Cyberscope

Audit Report

AlemX

July 2024

File	SHA256
AlemXToken	b89d05a99ee6d9057366d40c4f985786879107565c4b864517bf587be6cedc48
Airdrop	a260edfaaf84d453552f5e4991e1e48f14e6ffea0a2801ce82a98de79620ae5c
Audited by	© cyberscope

Table of Contents

Review

Contract Name	AlemXToken
Test Deploy Address	https://testnet.bscscan.com/address/0xb88786f56960C8Fe2d1618323a8a9c0Ae2611580
Explorer	0xb88786f56960C8Fe2d1618323a8a9c0Ae2611580

Contract Name	AlemXAirdrop
Test Deploy Address	https://testnet.bscscan.com/address/0xb134cD190C737F9E60B57f031BA45B701b7A8742
Explorer	0xb134cD190C737F9E60B57f031BA45B701b7A8742

Audit Updates

Initial Audit	04 Jul 2024 https://github.com/cyberscope-io/audits/blob/main/alem/v1/audit.pdf
Corrected Phase 2	18 Jul 2024

Source Files

Filename	SHA256
AlemXToken.sol	b89d05a99ee6d9057366d40c4f985786879107565c4b864517bf587be6cedc48
Airdrop.sol	a260edfaaf84d453552f5e4991e1e48f14e6ffea0a2801ce82a98de79620ae5c

Overview

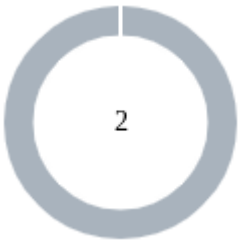
AlemXToken

The AlemXToken contract implements the ERC20 token standard, offering basic ERC20 functionalities with an additional `getOwner` method that returns a null address, emphasizing its decentralized nature. It is initialized with a name, symbol, and an initial supply that is minted to a specified receiver or defaults to the message sender if the receiver address is zero.

Airdrop

The Airdrop contract facilitates the distribution of tokens, utilizing the OpenZeppelin AccessControl for role management. It grants specific roles to address arrays, enabling them to initiate token drops or manage the contract.Functions within the contract enable the distribution of tokens either as a predefined amount specified by the sender or as a single token per recipient. The admin role has the authority to update the token address, ensuring that only valid contract addresses are used for airdrops, and withdraw any token amount from the contract.

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
●	CCR	Contract Centralization Risk	Unresolved
●	L04	Conformance to Solidity Naming Conventions	Unresolved

CCR - Contract Centralization Risk

Criticality	Minor / Informative
Location	Airdrop.sol#L79,157
Status	Unresolved

Description

The contract's functionality and behavior are heavily dependent on external parameters or configurations. While external configuration can offer flexibility, it also poses several centralization risks that warrant attention. Centralization risks arising from the dependence on external configuration include Single Point of Control, Vulnerability to Attacks, Operational Delays, Trust Dependencies, and Decentralization Erosion.

Specifically, the `DEFAULT_ADMIN_ROLE` has the authority to update the token used for airdrops. This capability allows the admin to change the token type at any point, potentially impacting the value or relevance of the tokens being airdropped. Additionally, the `SENDER_ROLE`, which can distribute tokens to specified addresses, adds another layer of centralization, as this role can selectively decide the recipients of the token distributions. This combination of centralized control points can lead to potential misuse or uneven distribution strategies.

```
    function dropTokensToAll(
        address[] memory recipients,
        uint256[] memory amounts
    ) external onlyRole(SENDER_ROLE) {
        ...
    }

    function updateToken(address newToken) public
onlyRole(DEFAULT_ADMIN_ROLE) {
        ...
        token = IERC20(newToken);
        ONE_TOKEN = 10 ** IERC20Metadata(newToken).decimals();
        emit TokenUpdated(newToken);
    }
```

Recommendation

To address this finding and mitigate centralization risks, it is recommended to evaluate the feasibility of migrating critical configurations and functionality into the contract's codebase itself. This approach would reduce external dependencies and enhance the contract's self-sufficiency. It is essential to carefully weigh the trade-offs between external configuration flexibility and the risks associated with centralization.

L04 - Conformance to Solidity Naming Conventions

Criticality	Minor / Informative
Location	Airdrop.sol#L31
Status	Unresolved

Description

The Solidity style guide is a set of guidelines for writing clean and consistent Solidity code. Adhering to a style guide can help improve the readability and maintainability of the Solidity code, making it easier for others to understand and work with.

The followings are a few key points from the Solidity style guide:

1. Use camelCase for function and variable names, with the first letter in lowercase (e.g., myVariable, updateCounter).
2. Use PascalCase for contract, struct, and enum names, with the first letter in uppercase (e.g., MyContract, UserStruct, ErrorEnum).
3. Use uppercase for constant variables and enums (e.g., MAX_VALUE, ERROR_CODE).
4. Use indentation to improve readability and structure.
5. Use spaces between operators and after commas.
6. Use comments to explain the purpose and behavior of the code.
7. Keep lines short (around 120 characters) to improve readability.

```
uint256 private ONE_TOKEN
```

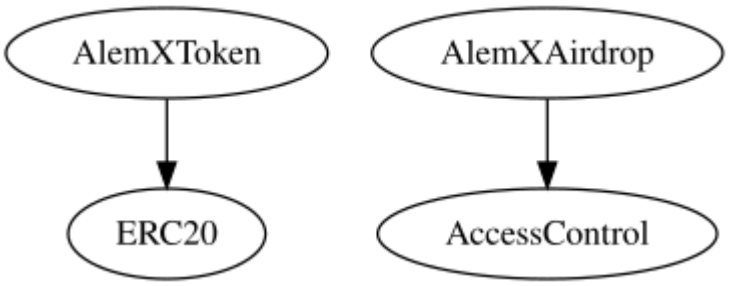
Recommendation

By following the Solidity naming convention guidelines, the codebase increased the readability, maintainability, and makes it easier to work with.
Find more information on the Solidity documentation
https://docs.soliditylang.org/en/v0.8.17/style-guide.html#naming-convention.

