STATE MIND

Lido roles analysis

28-08-2023 - 20-10-2023

Table of contents

1. Project Brief

Title	Description
Client	Lido
Project name	Lido roles analysis
Timeline	28-08-2023 – 20-10-2023

Short Overview

The Statemind team was asked by Lido DAO to provide a security analysis of Lido on Ethereum protocol roles and mutators.

Lido is the leading liquid staking solution – providing a simple way to get rewards on your digital tokens. By staking with Lido your tokens remain liquid and can be used across a range of DeFi applications, getting extra rewards.

There are several parts of the protocol:

- Staking pool. The main part of Lido that provides functionality to stake ETH and receive stETH. The staking pool contains several modules:
  - Lido/stETH staking pool and liquid token: manage deposits, staking rewards, and withdrawals.
  - Oracles: oracles send the Consensus and Execution layers data from the same reference slot to the Execution Layer.
  - StakingRouter: responsible for managing the list of modules, allocating stake to modules, calculating fees and sending deposits to DepositContract, a former responsibility of Lido. Lido distributes the protocol fee based on the calculations provided by StakingRouter.
  - NodeOperatorsRegistry: entities that manage a secure and stable infrastructure for running validator clients for the benefit of the protocols. They're dedicated staking providers who can ensure the safety of funds belonging to the protocol users and the correctness of validator operations.
- DAO. Lido liquid protocols management entity, is responsible for picking node operators, configuring the protocol parameters and much more. DAO includes two parts:
  - Aragon DAO Aragon is a DAO framework with on-chain voting as one of the crucial features. To reduce operational burden and voter fatigue several proposals are usually combined into a package. Such packages are called "Omnibus votes". Script on Aragon can do different operations: update smart contracts, any fund transfers, etc.
  - Easy Track. Easy Track is developed as an efficient mechanism to assist with routine and uncontentious governance proposals for the Lido DAO. It can do only the allowlisted type of actions via a registered set of specialized EVMScript factories. Importantly, flexibility and scalability are all paramount concerns throughout the development of Easy Track, with extensive measures taken to ensure that safety has not been compromised for convenience. Easy Track allows optimistical governance (the vote passes by default unless objected to by the LDO holders).

2. Methodology

This analysis aims to create an overview of possible security risks associated with the roles system. The Statemind team iterates over all roles and their security impact on the protocol by going through the following steps:

- Identify all roles and their rights to mutate protocol state and measure impact level. Sample questions to answer:
  - Can the role steal the user's funds?
  - Can the role permanently stop protocol?
  - Can the role temporarily stop protocol?
- Provide analysis of the role owners to measure their security level. Sample questions to answer:
  - Is the role owner an EOA?
  - Is the role owner a multisig? What parameters does it have? How the ownership can be overtaken?
  - Is the role owner a DAO? How the ownership can be overtaken?
  - How the owner is defined?
  - How the owner can be changed?
- Match the owner analysis with roles analysis to identify potential weaknesses
- Analyze the protocol mutators to identify potential weaknesses
- Provide recommendations to improve the protocol security

Common definitions

Authentication types

There are several auth types, which are used in the contracts. They have a common description and grant/revoke roles mechanism.

Aragon ACL

This implementation uses Aragon mechanism authentication. Checking the role and issuing it occurs through an Aragon contracts, regardless of the specific implementation, through a modifier or an internal call.

Custom ACL

Variable, which is set in storage, can be changed, added, removed, reset.

Custom ACL (OZ fork)

Fork of OpenZeppelin AccessControlEnumerable with unstructured storage, implements OpenZeppelin IAccessControlEnumerable.sol interface.

Custom ACL (immutable)

Variable, which is set in the constructor as immutable. Lies in the bytecode.

Custom ACL (off-chain)

Variable, which is set in storage, can be changed, added, removed, reset. Authentication is going through ERC-712 compliant signatures.

Custom ACL (over OZ ERC1967Proxy)

Variable, which is set at ADMIN_SLOT storage slot for ERC1967Proxy pattern.

OZ Ownable

OpenZeppelin Ownable contract implementation with owner storage variable.

OZ AccessControl

OpenZeppelin AccessControl implementation.

Owner types

There are several owner types, which own several roles.

Externally Owned Account (EOA)

Have a private key and perform any actions.

Multisig (Safe–Gnosis)

Multisig has a threshold > 0 signatures (Signers should have their private keys). After passing the threshold a transaction can be executed through CALL or DELEGATECALL. Transactions could be checked by the guard if set.

Easy Track

EasyTrack motion is a lightweight voting is considered to have passed if the minimum objections threshold hasn't been exceeded. EasyTrack contract is the main contract, which implements the Easy Track voting mechanism.

Oracle members quorum

The quorum members need to submit the same data hashes to submit the data itself later to the oracle.

Aragon Voting

Aragon contract allows creating new votes, voting for existing votes, and executing votes on behalf of token holders. Aragon voting can be compromised in the following cases:

1. Hidden issues in the Aragon Voting contract. However, Aragon OS successfully passed audits, and projects with high TVL have used Aragon in the production environment for a long time.
2. The attacker has a significant amount of voting tokens (LDO tokens) and the remaining voters don't get the necessary number of votes to reject.

The attacker can't manipulate LDO token balances without attacking other related roles, because it is protected by Aragon Voting. So, the more tokens an attacker has, the higher the probability of accepting a malicious offer. The attacker in the most cases is expected to rely on the potential economic benefits from the attack.

- Every vote uses snapshot voting token balances from previous blocks, so it excludes the voting impact from immediate buys votes from the market.
- Support = 50 %, min quorum = 5 % setting params should have enough value, so, it mitigates accepting voting with a single big stake.
- Voting token is sufficiently distributed between holders

So, part of the solution can be improved: In the worst scenario attacker can buy 5% of the total supply from the market (cost of around 200m$) and accept a negative proposal. So, other voters should have at least 5% "no" votes for rejecting the proposal.

However, we suggest evaluating the cost/impact of every vote suggested by the Lido DAO.

Aragon Agent

Hold DAO assets and execute actions from the Aragon contract. It can execute with some data (make a call), safe execute (without touching protected tokens), and execute a script (delegate call to an executor). Each of these actions requires a certain role.

Aragon Token Manager

Contract manages the DAO token and can burn, and mint tokens.

GateSeal

The Seal committee can pause withdrawals-related parts of some contracts. Need to have signatures of txn hash for 3 owners out of 6. All owners are EOA, 4 of them are historically active on-chain, causing a higher probability of receiving their signatures.

Lido and stEth token

Lido and stEth token contract. It's the main staking contract of this ecosystem.

Node Operators Registry

A contract that represents a curated set of the Lido-participating node operators. Stores the signing keys and keeps track of vetted/exited/deposited ones.

AccountingOracle

Contract for gathering and processing the protocol accounting updates (TVL, rewards accrued, withdrawals to be finalized, exited, and failed to timely exit validators).

EvmScriptExecutor

Contract for parsing different arguments and executing commands. EVMScriptExecutor itself can be compromised in the following cases:

1. EASY_TRACK role of EVMScriptExecutor is compromised. This is equivalent to the attack of Aragon Voting.
2. Attack of EasyTrack. This can be done generally in two ways. Adding new EVMScriptFactory with necessary permissions, but this requires an attack of Aragon Voting. Or an attack of existing permissions, exactly the attack of trusted parties like node operators and multisigs.

Also, it should be mentioned that if an attacker can create new motions, then it can DoS EasyTrack by creating several motions, reaching motionsCountLimit.

Staking Router

StakingRouter is a registry of staking modules, each encapsulating a certain validator subset, e.g. the Lido DAO-curated staking module (NodeOperatorsRegistry). The contract allocates stakes to modules, distributes protocol fees, and tracks relevant information.

Deposit Security Module

A contract that is a part of the deposit-frontrunning vulnerability mitigation mechanism. Security module which can deposit buffered ether after quorum voting, pause deposits for single EOA, and unpause for the owner.

3. Impact & attack complexity classification

All roles enabled in the protocol was classified by their impact to the overall protocol security if it's compromised:

Impact severity	Description
Critical	Role leading to direct funds stealing or irreversible lockage of funds.
High	Role that can trigger strictly limited funds losses or temporary lock the protocol.
Medium	Role that can block a minor protocol functionality without any affect to users' funds.
Low	Role that cannot impact any protocol functions.
No impact	The role has no negative impact.

Every owner type assigned to the role was classified by their attack complexity:

Attack complexity	Description
Low	Any owner controlled by single private key (e.g. EOA).
Medium	Any owner controlled by limited number of private keys (e.g. multisig, quorum of EOAs).
High	Any owner controlled by DAO voting or immutable smart contract.

4. Conclusion

- At the time of the report, the voting minimum quorum is 5%. The current configuration might pose a security issue as there are EOA addresses, which hold ~7% and ~5% of the total supply LDO tokens. This is enough to overcome the minimum quorum and create and potentially execute a malicious proposal.

- There are several multisig with non-unique accounts that are responsible for validating and executing various information. This is the data table with info about the users that are owners at the mutisigs.

Multisig\User	0x2CA...cA3	0x639...979	0xc7a...8CD	0x039...826	0x004...295	0x9A3...3D4	0x59d...EDf	0xcC6...9b3	0x04e...1cf	0xB33...F6C	0x8Ce...5C6
0x12a...030	X	X	-	-	-	-	-	-	-	-	-
0xe2A...c8C	-	X	X	X	X	X	-	-	-	-	-
0x87D...2B5	-	-	X	-	-	X	X	X	X	X	-
0x9B1...956	-	-	-	-	-	-	X	X	X	X	-
0x834...759	-	-	-	-	-	-	-	-	-	-	X
0xDE0...437	-	-	-	X	X	-	-	X	X	X	X
0x17F...33D	-	-	-	-	-	X	-	X	-	-	-
0x518...a53	X	-	-	-	X	X	-	-	-	-	-
0x877...60C (GateSeal Committee)	X	-	-	-	-	X	-	-	-	-	-

  We would recommend allocating unique EOA addresses for different multisigs.

