



Audit Report for Origin Protocol - May 31, 2021

Summary

Audit Report prepared by Solidified covering a security fix in the Origin protocol.

Process and Delivery

Two (2) independent Solidified experts performed an unbiased and isolated audit of the code below. The debrief took place on May 31, 2021, and the results are presented here.

Audited Files

The audit covers the security fix implemented in the following commit:

<https://github.com/OriginProtocol/origin-dollar/pull/592/files>

Intended Behavior

The fix addresses an incorrect interaction with the 3-pool contract. Instead of obtaining the ERC-20 balance of the pool, the contract now uses the Curve-provided function for accessing the balance through the internal bookkeeping of the pool contract.

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	High	-
Test Coverage	High	-



Audit Report for Origin Protocol - May 31, 2021

Issues Found

Solidified found that fix adequately addresses the vulnerability and does not introduce any additional issues.

Critical Issues

No critical issues have been found.

Major Issues

No major issues have been found.

Minor Issues

No major issues have been found.

Notes

No additional notes.



Audit Report for Origin Protocol - May 31, 2021

Disclaimer

Solidified audit is not a security warranty, investment advice, or an endorsement of Origin Protocol 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.