LIDO PROTOCOL SECURITY AUDITOR'S NOTE ON THE DEPLOYED CODE COMPLIANCE

August 24, 2022

LIDO

MixBytes()

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Disclaimer

The audit makes no statements or warranties about utility of the code, safety of the code, suitability of the business model, investment advice, endorsement of the platform or its products, regulatory regime for the business model, or any other statements about fitness of the contracts to purpose, or their bug free status. The audit documentation is for discussion purposes only. The information presented in this report is confidential and privileged. If you are reading this report, you agree to keep it confidential, not to copy, disclose or disseminate without the agreement of Lido. If you are not the intended recipient(s) of this document, please note that any disclosure, copying or dissemination of its content is strictly forbidden.

1.2 Audited project

This note should be considered as an standalone addendum for the reference audit report: Lido protocol security audit report.

1.3 Project scope

The audit covered the following files:

File name	Link
NodeOperatorsRegistry.sol	https://github.com/lidofinance/lido-dao/blob/08436ce13d67501fa723169c1dc69fe47b90cde4/contracts/0.4.24/nos/NodeOperatorsRegistry.sol
StETH.sol	https://github.com/lidofinance/lido-dao/blob/08436ce13d67501fa723169c1dc69fe47b90cde4/contracts/0.4.24/StETH.sol
Lido.sol	https://github.com/lidofinance/lido-dao/blob/08436ce13d67501fa723169c1dc69fe47b90cde4/contracts/0.4.24/Lido.sol
ReportUtils.sol	https://github.com/lidofinance/lido-dao/blob/08436ce13d67501fa723169c1dc69fe47b90cde4/contracts/0.4.24/oracle/ReportUtils.sol
LidoOracle.sol	https://github.com/lidofinance/lido-dao/blob/08436ce13d67501fa723169c1dc69fe47b90cde4/contracts/0.4.24/oracle/LidoOracle.sol

File name	Link
MemUtils.sol	https://github.com/lidofinance/lido-dao/blob/08436ce13d67501fa723169c1dc69fe47b90cde4/contracts/0.4.24/lib/MemUtils.sol
Pausable.sol	https://github.com/lidofinance/lido-dao/blob/08436ce13d67501fa723169c1dc69fe47b90cde4/contracts/0.4.24/lib/Pausable.sol
deposit_contract.sol	https://github.com/lidofinance/lido-dao/blob/08436ce13d67501fa723169c1dc69fe47b90cde4/contracts/0.6.11/deposit_contract.sol
WstETH.sol	https://github.com/lidofinance/lido-dao/blob/08436ce13d67501fa723169c1dc69fe47b90cde4/contracts/0.6.12/WstETH.sol
DepositSecurityModule.sol	https://github.com/lidofinance/lido-dao/blob/08436ce13d67501fa723169c1dc69fe47b90cde4/contracts/0.8.9/DepositSecurityModule.sol
ECDSA.sol	https://github.com/lidofinance/lido-dao/blob/08436ce13d67501fa723169c1dc69fe47b90cde4/contracts/0.8.9/lib/ECDSA.sol
CompositePostRebaseBeaconReceiver.sol	https://github.com/lidofinance/lido-dao/blob/08436ce13d67501fa723169c1dc69fe47b90cde4/contracts/0.8.9/CompositePostRebaseBeaconReceiver.sol
OrderedCallbacksArray.sol	https://github.com/lidofinance/lido-dao/blob/08436ce13d67501fa723169c1dc69fe47b90cde4/contracts/0.8.9/OrderedCallbacksArray.sol
SelfOwnedStETHBurner.sol	https://github.com/lidofinance/lido-dao/blob/08436ce13d67501fa723169c1dc69fe47b90cde4/contracts/0.8.9/SelfOwnedStETHBurner.sol
LidoExecutionLayerRewardsVault.sol	https://github.com/lidofinance/lido-dao/blob/08436ce13d67501fa723169c1dc69fe47b90cde4/contracts/0.8.9/LidoExecutionLayerRewardsVault.sol
StakeLimitUtils.sol	https://github.com/lidofinance/lido-dao/blob/08436ce13d67501fa723169c1dc69fe47b90cde4/contracts/0.4.24/lib/StakeLimitUtils.sol

1.4 Audit results

Smart contracts have been audited and several suspicious places have been detected. During the audit, no critical vulnerabilities were found. One high, seven medium, and seven low issues were identified. After working on the reported findings, all of them were confirmed and fixed by the client and two findings were acknowledged. Full info provided with the reference Lido protocol security audit report.

1.5 Deployed contracts code compliance

Final commit identifier with all fixes: `08436ce13d67501fa723169c1dc69fe47b90cde4`
corresponds to the code of smart contracts deployed on Ethereum mainnet network, the addresses of which are listed below:

File name / Contract deployed on mainnet	GitHub sources
Lido.sol `0x47EbaB13B806773ec2A2d16873e2dF770D130b50`	Lido.sol#08436ce, StETH.sol#08436ce, Pausable.sol#08436ce, StakeLimitUtils.sol#08436ce
WstETH.sol `0x7f39c581f595b53c5cb19bd0b3f8da6c935e2ca0`	WstETH.sol#08436ce
LidoOracle.sol `0x1430194905301504e8830ce4B0b0df7187E84AbD`	LidoOracle.sol#08436ce, ReportUtils.sol#08436ce
NodeOperatorsRegistry.sol `0x5d39ABaa161e622B99D45616afC8B837E9F19a25`	NodeOperatorsRegistry.sol#08436ce, MemUtils.sol#08436ce
LidoExecutionLayerRewardsVault.sol `0x388C818CA8B9251b393131C08a736A67ccB19297`	LidoExecutionLayerRewardsVault.sol#08436ce
DepositSecurityModule.sol `0x710B3303fB508a84F10793c1106e32bE873C24cd`	DepositSecurityModule.sol#08436ce, ECDSA.sol#08436ce
CompositePostRebaseBeaconReceiver.sol `0x55a7E1cbD678d9EbD50c7d69Dc75203B0dBdD431`	CompositePostRebaseBeaconReceiver.sol#08436ce, OrderedCallbacksArray.sol#08436ce
SelfOwnedStETHBurner.sol `0xB280E33812c0B09353180e92e27b8AD399B07f26`	SelfOwnedStETHBurner.sol#08436ce
deposit_contract.sol `0x00000000219ab540356cbb839cbe05303d7705fa`	deposit_contract.sol#08436ce

2. ABOUT MIXBYTES

MixBytes is a team of blockchain developers, auditors and analysts keen on decentralized systems. We build open-source solutions, smart contracts and blockchain protocols, perform security audits, work on benchmarking and software testing solutions, do research and tech consultancy

Contacts


https://github.com/mixbytes/audits_public

https://mixbytes.io/


hello@mixbytes.io


https://twitter.com/MixBytes