




# Smart Contract Audit

Skale Endpoint of the Multi-Chain NFT Bridge

CUSTOMER: XP.NETWORK

DATE: Mar 1st, 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:	Feb 23rd, 2023
TYPE, SUBTYPE:	NFT Contract	END DATE:	Mar 1st, 2023

## Scope

REPOSITORY:	<a href="https://github.com/XP-NETWORK/web3-contracts/blob/erc1155/contracts/MinterERC20.sol">https://github.com/XP-NETWORK/web3-contracts/blob/erc1155/contracts/MinterERC20.sol</a>
DOCUMENTATION:	No documentation
TESTS:	No tests cases
AUDITORS:	Andrey, Sasha
REVIEW \$ APPROVAL:	Alexander
SMART CONTRACT AUDITED;	web3-contracts/blob/erc1155/contracts/MinterERC20.sol

## Commit hashes:

BASE:	2E0E7978E1D97A5FAFCFDAC89733F1EC548B447C
-------	--

# 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

XPSKL-01 :	The return value of an external transfer/transferFrom call is not checked.	High	Fixed
------------	--	------	-------

## Finding: XPSKL-01

The return value of an external transfer/transferFrom call is not checked.

Base	Function	validateTransferFees	Line 309-322	● High	✓ Fixed
------	----------	----------------------	--------------	--------	---------

## Description

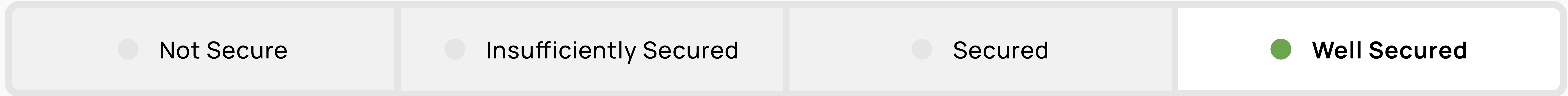
The return value of an external transfer/transferFrom call is not checked. Several tokens do not revert in case of failure and return false. If one of these tokens is used in MinterERC20, `validateTransferFees` will not revert if the transfer fails.

## Recommendation

Use SafeERC20, or ensure that transfer/transferFrom return value is checked.

## Executive Summary

Based on the audit findings the Client’s contracts are: Well Secured





# 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.