




# Smart Contract Audit

For smart contract vulnerabilities, security exploits  
and attack vectors

CUSTOMER: XP.NETWORK

DATE: May 09th, 2023

# Code review and security report

 **IMPORTANT:** This document likely contains critical information about the Client’s software and hardware systems, security susceptibilities, descriptions of possible exploits and attack vectors. The document shall remain undisclosed until any significant vulnerabilities are remedied.

CLIENT:

XP.NETWORK

START DATE:

March 1st, 2023

TYPE, SUBTYPE:

Bridge

END DATE:

May 9th, 2023

## Scope

REPOSITORY:

https://github.com/XP-NETWORK/secret-bridge

DOCUMENTATION:

No documentation

TESTS:

Passing

AUDITORS:

Isaac, Elijah

REVIEW \$ APPROVAL:

Jacob

SMART CONTRACT AUDITED;

src/lib.rs

## Commit hashes:

BASE

D157BDAC66D8D815E84983590B2B4475654522B7

UPDATE:

AAB02DD49F977C8F50B7FDD6C78FECF8759765DF

## Checked For:

| Category          | Check Item  |
|-------------------|---|
| Code Review       | <ul style="list-style-type: none"><li>ChairsStyle guide violation</li><li>Unchecked math</li><li>Data consistency</li><li>Costly loop</li><li>Gas limit and loops</li><li>Ownership takeover</li></ul>  |
| Functional Review | <ul style="list-style-type: none"><li>Business logic review</li><li>Functionality checks</li><li>Access control and authorization</li><li>Kill switch mechanism</li><li>Data consistency manipulation</li><li>Token supply manipulation</li><li>Assets integrity</li><li>User balance manipulation</li><li>Event generation</li></ul> |

# Definitions of vulnerability classification



## CRITICAL

Bug / Logic failures in the code that cause loss of assets / data manipulation.

## HIGH

Difficult to exploit problems which could result in elevated privileges, data loss etc.

## MEDIUM

Bug / Logic failures in the code which need to be fixed but cannot lead to loss of assets / data manipulation.

## LOW

Mostly related to unused code, style guide violations, code snippets with low effect etc.

Findings



Summary

|        |   |          |              |
|--------|---|----------|--------------|
| XPN-01 | Currency symbol incorrect in WithdrawFees function. | Critical | Fixed        |
| XPN-02 | Possible unnecessary gas usage.                     | Medium   | Fixed        |
| XPN-03 | Low test coverage.                                  | Medium   | Fixed        |
| XPN-04 | No minimum fee amount check.                        | Medium   | Fixed        |
| XPN-05 | No coverage for NFT without token_uri.              | Medium   | Acknowledged |
| XPN-06 | Magic numbers should not be used.                   | Low      | Fixed        |



## Finding: XPN-01

Wrong currency symbol in WithdrawFees function.

WithdrawFees

Function

WithdrawFees

Lines 202

●

Critical

✓

Fixed

## Description

The currency symbol for withdrawing the fee used in the function `WithdrawFees` on `line202` is incorrect which can cause loss of funds when withdrawing the fees stored in the bridge.

## Recommendation

It is recommended to change the symbol in function `WithdrawFees` on `Line 202` from `SCRT` to `uscr t`

## Finding: XPN-02

Possible unnecessary gas usage

|                          |          |                          |          |          |         |
|--------------------------|----------|--------------------------|----------|----------|---------|
| SetPause                 | Function | SetPause                 | Line 184 | ● Medium | ✓ Fixed |
| WithdrawFees             | Function | WithdrawFees             | Line 199 | ● Medium | ✓ Fixed |
| WhiteListNft             | Function | WhiteListNft             | Line 219 | ● Medium | ✓ Fixed |
| ValidateUnfreezeNft      | Function | ValidateUnfreezeNft      | Line 224 | ● Medium | ✓ Fixed |
| ValidateUnfreezeNftBatch | Function | ValidateUnfreezeNftBatch | Line 245 | ● Medium | ✓ Fixed |
| ValidateTransferNft      | Function | ValidateUnfreezeNftBatch | Line 281 | ● Medium | ✓ Fixed |
| ValidateTransferNftBatch | Function | ValidateUnfreezeNftBatch | Line 307 | ● Medium | ✓ Fixed |

## Description

The check for signature at the end of the function can cause unnecessary gas usage in case of failure of signature verification which can cause unnecessary gas usage.

