tokens to manipulate NFT ownership in order to receive more rewards.

A reentrance attack will occur if the user implements a receive callback, they will have the ability to execute any method again within the same execution thread.

For instance, a user could exploit the NFT reward mechanism by manipulating NFT ownership through buying and selling transactions near the same NFT reward index, leading to potential rewards manipulation.

```
(bool sent, ) = payable(nftOwner).call{value: nftPayout}(
    ""
);
```

Recommendation

The contract could disallow the use of contract addresses for transfer transactions and the contract could aggregate all rewards distributions for the NFTs and execute them all at once at the end of the function.

RMC - Redundant Method Calls

Criticality	Minor / Informative
Location	MoonLabs.sol#L317
Status	Unresolved

Description

There are code segments that could be optimized. A segment may be optimized so that it becomes a smaller size, consumes less memory, executes more rapidly, or performs fewer operations.

If there are no fees to distribute the methods `call` and `_addLiquidity` should not be called.

```
(treasuryWallet).call{
value: (ethBalance * (buyTax.treasuryTax + sellTax.treasuryTax)) /
    totalEthFee >
    0
    ? totalEthFee
    : 1
}("");
(teamWallet).call{
value: (ethBalance * (buyTax.teamTax + sellTax.teamTax)) /
    totalEthFee >
    0
    ? totalEthFee
    : 1
}("");

_addLiquidity(
    (addToLiquidityHalf),
    ((ethBalance * liquidityTax) / totalEthFee > 0 ? totalEthFee : 1) /
        2
);
```

Recommendation

The team is advised to take these segments into consideration and rewrite them so the runtime will be more performant. That way it will improve the efficiency and performance of the source code and reduce the cost of executing it.

MMSI - Max Mint Supply Inconsistency

Criticality	Minor / Informative
Location	MoonLabs.sol#L261
Status	Unresolved

Description

The contract uses a fixed value for the maximum mint amount instead of retrieving it from the linked NFT contract. This approach can lead to a discrepancy between the actual available max mint supply of NFTs and the preset fixed max mint supply.

```
if (nftIndex < 500) {
    nftIndex++;
} else {
    nftIndex = 1;
}
```

Recommendation

It is recommended to retrieve the maximum mint value from the linked NFT contract. This approach will ensure that the maximum mint value is updated according to the available supply of NFTs. Retrieving the maximum mint value from the NFT contract will also ensure that the contract's behavior is consistent with the linked NFT contract. The contract could initial the max mint amount on the contract constructor.

DDP - Decimal Division Precision

Criticality	Minor / Informative
Location	MoonLabs.sol#L317
Status	Unresolved

Description

Division of decimal (fixed point) numbers can result in rounding errors due to the way that division is implemented in Solidity. Thus, it may produce issues with precise calculations with decimal numbers.

Solidity represents decimal numbers as integers, with the decimal point implied by the number of decimal places specified in the type (e.g. decimal with 18 decimal places). When a division is performed with decimal numbers, the result is also represented as an integer, with the decimal point implied by the number of decimal places in the type. This can lead to rounding errors, as the result may not be able to be accurately represented as an integer with the specified number of decimal places.

Hence, the splitted shares will not have the exact precision and some funds may not be calculated as expected.

The taxes might not be splitted as expected.

```
uint addToLiquidityHalf = ((swapThreshold * liquidityTax) /
    totalTokenTax) / 2;
_addLiquidity((addToLiquidityHalf),
    ((ethBalance * liquidityTax) / totalEthFee > 0
    ? totalEthFee : 1) / 2 );

ethBalance * (buyTax.treasuryTax + sellTax.treasuryTax) /
    totalEthFee > 0 ? totalEthFee : 1
ethBalance * (buyTax.teamTax + sellTax.teamTax) / totalEthFee >
    0 ? totalEthFee : 1
ethBalance * buyTax.nftTax + sellTax.nftTax / totalEthFee >
    0 ? totalEthFee : 1
```

Recommendation

The contract could calculate the subtraction of the divided funds in the last calculation in order to avoid the division rounding issue.

MSC - Missing Sanity Check

Criticality	Minor / Informative
Location	MoonLabs.sol#L242
Status	Unresolved

Description

The contract is processing variables that have not been properly sanitized and checked that they form the proper shape. These variables may produce vulnerability issues.

The contract could transfer `nftPayout` to zero addresses.

```
(bool sent, ) = payable(nftOwner).call{ value: nftPayout }("");
```

Recommendation

The team is advised to properly check the variables according to the required specifications.

The variable `nftOwner` should be zero address.

