Debase Preliminary
Code Security Audit Report

Author: cyotee doge

This is a preliminary report to provide a documented result of the security analysis in advance of the complete reports. The conclusions in the preliminary report can be accepted as the final assessment of AuditDAO. Supporting evidence and analysis will be provided in the final report.

Project Definition

Debase is a rebasing elastic supply token providing yield farming options incorporating randomization. Debase adjusts its supply in an attempt to reach its peg price of 1 DAI.

Debase distinguishes itself as being the first, to the best of our knowledge, rebasing token to provide compatible yield farming using their randomization technology. This provides an as close to accurate yield calculation as possible without direct integration with the token. It appears Debase did not directly integrate their token's rebase with their yield farming platform as a proof that the technology can work with an rebasing token.

Per Contract Assessment

DaiPool

Safe for deposit.

BurnPool

Safe for deposit.

Curve

Safe if data retrieval.

Oracle / ExampleOracleSimple

Safe for data retrieval.

Protocol Assessment

The currently deployed Debase protocol as of 2021-01-29 is safe from external attack. User deposits and assets for dispersal are determined to be safe from manipulation by currently known attack vectors and basic functionality errors.

Contract owner does have the ability to add and adjust deposit terms of the protocol which could potentially be abused to extract funds on withdrawal by users. This can be mitigated by users by confirming the fee properties of the contract as set to the expected values prior to withdrawal. These controls can not be used to simply withdraw user assets. Thus while a risk, it is a mitigatable risk through user confirmation and stalemate.