- The current design of Aragon voting allows proposal spam. There is no holding/locking or slashing mechanism for malicious/copycat/spam proposals.

- LDO tokens are managed by several roles in Aragon Token Management contracts. EVMScriptRegistry has only a single CallScript contract for script execution which reverts if target contract addresses contain blacklist addresses. Token Manager adds LDO token as a blacklisted address when executing a script. However, we found some not obvious cases:

  1. If REGISTRY_ADD_EXECUTOR_ROLE adds a new executor implementation without blacklisting the attacker can unlimited mint, burn, and transfer LDO tokens.
  2. If REGISTRY_ADD_EXECUTOR_ROLE adds a new executor that uses "DELEGATE_CALL" opcode it can corrupt Token Manager storage during the execution of the script. The attacker can execute the script via "DELEGATE_CALL" executor and change the token storage variable to a fake token in the Token Manager contract. In the next step, execute a malicious script for minting/burning LDO tokens, because the blacklist will contain the address of the fake token.

  We recommend adding detailed descriptions to Lido docs. So, voters can read docs to make decisions for voting in case the vote adds a new executor.

- During the evolution of Lido, numerous protocol updates have been made and various roles have been removed or added, as a result, some roles become obsolete.

We recommend revoking managers for obsolete roles:

Role	Manager
MANAGE_MEMBERS (0xbf6336045918ae0015f4cdb3441a2fdbfaa4bcde6558c8692aac7f56c69fb067)	Aragon Voting
MANAGE_QUORUM (0xa5ffa9f45fa52c446078e834e1914561bd9c2ab1e833572d62af775da092ccbc)	Aragon Voting
SET_BEACON_SPEC (0x16a273d48baf8111397316e6d961e6836913acb23b181e6c5fb35ec0bd2648fc)	Aragon Voting
SET_REPORT_BOUNDARIES (0x44adaee26c92733e57241cb0b26ffaa2d182ed7120ba3ecd7e0dce3635c01dc1)	Aragon Voting
SET_BEACON_REPORT_RECEIVER (0xe22a455f1bfbaf705ac3e891a64e156da92cb0b42cfc389158e6e82bd57f37be)	Aragon Voting

MANAGE_WITHDRAWAL_KEY (0x96088a8483023eb2f67b12aabbaf17d1d055e6ef387e563902adc1bba1e4028b)	Aragon Voting
SET_ORACLE (0x11eba3f259e2be865238d718fd308257e3874ad4b3a642ea3af386a4eea190bd)	Aragon Voting
SET_TREASURY (0x9f6f8058e4bcbf364e89c9e8da7eb7cada9d21b7aea6e2fd355b4669842c5795)	Aragon Voting
SET_INSURANCE_FUND (0xd6c7fda17708c7d91354c17ac044fde6f58fb548a5ded80960beba862b1f1d7d)	Aragon Voting
DEPOSIT_ROLE (0x2561bf26f818282a3be40719542054d2173eb0d38539e8a8d3cff22f29fd2384)	Aragon Voting
SET_EL_REWARDS_VAULT_ROLE (0x9d68ad53a92b6f44b2e8fb18d211bf8ccb1114f6fafd56aa364515dfdf23c44f)	Aragon Voting
SET_EL_REWARDS_WITHDRAWAL_LIMIT_ROLE (0xca7d176c2da2028ed06be7e3b9457e6419ae0744dc311989e9b29f6a1ceb1003)	Aragon Voting
MANAGE_PROTOCOL_CONTRACTS_ROLE (0xeb7bfce47948ec1179e2358171d5ee7c821994c911519349b95313b685109031)	Aragon Voting
ADD_NODE_OPERATOR_ROLE (0xe9367af2d321a2fc8d9c8f1e67f0fc1e2adf2f9844fb89ffa212619c713685b2)	Aragon Voting
SET_NODE_OPERATOR_ACTIVE_ROLE (0xd856e115ac9805c675a51831fa7d8ce01c333d666b0e34b3fc29833b7c68936a)	Aragon Voting
SET_NODE_OPERATOR_NAME_ROLE (0x58412970477f41493548d908d4307dfca38391d6bc001d56ffef86bd4f4a72e8)	Aragon Voting
SET_NODE_OPERATOR_ADDRESS_ROLE (0xbf4b1c236312ab76e456c7a8cca624bd2f86c74a4f8e09b3a26d60b1ce492183)	Aragon Voting
REPORT_STOPPED_VALIDATORS_ROLE (0x18ad851afd4930ecc8d243c8869bd91583210624f3f1572e99ee8b450315c80f)	Aragon Voting

- In some contracts, there are unassigned roles, if we have set critical/high impact severity for these roles, then we propose to take into account, that for these roles would be desirable to appoint Aragon Voting/Agent.

Otherwise, we advise caution with these roles:

Contract	Role
Withdrawal Queue ERC721 (Implementation)	RESUME_ROLE
Staking Router (Implementation)	MANAGE_WITHDRAWAL_CREDENTIALS_ROLE
Staking Router (Implementation)	STAKING_MODULE_MANAGE_ROLE
Staking Router (Implementation)	UNSAFE_SET_EXITED_VALIDATORS_ROLE
Lido and stETH token (Implementation)	UNSAFE_CHANGE_DEPOSITED_VALIDATORS_ROLE
Accounting Oracle: AccountingOracle (Implementation)	SUBMIT_DATA_ROLE
Accounting Oracle: AccountingOracle (Implementation)	MANAGE_CONSENSUS_CONTRACT_ROLE
Accounting Oracle: AccountingOracle (Implementation)	MANAGE_CONSENSUS_VERSION_ROLE
Accounting Oracle: HashConsensus	MANAGE_MEMBERS_AND_QUORUM_ROLE
Accounting Oracle: HashConsensus	DISABLE_CONSENSUS_ROLE
Accounting Oracle: HashConsensus	MANAGE_FRAME_CONFIG_ROLE
Accounting Oracle: HashConsensus	MANAGE_FAST_LANE_CONFIG_ROLE
Accounting Oracle: HashConsensus	MANAGE_REPORT_PROCESSOR_ROLE
OracleReportSanityChecker	ALL_LIMITS_MANAGER_ROLE
OracleReportSanityChecker	CHURN_VALIDATORS_PER_DAY_LIMIT_MANAGER_ROLE
OracleReportSanityChecker	ONE_OFF_CL_BALANCE_DECREASE_LIMIT_MANAGER_ROLE
OracleReportSanityChecker	ANNUAL_BALANCE_INCREASE_LIMIT_MANAGER_ROLE
OracleReportSanityChecker	SHARE_RATE_DEVIATION_LIMIT_MANAGER_ROLE
OracleReportSanityChecker	MAX_VALIDATOR_EXIT_REQUESTS_PER_REPORT_ROLE
OracleReportSanityChecker	MAX_ACCOUNTING_EXTRA_DATA_LIST_ITEMS_COUNT_ROLE
OracleReportSanityChecker	MAX_NODE_OPERATORS_PER_EXTRA_DATA_ITEM_COUNT_ROLE
OracleReportSanityChecker	REQUEST_TIMESTAMP_MARGIN_MANAGER_ROLE
OracleReportSanityChecker	MAX_POSITIVE_TOKEN_REBASE_MANAGER_ROLE
Aragon Agent (Implementation)	SAFE_EXECUTE_ROLE
Aragon Agent (Implementation)	ADD_PROTECTED_TOKEN_ROLE
Aragon Voting (Implementation)	UNSAFELY_MODIFY_VOTE_TIME_ROLE
Aragon Token Manager (Implementation)	MINT_ROLE
Aragon Token Manager (Implementation)	ISSUE_ROLE
Aragon Token Manager (Implementation)	REVOKE_VESTINGS_ROLE
Aragon Token Manager (Implementation)	BURN_ROLE
Aragon Finance (Implementation)	CHANGE_BUDGETS_ROLE

Multisig/EOA impact severity analysis

Analysis of all multisig and EOA owners and linked roles:

Owner\Impact severity of role	LOW	MEDIUM	HIGH	CRITICAL
Multisig (Safe-Gnosis) (5 / 7)		1		
Multisig (Safe-Gnosis) (3 / 6)			1	
Multisig (Safe-Gnosis) (3 / 5)		1		4
Multisig (Safe-Gnosis) (4 / 8)		2		
Multisig (Safe-Gnosis) (4 / 6)		1		
Multisig (Safe-Gnosis) (4 / 7)		1		
Multisig (Safe-Gnosis) (4 / 7)		1		
Multisig (Safe-Gnosis) (4 / 7)		1		
Multisig (Safe-Gnosis) (3 / 5)	2	1		
Multisig (Safe-Gnosis) (4 / 8)	2	1		
Multisig (Safe-Gnosis) (4 / 7)	2	1		
EOA quorum (4 / 6)			1	
EOA quorum (5 / 9)		1	1	

EOA quorum (4 / 6) owners:

- https://etherscan.io/address/0x5fd0dDbC3351d009eb3f88DE7Cd081a614C519F1
- https://etherscan.io/address/0x7912Fa976BcDe9c2cf728e213e892AD7588E6AaF
- https://etherscan.io/address/0x14D5d5B71E048d2D75a39FfC5B407e3a3AB6F314
- https://etherscan.io/address/0xf82D88217C249297C6037BA77CE34b3d8a90ab43
- https://etherscan.io/address/0xa56b128Ea2Ea237052b0fA2a96a387C0E43157d8
- https://etherscan.io/address/0xd4EF84b638B334699bcf5AF4B0410B8CCD71943f

EOA quorum (5 / 9) owners:

- https://etherscan.io/address/0x140Bd8FbDc884f48dA7cb1c09bE8A2fAdfea776E
- https://etherscan.io/address/0x1d0813bf088BE3047d827D98524fBf779Bc25F00
- https://etherscan.io/address/0x404335BcE530400a5814375E7Ec1FB55fAff3eA2
- https://etherscan.io/address/0x946D3b081ed19173dC83Cd974fC69e1e760B7d78
- https://etherscan.io/address/0x007DE4a5F7bc37E2F26c0cb2E8A95006EE9B89b5
- https://etherscan.io/address/0xEC4BfbAF681eb505B94E4a7849877DC6c600Ca3A
- https://etherscan.io/address/0x61c91ECd902EB56e314bB2D5c5C07785444Ea1c8
- https://etherscan.io/address/0x1Ca0fEC59b86F549e1F1184d97cb47794C8Af58d
- https://etherscan.io/address/0xA7410857ABbf75043d61ea54e07D57A6EB6EF186

Summary table

A summary table that quantitatively displays the relationship between impact severity and attack complexity.

