Cyberscope

Audit Report

NaliAltair

December 2022

SHA256 13d88ae3af117596663e5cc000fff9f31ee862418f9c1091717bf0786a2f08b4

Audited by © cyberscope

Table of Contents

Contract Review

Contract Name	NaliAltair
Testing Deploy	https://testnet.bscscan.com/address/0x4ee43930936d8a1c3ddf90949f4a03490e9f76b8

Audit Updates

Initial Audit	16 Nov 2022 https://github.com/cyberscope-io/audits/blob/main/nali/v1/naliAltair.pdf
Corrected Phase 2	09 Dec 2022 https://github.com/cyberscope-io/audits/blob/main/nali/v2/naliAltair.pdf
Corrected Phase 3	22 Dec 2022

Source Files

Filename	SHA256
@openzeppelin/contracts-upgradeable/access/OwnableUpgradeable.sol	da66c17044345dc892d85bd7ddc9745d25df0b3dacfba8f84eb87c60d6e40fe3
@openzeppelin/contracts-upgradeable/proxy/utils/Initializable.sol	74def996fd6faf32f13ab9cacfc71d57400177de340fe5d5d7c6e805dfbab3bd
@openzeppelin/contracts-upgradeable/security/PausableUpgradeable.sol	c05b019a0b3bee8f3fac2da7c929f7d665b97d6d046aa35126615fff11205119
@openzeppelin/contracts-upgradeable/token/ERC1155/ERC1155Upgradeable.sol	8b4e2fd7e04b94b6717095b54aeb001f75e49b0e974b04a41ea2e7fb742877ea
@openzeppelin/contracts-upgradeable/token/ERC1155/extensions/ERC1155BurnableUpgradeable.sol	4cef49efc3c1d62289ff13b719092fd0191fd979448147f2b7588de4cea2cfae
@openzeppelin/contracts-upgradeable/token/ERC1155/extensions/ERC1155SupplyUpgradeable.sol	98d3570efe134810096cab2ce5d39c51323d9216e8528198fac44dd15cd3c841
@openzeppelin/contracts-upgradeable/token/ERC1155/extensions/ERC1155URIStorageUpgradeable.sol	7da34d679483559e38cbae26e66e21d39b4e5f191b1942669b45ac29cd965f09
@openzeppelin/contracts-upgradeable/token/ERC1155/extensions/IERC1155MetadataURIUpgradeable.sol	61e3317af2516530f091665d198fc3e27fb514038600fb07b7813913f439775f
@openzeppelin/contracts-upgradeable/token/ERC1155/IERC1155ReceiverUpgradeable.sol	7108589dbf9528c2ffe4f17fe489e8183be55c15b51af3b88c70252c13bac539
@openzeppelin/contracts-upgradeable/token/ERC1155/IERC1155Upgradeable.sol	5321f224c08b59651968dde0db5abeec4ea0bdf371c7b0c25707e56b455882fe
@openzeppelin/contracts-upgradeable/utils/AddressUpgradeable.sol	1d7d481b79fd54d957c9a0696f6227f7799fec01d8ba41f5c130a7cc6b4eddc9
@openzeppelin/contracts-upgradeable/utils/ContextUpgradeable.sol	5fb301961e45cb482fe4e05646d2f529aa449fe0e90c6671475d6a32356fa2d4
@openzeppelin/contracts-upgradeable/utils/introspection/ERC165Upgradeable.sol	fd84e5284eccc479268f0ef36b830019d4f7999ceb7959430d8d8d9e602dd4ef
@openzeppelin/contracts-upgradeable/utils/introspection/IERC165Upgradeable.sol	a39bc026ad6214e9ecd526bd4a1ddf9862d80bd4a9d0d031d9bafa4c3c147c0b

@openzeppelin/contracts-upgradeable/utils/math/MathUpgradeable.sol	158a0316fa289fad12c2ca764449e43e6724fb79c58fc438508d116f9af46b39
@openzeppelin/contracts-upgradeable/utils/StringsUpgradeable.sol	68f5690fc266a6b48386c28cbfd72ec67c24b05a51ce26d24103577c15f61401
contracts/interfaces/IRoles.sol	d13aac5175ddfd3af1ee4dc652d46b5f317214c0455a10ee580c0b2d414876e0
contracts/NaliAltair.sol	13d88ae3af117596663e5cc000fff9f31ee862418f9c1091717bf0786a2f08b4

Introduction

The NaliAltair contract implements an NFT contract. The contract is implemented as an upgradable proxy.

