Cyberscope

Audit Report

Tokenee

October 2023

Network	ETH
Address	0xd924099Cba78b5E045957f40306c437a192eE1E6
Audited by	© cyberscope

Table of Contents

Review

Explorer	https://etherscan.io/address/0xd924099cba78b5e045957f40306c437a192ee1e6

Audit Updates

Initial Audit	09 Oct 2023 https://github.com/cyberscope-io/audits/blob/main/v1/tokenee/audit.pdf
Corrected Phase 2	12 Oct 2023

Source Files

Filename	SHA256
AirdropDistributor.sol	8762548cc01c281fa0de0f1d0a2d68a3a4a6c8363d51d1f53dc6df04b4476c99

Overview

The AirdropDistributor contract is designed to facilitate the distribution of rewards in the form of a specific ERC-20 token, which is specified by the `rewardToken` variable. The key functionality of this contract includes the ability to transfer rewards to a group of investors defined in the `rewardData` array, with checks for valid parameters such as airdrop ID, treasury address, allocated budget, and investor details. The contract ensures that the total rewards transferred do not exceed the specified budget. Lastly, the contract enforces access control, ensuring that only operators with the `OPERATOR_ROLE` can execute certain functions, making it suitable for managing airdrop campaigns securely.

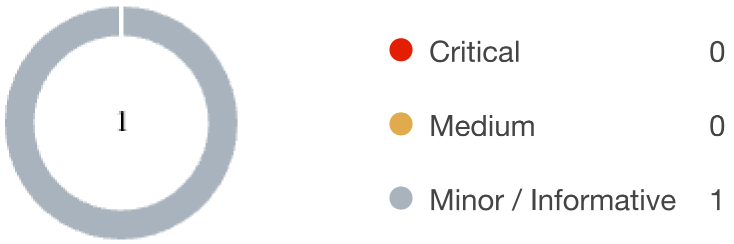
Roles

Operator

The operator has the authority to:

- transfer rewards to investors by calling the `transferRewards` function.
- update the reward token address using the `setRewardToken` function.

Findings Breakdown



Severity	Unresolved	Acknowledged	Resolved	Other
● Critical	0	0	0	0
● Medium	0	0	0	0
● Minor / Informative	1	0	0	0

Diagnostics

● Critical ● Medium ● Minor / Informative

Severity	Code	Description	Status
●	PTAI	Potential Transfer Amount Inconsistency	Unresolved

PTAI - Potential Transfer Amount Inconsistency

Criticality	Minor / Informative
Location	contracts/AirdropDistributor.sol#L1569
Status	Unresolved

Description

The `transfer()` and `transferFrom()` functions are used to transfer a specified amount of tokens to an address. The fee or tax is an amount that is charged to the sender of an ERC20 token when tokens are transferred to another address. According to the specification, the transferred amount could potentially be less than the expected amount. This may produce inconsistency between the expected and the actual behavior.

The following example depicts the diversion between the expected and actual amount.

Tax	Amount	Expected	Actual
No Tax	100	100	100
10% Tax	100	100	90

The contract currently tracks the sum of transferred tokens in the `totalTransfered` variable within the `transferRewards` function. However, if the `rewardToken` contract has logic that includes fees or deductions during the transfer process, the `totalTransfered` variable may not accurately represent the actual total transferred amount.

```
for (uint256 i; i < length; ) {
    InvestorReward memory investor = transferData[i];
    _checkInvestorData(totalTransfered, budget, investor);
    _transferTokens(treasury, investor);
    unchecked {
        totalTransfered += investor.reward;
        ++i;
    }
}
```

Recommendation

The team is advised to take into consideration the actual amount that has been transferred instead of the expected.

It is important to note that an ERC20 transfer tax is not a standard feature of the ERC20 specification, and it is not universally implemented by all ERC20 contracts. Therefore, the contract could produce the actual amount by calculating the difference between the transfer call.

```
 Actual Transferred Amount = Balance After Transfer - Balance Before Transfer
```

Functions Analysis

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
IAirdropDistributor	Interface			
	rewardToken	External		-
	setRewardToken	External	✓	-
	transferRewards	External	✓	-
Address	Library			
	isContract	Internal		
	sendValue	Internal	✓	
	functionCall	Internal	✓	
	functionCall	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionStaticCall	Internal		
	functionStaticCall	Internal		
	functionDelegateCall	Internal	✓	
	functionDelegateCall	Internal	✓	
	verifyCallResultFromTarget	Internal		
	verifyCallResult	Internal		