Impact severity \ Attack complexity	Low	Medium	High
Critical	0	5	56
High	1	1	71
Medium	0	12	33
Low	0	6	0
No impact	0	0	2

5. Role analysis

Domain	**Staking pool**
Contract	**MEV Boost Relay Allowed List**
Role name	**Owner**
Auth type	**custom-acl**
Role impact severity	**MEDIUM**
Attack complexity cumulative	**HIGH**

Role description

The role add/remove MEV relays from MEV registry. MEV registry is used by validators to maximize profits and follow a single censorship strategy. Also, the role adding/removing manager or owner role. The owner can transfer any ERC20 token from the registry contract. There is an important point that the relay updates are made by the node operators manually (can send an emergency signal from the Lido DAO to stop the ops of sync with the contract's data)

Impact description

The role can remove all MEV relays, decreasing rewards for Lido validators and APR for stakers of the protocol. To fix this the protocol will need to deploy a new registry and provide an address to all validators. Also, the attacker can fill a list with their own relayers. So, if Lido validators use MEV replayed only from this list the attacker can censor some transactions.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**Staking pool**
Contract	**MEV Boost Relay Allowed List**
Role name	**Manager**
Auth type	**custom-acl**
Role impact severity	**MEDIUM**
Attack complexity cumulative	**MEDIUM**

Role description

The role add/remove MEV relays from MEV registry. MEV registry is used by validators to maximize profits and follow a single censorship strategy.

Impact description

The role can remove all MEV relays, so it decreases rewards for Lido validators and APR for stakers of the protocol. However, the owner can restore all changes.

Owners

Owner type	**Multisig (Safe-Gnosis)**
Owner address	**0x98be4a407Bff0c125e25fBE9Eb1165504349c37d**
Attack complexity	**MEDIUM**

Attack scenario

Need to have signatures of txn hash for 5 owners out of 7. All owners are EOA, and 2 of them are historically active on-chain, causing a higher probability of receiving their signatures.

Domain	Staking pool
Contract	Burner
Role name	DEFAULT_ADMIN_ROLE
Auth type	custom-acl-oz-fork
Role impact severity	CRITICAL
Attack complexity cumulative	HIGH

Role description

The role grants/revokes REQUEST_BURN_SHARES_ROLE, REQUEST_BURN_MY_STETH_ROLE roles.

Impact description

The impact is a cumulative impact from REQUEST_BURN_SHARES_ROLE and REQUEST_BURN_MY_STETH_ROLE.

Owners

Owner type	Aragon Agent
Owner address	0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c
Attack complexity	HIGH

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**Staking pool**
Contract	**Burner**
Role name	**REQUEST_BURN_SHARES_ROLE**
Auth type	**custom-acl-oz-fork**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**HIGH**

Role description

The role allows transferring stETH shares "from" every address that provided the allowance to the role holder (the Burner contract). At the time of the report, only **WithdrawalQueue** and **NodeOperatorRegistry** provide unlimited allowance to the role holder. The burning will be performed during the processing of the Oracle report.

Impact description

The role can transfer all stETH from **WithdrawalQueue** and **NodeOperatorRegistry** to the Burner contract. Also, it blocks processing Oracle reports, because calculation **sharesToBurnFromWithdrawalQueue** in **WithdrawalQueue** may be calculated incorrectly or accounting Oracle check failure because the balance of contract < balance of report.

Owners

Owner type	**Lido and stETH token**
Owner address	**0xae7ab96520DE3A18E5e111B5EaAb095312D7fE84**
Attack complexity	**HIGH**

Attack scenario

Aragon voting can be compromised in the following cases:

1. The undiscovered bug in the implementation of Lido and stETH token contract. However, Lido successfully passed several audits and battle-tested in production, so the probability of this kind of bug can be considered low.
2. The implementation address of Lido and stETH contract can be updated using Aragon OS. The Kernel has a mechanism of apps that allows updating the app's address implementation for the **APP_MANAGER_ROLE** owner. So, an attacker must occupy **APP_MANAGER_ROLE** which is protected by Aragon Voting.

Owner type	**Node Operators Registry**
Owner address	**0x55032650b14df07b85bF18A3a3eC8E0Af2e028d5**
Attack complexity	**HIGH**

Attack scenario

It can be compromised to use this role by compromising **NodeOperatorsRegistry:STAKING_ROUTER_ROLE.**

Domain	**Staking pool**
Contract	**Burner**
Role name	**REQUEST_BURN_MY_STETH_ROLE**
Auth type	**custom-acl-oz-fork**
Role impact severity	**MEDIUM**
Attack complexity cumulative	**HIGH**

Role description

The role allows transferring stETH token "from" the role holder that provided the allowance.

Impact description

The role can transfer the input amount (and it has to be allowed) of stETH from the caller to the Burner contract.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**Staking pool**
Contract	**Withdrawal Vault (Proxy)**
Role name	**ADMIN**
Auth type	**custom-acl-over-oz-erc1967proxy**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**HIGH**

Role description

The role changes implementation, change/reset ADMIN role owner.

Impact description

The role can change implementation which can be used to steal withdrawal rewards in native ETH and steal tokens. In addition to this, implementation can be changed in a way that it will always revert, which will DoS the whole oracle report.

Owners

Owner type	**Aragon Voting**
Owner address	**0x2e59A20f205bB85a89C53f1936454680651E618e**
Attack complexity	**HIGH**

Attack scenario

This role is protected by the Aragon Voting contract and doesn't contain other significant conditions. Thus, the compromisation complexity is equivalent to a vote with a malicious script.

Domain	**Staking pool**
Contract	**Withdrawal Vault (Implementation)**
Role name	**Lido**
Auth type	**custom-acl-immutable**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**HIGH**

Role description

The role withdraws accumulated native CL withdrawals.

Impact description

The role can steal withdrawal rewards in native ETH.

Owners

Owner type	**Lido and stETH token**
Owner address	**0xae7ab96520DE3A18E5e111B5EaAb095312D7fE84**
Attack complexity	**HIGH**

Attack scenario

Aragon voting can be compromised in the following cases:

1. The undiscovered bug in the implementation of Lido and stETH token contract. However, Lido successfully passed several audits and battle-tested in production, so the probability of this kind of bug can be considered low.
2. Updating implementation, that required occupation ADMIN which is protected by Aragon Voting.

Domain	**Staking pool**
Contract	**Withdrawal Queue ERC721 (Proxy)**
Role name	**ADMIN**
Auth type	**custom-acl-over-oz-erc1967proxy**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**HIGH**

Role description

The role changes implementation, change/reset ADMIN role owner.

Impact description

The role can change implementation which can be used to steal stETH and native ETH from the contract and steal users' wstETH and stETH if it is permitted/approved to the contract. In addition to this, after implementation changes, finalization can always revert, which will DoS the whole report.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	Staking pool
Contract	Withdrawal Queue ERC721 (Implementation)
Role name	DEFAULT_ADMIN_ROLE
Auth type	custom-acl-oz-fork
Role impact severity	CRITICAL
Attack complexity cumulative	HIGH

Role description

The role is able to grant or revoke all roles.

Impact description

The role has a cumulative impact on all the roles of this contract. The worst case: the contract can accumulate the wstETH and stETH, while the claiming cannot be executed.

Owners

Owner type	Aragon Agent
Owner address	0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c
Attack complexity	HIGH

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**Staking pool**
Contract	**Withdrawal Queue ERC721 (Implementation)**
Role name	**PAUSE_ROLE**
Auth type	**custom-acl-oz-fork**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role pauses the contract. Paused functions: **requestWithdrawalsWstETH(), requestWithdrawals(), finalize().**

Impact description

The role can pause the contract partially (prevent new withdrawal requests creation and finalization, still allowing claims of the finalized ones).

Owners

Owner type	**GateSeal**
Owner address	**0x1aD5cb2955940F998081c1eF5f5F00875431aA90**
Attack complexity	**HIGH**

Attack scenario

The role can be compromised by compromising GateSeal:SEALING_COMMITTEE. The impact is limited with the duration provided still. GateSeal can't pause for more than 6 days.

Domain	Staking pool
Contract	Withdrawal Queue ERC721 (Implementation)
Role name	RESUME_ROLE
Auth type	custom-acl-oz-fork
Role impact severity	CRITICAL
Attack complexity cumulative	HIGH

Role description

The role resumes contract, only if paused.

Impact description

The role can maliciously resume the contract when the protocol has an inconsistent state.

Owners

Owner type	Unassigned
Owner address	N/A
Attack complexity	HIGH

Attack scenario

The owner is not assigned, so the attack complexity is equal to the attack complexity of APP_MANAGER_ROLE. The APP_MANAGER_ROLE is controlled by Aragon Voting, so the attacker has to execute a malicious proposal to compromise this role.

Domain	**Staking pool**
Contract	**Withdrawal Queue ERC721 (Implementation)**
Role name	**FINALIZE_ROLE**
Auth type	**custom-acl-oz-fork**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role finalizes requests.

Impact description

The role can temporarily lock the claim functionality.

Owners

Owner type	**Lido and stETH token**
Owner address	**0xae7ab96520DE3A18E5e111B5EaAb095312D7fE84**
Attack complexity	**HIGH**

Attack scenario

Aragon voting can be compromised in the following cases:

1. The undiscovered bug in the implementation of Lido and stETH token contract. However, Lido successfully passed several audits and battle-tested in production, so the probability of this kind of bug can be considered low.
2. Updating implementation, that required occupation ADMIN which is protected by Aragon Voting.

