Potential critical vulnerability Curve based contracts

experience, Killari

February 11, 2021

1 Overview

In this document, we describe what we believe constitutes a critical vulnerability in all of the the Curve pools contracts. Used by a malicious attacke, it could gradually empty the pool with a repeat attack. Due to the way the Stableswap invariant is calculated, it is possible to add tokens to the liquidity pools up to precise values found to break the computation. This results in a deviation of the spot price from the expected price of ~ 1, *even in the case of balanced pools.* The attacker can then arbitrage against that virtual pool to turn a profit and effectively steal from it in a single transaction. Attached to this report, we provide a collection of scripts used to find the values that break the invariant calculation, and a mainnet ready example of the exploit using Aave flash loans.