Neoki Multi Metaverse

Security Assessment – Re-audit

11th May 2023

TRUSCOVA

TRUSTED CODE VALIDATION

Prepared for: Neoki Multi Metaverse

Prepared by: Dr. Muhammad Hassan

WE SECURE YOUR SMART CONTRACTS

About Truscova

Founded in last quarter of 2022 and headquartered in Bremen, Germany, Truscova aims to secure Web 3.0 by providing security assessment, audit, advisory and training services using formal verification and other leading technologies. Truscova founders include eminent scientists with more than 35 books, several patents, and more than 20,000 google scholar citations in the areas of verification, testing, security, and machine learning.

We focus on smart contracts testing and code review projects in Ethereum ecosystem, supporting client organizations in technology, defense, and finance industries, as well as government entities. We specialize in applying formal verification, dynamic analysis, fuzz testing, metamorphic testing, advanced coverage metrics, and static analysis to secure Web 3.0 projects.

We maintain an exhaustive list of publications at https://github.com/Truscova, with links to papers, presentations, public audit reports, and blog articles.

To explore our latest news and developments, please follow @truscova on Twitter or LinkedIn. You can also explore our repository at https://github.com/Truscova or blog articles at https://truscova.com/blog.php. To engage us directly, visit our "Contact" page at https://www.truscova.com/.

Truscova GmbH
Wilhelm-Liebknecht-Str. 4
28329 Bremen, Germany

Geschäftsführung
Dr. Muhammad Hassan

Tel. +49 (162) 919 6783
E-Mail: hassan@truscova.com
https://www.truscova.com

SOLARIS
IBAN DE81 1101 0101 5569 4416 33
BIC SOBKDEB2XXX

Handelsregister: HRB 38524
Registergericht: Amtsgericht Bremen
Umsatzsteuer-ID: DE360065309

Notices and Remarks

Copyright and Distribution

This report is produced by Truscova for public information. It is licensed to Neoki Multi Metaverse under the terms of the project agreement and is being made public as per project agreement.

Test Coverage Disclaimer

All activities undertaken by Truscova in this project were performed in accordance with terms of the project agreement.

Truscova uses a combination of automated testing techniques and manual inspection to conduct security assessments and identify security flaws of the target system. Each method carries its own limitations.

Security assessments are time bound (hence not exhaustive) and are reliant on information provided by the client. As a result, the findings documented in this report should not be considered a comprehensive list of security issues, flaws, or defects in the target system or codebase.

Truscova GmbH
Wilhelm-Liebknecht-Str. 4
28329 Bremen, Germany

Geschäftsführung
Dr. Muhammad Hassan

Tel. +49 (162) 919 6783
E-Mail: hassan@truscova.com
https://www.truscova.com

SOLARIS
IBAN DE81 1101 0101 5569 4416 33
BIC SOBKDEB2XXX

Handelsregister: HRB 38524
Registergericht: Amtsgericht Bremen
Umsatzsteuer-ID: DE360065309

Contents

Truscova GmbH
Wilhelm-Liebknecht-Str. 4
28329 Bremen, Germany

Geschäftsführung
Dr. Muhammad Hassan

Tel. +49 (162) 919 6783
E-Mail: hassan@truscova.com
https://www.truscova.com

SOLARIS
IBAN DE81 1101 0101 5569 4416 33
BIC SOBKDEB2XXX

Handelsregister: HRB 38524
Registergericht: Amtsgericht Bremen
Umsatzsteuer-ID: DE360065309

Executive Summary

Engagement Overview and Scope

Neoki Multi Metaverse engaged Truscova GmbH from 20th April 2023 till 11th May 2023 to re-audit the code base provided via online repository available at following link:

https://github.com/ojoaoguilherme-neoki

The scope of audit is limited to the following:

https://github.com/ojoaoguilherme-neoki/re-audit (commit febf463d476e928820ed9135324a0252345c0116)

One security expert at Truscova audited the above code base using static analysis, symbolic execution, fuzzing, formal verification, and manual inspection. A summary of findings is discussed in the next subsection.