Domain	**Staking pool**
Contract	**Withdrawal Queue ERC721 (Implementation)**
Role name	**ORACLE_ROLE**
Auth type	**custom-acl-oz-fork**
Role impact severity	**MEDIUM**
Attack complexity cumulative	**HIGH**

Role description

The role updates the bunker mode state and last report timestamp on oracle report.

Impact description

The role can turn on/off bunkerMode.

Owners

Owner type	**AccountingOracle**
Owner address	**0x852deD011285fe67063a08005c71a85690503Cee**
Attack complexity	**HIGH**

Attack scenario

The method at AccountingOracle can be executed only by **AccountingOracle:SUBMIT_DATA_ROLE** or by anyone from AccountingOracle:HashConsensus:QuorumMembers. However, there is no owner for **SUBMIT_DATA_ROLE**. So it is needed to get the private key of some quorum members.

Domain	**Staking pool**
Contract	**Withdrawal Queue ERC721 (Implementation)**
Role name	**MANAGE_TOKEN_URI_ROLE**
Auth type	**custom-acl-oz-fork**
Role impact severity	**MEDIUM**
Attack complexity cumulative	**HIGH**

Role description

The role sets the Base URI for computing tokenURI and sets the address of NFTDescriptor contract that is responsible for tokenURI generation

Impact description

The role can break tokenURIs for UI.

Owners

Owner type	**Unassigned**
Owner address	**N/A**
Attack complexity	**HIGH**

Attack scenario

The owner is not assigned, so the attack complexity is equal to the attack complexity of APP_MANAGER_ROLE. The APP_MANAGER_ROLE is controlled by Aragon Voting, so the attacker has to execute a malicious proposal to compromise this role.

Domain	**Staking pool**
Contract	**Execution Layer Rewards Vault**
Role name	**Lido**
Auth type	**custom-acl-immutable**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**HIGH**

Role description

The role withdraws execution layer rewards to the treasury address.

Impact description

The role can steal execution rewards in native ETH. However, If the vault contract is deployed correctly with a trusted Lido owner there is no impact.

Owners

Owner type	**Lido and stETH token**
Owner address	**0xae7ab96520DE3A18E5e111B5EaAb095312D7fE84**
Attack complexity	**HIGH**

Attack scenario

Aragon voting can be compromised in the following cases:

1. The undiscovered bug in the implementation of Lido and stETH token contract. However, Lido successfully passed several audits and battle-tested in production, so the probability of this kind of bug can be considered low. The contract is non-upgradable.

Domain	**Staking pool**
Contract	**Deposit Security Module**
Role name	**Owner**
Auth type	**custom-acl**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**HIGH**

Role description

The role sets owner/guardian/quorum, unpauses deposits, sets max deposits, min deposit block distance, pauses intent validity period blocks.

Impact description

The role can reset guardians, this will lead to unpausing/pausing deposits, for several/certain/all staking modules. Can set up parameters, which will lead to DoS of deposits for buffered ETH. In addition, if malicious guardians are installed, this will allow performing a malicious pre-deposit front-running attack.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**Staking pool**
Contract	**Deposit Security Module**
Role name	**Guardians**
Auth type	**custom-acl-offchain**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**MEDIUM**

Role description

The role pauses deposits, deposit buffered ether.

Impact description

The role can pause deposits. To trigger a pause, at least a single honest guardian can intrude. Can deposit buffered ETH to certain stakingModuleId's. Also, allowing the malicious pre-deposits to pass.

Owners

Owner type	**EOA**
Owner address	**0x5fd0dDbC3351d009eb3f88DE7Cd081a614C519F1**
Attack complexity	**LOW**

Attack scenario

The current quorum is 4, so it is needed to get a private keys or signatures of a minimum of 4 out of 6 members.

Owner type	**EOA**
Owner address	**0x7912Fa976BcDe9c2cf728e213e892AD7588E6AaF**
Attack complexity	**LOW**

Attack scenario

The current quorum is 4, so it is needed to get a private keys or signatures of a minimum of 4 out of 6 members.

Owner type	**EOA**
Owner address	**0x14D5d5B71E048d2D75a39FfC5B407e3a3AB6F314**
Attack complexity	**LOW**

Attack scenario

The current quorum is 4, so it is needed to get a private keys or signatures of a minimum of 4 out of 6 members.

Owner type	**EOA**
Owner address	**0xf82D88217C249297C6037BA77CE34b3d8a90ab43**
Attack complexity	**LOW**

Attack scenario

The current quorum is 4, so it is needed to get a private keys or signatures of a minimum of 4 out of 6 members.

Owner type	**EOA**
Owner address	**0xa56b128Ea2Ea237052b0fA2a96a387C0E43157d8**
Attack complexity	**LOW**

Attack scenario

The current quorum is 4, so it is needed to get a private keys or signatures of a minimum of 4 out of 6 members.

Owner type	**EOA**
Owner address	**0xd4EF84b638B334699bcf5AF4B0410B8CCD71943f**
Attack complexity	**LOW**

Attack scenario

The current quorum is 4, so it is needed to get a private keys or signatures of a minimum of 4 out of 6 members.

Domain	**Staking pool**
Contract	**Node Operators registry (Implementation)**
Role name	**SET_NODE_OPERATOR_LIMIT_ROLE**
Auth type	**aragon-acl**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role sets the maximum number of validators for the node operator.

Impact description

The role can prevent node operators from using more validators than they might want/need to use in the future.

Owners

Owner type	**Aragon Voting**
Owner address	**0x2e59A20f205bB85a89C53f1936454680651E618e**
Attack complexity	**HIGH**

Attack scenario

This role is protected by the Aragon Voting contract and doesn't contain other significant conditions. Thus, the compromisation complexity is equivalent to a vote with a malicious script.

Owner type	**EVMScriptExecutor**
Owner address	**0xFE5986E06210aC1eCC1aDCafc0cc7f8D63B3F977**
Attack complexity	**HIGH**

Attack scenario

Aragon voting can be compromised in the following cases:

1. The undiscovered bug in the implementation of **EVMScriptExecutor** contract. However, EasyTrack contracts(including **EVMScriptExecutor**) successfully passed several audits and battle-tested in production, so the probability of this kind of bug can be considered low.
2. Accepts malicious proposals in EasyTrack.

Domain	Staking pool
Contract	Node Operators registry (Implementation)
Role name	MANAGE_SIGNING_KEYS
Auth type	aragon-acl
Role impact severity	CRITICAL
Attack complexity cumulative	HIGH

Role description

The role adds new validator keys.

Impact description

The role can add improper signing keys. It leads to a possible partial loss of funds and DoS of new deposits.

Owners

Owner type	Aragon Voting
Owner address	0x2e59A20f205bB85a89C53f1936454680651E618e
Attack complexity	HIGH

Attack scenario

This role is protected by the Aragon Voting contract and doesn't contain other significant conditions. Thus, the compromisation complexity is equivalent to a vote with a malicious script.

Domain	**Staking pool**
Contract	**Node Operators registry (Implementation)**
Role name	**MANAGE_NODE_OPERATOR_ROLE**
Auth type	**aragon-acl**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role adds node operators, sets stats, sets reward address, invalidate unused keys to deposit, and sets stuck delay.

Impact description

The role can lead to a partial loss of funds by changing the reward addresses of operators and DoS of the curated staking module via deactivating operators.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**Staking pool**
Contract	**Node Operators registry (Implementation)**
Role name	**STAKING_ROUTER_ROLE**
Auth type	**aragon-acl**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**HIGH**

Role description

The role updates the number of the validators (stuck/exited/refunded), leads to distribution rewards, can do this in an unsafe way, and change withdrawal credentials, which leads to the invalidation of unused keys.

Impact description

The role can change withdrawal credentials and validator info which leads to the total DoS of the curated staking module until the role is renounced.

Owners

Owner type	**Staking Router**
Owner address	**0xfddf38947afb03c621c71b06c9c70bce73f12999**
Attack complexity	**HIGH**

Attack scenario

For the current owner the compromisation complexity differs for different functions: onRewardsMinted()'s compromisation is equal to **StakingRouter:REPORT_REWARDS_MINTED_ROLE** compromisation updateStuckValidatorsCount() – **StakingRouter:REPORT_EXITED_VALIDATORS_ROLE** updateExitedValidatorsCount() – **StakingRouter:REPORT_EXITED_VALIDATORS_ROLE** updateRefundedValidatorsCount() – **StakingRouter:STAKING_MODULE_MANAGE_ROLE** onExitedAndStuckValidatorsCountsUpdated() – **StakingRouter:UNSAFE_SET_EXITED_VALIDATORS_ROLE** or **StakingRouter:REPORT_EXITED_VALIDATORS_ROLE** unsafeUpdateValidatorsCount() – **StakingRouter:UNSAFE_SET_EXITED_VALIDATORS_ROLE** updateTargetValidatorsLimits() – **StakingRouter:STAKING_MODULE_MANAGE_ROLE** onWithdrawalCredentialsChanged() – **StakingRouter:MANAGE_WITHDRAWAL_CREDENTIALS_ROLE** obtainDepositData() – **StakingRouter:Lido**

Domain	**Staking pool**
Contract	**Staking Router (Proxy)**
Role name	**ADMIN**
Auth type	**custom-acl-over-oz-erc1967proxy**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**HIGH**

Role description

The role changes implementation, changes/resets ADMIN role owner.

Impact description

The role can change implementation which can be used to steal native ETH from new deposits. In addition to this, after implementation changes, rebases can be stopped.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**Staking pool**
Contract	**Staking Router (Implementation)**
Role name	**DEFAULT_ADMIN_ROLE**
Auth type	**custom-acl-oz-fork**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**HIGH**

Role description

The super-role manages other specific roles in the contract.