## Recommendation

It is recommended to check for signature verification before any loops or any calculation in the function.

## Finding: XPN-03

Low test coverage

src/tests.rs

src/tests.rs

● Medium

✓ Fixed

### Description

Test coverage is provided for a very limited number of functions in the bridge contract.

### Recommendation

It is recommended to have test coverage for all the use cases in a smart contract.

## Finding: XPN-04

No minimum fee amount check

handle

Function

handle

Line 167

● Medium

✓ Fixed

## Description

The only check in the bridge contract for the fee amount is that the fee cannot be zero, other than that it can be any amount.

## Recommendation

It is recommended to have a minimum fee amount check in function 

handle

line 167



## Finding: XPN-05

No coverage for NFTs without token\_uri.

|                          |          |                          |        |              |
|--------------------------|----------|--------------------------|--------|--------------|
| WithdrawNft              | Function | WithdrawNft              | Medium | Acknowledged |
| WithdrawNftBatch         | Function | WithdrawNftBatch         | Medium | Acknowledged |
| ValidateTransferNft      | Function | ValidateTransferNft      | Medium | Acknowledged |
| ValidateTransferNftBatch | Function | ValidateTransferNftBatch | Medium | Acknowledged |

## Description

In Secret Network, NFTs can have either token\_uri or extension for NFT metadata but in the bridge contract only token\_uri is being checked.

## Recommendation

It is recommended to have a check for token\_uri as well as extension when checking for metadata.

## Finding: XPN-06

Magic numbers should not be used.

WithdrawNft

Function

WithdrawNft

Line 510

●

Low

✓

Fixed

## Description

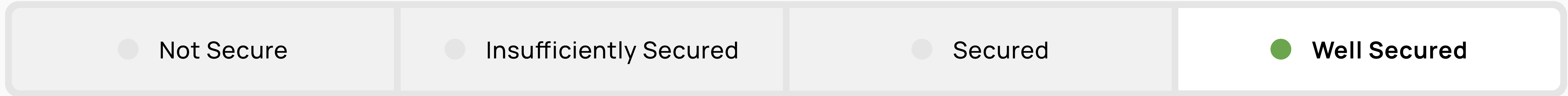
Magic number is used in `WithdrawNft` on `line 510` even though the same value is being used in other places and also a constant is already present for the said value.

## Recommendation

It is recommended to use the constant BLOCK\_SIZE instead of the magic number in `WithdrawNft` function `line 510`

## Executive Summary

Based on the audit findings the Client’s contracts are: Not Secure



# Disclaimers

## SafePress Disclaimer

The smart contracts given for audit have been analyzed by the best industry practices at the date of this report, with cybersecurity vulnerabilities and issues in smart contract source code, the details of which are disclosed in this report (Source Code); the Source Code compilation, deployment, and functionality (performing the intended functions). The audit makes no statements or warranties on the security of the code. It also cannot be considered a sufficient assessment regarding the utility and safety of the code, bug-free status, or any other contract statements. While we have done our best in conducting the analysis and producing this report, it is important to note that you should not rely on this report only – we recommend proceeding with several independent audits and a public bug bounty program to ensure the security of smart contracts.

## Technical Disclaimer

Smart contracts are deployed and executed on a blockchain platform. The platform, its programming language, and other software related to the smart contract can have vulnerabilities that can lead to hacks. Thus, the audit cannot guarantee the explicit security of the audited smart contracts.