Cyberscope

Audit Report

iobeats

June 2024

SHA256 2bf0abe5ce2059d39b0a1c70efed4fe10c054a7fdda9bbe371921fc338df412c

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
●	RFO	Redundant Function Override	Unresolved
●	RI	Redundant Inheritance	Unresolved
●	L18	Multiple Pragma Directives	Unresolved

Table of Contents

Review

Contract Name	iobeats
Repository	https://github.com/iobeatss
Commit	f20568b36f7477d70a23469cc7be4ad3c676bafe
Testing Deploy	https://testnet.bscscan.com/address/0x1f4c44527c8058477dc18647b45c198fe639251e
Symbol	IOB
Decimals	18
Total Supply	10,000,000,000
Badge Eligibility	Yes

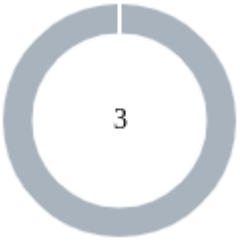
Audit Updates

Initial Audit	06 Jun 2024

Source Files

Filename	SHA256
contracts/iobeats.sol	2bf0abe5ce2059d39b0a1c70efed4fe10c054a7fdda9bbe371921fc338df412c

Findings Breakdown



Critical	0
Medium	0
Minor / Informative	3

Severity	Unresolved	Acknowledged	Resolved	Other
Critical	0	0	0	0
Medium	0	0	0	0
Minor / Informative	3	0	0	0

RFO - Redundant Function Override

Criticality	Minor / Informative
Location	contracts/iobeats.sol#L630,634
Status	Unresolved

Description

The contract `iobeats` inherits from `ERC20` , `ERC20Burnable` , and `Ownable` . Within this contract, the `_beforeTokenTransfer` and `_transfer` functions are overridden, but these overrides only call the parent's implementation without introducing any new logic or modifications.

```
function _beforeTokenTransfer(address from, address to, uint256 amount)
internal override(ERC20) {
    super._beforeTokenTransfer(from, to, amount);
}

function _transfer(address sender, address recipient, uint256 amount)
internal virtual override(ERC20) {
    super._transfer(sender, recipient, amount);
}
```

Recommendation

The team is advised to remove the redundant overrides of `_beforeTokenTransfer` and `_transfer` unless you plan to introduce custom logic in these functions. The parent implementation will be used by default if these functions are not overridden.

RI - Redundant Inheritance

Criticality	Minor / Informative
Location	contracts/iobeats.sol#L625
Status	Unresolved

Description

The `iobeats` contract inherits both `ERC20` and `ERC20Burnable`. However, `ERC20Burnable` already inherits `ERC20`, making the direct inheritance of `ERC20` redundant.

```
contract iobeats is ERC20, ERC20Burnable, Ownable {
    constructor() ERC20("iobeats", "IOB") {
        _mint(msg.sender, 10000000000 * 10 ** decimals());
    }
    ...
}
```

Recommendation

The team is advised to remove the direct inheritance of `ERC20` from the `iobeats` contract. This will simplify the inheritance hierarchy without affecting the functionality, as `ERC20Burnable` already provides the `ERC20` functionality.

L18 - Multiple Pragma Directives

Criticality	Minor / Informative
Location	contracts/iobeats.sol#L6,32,115,195,223,587,623
Status	Unresolved

Description

If the contract includes multiple conflicting pragma directives, it may produce unexpected errors. To avoid this, it's important to include the correct pragma directive at the top of the contract and to ensure that it is the only pragma directive included in the contract.

```
pragma solidity ^0.8.16;
```

Recommendation

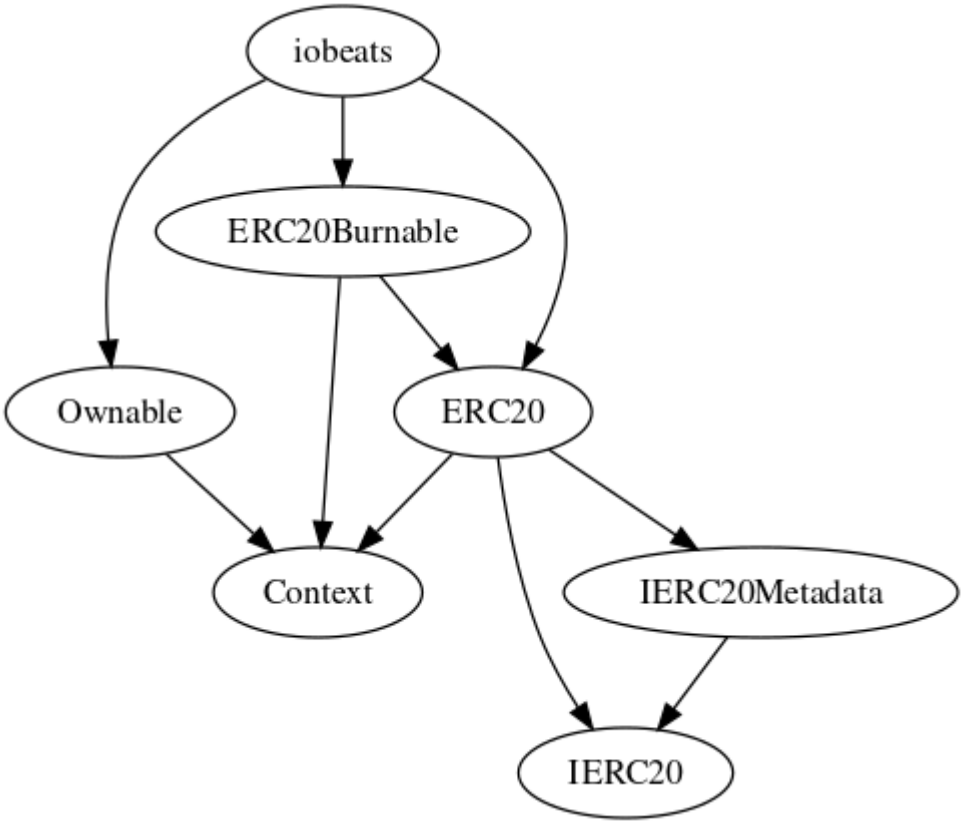
It is important to include only one pragma directive at the top of the contract and to ensure that it accurately reflects the version of Solidity that the contract is written in.