Impact description

The role can pause all modules. Total DoS of the contract.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	Staking pool
Contract	Staking Router (Implementation)
Role name	MANAGE_WITHDRAWAL_CREDENTIALS_ROLE
Auth type	custom-acl-oz-fork
Role impact severity	HIGH
Attack complexity cumulative	HIGH

Role description

The role sets new withdrawal credentials and discards all unused deposits.

Impact description

The role can depend on the realization of the staking module. The curated staking module will only discard unused deposits. If withdrawal credentials change and no one notices – new deposits will be withdrawn to the wrong address.

Owners

Owner type	Unassigned
Owner address	N/A
Attack complexity	HIGH

Attack scenario

The owner is not assigned, so the attack complexity is equal to the attack complexity of APP_MANAGER_ROLE. The APP_MANAGER_ROLE is controlled by Aragon Voting, so the attacker has to execute a malicious proposal to compromise this role.

Domain	**Staking pool**
Contract	**Staking Router (Implementation)**
Role name	**STAKING_MODULE_PAUSE_ROLE**
Auth type	**custom-acl-oz-fork**
Role impact severity	**HIGH**
Attack complexity cumulative	**LOW**

Role description

The role pauses deposits for the staking module.

Impact description

The role can pause right before deposit -> deposit wont be performed.

Owners

Owner type	**Deposit Security Module (1 of guardian)**
Owner address	**0xC77F8768774E1c9244BEed705C4354f2113CFc09**
Attack complexity	**LOW**

Attack scenario

It is needed to get a private key or a signature of only one of Guardians in **DepositSecurityModule**.

Domain	**Staking pool**
Contract	**Staking Router (Implementation)**
Role name	**STAKING_MODULE_RESUME_ROLE**
Auth type	**custom-acl-oz-fork**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**HIGH**

Role description

The role resumes deposits for the staking module.

Impact description

The role can resume broken or malicious staking modules.

Owners

Owner type	**Deposit Security Module**
Owner address	**0xC77F8768774E1c9244BEed705C4354f2113CFc09**
Attack complexity	**HIGH**

Attack scenario

It can be compromised to use this role by compromising Aragon Agent.

Domain	**Staking pool**
Contract	**Staking Router (Implementation)**
Role name	**STAKING_MODULE_MANAGE_ROLE**
Auth type	**custom-acl-oz-fork**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**HIGH**

Role description

The role adds new staking modules and updates stats like fees and validators count.

Impact description

The role can change the percentage of fees from modules. Thus, all the fees can go to the treasury or to the module. Also can block updating information about validators. Add broken staking module. Then the call of onValidatorsCountsByNodeOperatorReportingFinished will revert.

Owners

Owner type	**Unassigned**
Owner address	**N/A**
Attack complexity	**HIGH**

Attack scenario

The owner is not assigned, so the attack complexity is equal to the attack complexity of **APP_MANAGER_ROLE**. The **APP_MANAGER_ROLE** is controlled by Aragon Voting, so the attacker has to execute a malicious proposal to compromise this role.

Domain	**Staking pool**
Contract	**Staking Router (Implementation)**
Role name	**REPORT_EXITED_VALIDATORS_ROLE**
Auth type	**custom-acl-oz-fork**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role updates the exited validators count, which can be dangerous for funds.

Impact description

The role can set all the deposited validators to be exited. Can only be fixed with **UNSAFE_SET_EXITED_VALIDATORS_ROLE**. Also affects modules.

Owners

Owner type	**Accounting Oracle**
Owner address	**0x852deD011285fe67063a08005c71a85690503Cee**
Attack complexity	**HIGH**

Attack scenario

It can be compromised by compromising AragonAgent or by anyone from **AccountingOracle:HashConsensus:QuorumMembers**. However, there is no owner for **SUBMIT_DATA_ROLE**. So it is needed to get the private key of some quorum members.

Domain	Staking pool
Contract	Staking Router (Implementation)
Role name	UNSAFE_SET_EXITED_VALIDATORS_ROLE
Auth type	custom-acl-oz-fork
Role impact severity	CRITICAL
Attack complexity cumulative	HIGH

Role description

The role sets exited validators count without checks, leads to DoS or loss.

Impact description

The role has the same impact as REPORT_EXITED_VALIDATORS_ROLE. Also can DoS new deposits and cause incorrect calculation of rewards.

Owners

Owner type	Unassigned
Owner address	N/A
Attack complexity	HIGH

Attack scenario

The owner is not assigned, so the attack complexity is equal to the attack complexity of APP_MANAGER_ROLE. The APP_MANAGER_ROLE is controlled by Aragon Voting, so the attacker has to execute a malicious proposal to compromise this role.

Domain	**Staking pool**
Contract	**Staking Router (Implementation)**
Role name	**REPORT_REWARDS_MINTED_ROLE**
Auth type	**custom-acl-oz-fork**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**HIGH**

Role description

The role reports rewards minted, can lead to partial loss of funds.

Impact description

The role can report incorrect rewards to modules so the module can take all the profit. Doesn't affect the current Curated staking module.

Owners

Owner type	**Lido and stETH token**
Owner address	**0xae7ab96520DE3A18E5e111B5EaAb095312D7fE84**
Attack complexity	**HIGH**

Attack scenario

Aragon voting can be compromised in the following cases:

1. The undiscovered bug in the implementation of Lido and stETH token contract. However, Lido successfully passed several audits and battle-tested in production, so the probability of this kind of bug can be considered low.
2. Updating implementation, that required occupation ADMIN which is protected by Aragon Voting.

Domain	**Staking pool**
Contract	**Staking Router (Implementation)**
Role name	**Lido**
Auth type	**custom-acl**
Role impact severity	**MEDIUM**
Attack complexity cumulative	**HIGH**

Role description

The role invokes a deposit call to the official Deposit contract.

Impact description

The role can call the function with zero value and update the contract's state about the deposit timestamp.

Owners

Owner type	**Lido and stETH token**
Owner address	**0xae7ab96520DE3A18E5e111B5EaAb095312D7fE84**
Attack complexity	**HIGH**

Attack scenario

To compromise the Deposit Security Module: the attacker must compromise the quorum of guardians.

Domain	**Staking pool**
Contract	**Lido and stETH token (Implementation)**
Role name	**PAUSE_ROLE**
Auth type	**aragon-acl**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role pausing of the main Lido contract occurs in 2 stages: 1) Pausing of the internal contract state. Switch the **ACTIVE_FLAG_POSITION** to false. 2) Pausing staking of an internal variable. Call **setStakeLimitPauseState(true)** for **STAKING_STATE_POSITION**

Impact description

The role can block stETH transfer functions (**stETH:_transferShares**, **stETH:transferShares**, **stETH:transferSharesFrom**, **stETH:_transfer**, **stETH:transfer**, **stETH:transferFrom**), oracle report processing (**Lido:handleOracleReport**), deposits in the protocol (**Lido:canDeposit**, **Lido:deposit**), and issuing stETH by sending native ETH (**Lido:_submit Lido:submit**, **Lido:fallback**).

Owners

Owner type	**Aragon Voting**
Owner address	**0x2e59A20f205bB85a89C53f1936454680651E618e**
Attack complexity	**HIGH**

Attack scenario

This role is protected by the Aragon Voting contract and doesn't contain other significant conditions. Thus, the compromisation complexity is equivalent to a vote with a malicious script.

Domain	**Staking pool**
Contract	**Lido and stETH token (Implementation)**
Role name	**RESUME_ROLE**
Auth type	**aragon-acl**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**HIGH**

Role description

The resuming of the main Lido contract occurs in 2 stages: 1) Resuming of the internal contract state. Switch the ACTIVE_FLAG_POSITION to true. 2) Resuming staking of an internal variable. Call **setStakeLimitPauseState(false)** for STAKING_STATE_POSITION

Impact description

The role can block enabling next features: stETH transfer (**stETH:_transferShares**, **stETH:transferShares**, **stETH:transferSharesFrom**, **stETH:_transfer**, **stETH:transfer**, **stETH:transferFrom**), oracle report processing(**Lido:handleOracleReport**), deposits in the protocol (**Lido:canDeposit**, **Lido:deposit**), and issuing stETH by sending native ETH (**Lido:_submit**, **Lido:submit**, **Lido:fallback**).

Owners

Owner type	**Aragon Voting**
Owner address	**0x2e59A20f205bB85a89C53f1936454680651E618e**
Attack complexity	**HIGH**

Attack scenario

This role is protected by the Aragon Voting contract and doesn't contain other significant conditions. Thus, the compromisation complexity is equivalent to a vote with a malicious script.

Domain	**Staking pool**
Contract	**Lido and stETH token (Implementation)**
Role name	**STAKING_PAUSE_ROLE**
Auth type	**aragon-acl**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

Pausing staking of an internal variable. Call **setStakeLimitPauseState(true)** for **STAKING_STATE_POSITION**.

Impact description

The role can block issuing stETH by sending native ETH (**Lido:_submit**, **Lido:submit**, **Lido:fallback**).

Owners

Owner type	**Aragon Voting**
Owner address	**0x2e59A20f205bB85a89C53f1936454680651E618e**
Attack complexity	**HIGH**

Attack scenario

This role is protected by the Aragon Voting contract and doesn't contain other significant conditions. Thus, the compromisation complexity is equivalent to a vote with a malicious script.

Domain	**Staking pool**
Contract	**Lido and stETH token (Implementation)**
Role name	**STAKING_CONTROL_ROLE**
Auth type	**aragon-acl**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The resuming staking of an internal variable. Call **setStakeLimitPauseState(false)** for **STAKING_STATE_POSITION**. Also, the role can set/remove the staking limit.

Impact description

The role can block enabling of issuing stETH by sending native ETH (**Lido:_submit**, **Lido:submit**, **Lido:fallback**). Also, the role can set/remove of staking limit, so it has an impact on deposit throughput and APR decreasing if deposits buffer size in protocol is more than the deposit throughput for a long time.

Owners

Owner type	**Aragon Voting**
Owner address	**0x2e59A20f205bB85a89C53f1936454680651E618e**
Attack complexity	**HIGH**

Attack scenario

This role is protected by the Aragon Voting contract and doesn't contain other significant conditions. Thus, the compromisation complexity is equivalent to a vote with a malicious script.