Roles

The contract roles are provided by an outside source. The Roles contract is out of the scope of this audit. The contract has an admin role.

The admin has the authority to

- Mint and MintBatch NFTs.
- Pause and Unpause contract transactions.
- Change the Roles Contract.
- Set approval for all.

Users have the authority to view contracts URI.

Contract Diagnostics

Critical Medium Minor / Informative

Severity	Code	Description	Status
	ST	Stops Transactions	Unresolved

ST - Stops Transactions

Criticality	Minor / Informative
Locations	contracts/NaliAltair.sol#L104
Status	Unresolved

Description

The contract owner has the authority to stop the transactions for all users including the owner. The owner may take advantage of it by calling the pause method.

```
function _beforeTokenTransfer(
    address operator,
    address from,
    address to,
    uint256[] memory ids,
    uint256[] memory amounts,
    bytes memory data
)
    internal
    override(ERC1155Upgradeable, ERC1155SupplyUpgradeable)
    whenNotPaused
{
    super._beforeTokenTransfer(operator, from, to, ids, amounts, data);

}
```

Recommendation

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. That risk can be prevented by temporarily locking the contract or renouncing ownership.

Contract Functions

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
OwnableUpgradeable	Implementation	Initializable, ContextUpgradeable		
	__Ownable_init	Internal	✓	onlyInitializing
	__Ownable_init_unchained	Internal	✓	onlyInitializing
	owner	Public		-
	_checkOwner	Internal		
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	_transferOwnership	Internal	✓	
Initializable	Implementation			
	_disableInitializers	Internal	✓	
PausableUpgradeable	Implementation	Initializable, ContextUpgradeable		
	__Pausable_init	Internal	✓	onlyInitializing
	__Pausable_init_unchained	Internal	✓	onlyInitializing
	paused	Public		-
	_requireNotPaused	Internal		
	_requirePaused	Internal		
	_pause	Internal	✓	whenNotPaused
	_unpause	Internal	✓	whenPaused