Summary of Findings

The uncovered vulnerabilities in codebase during the course of the audit are summarized in the following table:

Vulnerability Classification

Classification	*Count*
High Impact	1
Medium Impact	1
Low Impact	2
Informational	1

Vulnerability Categorization

Category	*Count*
Data Validation	3
Arithmetic	1

Truscova GmbH
Wilhelm-Liebknecht-Str. 4
28329 Bremen, Germany

Geschäftsführung
Dr. Muhammad Hassan

Tel. +49 (162) 919 6783
E-Mail: hassan@truscova.com
https://www.truscova.com

SOLARIS
IBAN DE81 1101 0101 5569 4416 33
BIC SOBKDEB2XXX

Handelsregister: HRB 38524
Registergericht: Amtsgericht Bremen
Umsatzsteuer-ID: DE360065309

Notable Findings

Significant flaws that impact system are listed below.

- **TCV-NK-5**

  The comparison operation is inverted.

Truscova GmbH
Wilhelm-Liebknecht-Str. 4
28329 Bremen, Germany

Geschäftsführung
Dr. Muhammad Hassan

Tel. +49 (162) 919 6783
E-Mail: hassan@truscova.com
https://www.truscova.com

SOLARIS
IBAN DE81 1101 0101 5569 4416 33
BIC SOBKDEB2XXX

Handelsregister: HRB 38524
Registergericht: Amtsgericht Bremen
Umsatzsteuer-ID: DE360065309

Project Summary

Contact Information

Following officials from Truscova participated in this project.

Dr. Muhammad Naiman Jalil, naiman@truscova.com	Project Coordination
Dr. Muhammad Hassan, hassan@truscova.com	Security Assessment Expert

Project Timeline

The significant project events and milestones are as follows:

Date	Event
24th March 2023	Audit Report for Neoki Multi Metaverse Submitted
20th April 2023	Re-Worked Code Shared by Neoki for Re-Audit Assessment
11th May 2023	Re-Audit Report Shared with Neoki

Truscova GmbH
Wilhelm-Liebknecht-Str. 4
28329 Bremen, Germany

Geschäftsführung
Dr. Muhammad Hassan

Tel. +49 (162) 919 6783
E-Mail: hassan@truscova.com
https://www.truscova.com

SOLARIS
IBAN DE81 1101 0101 5569 4416 33
BIC SOBKDEB2XXX

Handelsregister: HRB 38524
Registergericht: Amtsgericht Bremen
Umsatzsteuer-ID: DE360065309

Project Goals

The engagement was scoped to assess the security of Neoki Multi Metaverse's Lands, Marketplace, Token, and NFT contracts. Specifically, we focused to answer the following non-exhaustive list of questions:

- Are there appropriate access controls in place?
- Are user-provided parameters sufficiently validated?
- Are the arithmetic calculations and state changes performed during NFT purchases and token purchases, correct?
- How is oracle data obtained and handled?
- Could an attacker steal funds from the system?
- Is there a way for users to circumvent fees?
- Could an attacker take over the contract's ADMIN_ROLE?
- How does the minting of NFTs work?

Truscova GmbH
Wilhelm-Liebknecht-Str. 4
28329 Bremen, Germany

Geschäftsführung
Dr. Muhammad Hassan

Tel. +49 (162) 919 6783
E-Mail: hassan@truscova.com
https://www.truscova.com

SOLARIS
IBAN DE81 1101 0101 5569 4416 33
BIC SOBKDEB2XXX

Handelsregister: HRB 38524
Registergericht: Amtsgericht Bremen
Umsatzsteuer-ID: DE360065309

Project Targets

The engagement involved a review and testing of the following targets:

Neoki Multi Metaverse

1. Repository https://github.com/ojoaoguilherme-neoki/re-audit (commit febf463d476e928820ed9135324a0252345c0116)

Codebase Type: Solidity

Truscova GmbH
Wilhelm-Liebknecht-Str. 4
28329 Bremen, Germany

Geschäftsführung
Dr. Muhammad Hassan

Tel. +49 (162) 919 6783
E-Mail: hassan@truscova.com
https://www.truscova.com

SOLARIS
IBAN DE81 1101 0101 5569 4416 33
BIC SOBKDEB2XXX

Handelsregister: HRB 38524
Registergericht: Amtsgericht Bremen
Umsatzsteuer-ID: DE360065309

Summary of Findings

The table below summarizes the findings of the review, including type and severity details.