Domain	**Staking pool**
Contract	**Lido and stETH token (Implementation)**
Role name	**UNSAFE_CHANGE_DEPOSITED_VALIDATORS_ROLE**
Auth type	**aragon-acl**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**HIGH**

Role description

The role can change the internal accounting of the deposited validators' amount.

Impact description

The role can change the internal accounting of the deposited validators' amount. It has an impact on stETH balance, rebase mechanic, and block oracle processing reports. Change the ratio between the number of shares and the deposited ETH amount for the stETH token. This would in turn increase **stETH:balanceOf** and role owner steal funds from external protocols.

Owners

Owner type	**Unassigned**
Owner address	**N/A**
Attack complexity	**HIGH**

Attack scenario

The owner is not assigned, so the attack complexity is equal to the attack complexity of **APP_MANAGER_ROLE**. The **APP_MANAGER_ROLE** is controlled by Aragon Voting, so the attacker has to execute a malicious proposal to compromise this role.

Domain	**Staking pool**
Contract	**Lido Locator (Proxy)**
Role name	**ADMIN**
Auth type	**custom-acl-over-oz-erc1967proxy**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**HIGH**

Role description

The admin of the proxy can change implementation, beacon, and admin.

Impact description

The role can upgrade contracts and provide other addresses for all core contracts of Lido. These addresses usually are used for authentication between Lido contracts, getting protocol parameters, calculating protocol amounts, and sending funds between protocol components.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**Staking pool**
Contract	**Accounting Oracle:AccountingOracle (Proxy)**
Role name	**ADMIN**
Auth type	**custom-acl-over-oz-erc1967proxy**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**HIGH**

Role description

The role changes implementation, changes/resets **ADMIN** role owner.

Impact description

The role can upgrade the contract and can violate (or stop) the oracle rebasing the stETH (but not too chaotic as there are sanity checkers).

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**Staking pool**
Contract	**Accounting Oracle:AccountingOracle (Implementation)**
Role name	**DEFAULT_ADMIN_ROLE**
Auth type	**custom-acl-oz-fork**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**HIGH**

Role description

The role is able to grant or revoke all roles.

Impact description

The impact is a cumulative impact from all the roles of this contract.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**Staking pool**
Contract	**Accounting Oracle:AccountingOracle (Implementation)**
Role name	**SUBMIT_DATA_ROLE**
Auth type	**custom-acl-oz-fork**
Role impact severity	**MEDIUM**
Attack complexity cumulative	**HIGH**

Role description

The role submits report data for processing:

1. An amount of ETH and a number of validators on the Beacon Chain.
2. How many requests for withdrawal of ETH (from stETH) can be satisfied and at what rate.

Ranges of the data manipulation are controlled by the OracleReportSanityChecker.

Impact description

The role can partially stop submitting the report. However, the Oracle committee members are able to submit the data even without this role assigned at all. Thus, a stop to the rebasing is unlikely.

Owners

Owner type	**Unassigned**
Owner address	**N/A**
Attack complexity	**HIGH**

Attack scenario

The owner is not assigned, so the attack complexity is equal to the attack complexity of APP_MANAGER_ROLE. The APP_MANAGER_ROLE is controlled by Aragon Voting, so the attacker has to execute a malicious proposal to compromise this role.

Domain	**Staking pool**
Contract	**Accounting Oracle:AccountingOracle (Implementation)**
Role name	**MANAGE_CONSENSUS_CONTRACT_ROLE**
Auth type	**custom-acl-oz-fork**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**HIGH**

Role description

The role sets the HashConsensus contract.

Impact description

The role can change the consensus contract to malicious and allow more volatility for data reported to Lido.

Owners

Owner type	**Unassigned**
Owner address	**N/A**
Attack complexity	**HIGH**

Attack scenario

The owner is not assigned, so the attack complexity is equal to the attack complexity of APP_MANAGER_ROLE. The APP_MANAGER_ROLE is controlled by Aragon Voting, so the attacker has to execute a malicious proposal to compromise this role.

Domain	**Staking pool**
Contract	**Accounting Oracle:AccountingOracle (Implementation)**
Role name	**MANAGE_CONSENSUS_VERSION_ROLE**
Auth type	**custom-acl-oz-fork**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role sets the consensus version expected by the oracle contract

Impact description

The role can block the submit report functionality.

Owners

Owner type	**Unassigned**
Owner address	**N/A**
Attack complexity	**HIGH**

Attack scenario

The owner is not assigned, so the attack complexity is equal to the attack complexity of APP_MANAGER_ROLE. The APP_MANAGER_ROLE is controlled by Aragon Voting, so the attacker has to execute a malicious proposal to compromise this role.

Domain	**Staking pool**
Contract	**Accounting Oracle:HashConsensus**
Role name	**DEFAULT_ADMIN_ROLE**
Auth type	**custom-acl-oz-fork**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**HIGH**

Role description

The role is able to grant or revoke all roles.

Impact description

The impact is a cumulative impact from all the roles of this contract.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**Staking pool**
Contract	**Accounting Oracle:HashConsensus**
Role name	**MANAGE_MEMBERS_AND_QUORUM_ROLE**
Auth type	**custom-acl-oz-fork**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**HIGH**

Role description

The role modifies members list members and changes the quorum by calling addMember, removeMember, and setQuorum functions.

Impact description

The role can add malicious members to violate rebasing.

Owners

Owner type	**Unassigned**
Owner address	**N/A**
Attack complexity	**HIGH**

Attack scenario

The owner is not assigned, so the attack complexity is equal to the attack complexity of APP_MANAGER_ROLE. The APP_MANAGER_ROLE is controlled by Aragon Voting, so the attacker has to execute a malicious proposal to compromise this role.

Domain	**Staking pool**
Contract	**Accounting Oracle:HashConsensus**
Role name	**DISABLE_CONSENSUS_ROLE**
Auth type	**custom-acl-oz-fork**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role disables the consensus by calling the disableConsensus function.

Impact description

The role can stop **AccountingOracle** processing and, therefore, stop the rebasing.

Owners

Owner type	**Unassigned**
Owner address	**N/A**
Attack complexity	**HIGH**

Attack scenario

The owner is not assigned, so the attack complexity is equal to the attack complexity of **APP_MANAGER_ROLE**. The **APP_MANAGER_ROLE** is controlled by Aragon Voting, so the attacker has to execute a malicious proposal to compromise this role.

Domain	**Staking pool**
Contract	**Accounting Oracle:HashConsensus**
Role name	**MANAGE_FRAME_CONFIG_ROLE**
Auth type	**custom-acl-oz-fork**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role changes reporting interval duration and fast lane reporting interval length by calling setFrameConfig.

Impact description

The role can decrease/increase the frequency of the rebasings.

Owners

Owner type	**Unassigned**
Owner address	**N/A**
Attack complexity	**HIGH**

Attack scenario

The owner is not assigned, so the attack complexity is equal to the attack complexity of APP_MANAGER_ROLE. The APP_MANAGER_ROLE is controlled by Aragon Voting, so the attacker has to execute a malicious proposal to compromise this role.

Domain	**Staking pool**
Contract	**Accounting Oracle:HashConsensus**
Role name	**MANAGE_FAST_LANE_CONFIG_ROLE**
Auth type	**custom-acl-oz-fork**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role changes fast lane reporting interval length by calling **setFastLaneLengthSlots**.

Impact description

The role can decrease/increase the frequency of the rebasings.

Owners

Owner type	**Unassigned**
Owner address	**N/A**
Attack complexity	**HIGH**

Attack scenario

The owner is not assigned, so the attack complexity is equal to the attack complexity of **APP_MANAGER_ROLE**. The **APP_MANAGER_ROLE** is controlled by Aragon Voting, so the attacker has to execute a malicious proposal to compromise this role.

Domain	**Staking pool**
Contract	**Accounting Oracle:HashConsensus**
Role name	**MANAGE_REPORT_PROCESSOR_ROLE**
Auth type	**custom-acl-oz-fork**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role changes the report processor contract by calling **setReportProcessor**.

Impact description

The role can change the report processor and, therefore, stop reporting data by the current processor (stop rebasing).

Owners

Owner type	**Unassigned**
Owner address	**N/A**
Attack complexity	**HIGH**

Attack scenario

The owner is not assigned, so the attack complexity is equal to the attack complexity of **APP_MANAGER_ROLE**. The **APP_MANAGER_ROLE** is controlled by Aragon Voting, so the attacker has to execute a malicious proposal to compromise this role.

Domain	**Staking pool**
Contract	**Accounting Oracle:HashConsensus**
Role name	**Quorum**
Auth type	**custom-acl**
Role impact severity	**HIGH**
Attack complexity cumulative	**MEDIUM**

Role description

The role submits report data to consensus (if the consensus is met, it provides the data to the oracle):

1. An amount of ETH and a number of validators on the Beacon Chain.
2. How many requests for withdrawal of ETH (from stETH) can be satisfied and at what rate.

Impact description

A group of quorum members can submit malicious data.

Owners

Owner type	**EOA**
Owner address	**0x140Bd8FbDc884f48dA7cb1c09bE8A2fAdfea776E**
Attack complexity	**LOW**

Attack scenario

The current quorum is 5, so it is needed to get private keys of a minimum of 5 out of 9 members.

Owner type	**EOA**
Owner address	**0x1d0813bf088BE3047d827D98524fBf779Bc25F00**
Attack complexity	**LOW**

Attack scenario

The current quorum is 5, so it is needed to get private keys of a minimum of 5 out of 9 members.

Owner type	**EOA**
Owner address	0x404335BcE530400a5814375E7Ec1FB55fAff3eA2
Attack complexity	**LOW**

Attack scenario

The current quorum is 5, so it is needed to get private keys of a minimum of 5 out of 9 members.

Owner type	**EOA**
Owner address	0x946D3b081ed19173dC83Cd974fC69e1e760B7d78
Attack complexity	**LOW**

Attack scenario

The current quorum is 5, so it is needed to get private keys of a minimum of 5 out of 9 members.