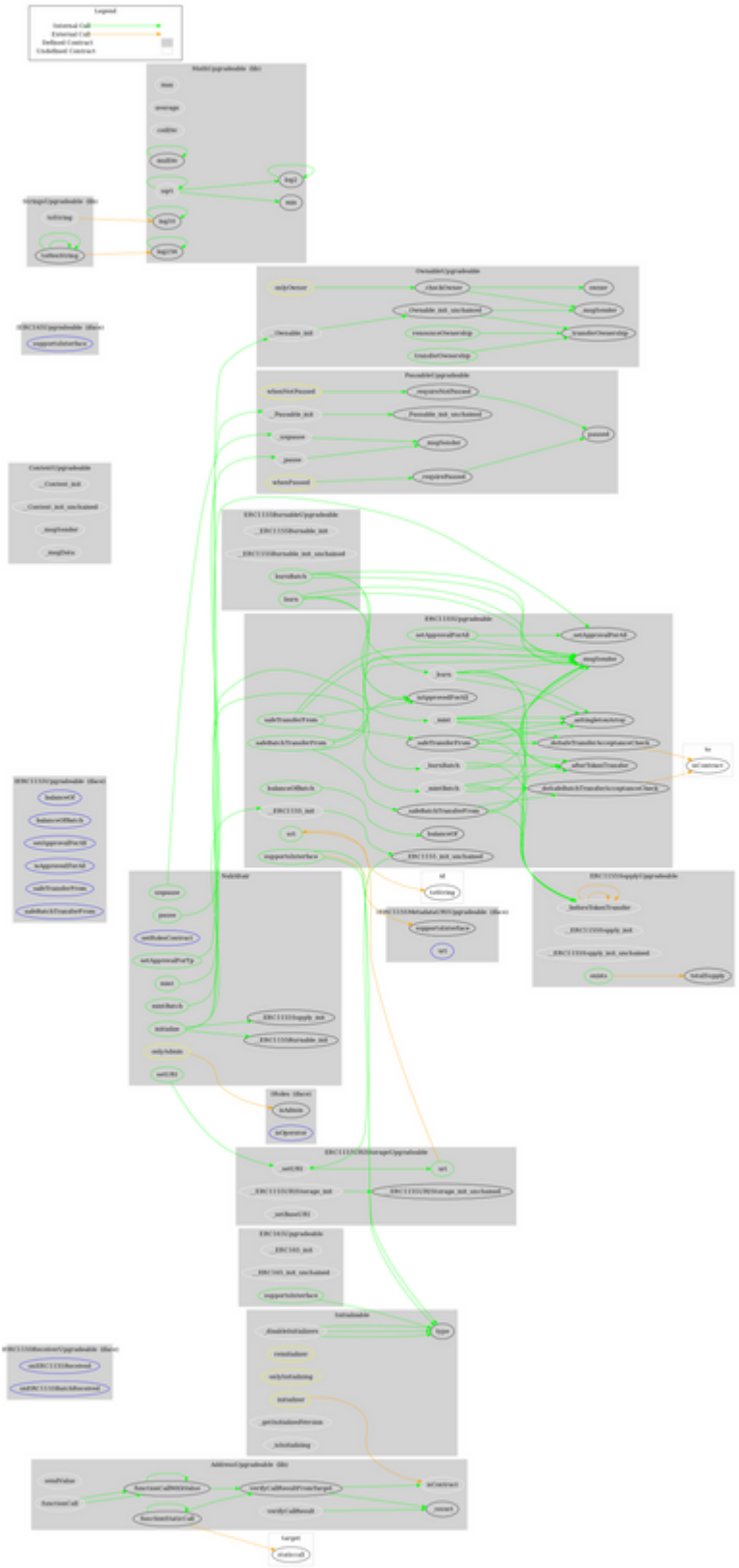
ERC1155Upgradeable	Implementation	Initializable, ContextUpgradeable, ERC165Upgradeable, IERC1155Upgradeable, IERC1155MetadataURIUpgradeable		
	__ERC1155_init	Internal	✓	onlyInitializing
	__ERC1155_init_unchained	Internal	✓	onlyInitializing
	supportsInterface	Public		-
	uri	Public		-
	balanceOf	Public		-
	balanceOfBatch	Public		-
	setApprovalForAll	Public	✓	-
	isApprovedForAll	Public		-
	safeTransferFrom	Public	✓	-
	safeBatchTransferFrom	Public	✓	-
	_safeTransferFrom	Internal	✓	
	_safeBatchTransferFrom	Internal	✓	
	_setURI	Internal	✓	
	_mint	Internal	✓	
	_mintBatch	Internal	✓	
	_burn	Internal	✓	
	_burnBatch	Internal	✓	
	_setApprovalForAll	Internal	✓	
	_beforeTokenTransfer	Internal	✓	
	_afterTokenTransfer	Internal	✓	
	_doSafeTransferAcceptanceCheck	Private	✓	
	_doSafeBatchTransferAcceptanceCheck	Private	✓	
	_asSingletonArray	Private		
ERC1155BurnableUpgradeable	Implementation	Initializable, ERC1155Upgradeable		

	__ERC1155Burnable_init	Internal	✓	onlyInitializing
	__ERC1155Burnable_init_unchained	Internal	✓	onlyInitializing
	burn	Public	✓	-
	burnBatch	Public	✓	-
ERC1155SupplyUpgradeable	Implementation	Initializable, ERC1155Upgradeable		
	__ERC1155Supply_init	Internal	✓	onlyInitializing
	__ERC1155Supply_init_unchained	Internal	✓	onlyInitializing
	totalSupply	Public		-
	exists	Public		-
	_beforeTokenTransfer	Internal	✓	
ERC1155URIStorageUpgradeable	Implementation	Initializable, ERC1155Upgradeable		
	__ERC1155URIStorage_init	Internal	✓	onlyInitializing
	__ERC1155URIStorage_init_unchained	Internal	✓	onlyInitializing
	uri	Public		-
	_setURI	Internal	✓	
	_setBaseURI	Internal	✓	
IERC1155MetadataURIUpgradeable	Interface	IERC1155Upgradeable		
	uri	External		-
IERC1155ReceiverUpgradeable	Interface	IERC165Upgradeable		
	onERC1155Received	External	✓	-
	onERC1155BatchReceived	External	✓	-
IERC1155Upgradeable	Interface	IERC165Upgradeable		
	balanceOf	External		-