	_revert	Private		
IERC20Permit	Interface			
	permit	External	✓	-
	nonces	External		-
	DOMAIN_SEPARATOR	External		-
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
SafeERC20	Library			
	safeTransfer	Internal	✓	
	safeTransferFrom	Internal	✓	
	safeApprove	Internal	✓	
	safeIncreaseAllowance	Internal	✓	
	safeDecreaseAllowance	Internal	✓	
	forceApprove	Internal	✓	
	safePermit	Internal	✓	

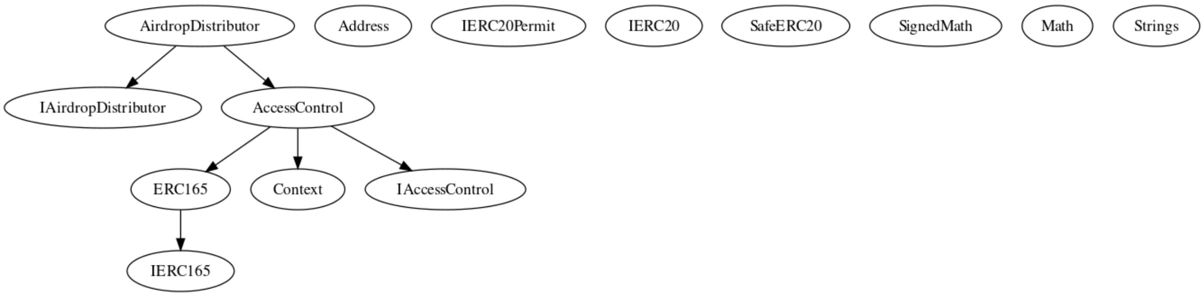
	_callOptionalReturn	Private	✓	
	_callOptionalReturnBool	Private	✓	
IERC165	Interface			
	supportsInterface	External		-
ERC165	Implementation	IERC165		
	supportsInterface	Public		-
SignedMath	Library			
	max	Internal		
	min	Internal		
	average	Internal		
	abs	Internal		
Math	Library			
	max	Internal		
	min	Internal		
	average	Internal		
	ceilDiv	Internal		
	mulDiv	Internal		
	mulDiv	Internal		
	sqrt	Internal		

	sqrt	Internal		
	log2	Internal		
	log2	Internal		
	log10	Internal		
	log10	Internal		
	log256	Internal		
	log256	Internal		
Strings	Library			
	toString	Internal		
	toString	Internal		
	toHexString	Internal		
	toHexString	Internal		
	toHexString	Internal		
	equal	Internal		
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
IAccessControl	Interface			
	hasRole	External		-
	getRoleAdmin	External		-