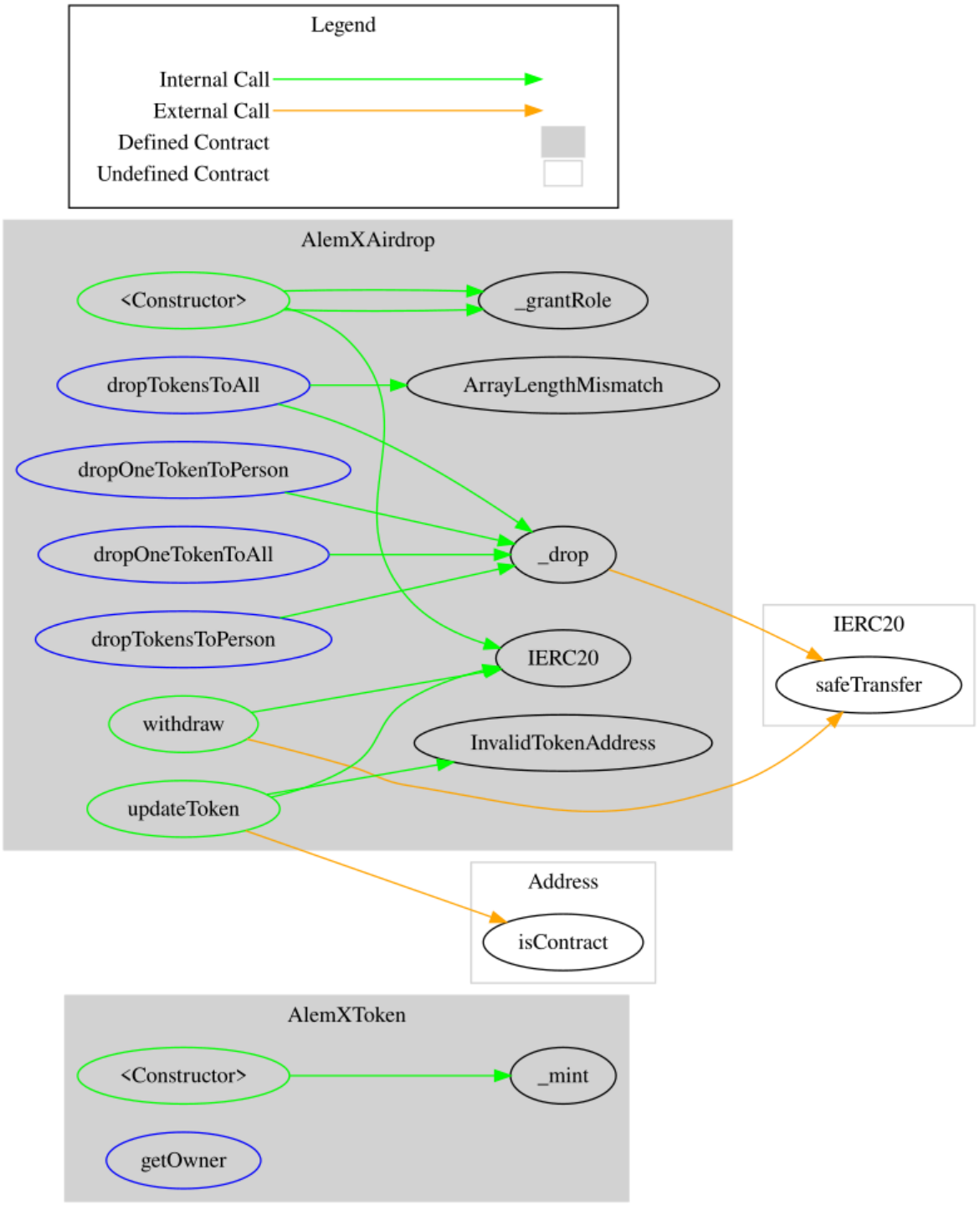
Functions Analysis

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
AlemXToken	Implementation	ERC20		
		Public	✓	ERC20
	getOwner	External		-
AlemXAirdrop	Implementation	AccessControl		
		Public	✓	-
	dropTokensToAll	External	✓	onlyRole
	dropOneTokenToAll	External	✓	onlyRole
	dropTokensToPerson	External	✓	onlyRole
	dropOneTokenToPerson	External	✓	onlyRole
	_drop	Internal	✓	
	withdraw	Public	✓	onlyRole
	updateToken	Public	✓	onlyRole

Inheritance Graph



Flow Graph


Legend
Internal Call
External Call
Defined Contract
Undefined Contract
AlemXAirdrop
<Constructor>
_grantRole
dropTokensToAll
ArrayLengthMismatch
dropOneTokenToPerson
dropOneTokenToAll
_drop
dropTokensToPerson
IERC20
withdraw
InvalidTokenAddress
updateToken
IERC20
safeTransfer
Address
isContract
AlemXToken
<Constructor>
_mint
getOwner

Summary

AlemX is a project that leverages two smart contracts, AlemXToken and AlemXAirdrop. The AlemXToken contract implements a decentralized token system with no specific owner, emphasizing its unique governance structure. Meanwhile, the AlemXAirdrop contract offers functionality for both bulk and individual airdrops, incorporating security features like role-based permissions. This audit assesses security vulnerabilities, business logic flaws, and identifies opportunities for optimization within these contracts.

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