Cyberscope

Audit Report

Litas

March 2025

Repository

https://github.com/litas-io/Litas-token/blob/main/token.sol

Commit 0f05766c3676c9d7aca45c6a15b9a141f988230c

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
	MC	Missing Check	Unresolved
	MSR	Missing Staking Rewards	Unresolved

Table of Contents

Risk Classification

The criticality of findings in Cyberscope's smart contract audits is determined by evaluating multiple variables. The two primary variables are:

1. **Likelihood of Exploitation**: This considers how easily an attack can be executed, including the economic feasibility for an attacker.
2. **Impact of Exploitation**: This assesses the potential consequences of an attack, particularly in terms of the loss of funds or disruption to the contract's functionality.

Based on these variables, findings are categorized into the following severity levels:

1. **Critical**: Indicates a vulnerability that is both highly likely to be exploited and can result in significant fund loss or severe disruption. Immediate action is required to address these issues.
2. **Medium**: Refers to vulnerabilities that are either less likely to be exploited or would have a moderate impact if exploited. These issues should be addressed in due course to ensure overall contract security.
3. **Minor**: Involves vulnerabilities that are unlikely to be exploited and would have a minor impact. These findings should still be considered for resolution to maintain best practices in security.
4. **Informative**: Points out potential improvements or informational notes that do not pose an immediate risk. Addressing these can enhance the overall quality and robustness of the contract.

Severity	Likelihood / Impact of Exploitation
Critical	Highly Likely / High Impact
Medium	Less Likely / High Impact or Highly Likely/ Lower Impact
Minor / Informative	Unlikely / Low to no Impact

Review

Repository	https://github.com/litas-io/Litas-token/blob/main/token.sol
Commit	0f05766c3676c9d7aca45c6a15b9a141f988230c

Audit Updates

Initial Audit	28 Feb 2025

Source Files

Filename	SHA256
token.sol	76a0f46ae22b33d39ddf0c47c504ff3e9eb59539ac7519a3fd14e7016441b60f

Overview

Litas Token Contract

The Litas contract is an ERC20 token implementation that includes additional functionality for burning tokens and staking. It utilizes OpenZeppelin's standard implementations for ERC20 and security features such as `ReentrancyGuard` to prevent reentrancy attacks. The contract allows users to stake their tokens for a specified duration and claim them once the lock period ends.

Token Initialization

The contract is initialized with a specified name, symbol, and initial supply, which is minted to a designated owner. It follows the ERC20 standard from OpenZeppelin, ensuring compatibility with existing token infrastructure.

Token Burning

The `burn` function allows users to destroy a specified amount of their tokens, permanently reducing the total supply. When tokens are burned, the contract emits a `TokensBurned` event, logging the burner's address and the amount burned.

Staking Mechanism

The contract enables users to stake their tokens for a given duration. When a user stakes tokens, the contract transfers the tokens from the user's balance to itself and records the stake details, including the amount of tokens staked, the start timestamp of the stake, the end timestamp when the stake can be claimed, and a flag indicating whether the stake has been claimed. Stakes are stored in a mapping, allowing each user to maintain multiple active stakes. The contract emits a `TokensStaked` event upon successful staking.

Claiming Staked Tokens

After the staking period ends, users can claim their staked tokens using the `claimStakedTokens` function. This function verifies that the stake exists, ensures the lock period has expired, and checks that the stake has not already been claimed. Once verified, the contract marks the stake as claimed and transfers the tokens back to the user. A `TokensClaimed` event is emitted to record the transaction.

Retrieving Stake Details

The contract provides a getStakeDetails function, which allows users to retrieve information about a specific stake.

