Cyberscope

Audit Report

ABPToken

September 2022

SHA256	1a909009cf62ce38fa8fb84cd70861396ad89447157b5d90f307a1113838c52d
Audited by	© cyberscope

Table of Contents

Contract Review

Contract Name	ABPToken
Symbol	XXX
Decimals	18

Audit Updates

Initial Audit	23rd September 2022
Corrected	

Source Files

Filename	SHA256
@openzeppelin/contracts/token/ERC20/ERC20.sol	5031430cc2613c32736d598037d3075985a2a09e61592a013dbd09a5bc2041b8
@openzeppelin/contracts/token/ERC20/extensions/IERC20Metadata.sol	af5c8a77965cc82c33b7ff844deb9826166689e55dc037a7f2f790d057811990
@openzeppelin/contracts/token/ERC20/IERC20.sol	94f23e4af51a18c2269b355b8c7cf4db8003d075c9c541019eb8dcf4122864d5
@openzeppelin/contracts/utils/Context.sol	1458c260d010a08e4c20a4a517882259a23a4baa0b5bd9add9fb6d6a1549814a
contracts/ABPToken.sol	1a909009cf62ce38fa8fb84cd70861396ad89447157b5d90f307a1113838c52d

Introduction

ABPToken implements the standard ERC20 interface enriched with mint functionality. The contract owner can whitelist addresses, these addresses have the ability to arbitrary mint tokens. This token does not permit transfers. As a result, it is not operating as an ordinary transferable token.

Contract Diagnostics

🔴 Critical 🟠 Medium ⚪ Minor / Informative

Severity	Code	Description	Status
🟠	MT	Mints Tokens	Unresolved
⚪	L01	Public Function could be Declared External	Unresolved
⚪	L04	Conformance to Solidity Naming Conventions	Unresolved

MT - Mints Tokens

Criticality	medium
Location	contract.sol#L23
Status	Unresolved

Description

The contract owner has the authority to mint tokens. The owner may take advantage of it by calling the mintArbitrary function. As a result the contract tokens will be highly inflated.

```
function mintArbitrary(address _to, uint256 _amount) public {
        require(
            whitelistedMinters[msg.sender],
            "You don't have access to mint!"
        );
        _mint(_to, _amount);
}
```

Recommendation

The owner should carefully manage the credentials of the owner’s account. We advised considering an extra-strong security mechanism that the actions may be quarantined by many users instead of one. The owner could also renounce the contract ownership for a period of time or pass the access to the zero address.

L01 - Public Function could be Declared External

Criticality	minor / informative
Location	contracts/ABPToken.sol#L23
Status	Unresolved

Description

Public functions that are never called by the contract should be declared external to save gas.

```
mintArbitrary
```

Recommendation

Use the external attribute for functions never called from the contract.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor / informative
Location	contracts/ABPToken.sol#L39,23,31
Status	Unresolved

Description

Solidity defines a naming convention that should be followed. Rule exceptions:

- Allow constant variable name/symbol/decimals to be lowercase.
- Allow _ at the beginning of the mixed_case match for private variables and unused parameters.

```
_newMinter
_to
_amount
_newOwner
```

Recommendation

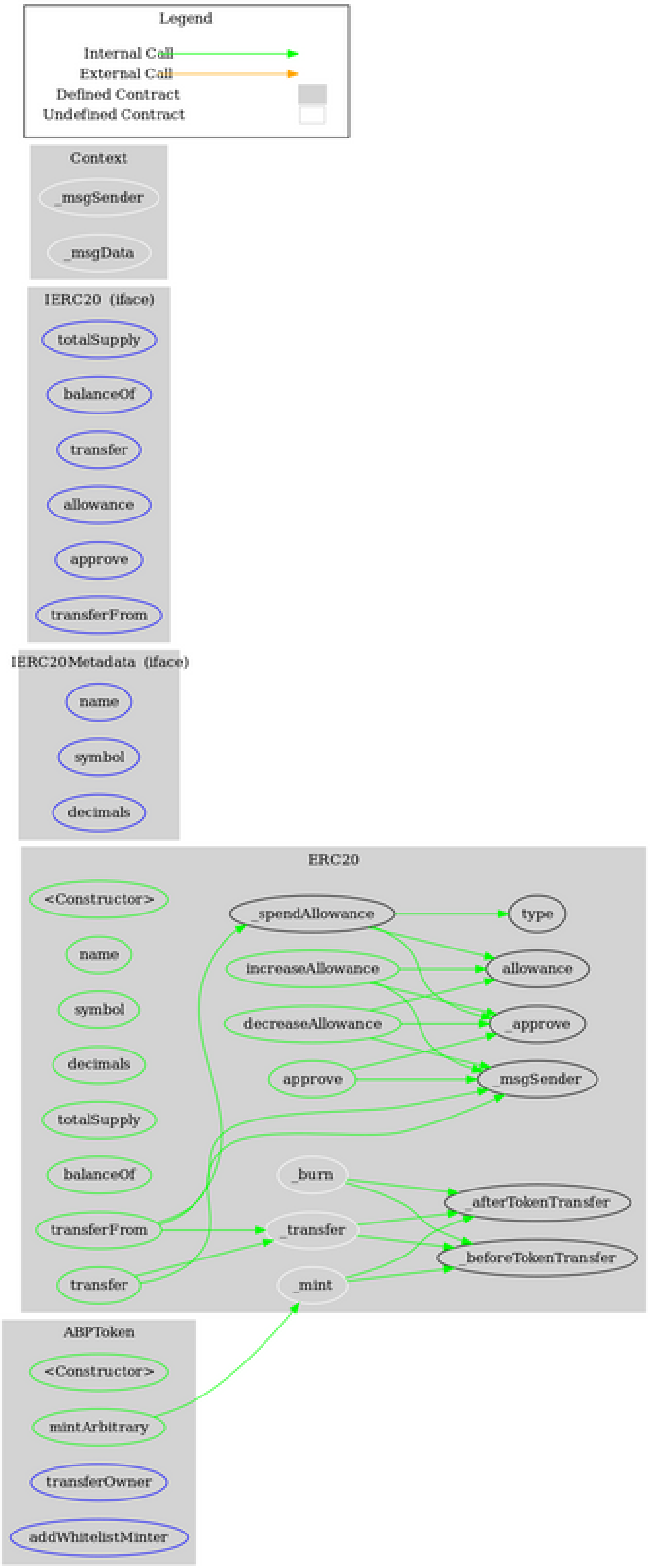
Follow the Solidity naming convention.
https://docs.soliditylang.org/en/v0.4.25/style-guide.html#naming-conventions.

Contract Functions

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
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	✓	
IERC20Metadata	Interface	IERC20		
	name	External		-
	symbol	External		-
	decimals	External		-

IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
ABPToken	Implementation	ERC20		
	<Constructor>	Public	✓	ERC20
	_transfer	Internal	✓	
	mintArbitrary	Public	✓	-
	transferOwner	External	✓	-
	addWhitelistMinter	External	✓	-

Contract Flow



Summary

ABPToken implements the ERC20 interface without allowing to transfer tokens. The Smart Contract analysis reported one critical severity issue. The contract owner has the authority to mint tokens. if the contract owner abuses the mint functionality, then the contract will be highly inflated. A multi-wallet signing pattern will provide security against potential hacks. Temporarily locking the contract or renouncing ownership will eliminate all the contract threats.

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