RCS - Redundant Code Statement

Criticality	Minor / Informative
Location	MoonLabs.sol#L273
Status	Unresolved

Description

There are code segments that could be optimized. A segment may be optimized so that it becomes a smaller size, consumes less memory, executes more rapidly, or performs fewer operations.

The contract is utilizing a redundant boolean variable. The functionality of distributed variable could be replaced with a pre existing variable.

```
bool distributed;

for (uint i = 0; i < maxNftDistribution; i++) {
    /// Set distributed to true if not true
    if (!distributed) distributed = true;
    ...
}

/// Emit event if nft payout
if (distributed) emit DistributeNftPayout(addressArray,
indexArray, nftPayout);
```

Recommendation

The team is advised to take these segments into consideration and rewrite them so the runtime will be more performant. That way it will improve the efficiency and performance of the source code and reduce the cost of executing it.

The contract could remove the distributed variable and use maxNftDistribution variable. For instance,

```
if (maxNftDistribution > 0) emit
DistributeNftPayout(addressArray, indexArray, nftPayout);
```

L04 - Conformance to Solidity Naming Conventions

Criticality	Minor / Informative
Location	MoonLabs.sol#L121,125,131,137,142,147,152,157,197
Status	Unresolved

Description

The Solidity style guide is a set of guidelines for writing clean and consistent Solidity code. Adhering to a style guide can help improve the readability and maintainability of the Solidity code, making it easier for others to understand and work with.

The followings are a few key points from the Solidity style guide:

1. Use camelCase for function and variable names, with the first letter in lowercase (e.g., myVariable, updateCounter).
2. Use PascalCase for contract, struct, and enum names, with the first letter in uppercase (e.g., MyContract, UserStruct, ErrorEnum).
3. Use uppercase for constant variables and enums (e.g., MAX_VALUE, ERROR_CODE).
4. Use indentation to improve readability and structure.
5. Use spaces between operators and after commas.
6. Use comments to explain the purpose and behavior of the code.
7. Keep lines short (around 120 characters) to improve readability.

```
uint _nftPayout
uint8 _maxNftDistribution
address payable _treasuryWallet
address payable _teamWallet
address payable _liqWallet
address _address
bool _taxSwap
uint _swapThreshold
```

Recommendation

By following the Solidity naming convention guidelines, the codebase increased the readability, maintainability, and makes it easier to work with.
Find more information on the Solidity documentation
https://docs.soliditylang.org/en/v0.8.17/style-guide.html#naming-convention.

L07 - Missing Events Arithmetic

Criticality	Minor / Informative
Location	MoonLabs.sol#L122,127,199
Status	Unresolved

Description

Events are a way to record and log information about changes or actions that occur within a contract. They are often used to notify external parties or clients about events that have occurred within the contract, such as the transfer of tokens or the completion of a task.

It's important to carefully design and implement the events in a contract, and to ensure that all required events are included. It's also a good idea to test the contract to ensure that all events are being properly triggered and logged.

```
nftPayout = _nftPayout
maxNftDistribution = _maxNftDistribution
swapThreshold = _swapThreshold
```

Recommendation

By including all required events in the contract and thoroughly testing the contract's functionality, the contract ensures that it performs as intended and does not have any missing events that could cause issues with its arithmetic.

L14 - Uninitialized Variables in Local Scope

Criticality	Minor / Informative
Location	MoonLabs.sol#L228,266,309
Status	Unresolved

Description

Using an uninitialized local variable can lead to unpredictable behavior and potentially cause errors in the contract. It's important to always initialize local variables with appropriate values before using them.

```
bool distributed
uint fees
uint burnTokenCut
```

Recommendation

By initializing local variables before using them, the contract ensures that the functions behave as expected and avoid potential issues.

L16 - Validate Variable Setters

Criticality	Minor / Informative
Location	MoonLabs.sol#L71,72,73
Status	Unresolved

Description

The contract performs operations on variables that have been configured on user-supplied input. These variables are missing of proper check for the case where a value is zero. This can lead to problems when the contract is executed, as certain actions may not be properly handled when the value is zero.

```
treasuryWallet = _treasuryWallet
teamWallet = _teamWallet
liqWallet = _liqWallet
```