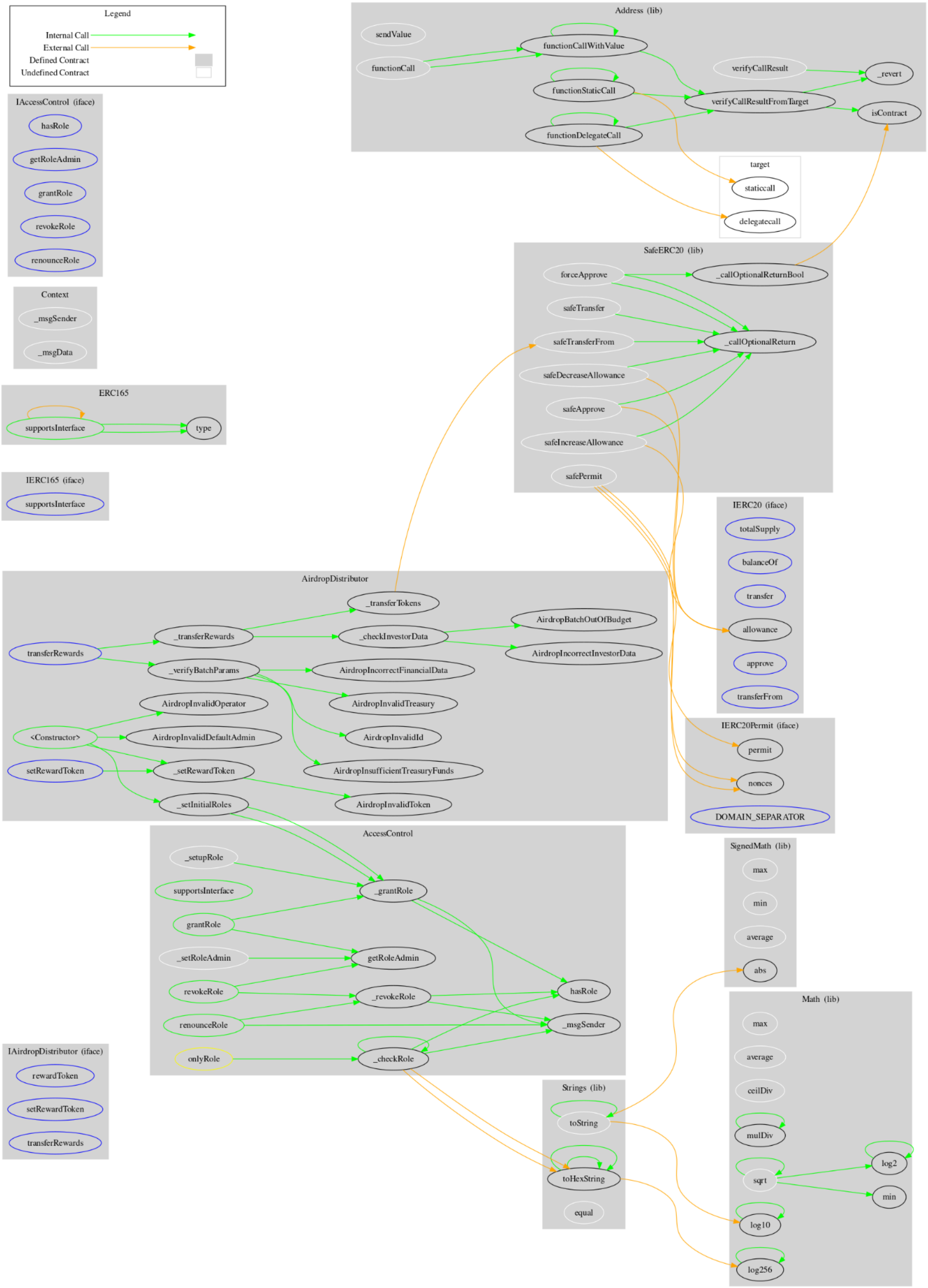
	grantRole	External	✓	-
	revokeRole	External	✓	-
	renounceRole	External	✓	-
AccessControl	Implementation	Context, IAccessControl, ERC165		
	supportsInterface	Public		-
	hasRole	Public		-
	_checkRole	Internal		
	_checkRole	Internal		
	getRoleAdmin	Public		-
	grantRole	Public	✓	onlyRole
	revokeRole	Public	✓	onlyRole
	renounceRole	Public	✓	-
	_setupRole	Internal	✓	
	_setRoleAdmin	Internal	✓	
	_grantRole	Internal	✓	
	_revokeRole	Internal	✓	
AirdropDistributor	Implementation	IAirdropDistributor, AccessControl		
		Public	✓	-
	transferRewards	External	✓	onlyRole
	setRewardToken	External	✓	onlyRole

	_setRewardToken	Internal	✓	
	_setInitialRoles	Internal	✓	
	_verifyBatchParams	Internal		
	_transferRewards	Internal	✓	
	_checkInvestorData	Internal		
	_transferTokens	Internal	✓	

Inheritance Graph



Flow Graph


Legend
Internal Call
External Call
Defined Contract
Undefined Contract
IAccessControl (iface)
hasRole
getRoleAdmin
grantRole
revokeRole
renounceRole
Context
_msgSender
_msgData
ERC165
supportsInterface
type
IERC165 (iface)
supportsInterface
Address (lib)
sendValue
functionCall
functionCallWithValue
functionStaticCall
functionDelegateCall
verifyCallResult
verifyCallResultFromTarget
_revert
isContract
target
staticcall
delegatecall
SafeERC20 (lib)
forceApprove
safeTransfer
safeTransferFrom
safeDecreaseAllowance
safeApprove
safeIncreaseAllowance
safePermit
_callOptionalReturnBool
_callOptionalReturn
IERC20 (iface)
totalSupply
balanceOf
transfer
allowance
approve
transferFrom
IERC20Permit (iface)
permit
nonces
DOMAIN_SEPARATOR
AirdropDistributor
_transferTokens
transferRewards
_transferRewards
_checkInvestorData
AirdropBatchOutOfBudget
AirdropIncorrectInvestorData
_verifyBatchParams
AirdropIncorrectFinancialData
AirdropInvalidOperator
AirdropInvalidTreasury
<Constructor>
AirdropInvalidDefaultAdmin
AirdropInvalidId
setRewardToken
_setRewardToken
AirdropInsufficientTreasuryFunds
_setInitialRoles
AirdropInvalidToken
AccessControl
_setupRole
supportsInterface
_grantRole
grantRole
_setRoleAdmin
getRoleAdmin
revokeRole
_revokeRole
hasRole
renounceRole
_msgSender
onlyRole
_checkRole
SignedMath (lib)
max
min
average
abs
Math (lib)
max
average
ceilDiv
mulDiv
sqrt
log2
min
log10
log256
Strings (lib)
toString
toHexString
equal
IAirdropDistributor (iface)
rewardToken
setRewardToken
transferRewards

Summary

Tokenee contract implements a rewards and utility mechanism. 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