16th OCTOBER 2020

SMART CONTRACT AUDIT REPORT

-

version v1.1

Smart Contract Security Audit and General Analysis

HAECHI AUDIT

Table of Contents

2 Issues (1 Critical, 0 Major, 1 Minor) Found

About HAECHI AUDIT

HAECHI AUDIT is a global leading smart contract security audit and development firm operated by HAECHI LABS. HAECHI AUDIT consists of professionals with years of experience in blockchain R&D and provides the most reliable smart contract security audit and development services.

So far, based on the HAECHI AUDIT's security audit report, our clients have been successfully listed on the global cryptocurrency exchanges such as Huobi, Upbit, OKEX, and others.

Our notable portfolios include SK Telecom, Ground X by Kakao, and Carry Protocol while HAECHI AUDIT has conducted security audits for the world's top projects and enterprises.

Trusted by the industry leaders, we have been incubated by Samsung Electronics and awarded the Ethereum Foundation Grants and Ethereum Community Fund.

Contact : audit@haechi.io
Website : audit.haechi.io

01. Introduction

This report was written to provide a security audit for the arNFT smart contract. HAECHI AUDIT conducted the audit focusing on whether arNFT smart contract is designed and implemented in accordance with publicly released information and whether it has any security vulnerabilities.

The issues found are classified as CRITICAL, MAJOR, MINOR or TIPS according to their severity.

CRITICAL	Critical issues are security vulnerabilities that MUST be addressed in order to prevent widespread and massive damage.
MAJOR	Major issues contain security vulnerabilities or have faulty implementation issues and need to be fixed.
MINOR	Minor issues are some potential risks that require some degree of modification.
TIPS	Tips could help improve the code's usability and efficiency

HAECHI AUDIT advises addressing all the issues found in this report.

02. Summary

Issues

HAECHI AUDIT has 1 Critical Issues, 0 Major Issues, and 1 Minor Issue; also, we included 1 Tip category that would improve the usability and/or efficiency of the code.

Severity	Issue	Status
CRITICAL	Cannot redeem yInsure swapped tokens	(Found - v1.0)
MINOR	Use SafeERC20	(Found - v1.0) (Resolved - v2.0)
TIPS	Missing events	(Found - v1.0) (Resolved - v2.0)
Notice	Need confirmation from yInsure and Nexus Mutual for an upgrade to support arNFT.	(Found - v1.0)

03. Overview

Features

ARMOR team has implemented ERC721 token with following features.

- buy Nexus Mutual[1] Quotation
- claim coverage
- redeem coverage
- swap yInsure to arNFT

Contracts Subject to Audit

- arNFT
- ERC721Full
- ERC721Enumerable
- ERC721Metadata
- ERC721
- ERC165
- Context
- Address
- SafeMath
- ReentrancyGuard
- Ownable

[1] https://nexusmutual.io/

Roles

The arNFT Smart contract has the following authorizations:

- **Owner**

The features accessible by each level of authorization is as follows:

Role	Functions
Owner	● arNFT ○ switchMembership() ○ nxmTokenApprove() ○ activateSwap() ● Ownable ○ transferOwnership() ○ renounceOwnership()

Notice

- **Need confirmation from yInsure and Nexus Mutual for an upgrade to support arNFT.**

  ARMOR team claims that the arNFT is for replacing the yInsure, which acts similar to arNFT but has some bugs.

  1. yInsure cannot redeem since it uses CoverId instead of ClaimId in yInsure#_payoutIsCompleted().
  2. yInsure#_sendAssuredSum() sends without multiplying decimals

  ARMOR team insists that according to these bugs, yInsure team has agreed to migrate all Quotations yInsure has on their contract to arNFT. To achieve this, they also mentioned that Nexus Mutual is helping the ARMOR team to be able to receive cover amounts of Quotations that yInsure owns to arNFT address.

  Although this statement seems promising and will solve issues of locked redeem amounts on yInsure, HAECHI AUDIT could not confirm any of these statements.

  If these statements were confirmed or announced prior to audit, arNFT would not have any issues beside the TIPS.

  As soon as these statements are confirmed, we are going to resolve the issue.

  We, HAECHI AUDIT, are looking forward to the official statements/announcements from the yInsure team and Nexus Mutual team.

Update

ARMOR team has introduced swapActivated variable to enable swap functionality after the official announcement.

04. Issues Found

CRITICAL : Cannot redeem yInsure swapped tokens (Found - v1.0)

CRITICAL

```
161.   function redeemClaim(uint256 _tokenId) public onlyTokenApprovedOrOwner(_tokenId)
       nonReentrant {
162.       require(claimIds[_tokenId] != 0, "No claim is in progress.");
163.
164.       (/*cid*/, /*memberAddress*/, /*scAddress*/, bytes4 currencyCode, /*sumAssured*/,
       /*premiumNXM*/) = _getCover1(_tokenId);
165.       ( , uint8 coverStatus, uint256 sumAssured, , ) = _getCover2(_tokenId);
166.
167.       require(coverStatus == uint8(CoverStatus.ClaimAccepted), "Claim is not accepted");
168.       require(_payoutIsCompleted(claimIds[_tokenId]), "Claim accepted but payout not completed");
169.
170.       _burn(_tokenId);
171.
172.       _sendAssuredSum(currencyCode, sumAssured);
173.
174.       emit ClaimRedeemed(msg.sender, sumAssured, currencyCode);
175.   }
```

Problem Statement

arNFT#redeemClaim() cannot redeem yInsure swapped tokens since arNFT is not the one who receives payout from nexus mutual when claim is accepted. ARMOR team insists that they are being supported by Nexus Mutual team to enable these, but we could not confirm if these are true since it will be disclosed after the audit report. This issue will be removed as soon as HAECHI AUDIT confirms the update from Nexus Mutual.

Update

ARMOR team has introduced swapActivated variable to enable swap functionality after the official announcement.

MINOR : Use SafeERC20 (Found - v1.0) (Resolved - v2.0)

MINOR

Problem Statement

Since arNFT should support all tokens available on Nexus Mutual, the ARMOR team does not have authority to handle which tokens can be used for buying Quotation. Although the erc20 standard states that erc20 should return bool when functions are called, there are many tokens that do not return bool.
Which can break the arNFT contract when these tokens are used to buy Quotation.

Recommendation

Use SafeERC20 library to interact with ERC20 tokens.

Update

arNFT is now using SafeERC20 library on all ERC20 token interactions

TIPS: Missing events

TIPS

arNFT#swapYnft(), arNFT#buyCover(), arNFT#submitClaim() does not emit Swap, BuyCover, SubmitClaim events. Although these functions do emit other events on other contracts, adding events on arNFT will increase user experience and clarity.

Update

arNFT now emits appropriate events on swapYnft(), buyCover(), submitClaim()

05. Disclaimer

This report is not an advice on investment, nor does it guarantee adequacy of a business model and/or a bug-free code. This report should be used only to discuss known technical problems. The code may include problems on Ethereum that are not included in this report. It will be necessary to resolve addressed issues and conduct thorough tests to ensure the safety of the smart contract.