Recommendation

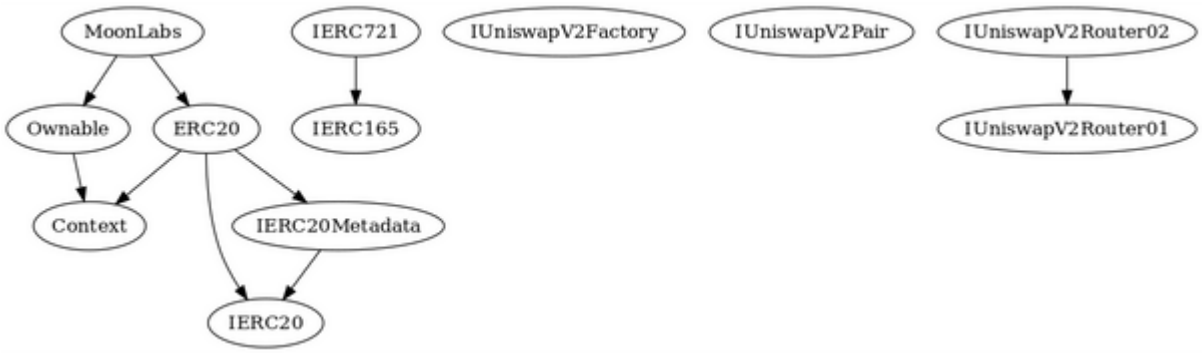
By adding the proper check, the contract will not allow the variables to be configured with zero value. This will ensure that the contract can handle all possible input values and avoid unexpected behavior or errors. Hence, it can help to prevent the contract from being exploited or operating unexpectedly.

Functions Analysis

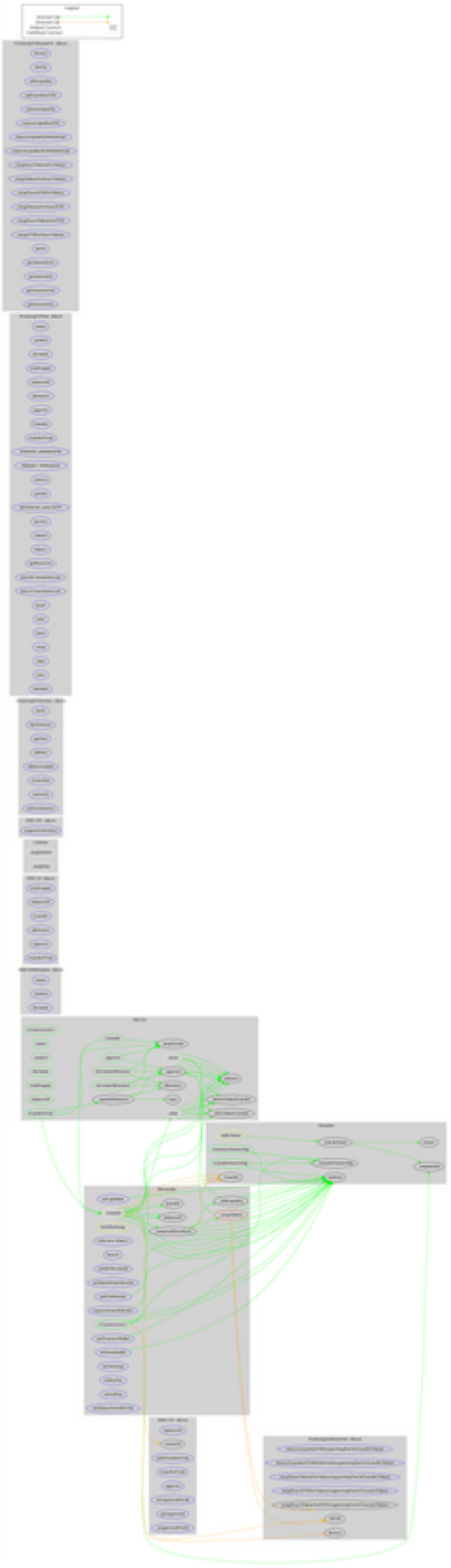
Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
MoonLabs	Implementation	ERC20, Ownable, ReentrancyGuard		
		Public	✓	ERC20
		External	Payable	-
	launch	External	✓	onlyOwner
	setNftThreshold	External	✓	onlyOwner
	setMaxNftDistribution	External	✓	onlyOwner
	setTreasuryWallet	External	✓	onlyOwner
	setTeamWallet	External	✓	onlyOwner
	setLiqWallet	External	✓	onlyOwner
	addToWhitelist	External	✓	onlyOwner
	removeFromWhitelist	External	✓	onlyOwner
	setTaxSwap	External	✓	onlyOwner
	setBuyTax	External	✓	onlyOwner
	setSellTax	External	✓	onlyOwner
	setTokensToSellForTax	External	✓	onlyOwner
	_transfer	Internal	✓	nonReentrant
	_swapTokens	Private	✓	lockTheSwap

	_swapAndDistribute	Private	✓	lockTheSwap
	_addLiquidity	Private	✓	lockTheSwap

Inheritance Graph



Flow Graph



Summary

Moonlabs contract implements a token mechanism. This audit investigates security issues, business logic concerns and potential improvements. Moonlabs is an interesting project that has a friendly and growing community. The Smart Contract analysis reported no compiler error 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