ID	Title	Type	Severity
1	Unnecessary variables used	-	Informational
2	removeLandFromLandsArray lacks input validation	Data validation	Medium
3	removeLandFromLandsArray lacks data validation	Data validation	Low
4	Address validation for zero address	Data validation	Low
5	Incorrect comparison operation	Arithmetic	High

Truscova GmbH
Wilhelm-Liebknecht-Str. 4
28329 Bremen, Germany

Geschäftsführung
Dr. Muhammad Hassan

Tel. +49 (162) 919 6783
E-Mail: hassan@truscova.com
https://www.truscova.com

SOLARIS
IBAN DE81 1101 0101 5569 4416 33
BIC SOBKDEB2XXX

Handelsregister: HRB 38524
Registergericht: Amtsgericht Bremen
Umsatzsteuer-ID: DE360065309

Detailed Findings

1. Unnecessary variables used

Severity: Informational	Difficulty: -
Type: -	Finding ID: TCV-NK-1
Target: LandSell	

Description

The function is using i and index for the same purpose.

```
function getAllSellingLands() external view returns (Map[] memory) {
        Map[] memory landsForSell = new Map[](tokensForSell.length);
        uint256 index = 0;
        for (uint i = 0; i < tokensForSell.length; i++) {
            landsForSell[index] = landMap[tokensForSell[i]];
            index++;
        }
        return landsForSell;
    }
```

Recommendation

Remove index to make code easier to read and maintain.

Truscova GmbH
Wilhelm-Liebknecht-Str. 4
28329 Bremen, Germany

Geschäftsführung
Dr. Muhammad Hassan

Tel. +49 (162) 919 6783
E-Mail: hassan@truscova.com
https://www.truscova.com

SOLARIS
IBAN DE81 1101 0101 5569 4416 33
BIC SOBKDEB2XXX

Handelsregister: HRB 38524
Registergericht: Amtsgericht Bremen
Umsatzsteuer-ID: DE360065309

2. removeLandFromLandsArray lacks input validation

Severity: Medium	Difficulty: Low
Type: input validation	Finding ID: TCV-NK-2
Target: LandSell	

Description

The function accepts a tokenId and removes it from the tokensForSell array. However, it does not validate if the tokenId exists in the tokensForSell array or not. In case the tokenId does not exist, the last Land will be popped anyway resulting in loss of Land.

As a side note, the function is defined internal, so whichever function will call this has to do validation. It is better to validate the input here to make it less error prone.

```
function removeLandFromLandsArray(uint256 tokenId) internal {
        uint256 removeIndex = 0;
        for (uint256 i = 0; i < tokensForSell.length; i++) {
            if (tokensForSell[i] == tokenId) {
                delete tokensForSell[i];
                removeIndex = i;
            }
        }

        tokensForSell[removeIndex] = tokensForSell[tokensForSell.length - 1];
        tokensForSell.pop();
    }
```

Recommendation

Validate the tokenId if it exists in the tokensForSell.

Truscova GmbH
Wilhelm-Liebknecht-Str. 4
28329 Bremen, Germany

Geschäftsführung
Dr. Muhammad Hassan

Tel. +49 (162) 919 6783
E-Mail: hassan@truscova.com
https://www.truscova.com

SOLARIS
IBAN DE81 1101 0101 5569 4416 33
BIC SOBKDEB2XXX

Handelsregister: HRB 38524
Registergericht: Amtsgericht Bremen
Umsatzsteuer-ID: DE360065309

3. removeLandFromLandsArray lacks data validation

Severity: Low	Difficulty: Low
Type: Data validation	Finding ID: TCV-NK-3
Target: LandSell	

Description

The function accepts a tokenId and removes it from the tokensForSell array. However, it does not validate if the tokensForSell is empty or not. In case the tokensForSell is empty, the last Land will be popped anyway resulting transaction revert.

As a side note, the function is defined internal, so whichever function will call this has to do validation. It is better to validate the input here to make it less error prone.

```
function removeLandFromLandsArray(uint256 tokenId) internal {
        uint256 removeIndex = 0;
        for (uint256 i = 0; i < tokensForSell.length; i++) {
            if (tokensForSell[i] == tokenId) {
                delete tokensForSell[i];
                removeIndex = i;
            }
        }

        tokensForSell[removeIndex] = tokensForSell[tokensForSell.length - 1];
        tokensForSell.pop();
    }
```

Recommendation

Validate the tokensForSell if it is empty or not.