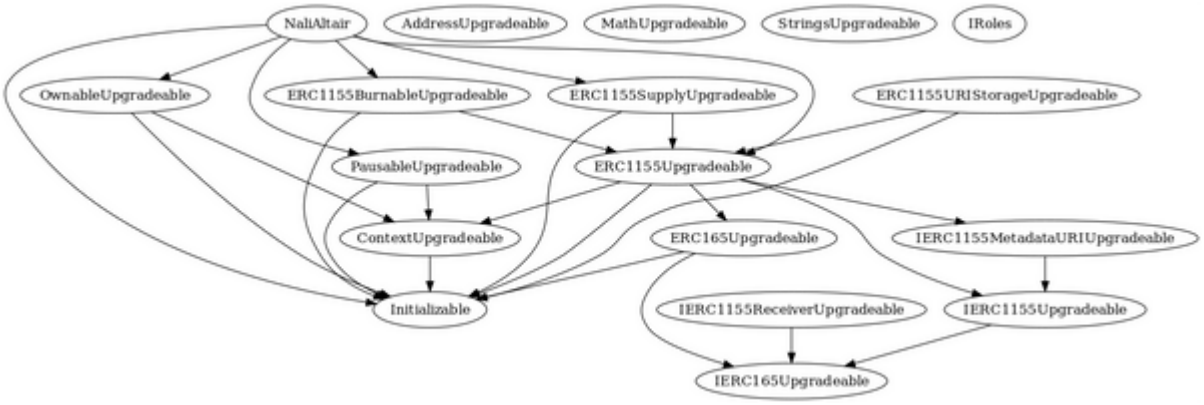
	balanceOfBatch	External		-
	setApprovalForAll	External	✓	-
	isApprovedForAll	External		-
	safeTransferFrom	External	✓	-
	safeBatchTransferFrom	External	✓	-
AddressUpgradeable	Library			
	isContract	Internal		
	sendValue	Internal	✓	
	functionCall	Internal	✓	
	functionCall	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionStaticCall	Internal		
	functionStaticCall	Internal		
	verifyCallResult	Internal		
ContextUpgradeable	Implementation	Initializable		
	__Context_init	Internal	✓	onlyInitializing
	__Context_init_unchained	Internal	✓	onlyInitializing
	_msgSender	Internal		
	_msgData	Internal		
ERC165Upgradeable	Implementation	Initializable, IERC165Upgradeable		
	__ERC165_init	Internal	✓	onlyInitializing
	__ERC165_init_unchained	Internal	✓	onlyInitializing
	supportsInterface	Public		-
IERC165Upgradeable	Interface			
	supportsInterface	External		-

StringsUpgradeable	Library			
	toString	Internal		
	toHexString	Internal		
	toHexString	Internal		
	toHexString	Internal		
IRoles	Interface			
	isAdmin	External		-
	isOperator	External		-
NaliAltair	Implementation	Initializable, ERC1155Upgradeable, OwnableUpgradeable, PausableUpgradeable, ERC1155BurnableUpgradeable, ERC1155SupplyUpgradeable		
	initialize	Public	✓	initializer
	setRolesContract	External	✓	onlyAdmin
	uri	Public		-
	setURI	Public	✓	onlyAdmin
	pause	Public	✓	onlyAdmin
	unpause	Public	✓	onlyAdmin
	mint	Public	✓	onlyAdmin
	mintBatch	Public	✓	onlyAdmin
	_beforeTokenTransfer	Internal	✓	whenNotPaused
	setApprovalForTp	Public	✓	onlyAdmin

Contract Flow



Inheritance Graph



Summary

The NaliAlrair operates as an upgradable NFT contract. The Smart Contract analysis reported no compiler errors or critical issues. This audit focused on investigating possible security issues and potential improvements.

We state that admin privileges are necessary and required for proper protocol operations. Thus, we emphasize the contract owner to be extra careful with the credentials.

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