G0 Group

Security Review of
Argent L2 Bridge Swapper
May 2022

Argent L2 Bridge Swapper / May 2022

Files in scope

Following solidity files:

https://github.com/argentlabs/l2-bridge-swapper/tree/082fe491d26af1266c08addcdb0460d650aea247/contracts

- AaveBridgeSwapper.sol
- BoostedEthBridgeSwapper.sol
- GroGvtBridgeSwapper.sol
- LidoBridgeSwapper.sol
- YearnBridgeSwapper.sol
- ZkSyncBridgeSwapper.sol

Current status

All discovered issues have been fixed by the developer. There are no known issues in the relevant contracts in https://github.com/argentlabs/l2-bridge-swapper/tree/7d915463a4cc09f523084a66401894defebc8b38/contracts

Issues

1. Price manipulation attack

type: security / severity: major

In `BoostedEthBridgeSwapper` an attacker can call `add_liquidity` on the `CurvePool` contract driving the price up, then trigger `BoostedEthBridgeSwapper.exchange` and call `remove_liquidity` making profit in the process. Analogous issues are also present in other swapper contracts.

status - fixed

Issue has been fixed and is no longer present in

https://github.com/argentlabs/l2-bridge-swapper/tree/7d915463a4cc09f523084a66401894defebc8b38/contracts