Owner type	**EOA**
Owner address	0x007DE4a5F7bc37E2F26c0cb2E8A95006EE9B89b5
Attack complexity	**LOW**

Attack scenario

The current quorum is 5, so it is needed to get private keys of a minimum of 5 out of 9 members.

Owner type	**EOA**
Owner address	0xEC4BfbAF681eb505B94E4a7849877DC6c600Ca3A
Attack complexity	**LOW**

Attack scenario

The current quorum is 5, so it is needed to get private keys of a minimum of 5 out of 9 members.

Owner type	**EOA**
Owner address	**0x61c91ECd902EB56e314bB2D5c5C07785444Ea1c8**
Attack complexity	**LOW**

Attack scenario

The current quorum is 5, so it is needed to get private keys of a minimum of 5 out of 9 members.

Owner type	**EOA**
Owner address	**0x1Ca0fEC59b86F549e1F1184d97cb47794C8Af58d**
Attack complexity	**LOW**

Attack scenario

The current quorum is 5, so it is needed to get private keys of a minimum of 5 out of 9 members.

Owner type	**EOA**
Owner address	**0xA7410857ABbf75043d61ea54e07D57A6EB6EF186**
Attack complexity	**LOW**

Attack scenario

The current quorum is 5, so it is needed to get private keys of a minimum of 5 out of 9 members.

Domain	**Staking pool**
Contract	**Validators Exit Bus Oracle:ValidatorsExitBusOracle (Proxy)**
Role name	**ADMIN**
Auth type	**custom-acl-over-oz-erc1967proxy**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**HIGH**

Role description

The role changes implementation, change/reset **ADMIN** role owner.

Impact description

The contract is responsible for processing validator exit requests in the Lido. It includes functionality to submit and process reports related to validator exits, manage the state of these processes, and ensure that the data submitted adheres to the expected format and rules. The role can completely block correct validator exit functionality. So, Lido contracts can't have the correct validator and balances state.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**Staking pool**
Contract	**Validators Exit Bus Oracle:ValidatorsExitBusOracle (Implementation)**
Role name	**DEFAULT_ADMIN_ROLE**
Auth type	**custom-acl-oz-fork**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role is able to grant or revoke all roles.

Impact description

The impact is a cumulative impact from all the roles of this contract.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**Staking pool**
Contract	**Validators Exit Bus Oracle:ValidatorsExitBusOracle (Implementation)**
Role name	**SUBMIT_DATA_ROLE**
Auth type	**custom-acl-oz-fork**
Role impact severity	**MEDIUM**
Attack complexity cumulative	**HIGH**

Role description

The role submits report data for processing, that result informs (through sending events) the node operators that it is necessary to initiate the exit of some validators. The maximum number of validators for the single report is limited by the OracleReportSanityChecker.

Impact description

The role can stop submitting the report and stop data providing to off-chain oracles/observers for some time.

Owners

Owner type	**Unassigned**
Owner address	**N/A**
Attack complexity	**HIGH**

Attack scenario

The owner is not assigned, so the attack complexity is equal to the attack complexity of APP_MANAGER_ROLE. The APP_MANAGER_ROLE is controlled by Aragon Voting, so the attacker has to execute a malicious proposal to compromise this role.

Domain	**Staking pool**
Contract	**Validators Exit Bus Oracle:ValidatorsExitBusOracle (Implementation)**
Role name	**MANAGE_CONSENSUS_CONTRACT_ROLE**
Auth type	**custom-acl-oz-fork**
Role impact severity	**MEDIUM**
Attack complexity cumulative	**HIGH**

Role description

The role sets the HashConsensus contract.

Impact description

The role can change the consensus contract and allow more volatility for data reported to off-chain instances.

Owners

Owner type	**Unassigned**
Owner address	**N/A**
Attack complexity	**HIGH**

Attack scenario

The owner is not assigned, so the attack complexity is equal to the attack complexity of APP_MANAGER_ROLE. The APP_MANAGER_ROLE is controlled by Aragon Voting, so the attacker has to execute a malicious proposal to compromise this role.

Domain	**Staking pool**
Contract	**Validators Exit Bus Oracle:ValidatorsExitBusOracle (Implementation)**
Role name	**MANAGE_CONSENSUS_VERSION_ROLE**
Auth type	**custom-acl-oz-fork**
Role impact severity	**MEDIUM**
Attack complexity cumulative	**HIGH**

Role description

The role sets the consensus version expected by the oracle contract.

Impact description

The role can block the submit report functionality.

Owners

Owner type	**Unassigned**
Owner address	**N/A**
Attack complexity	**HIGH**

Attack scenario

The owner is not assigned, so the attack complexity is equal to the attack complexity of APP_MANAGER_ROLE. The APP_MANAGER_ROLE is controlled by Aragon Voting, so the attacker has to execute a malicious proposal to compromise this role.

Domain	**Staking pool**
Contract	**Validators Exit Bus Oracle:ValidatorsExitBusOracle (Implementation)**
Role name	**PAUSE_ROLE**
Auth type	**custom-acl-oz-fork**
Role impact severity	**MEDIUM**
Attack complexity cumulative	**HIGH**

Role description

The role pauses if it isn't paused. Paused functions: **submitReportData()**

Impact description

The role can block the submit report functionality.

Owners

Owner type	**GateSeal**
Owner address	**0x1aD5cb2955940F998081c1eF5f5F00875431aA90**
Attack complexity	**HIGH**

Attack scenario

Aragon voting can be compromised in the following cases:

1. The undiscovered bug in the implementation of GateSeal token contract. However, GateSeal successfully passed several audits and battle-tested in production, so the probability of this kind of bug is low.
2. Control 3/6 EOA from multisig contract.

The impact is limited with the duration provided still. GateSeal can't pause for more than 6 days.

Domain	**Staking pool**
Contract	**Validators Exit Bus Oracle:ValidatorsExitBusOracle (Implementation)**
Role name	**RESUME_ROLE**
Auth type	**custom-acl-oz-fork**
Role impact severity	**MEDIUM**
Attack complexity cumulative	**HIGH**

Role description

The role resumes contract if paused.

Impact description

The role can maliciously resume the contract when it needs to be paused.

Owners

Owner type	**Unassigned**
Owner address	**N/A**
Attack complexity	**HIGH**

Attack scenario

The owner is not assigned, so the attack complexity is equal to the attack complexity of APP_MANAGER_ROLE. The APP_MANAGER_ROLE is controlled by Aragon Voting, so the attacker has to execute a malicious proposal to compromise this role.

Domain	**Staking pool**
Contract	**Validators Exit Bus Oracle:HashConsensus**
Role name	**DEFAULT_ADMIN_ROLE**
Auth type	**custom-acl-oz-fork**
Role impact severity	**MEDIUM**
Attack complexity cumulative	**HIGH**

Role description

The role is able to grant or revoke all roles.

Impact description

The impact is a cumulative impact from all the roles of this contract.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**Staking pool**
Contract	**Validators Exit Bus Oracle:HashConsensus**
Role name	**MANAGE_MEMBERS_AND_QUORUM_ROLE**
Auth type	**custom-acl-oz-fork**
Role impact severity	**MEDIUM**
Attack complexity cumulative	**HIGH**

Role description

The role modifies members list members and changes the quorum by calling **addMember**, **removeMember**, and **setQuorum** functions.

Impact description

The role can add malicious members to violate data provided to off-chain oracles/observers.

Owners

Owner type	**Unassigned**
Owner address	**N/A**
Attack complexity	**HIGH**

Attack scenario

The owner is not assigned, so the attack complexity is equal to the attack complexity of **APP_MANAGER_ROLE**. The **APP_MANAGER_ROLE** is controlled by Aragon Voting, so the attacker has to execute a malicious proposal to compromise this role.

Domain	**Staking pool**
Contract	**Validators Exit Bus Oracle:HashConsensus**
Role name	**DISABLE_CONSENSUS_ROLE**
Auth type	**custom-acl-oz-fork**
Role impact severity	**MEDIUM**
Attack complexity cumulative	**HIGH**

Role description

The role disables the consensus by calling the disableConsensus function.

Impact description

The role can stop Validators Exit Bus processing and, therefore, stop data providing to off-chain oracles/observers.

Owners

Owner type	**Unassigned**
Owner address	**N/A**
Attack complexity	**HIGH**

Attack scenario

The owner is not assigned, so the attack complexity is equal to the attack complexity of APP_MANAGER_ROLE. The APP_MANAGER_ROLE is controlled by Aragon Voting, so the attacker has to execute a malicious proposal to compromise this role.

Domain	**Staking pool**
Contract	**Validators Exit Bus Oracle:HashConsensus**
Role name	**MANAGE_FRAME_CONFIG_ROLE**
Auth type	**custom-acl-oz-fork**
Role impact severity	**MEDIUM**
Attack complexity cumulative	**HIGH**

Role description

The role changes reporting interval duration and fast lane reporting interval length by calling **setFrameConfig**.

Impact description

The role can decrease/increase the frequency of the data reporting.

Owners

Owner type	**Unassigned**
Owner address	**N/A**
Attack complexity	**HIGH**

Attack scenario

The owner is not assigned, so the attack complexity is equal to the attack complexity of **APP_MANAGER_ROLE**. The **APP_MANAGER_ROLE** is controlled by Aragon Voting, so the attacker has to execute a malicious proposal to compromise this role.

Domain	**Staking pool**
Contract	**Validators Exit Bus Oracle:HashConsensus**
Role name	**MANAGE_FAST_LANE_CONFIG_ROLE**
Auth type	**custom-acl-oz-fork**
Role impact severity	**MEDIUM**
Attack complexity cumulative	**HIGH**

Role description

The role changes fast lane reporting interval length by calling setFastLaneLengthSlots.

Impact description

The role can decrease/increase the frequency of the data reporting.

