SOLIDIFIED

Audit Report for The Sandbox Asset Contract Vulnerability Fix - January 15, 2021

Summary

Audit Report prepared by Solidified covering the bugfixes applied to the Sandbox mixed ERC1155 and ERC721 contract.

Process and Delivery

Three (3) independent Solidified experts performed an unbiased and isolated audit of the code below. The debrief took place on January 15, 2021, and the results are presented here.

Audited Files

The following contracts were covered during the audit:

`src/solc_0.5/Asset/ERC1155ERC721.sol`

The fixes were supplied in commit number: `28510fd393d7ee6977055f2e06aca998a6025c2d`

Intended Behavior

The fixes prevent users from employing the batch transfer facility to transfer tokens to themselves.

SOLIDIFIED

Audit Report for The Sandbox Asset Contract Vulnerability Fix - January 15, 2021

Executive Summary

Smart contract audits are an important step to improve the security of smart contracts and can find many issues. However, auditing complex codebases has its limits and a remaining risk is present (see disclaimer).

Users of a smart contract system should exercise caution. In order to help with the evaluation of the remaining risk, we provide a measure of the following key indicators: **code complexity**, **code readability**, **level of documentation**, and **test coverage**.

Note, that high complexity or lower test coverage does not necessarily equate to a higher risk, although certain bugs are more easily detected in unit testing than a security audit and vice versa.

Criteria	Status	Comment
Code complexity	Medium	-
Code readability and clarity	High	-
Level of Documentation	Medium	-
Test Coverage	High	-

SOLIDIFIED

Audit Report for The Sandbox Asset Contract Vulnerability Fix - January 15, 2021

Issues Found

Solidified found that the bug discovered by the team has been adequately solved. No additional issues have been identified.

Issue #	Description	Severity	Status
1	User can manipulate balances by batch transferring tokens to own address	Critical	Resolved

SOLIDIFIED

Audit Report for The Sandbox Asset Contract Vulnerability Fix - January 15, 2021

Critical Issues

1. User can manipulate balances by batch transferring tokens to own address

Users can use the `batchTransfer()` function to send tokens to themselves. This causes the transferred funds to be added to the user's balance, resulting in an incorrect balance, which could be exploited maliciously.

Fix
The team has fixed the issue by ensuring that the sender and receiver addresses are different.

Major Issues

No major issues have been found.

Minor Issues

No minor issues have been found.

Notes

No additional observations.

Disclaimer

Solidified audit is not a security warranty, investment advice, or an endorsement of TSB GAMING LTD or its products. This audit does not provide a security or correctness guarantee of the audited smart contract. Securing smart contracts is a multistep process, therefore running a bug bounty program as a complement to this audit is strongly recommended.

The individual audit reports are anonymized and combined during a debrief process, in order to provide an unbiased delivery and protect the auditors of Solidified platform from legal and financial liability.

Solidified Technologies Inc.