Truscova GmbH
Wilhelm-Liebknecht-Str. 4
28329 Bremen, Germany

Geschäftsführung
Dr. Muhammad Hassan

Tel. +49 (162) 919 6783
E-Mail: hassan@truscova.com
https://www.truscova.com

SOLARIS
IBAN DE81 1101 0101 5569 4416 33
BIC SOBKDEB2XXX

Handelsregister: HRB 38524
Registergericht: Amtsgericht Bremen
Umsatzsteuer-ID: DE360065309

4. Address validation for zero address

Severity: Low	Difficulty: Low
Type: Data validation	Finding ID: TCV-NK-4
Target: NeokiMarketplaceV2	

Description

The _nko address is not validated for zero address.

```
constructor(
        address _foundation,
        address _stakingPool,
        address _nko,
        address _admin
    ) {
        require(
            _foundation != address(0),
            "Foundation address cannot be set to zero"
        );
        require(
            _stakingPool != address(0),
            "Staking Pool address cannot be set to zero"
        );
        require(_admin != address(0), "Admin address cannot be set to zero");
        foundation = _foundation;
        stakingPool = _stakingPool;
        nko = IERC20(_nko);
        _grantRole(DEFAULT_ADMIN_ROLE, msg.sender);
        _grantRole(FOUNDATION_ROLE, msg.sender);
        _grantRole(MARKETPLACE_ADMIN_ROLE, _admin);
        _grantRole(FOUNDATION_ROLE, foundation);
    }
```

Recommendation

Check that the address is not zero.

Truscova GmbH
Wilhelm-Liebknecht-Str. 4
28329 Bremen, Germany

Geschäftsführung
Dr. Muhammad Hassan

Tel. +49 (162) 919 6783
E-Mail: hassan@truscova.com
https://www.truscova.com

SOLARIS
IBAN DE81 1101 0101 5569 4416 33
BIC SOBKDEB2XXX

Handelsregister: HRB 38524
Registergericht: Amtsgericht Bremen
Umsatzsteuer-ID: DE360065309

5. Incorrect comparison operation

Severity: High	Difficulty: Low
Type: Arithmetic	Finding ID: TCV-NK-5
Target: NeokiMarketplaceV2	

Description

The amount of items available in the marketplace is compared with _removeAmount. The function removes the amount of items from the marketplace. However, the require statement is doing the wrong comparison, i.e., it ensures that items listed in marketplace are always less than or equal to the amount of items to be removed. This function will always revert unless the listed items and items to be removed are same.

```
function removeMyListingItemAmount(
        uint256 _itemId,
        uint256 _removeAmount
    ) external nonReentrant {
        MarketItem storage item = marketItem[_itemId];
        require(
            item.owner == msg.sender,
            "Marketplace: Not the owner of the listed item"
        );
        require(item.amount > 0, "Marketplace: There is no NFT to withdraw");

        require(
            item.amount <= _removeAmount,
            "Marketplace: Caller requested higher amount than balance"
        );
        require(
            item.amount - _removeAmount >= 0,
            "Marketplace: Cannot withdraw more than balance"
        );
```

Recommendation

The require statement should check if item.amount >= _removeAmount.

Truscova GmbH
Wilhelm-Liebknecht-Str. 4
28329 Bremen, Germany

Geschäftsführung
Dr. Muhammad Hassan

Tel. +49 (162) 919 6783
E-Mail: hassan@truscova.com
https://www.truscova.com

SOLARIS
IBAN DE81 1101 0101 5569 4416 33
BIC SOBKDEB2XXX

Handelsregister: HRB 38524
Registergericht: Amtsgericht Bremen
Umsatzsteuer-ID: DE360065309

Summary of Recommendations

The Neoki Multi Metaverse is a work in progress with multiple planned iterations. Truscova recommends that Neoki Multi Metaverse address the findings detailed in this report and take the following additional steps prior to deployment:

- Identify and analyze all system properties that are expected to hold.
- Use Fuzz testing with Foundry or Echidna to test and validate those system properties.
- Develop a detailed incident response plan to ensure that any issues that arise can be addressed promptly and without confusion.
- Ensure that all arithmetic is performed correctly.
- Ensure proper access control.
- Create good documentation.

Truscova GmbH
Wilhelm-Liebknecht-Str. 4
28329 Bremen, Germany

Geschäftsführung
Dr. Muhammad Hassan

Tel. +49 (162) 919 6783
E-Mail: hassan@truscova.com
https://www.truscova.com

SOLARIS
IBAN DE81 1101 0101 5569 4416 33
BIC SOBKDEB2XXX

Handelsregister: HRB 38524
Registergericht: Amtsgericht Bremen
Umsatzsteuer-ID: DE360065309