Roles

Users

Users (token holders and stakers) can interact with the following functions:

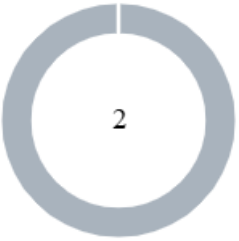
- `function burn(uint256 amount)`
- `function stake(uint256 amount, uint256 durationInDays)`
- `function claimStakedTokens(uint256 stakeIndex)`

Retrieval Functions

The following functions can be used to retrieve staking-related information:

- `function getStakeDetails(address user, uint256 stakeIndex)`

Findings Breakdown



Critical	0
Medium	0
Minor / Informative	2

Severity	Unresolved	Acknowledged	Resolved	Other
Critical	0	0	0	0
Medium	0	0	0	0
Minor / Informative	2	0	0	0

MC - Missing Check

Criticality	Minor / Informative
Location	token.sol#L49,75
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.

Specifically, in the `constructor` a check is missing to ensure that `initialSupply` is not zero. Additionally, in the `stake` function, a check is missing to ensure that the staking happens for more than zero days.

```
constructor(
    /*..args..*/,
    uint256 initialSupply,
    address initialOwner
)
    ERC20(name, symbol)
{
    _mint(initialOwner, initialSupply * 10**decimals());
}
function stake(uint256 amount, uint256 durationInDays) public
nonReentrant {
    require(amount > 0, "Cannot stake 0 tokens");
    require(balanceOf(msg.sender) >= amount, "Insufficient
token balance");
    //...
}
```

Recommendation

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

MSR - Missing Staking Rewards

Criticality	Minor / Informative
Location	token.sol#L75,99
Status	Unresolved

Description

The contract has a staking system that allows users to stake their tokens by storing them inside the contract. Users are able to choose the amount of time (in days) they want to stake their tokens. Normally, staking contracts provide a form of reward, usually depending on the amount of time users keep their tokens staked. This incentivizes users to keep their tokens staked for longer periods of time. However, the contract does not implement any functionality that rewards users the longer they keep their tokens staked.

```
function stake(uint256 amount, uint256 durationInDays) public
nonReentrant {/*...*/}

function claimStakedTokens(uint256 stakeIndex) public
nonReentrant {
    //...
    require(block.timestamp >= stakeData.endTime, "Stake is
still locked");
    //...
    _transfer(address(this), msg.sender, stakeData.amount);
    //...
}
```

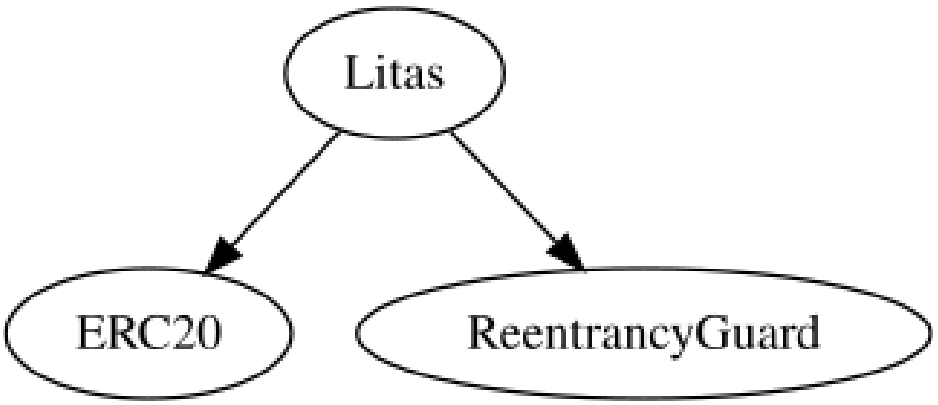
Recommendation

The team could consider adding some form of reward mechanism that accounts for the duration users keep their tokens staked. This will potentially encourage more users into staking their tokens in the protocol for longer periods of time.

