




Smart Contract Audit

For smart contract vulnerabilities, security exploits
and attack vectors

CUSTOMER: XP.NETWORK

DATE: March 25th, 2024

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 25th, 2024

TYPE, SUBTYPE:

Bridge

END DATE:

May 29th, 2024

Scope

REPOSITORY:

https://github.com/XP-NETWORK/decentralized-bridge-smart-contracts/tree/main/cosmos

DOCUMENTATION:

No documentation

TESTS:

Passing

AUDITORS:

Muhammad Shoaib

REVIEW \$ APPROVAL:

Saad Saeed

SMART CONTRACT AUDITED;

/*

Commit hashes:

BASE

C7103DD1781AD2183CB580E38484BC6CD56D1C82

UPDATE:

E168004FC9DC9137E3ECFFC96E4DB9C6AE937CB6

Checked For:

Category	Check Item
Code Review	<ul style="list-style-type: none">ChairsStyle guide violationUnchecked mathData consistencyCostly loopGas limit and loopsOwnership takeover
Functional Review	<ul style="list-style-type: none">Business logic reviewFunctionality checksAccess control and authorizationKill switch mechanismData consistency manipulationToken supply manipulationAssets integrityUser balance manipulationEvent generation

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	Unique validator check in signature verification.	<div>Critical</div>	<div>Fixed</div>
XPN-02	Missing token id and contract in claimed event.	<div>Medium</div>	<div>Fixed</div>
XPN-03	Conversion and types issues.	<div>Medium</div>	<div>Fixed</div>

Finding: XPN-01

Unique validator check in signature verification.

validate_signatures

Function

validate_signatures

Lines 216

●

Critical

✓

Fixed

Description

Unique validator check is missing in the `validate_signatures` on `line 216` which can cause issue incase if a single validator signed all the threshold signatures and send to the bridge in a transaction.

Recommendation

It is recommended to make a check in function `validate_signatures` on `line 216` for unique validator to validate all the signatures in contract.

Finding: XPN-02

Missing token id and contract in claimed event.

claim721

Function

claim721

Line 822

●

Medium

✓

Fixed

Description

It is hard to identify or track the token id and contract address of the NFT that user claimed.

Recommendation

It is recommended to add token id and contract address of the claimed NFT in event `ClaimedEventInfo` in function `claim721`

Finding: XPN-03

Conversion and types issues

instantiate	Function	instantiate	Line 88, 103	● Medium	✓ Fixed
transfer_to_storage_721	Function	transfer_to_storage_721	Line 386	● Medium	✓ Fixed
lock721	Function	lock721	Lines 399, 420, 447	● Medium	✓ Fixed

Description

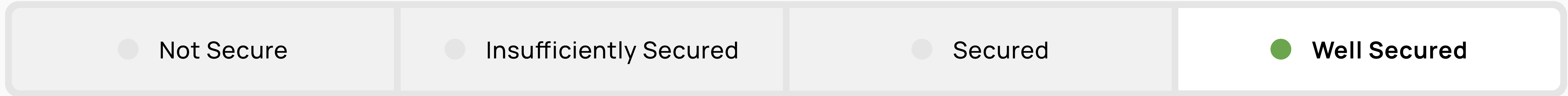
There are hard coded strings in this file and some of the strings and addresses missing type conversions.

Recommendation

It is recommended to remove the hardcoded strings with variables and fix the type conversions.

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.