Cyberscope

Audit Report

ZayaAI

July 2024

Network	BSC
Address	0x316Ec9EA88d17656c2F20CED6b9c7eA31BABC84B
Audited by	© cyberscope

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

Contract Name	Token
Compiler Version	v0.8.20+commit.a1b79de6
Optimization	10000000 runs
Explorer	https://bscscan.com/address/0x316ec9ea88d17656c2f20ced6b9c7ea31babc84b
Address	0x316ec9ea88d17656c2f20ced6b9c7ea31babc84b
Network	BSC
Decimals	18

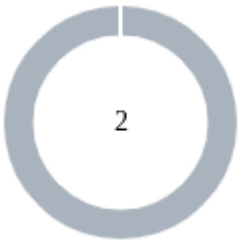
Audit Updates

Initial Audit	29 Jul 2024

Source Files

Filename	SHA256
Token.sol	aaa3c8f62dfea3018653b66a3d5afa796922d3c4dca5e56b708bd9a9aaf1edb8

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

Diagnostics

Critical Medium Minor / Informative

Severity	Code	Description	Status
●	ST	Stops Transactions	Unresolved
●	L19	Stable Compiler Version	Unresolved

ST - Stops Transactions

Criticality	Minor / Informative
Location	Token.sol#L38,42
Status	Unresolved

Description

The contract is designed with a mechanism that allows the owner to pause and unpause all transactions by invoking the `pause` and `unpause` functions, respectively. This functionality grants the owner the authority to halt all activities, effectively stopping all transactions for all users, including the owner. While this can be useful for emergency scenarios, it also introduces a potential risk in case where the owner's wallet is compromised. When the contract is paused, any attempted transactions will revert, causing potential disruptions and loss of functionality for the users.

```
    function pause() public onlyOwner {
        _pause();
    }

    function unpause() public onlyOwner {
        _unpause();
    }
```

Recommendation

It is recommended to implement additional safeguards and transparency measures to ensure the pause functionality is used responsibly. 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.

Temporary Solutions:

These measurements do not decrease the severity of the finding

- Introduce a time-locker mechanism with a reasonable delay.
- Introduce a multi-signature wallet so that many addresses will confirm the action.

- Introduce a governance model where users will vote about the actions.

Permanent Solution:

- Renouncing the ownership, which will eliminate the threats but it is non-reversible.

L19 - Stable Compiler Version

Criticality	Minor / Informative
Location	Token.sol#L2
Status	Unresolved

Description

The `^` symbol indicates that any version of Solidity that is compatible with the specified version (i.e., any version that is a higher minor or patch version) can be used to compile the contract. The version lock is a mechanism that allows the author to specify a minimum version of the Solidity compiler that must be used to compile the contract code. This is useful because it ensures that the contract will be compiled using a version of the compiler that is known to be compatible with the code.

```
pragma solidity ^0.8.20;
```

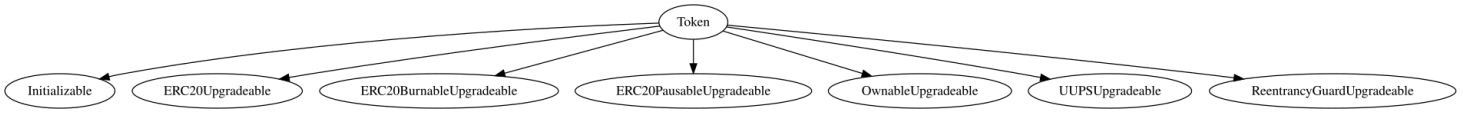
Recommendation

The team is advised to lock the pragma to ensure the stability of the codebase. The locked pragma version ensures that the contract will not be deployed with an unexpected version. An unexpected version may produce vulnerabilities and undiscovered bugs. The compiler should be configured to the lowest version that provides all the required functionality for the codebase. As a result, the project will be compiled in a well-tested LTS (Long Term Support) environment.

