ZEROPOOL

Tornado.Cash Proxy Audit

Igor Gulamov, 13 March 2021

Introduction

ZeroPool conducted the audit of Tornado.Cash Proxy smart contract ERC20 fix.

This review was performed by an independent reviewer under a fixed rate.

Scope

https://github.com/tornadocash/tornado-anonymity-mining/pull/1/files

Issues

No critical and major issues found.

We consider the commit f9af21d9f15643733cca3373d8dde93c189f971c as a safe version from the informational security point of view.

Comment TornadoProxy.sol#L21-L22

We recommend using a special predefined token address for native token, for example, `0x0000000000000000000000000000000000000000` or `0xEeeeeEeeeEeEeeEeEeEeeEEEeeeeEeeeeeeeEEeE` to reduce size of structures and calldata.