Cyberscope

Audit Report

CardFi

January 2023

cardFI_NFT 65bed586f903e661b811122a68ccbc6f971091acc50e04c21566cacda0b649cb

cardFi fadb97ed55afe4d2c93c42e4ac22549bbe848e5b9206f7ab373def58d1b2d1f0

Audited by © cyberscope

Table of Contents

Table of Contents 1
Review 2
Audit Updates 2
Source Files 3
Introduction 4
Roles 4
Admin 4
User 4
Diagnostics 5
STC - Succeeded Transfer Check 6
Description 6
Recommendation 6
DSM - Data Structure Misuse 7
Description 7
Recommendation 7
Contract Functions 8
Inheritance Graph 10
Flow Graph 11
Domain Info 12
Summary 13
Disclaimer 14
About Cyberscope 15

Review

Contract Name	cardFi_2
Compiler Version	v0.8.17+commit.8df45f5f
Optimization	200 runs
CardFi Test Deploy	https://testnet.bscscan.com/address/0xc695d2856a9346dc00d2eb8295552385569d7ca0
CardFI_NFT Test Deploy	https://testnet.bscscan.com/token/0x0De146Cb82099BEc981b79a8343aaDA00Ca2A922
Domain	cardfi.co

Audit Updates

Initial Audit	05 Dec 2022 https://github.com/cyberscope-io/audits/tree/main/cardfi/v1/audit.pdf
Corrected Phase 2	13 Dec 2022 https://github.com/cyberscope-io/audits/tree/main/cardfi/v2/audit.pdf
Corrected Phase 3	10 Jan 2023

Source Files

Filename	SHA256
cardFi_2.sol	fadb97ed55afe4d2c93c42e4ac22549bbe848e5b9206f7ab373def58d1b2d1f0
cardFI_NFT.sol	65bed586f903e661b811122a68ccbc6f971091acc50e04c21566cacda0b649cb
IcardFi.sol	825bbe0a96079b47fb31ac478a98b681b960599bf460cfc80cb02b99bb417472

Introduction

The project consists of two contracts, **cardFi** and **cardFi_NFT**.

The user deposits native currency to receive NFT.

The are two options:

- Pay to receive NFT.
- Pay to receive NFT and lock cardFi tokens to redeem later.

The payment amount, native currency cost, lock period and cardFi amount depends on the card type.

Roles

The projects includes two roles, Admin and User.

Admin

The Admin Role has the authority to:

- Alter NFT card type properties.
- Alter deposit and withdraw fees.

User

The User Role has the authority to:

- Register new currency.
- Register new tokens.
- Deposit native currency to receive NFT.

Diagnostics

Critical Medium Minor / Informative

Severity	Code	Description	Status
●	STC	Succeeded Transfer Check	Acknowledged
●	DSM	Data Structure Misuse	Acknowledged

STC - Succeeded Transfer Check

Criticality	Minor / Informative
Location	cardFI_NFT.sol#L142
Status	Acknowledged

Description

According to the ERC20 specification, the transfer methods should be checked if the result is successful. Otherwise, the contract may wrongly assume that the transfer has been established.

```
function topUpBalance(uint256 amount) public onlyOwner{
    currency.transferFrom(msg.sender, address(this), amount);
}
```

Recommendation

The contract should check if the result of the transfer methods is successful. The team is advised to check the SafeERC20 library from the Openzeppelin library.

DSM - Data Structure Misuse

Criticality	Minor / Informative
Location	cardFi_2.sol#L110
Status	Acknowledged

Description

The contract uses the valuable `allowedCrypto` as an array. The business logic of the contract does not require to iterate this structure sequentially. Thus, unnecessary loops are produced that increase the required gas.

```
IERC20Upgradeable[] public allowedCrypto;
...
function tokenExist(IERC20Upgradeable tokenAddress) public view returns(bool
ifExist) {
    for (uint256 i = 0; i < allowedCrypto.length; i++) {
        if (allowedCrypto[i] == tokenAddress) {
            return true;
        }
    }
    return false;
}
```

Recommendation

The contract could use a data structure that provides instant access. For instance, a Set or a Map would fit better to the business logic of the contract. This way the time complexity will be reduced from o(n) to o(1).

Contract Functions

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
cardFi_2	Implementation	Initializable, OwnableUpgradeable		
	initialize	Public	✓	initializer
	setRoyaltyAddress	Public	✓	onlyOwner
	setRoyalty_native	Public	✓	onlyOwner
	setRoyalty_ERC20	Public	✓	onlyOwner
	seeRoyalty_native	Public		onlyOwner
	seeRoyalty_ERC20	Public		onlyOwner
	tokenExist	Public		-
	showAllowedCrypto	Public		-
	addCurrency	Public	✓	-
	tokenToNft	Private	✓	
	deposit_ERC20	Public	✓	-
	deposit_native	Public	Payable	-
	contractBalance_ERC20	Public		onlyOwner
	contractBalance_native	Public		onlyOwner
	cardInfo	Public		-
	redeem	Public	✓	-
cardFi_NFT	Implementation	ERC721URIStorage, IERC721Receiver, Ownable		
		Public	✓	ERC721
	mintNft	Public	Payable	-

	mintNftCustom	Public	Payable	-
	viewTokenURI	Public		-
	setCardFiAddress	Public	✓	onlyOwner
	viewCardFiAddress	Public		onlyOwner
	setRoyaltyAddress	Public	✓	onlyOwner
	viewRoyaltyAddress	Public		onlyOwner
	setNftType	Public	✓	onlyOwner
	viewNftType	Public		-
	contractBalance	Public		onlyOwner
	topUpBalance	Public	✓	onlyOwner
	viewCurrency	Public		-
	onERC721Received	External		-
IcardFi	Interface			
	deposit_ERC20	External	Payable	-

Inheritance Graph

Flow Graph


Legend
Internal Call
External Call
Defined Contract
Undefined Contract
IcardFi (iface)
deposit_ERC20
cardFi_2
initialize
__Ownable_init
setRoyaltyAddress
setRoyalty_native
setRoyalty_ERC20
seeRoyalty_native
seeRoyalty_ERC20
showAllowedCrypto
deposit_ERC20
cardInfo
contractBalance_native
deposit_native
redeem
payable
tokenToNft
addCurrency
tokenExist
contractBalance_ERC20
IERC721Upgradeable
ownerOf
royaltyAddress
transfer
IERC20Upgradeable
transferFrom
transfer
balanceOf
approve
cardFi_NFT
topUpBalance
contractBalance
<Constructor>
mintNft
viewCardFiAddress
viewRoyaltyAddress
viewNftType
mintNftCustom
viewTokenURI
viewCurrency
onERC721Received
setRoyaltyAddress
setCardFiAddress
payable
IERC20Upgradeable
setNftType
IERC721Upgradeable
_safeMint
_setTokenURI
tokenURI
_royaltyAddress
transfer

Domain Info

Domain Name	cardfi.co
Registry Domain ID	D47284542FEC9472C9A129B2E3F85D44F-GDREG
Creation Date	2022-09-23T03:29:14Z
Updated Date	2022-09-28T03:29:14Z
Registry Expiry Date	2023-09-23T03:29:14Z
Registrar WHOIS Server	whois.godaddy.com
Registrar URL	whois.godaddy.com
Registrar	GoDaddy.com, LLC
Registrar IANA ID	146

The domain was created 3 months before the creation of the audit. It will expire in 9 months.

There is no public billing information, the creator is protected by the privacy settings.

Summary

This audit focused on investigating possible security issues 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