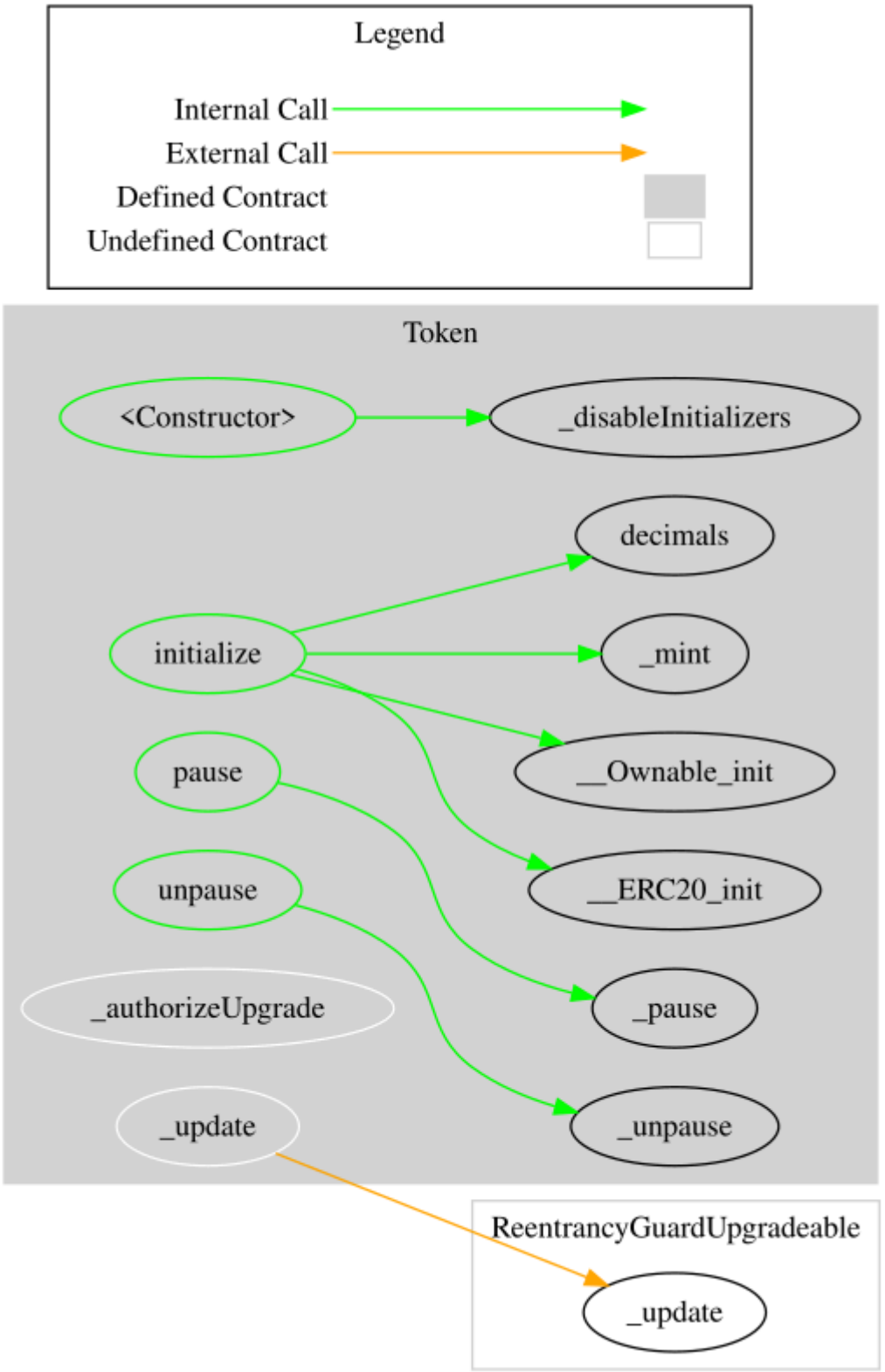
Functions Analysis

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
Token	Implementation	Initializable, ERC20Upgradeable, ERC20BurnableUpgradeable, ERC20PausableUpgradeable, OwnableUpgradeable, UUPSUpgradeable, ReentrancyGuardUpgradeable		
		Public	✓	-
	initialize	Public	✓	initializer
	pause	Public	✓	onlyOwner
	unpause	Public	✓	onlyOwner
	_authorizeUpgrade	Internal	✓	onlyOwner
	_update	Internal	✓	

Inheritance Graph



Flow Graph


Legend
Internal Call
External Call
Defined Contract
Undefined Contract
Token
<Constructor>
_disableInitializers
decimals
initialize
_mint
__Ownable_init
pause
__ERC20_init
unpause
_authorizeUpgrade
_pause
_update
_unpause
ReentrancyGuardUpgradeable
_update

Summary

ZayaAI 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 has access to some administrative functions, such as pausing and unpausing transactions, which can halt or resume contract activities. These functions are designed to ensure security and proper management without maliciously disrupting the 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

cyberscope.io