sec3™

Security Assessment Report

Holasui Escrow Contract

August 3rd, 2023

Summary

The sec3 team (formerly Soteria) was engaged to do a thorough security analysis of the Holasui escrow smart contract. The artifact of the audit was the source code in https://github.com/LoyaltyGM/escrow-contract/blob/dd51b71/sources/escrow.move

The initial audit was done on commit dd51b7111b0b8513eaf4b041757f098b5e0883f3 and revealed 2 issues.

This report describes the findings and resolutions in detail.

Table of Contents

Result Overview

Issue	Impact	Status
[L-1] Missing checks of verified NFTs	Low	Resolved
[I-1] Unsafe coding practice in check_items_ids	Informational	Resolved

Findings in Detail

[L -1] Missing checks of verified NFTs

According to the description at https://holasui.notion.site/Hola-P2P-Swap-Verified-Collections-4974a982a2c548a4af2e9391a5538d6c, this contract is designed for exchanging verified NFTs.

However, there is no relevant whitelist validation at the contract level to ensure that creator_items are all verified NFTs.

Moreover, there are no checks or prompts on the page for receiving offers (https://github.com/LoyaltyGM/holasui-website/blob/main/src/pages/swap/history/%5BofferId%5D.tsx).

As a result, a malicious user could create their own NFTs with identical images and deceive other users into exchanging with them.

Possible repair

Add a check in the contract or on the page for receiving offers to verify whether the CreatorObjects belong to validated collections.

Resolution

A badge has been added in the front end to indicate if the collection is verified or not. This issue has been resolved.

[I - 1] Unsafe coding practice in check_items_ids

```
/* sources/escrow.move */
fun check_items_ids<T: key + store>(
    items: &vector<T>,
    ids: &vector<ID>
) {
    assert!(vector::length(items) == vector::length(ids), EWrongItem);

    let i = 0;
    while (i < vector::length(items)) {
        assert!(
            vector::contains(ids,&object::id(vector::borrow(items, i))),
            EWrongItem
        );
        i = i + 1;
    };
}
```

When ensuring that the items provided by the recipient for completing the swap meet the requirements, the contract first checks whether the quantity of items provided by the recipient matches the quantity required by the escrow creator. Then, it verifies if each item's ID provided by the recipient is present in the list required by the creator.

This coding practice can be further improved. Since the variable `items` is not entirely reliable, a better approach would be to verify whether each item's ID required by the creator is present among the items provided by the recipient. However, in this particular scenario, since the `items` generally does not have a `copy` ability, this will not introduce any security risks.

Resolution

This is an informational issue, and no action is needed. This issue is resolved.

Appendix: Methodology and Scope of Work

The sec3 (formerly Soteria) audit team, which consists of Computer Science professors and industrial researchers with extensive experience in smart contract security, program analysis, testing and formal verification, performed a comprehensive manual code review, software static analysis and penetration testing.

Assisted by the sec3 Scanner developed in-house, the audit team particularly focused on the following work items:

- Check common security issues
- Check program logic implementation against available design specifications
- Check poor coding practices and unsafe behavior
- The soundness of the economics design and algorithm is out of the scope of this work

DISCLAIMER

The instance report ("Report") was prepared pursuant to an agreement between Coderrect Inc. d/b/a sec3 (the "Company") and HolaSui (the "Client"). This Report solely includes the results of a technical assessment of a specific build and/or version of the Client's code specified in the Report ("Assessed Code") by the Company. The sole purpose of the Report is to provide the Client with the results of the technical assessment of the Assessed Code. The Report does not apply to any other version and/or build of the Assessed Code. Regardless of the contents of the Report, the Report does not (and should not be interpreted to) provide any warranty, representation, or covenant that the Assessed Code: (i) is error and/or bug-free, (ii) has no security vulnerabilities, and/or (iii) does not infringe any third-party rights. Moreover, the Report is not, and should not be considered, an endorsement by the Company of the Assessed Code and/or of the Client. Finally, the Report should not be considered investment advice or a recommendation to invest in the Assessed Code and/or the Client.

This Report is considered null and void if the Report (or any portion thereof) is altered in any manner.

ABOUT

Founded by leading academics in the field of software security and senior industrial veterans, sec3 (formerly Soteria) is a leading blockchain security company. We are also building sophisticated security tools that incorporate static analysis, penetration testing, and formal verification.

At sec3, we identify and eliminate security vulnerabilities through the most rigorous process and aided by the most advanced analysis tools.

For more information, check out our website and follow us on twitter.

sec3™