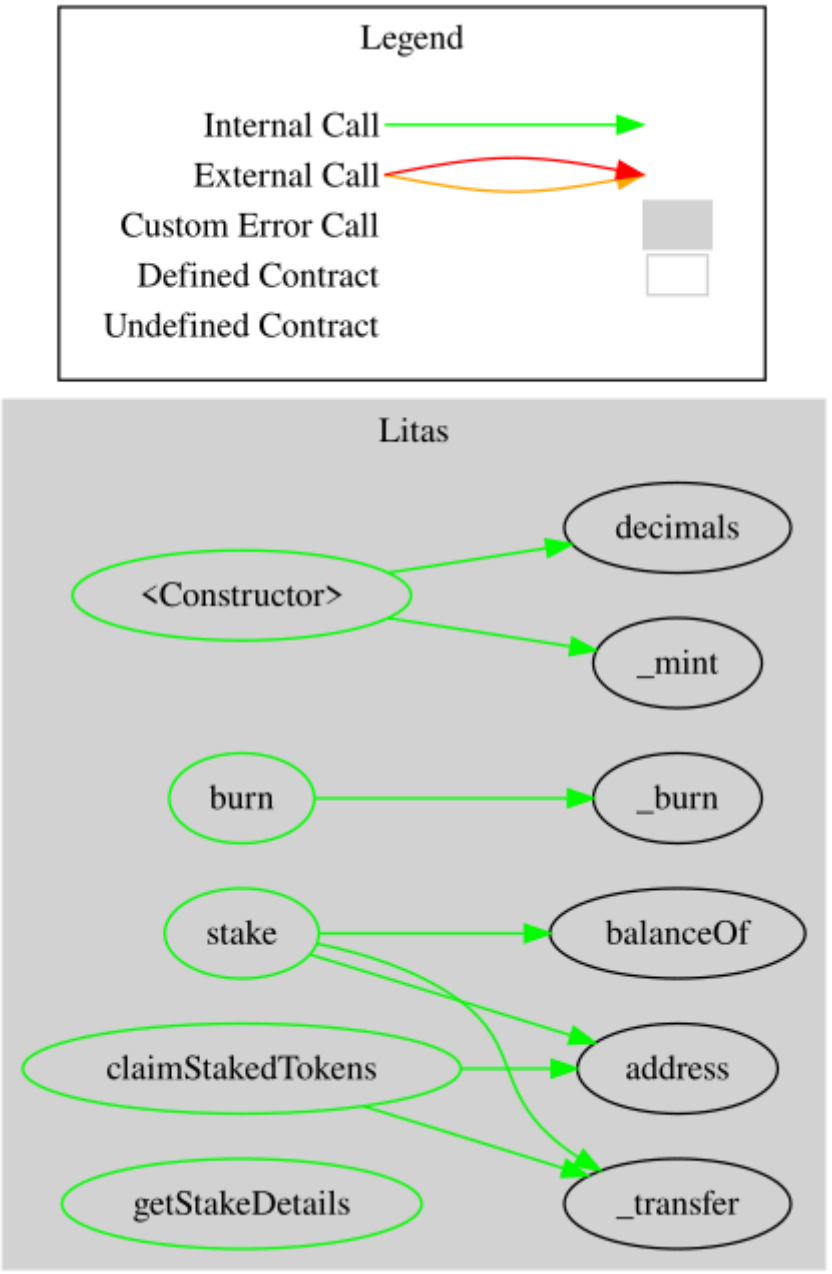
Functions Analysis

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
Litas	Implementation	ERC20, ReentrancyGuard		
		Public	✓	ERC20
	burn	Public	✓	-
	stake	Public	✓	nonReentrant
	claimStakedTokens	Public	✓	nonReentrant
	getStakeDetails	Public		-

Inheritance Graph



Flow Graph


Legend
Internal Call
External Call
Custom Error Call
Defined Contract
Undefined Contract
Litas
decimals
<Constructor>
_mint
burn
_burn
stake
balanceOf
claimStakedTokens
address
getStakeDetails
_transfer

Summary

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

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

cyberscope.io