By including all required compiler options and flags in a single pragma directive, the potential conflicts could be avoided and ensure that the contract can be compiled correctly.

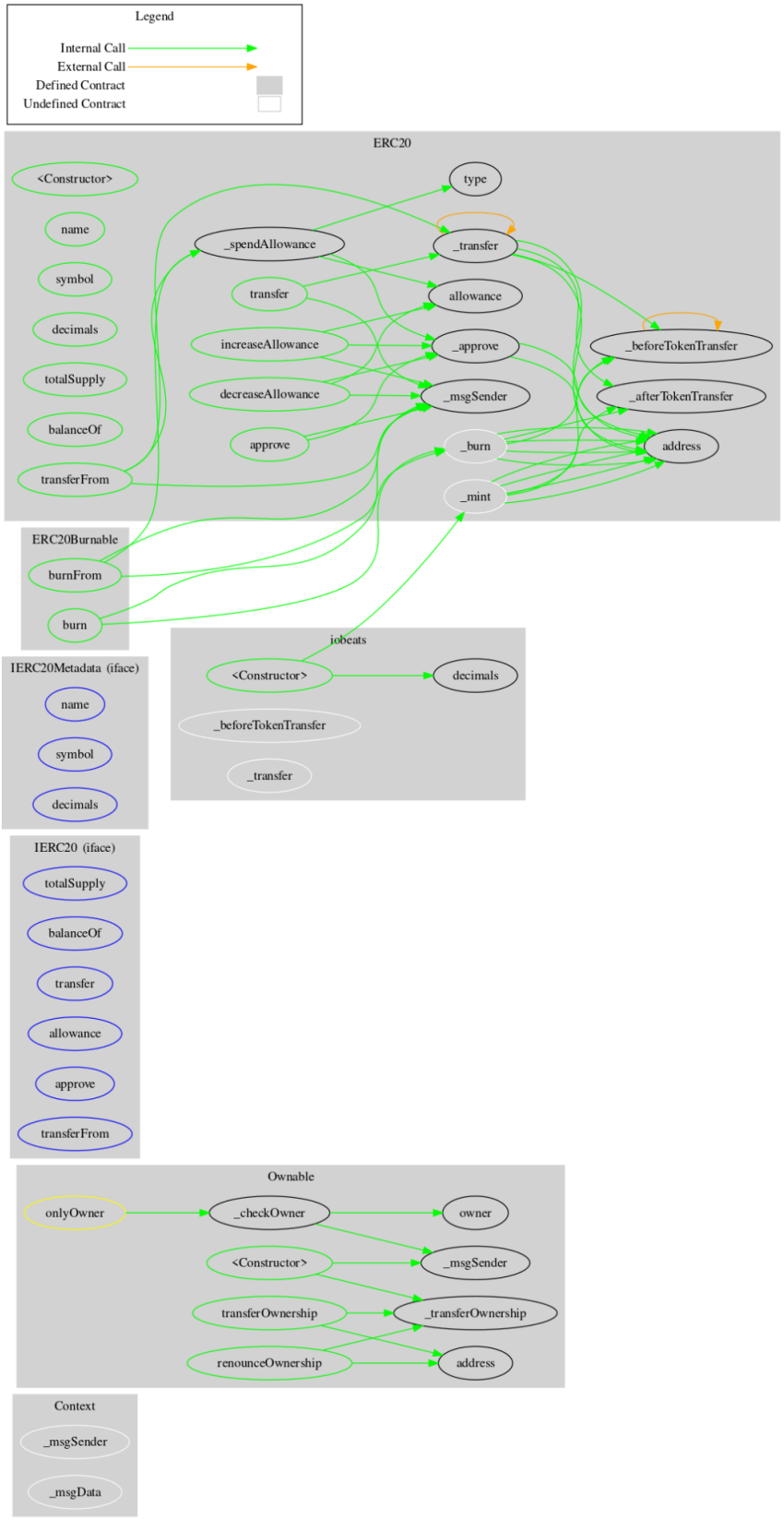
Functions Analysis

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
iobeats	Implementation	ERC20, ERC20Burnable, Ownable		
		Public	✓	ERC20
	_beforeTokenTransfer	Internal	✓	
	_transfer	Internal	✓	

Inheritance Graph



Flow Graph


Legend
Internal Call
External Call
Defined Contract
Undefined Contract
ERC20
<Constructor>
name
symbol
decimals
totalSupply
balanceOf
transferFrom
type
_transfer
_spendAllowance
transfer
allowance
increaseAllowance
_approve
decreaseAllowance
_msgSender
approve
_burn
_mint
_beforeTokenTransfer
_afterTokenTransfer
address
ERC20Burnable
burnFrom
burn
jobeats
<Constructor>
decimals
_beforeTokenTransfer
_transfer
IERC20Metadata (iface)
name
symbol
decimals
IERC20 (iface)
totalSupply
balanceOf
transfer
allowance
approve
transferFrom
Ownable
onlyOwner
_checkOwner
owner
<Constructor>
_msgSender
transferOwnership
_transferOwnership
renounceOwnership
address
Context
_msgSender
_msgData

Summary

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

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