Owners

Owner type	**Unassigned**
Owner address	**N/A**
Attack complexity	**HIGH**

Attack scenario

The owner is not assigned, so the attack complexity is equal to the attack complexity of APP_MANAGER_ROLE. The APP_MANAGER_ROLE is controlled by Aragon Voting, so the attacker has to execute a malicious proposal to compromise this role.

Domain	**Staking pool**
Contract	**Validators Exit Bus Oracle:HashConsensus**
Role name	**MANAGE_REPORT_PROCESSOR_ROLE**
Auth type	**custom-acl-oz-fork**
Role impact severity	**MEDIUM**
Attack complexity cumulative	**HIGH**

Role description

The role changes the report processor contract by calling setReportProcessor.

Impact description

The role can change the report processor and, therefore, stop reporting data by the current processor (stop data providing).

Owners

Owner type	**Unassigned**
Owner address	**N/A**
Attack complexity	**HIGH**

Attack scenario

The owner is not assigned, so the attack complexity is equal to the attack complexity of APP_MANAGER_ROLE. The APP_MANAGER_ROLE is controlled by Aragon Voting, so the attacker has to execute a malicious proposal to compromise this role.

Domain	**Staking pool**
Contract	**Validators Exit Bus Oracle:HashConsensus**
Role name	**Quorum**
Auth type	**custom-acl**
Role impact severity	**MEDIUM**
Attack complexity cumulative	**MEDIUM**

Role description

The role submits the report data (validator exit requests) to the consensus (if the consensus is met, it provides the data to the oracle).

Impact description

A group of members can submit malicious data.

Owners

Owner type	**EOA**
Owner address	**0x140Bd8FbDc884f48dA7cb1c09bE8A2fAdfea776E**
Attack complexity	**LOW**

Attack scenario

The current quorum is 5, so it is needed to get private keys of a minimum of 5 out of 9 members.

Owner type	**EOA**
Owner address	**0x1d0813bf088BE3047d827D98524fBf779Bc25F00**
Attack complexity	**LOW**

Attack scenario

The current quorum is 5, so it is needed to get private keys of a minimum of 5 out of 9 members.

Owner type	**EOA**
Owner address	0x404335BcE530400a5814375E7Ec1FB55fAff3eA2
Attack complexity	**LOW**

Attack scenario

The current quorum is 5, so it is needed to get private keys of a minimum of 5 out of 9 members.

Owner type	**EOA**
Owner address	0x946D3b081ed19173dC83Cd974fC69e1e760B7d78
Attack complexity	**LOW**

Attack scenario

The current quorum is 5, so it is needed to get private keys of a minimum of 5 out of 9 members.

Owner type	**EOA**
Owner address	0x007DE4a5F7bc37E2F26c0cb2E8A95006EE9B89b5
Attack complexity	**LOW**

Attack scenario

The current quorum is 5, so it is needed to get private keys of a minimum of 5 out of 9 members.

Owner type	**EOA**
Owner address	0xEC4BfbAF681eb505B94E4a7849877DC6c600Ca3A
Attack complexity	**LOW**

Attack scenario

The current quorum is 5, so it is needed to get private keys of a minimum of 5 out of 9 members.

Owner type	**EOA**
Owner address	**0x61c91ECd902EB56e314bB2D5c5C07785444Ea1c8**
Attack complexity	**LOW**

Attack scenario

The current quorum is 5, so it is needed to get private keys of a minimum of 5 out of 9 members.

Owner type	**EOA**
Owner address	**0x1Ca0fEC59b86F549e1F1184d97cb47794C8Af58d**
Attack complexity	**LOW**

Attack scenario

The current quorum is 5, so it is needed to get private keys of a minimum of 5 out of 9 members.

Owner type	**EOA**
Owner address	**0xA7410857ABbf75043d61ea54e07D57A6EB6EF186**
Attack complexity	**LOW**

Attack scenario

The current quorum is 5, so it is needed to get private keys of a minimum of 5 out of 9 members.

Domain	**Staking pool**
Contract	**OracleReportSanityChecker**
Role name	**DEFAULT_ADMIN_ROLE**
Auth type	**custom-acl-oz-fork**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**HIGH**

Role description

The role is able to grant or revoke all roles.

Impact description

The impact is a cumulative impact from all the roles of this contract.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**Staking pool**
Contract	**OracleReportSanityChecker**
Role name	**ALL_LIMITS_MANAGER_ROLE**
Auth type	**custom-acl-oz-fork**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**HIGH**

Role description

The role sets the new values for the limits list.

Impact description

The role can set any limit parameter and, therefore, allow TVL manipulations.

Owners

Owner type	**Unassigned**
Owner address	**N/A**
Attack complexity	**HIGH**

Attack scenario

The owner is not assigned, so the attack complexity is equal to the attack complexity of APP_MANAGER_ROLE. The APP_MANAGER_ROLE is controlled by Aragon Voting, so the attacker has to execute a malicious proposal to compromise this role.

Domain	Staking pool
Contract	OracleReportSanityChecker
Role name	CHURN_VALIDATORS_PER_DAY_LIMIT_MANAGER_ROLE
Auth type	custom-acl-oz-fork
Role impact severity	HIGH
Attack complexity cumulative	HIGH

Role description

The role sets the new value for the churnValidatorsPerDayLimit.

Impact description

The role can change churnValidatorsPerDayLimit to allow manipulation of the data about the appeared and exited validators possibly indicating oracle members colluding to manipulate the protocol's TVL.

Owners

Owner type	Unassigned
Owner address	N/A
Attack complexity	HIGH

Attack scenario

The owner is not assigned, so the attack complexity is equal to the attack complexity of APP_MANAGER_ROLE. The APP_MANAGER_ROLE is controlled by Aragon Voting, so the attacker has to execute a malicious proposal to compromise this role.

Domain	**Staking pool**
Contract	**OracleReportSanityChecker**
Role name	**ONE_OFF_CL_BALANCE_DECREASE_LIMIT_MANAGER_ROLE**
Auth type	**custom-acl-oz-fork**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role sets the new value for the oneOffCLBalanceDecreaseBPLimit.

Impact description

The role can change **oneOffCLBalanceDecreaseBPLimit** to allow manipulation of the CL balance of validators possibly indicating oracle members colluding to lower the protocol's TVL.

Owners

Owner type	**Unassigned**
Owner address	**N/A**
Attack complexity	**HIGH**

Attack scenario

The owner is not assigned, so the attack complexity is equal to the attack complexity of **APP_MANAGER_ROLE**. The **APP_MANAGER_ROLE** is controlled by Aragon Voting, so the attacker has to execute a malicious proposal to compromise this role.

Domain	**Staking pool**
Contract	**OracleReportSanityChecker**
Role name	**ANNUAL_BALANCE_INCREASE_LIMIT_MANAGER_ROLE**
Auth type	**custom-acl-oz-fork**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role sets the new value for the **annualBalanceIncreaseBPLimit.**

Impact description

The role can make the **oneOffCLBalanceDecreaseBPLimit** too low making the oracle report be blocked by the sanity check or too high making it possible for oracle consensus members to collude to manipulate the protocol's TVL.

Owners

Owner type	**Unassigned**
Owner address	**N/A**
Attack complexity	**HIGH**

Attack scenario

The owner is not assigned, so the attack complexity is equal to the attack complexity of **APP_MANAGER_ROLE.** The **APP_MANAGER_ROLE** is controlled by Aragon Voting, so the attacker has to execute a malicious proposal to compromise this role.

Domain	Staking pool
Contract	OracleReportSanityChecker
Role name	SHARE_RATE_DEVIATION_LIMIT_MANAGER_ROLE
Auth type	custom-acl-oz-fork
Role impact severity	HIGH
Attack complexity cumulative	HIGH

Role description

The role sets the new value for the **simulatedShareRateDeviationBPLimit**.

Impact description

The role can make the **simulatedShareRateDeviationBPLimit** too low making withdrawal finalization be stopped or too high allowing unfair withdrawal finalization stETH/ETH share rate.

Owners

Owner type	Unassigned
Owner address	N/A
Attack complexity	HIGH

Attack scenario

The owner is not assigned, so the attack complexity is equal to the attack complexity of **APP_MANAGER_ROLE**. The **APP_MANAGER_ROLE** is controlled by Aragon Voting, so the attacker has to execute a malicious proposal to compromise this role.

Domain	**Staking pool**
Contract	**OracleReportSanityChecker**
Role name	**MAX_VALIDATOR_EXIT_REQUESTS_PER_REPORT_ROLE**
Auth type	**custom-acl-oz-fork**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role sets the new value for the **maxValidatorExitRequestsPerReport**.

Impact description

The role can allow too low a number of exit requests which can extend withdrawal finalization time for unstaking users.

Owners

Owner type	**Unassigned**
Owner address	**N/A**
Attack complexity	**HIGH**

Attack scenario

The owner is not assigned, so the attack complexity is equal to the attack complexity of **APP_MANAGER_ROLE**. The **APP_MANAGER_ROLE** is controlled by Aragon Voting, so the attacker has to execute a malicious proposal to compromise this role.

Domain	**Staking pool**
Contract	**OracleReportSanityChecker**
Role name	**MAX_ACCOUNTING_EXTRA_DATA_LIST_ITEMS_COUNT_ROLE**
Auth type	**custom-acl-oz-fork**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role sets the new value for the **maxAccountingExtraDataListItemsCount**.

Impact description

The role can change the **maxAccountingExtraDataListItemsCount** to allow too much extra data, which is inefficient and can cause out-of-gas or change to not enough count making it impossible to report proper data.

Owners

Owner type	**Unassigned**
Owner address	**N/A**
Attack complexity	**HIGH**

Attack scenario

The owner is not assigned, so the attack complexity is equal to the attack complexity of **APP_MANAGER_ROLE**. The **APP_MANAGER_ROLE** is controlled by Aragon Voting, so the attacker has to execute a malicious proposal to compromise this role.

Domain	**Staking pool**
Contract	**OracleReportSanityChecker**
Role name	**MAX_NODE_OPERATORS_PER_EXTRA_DATA_ITEM_COUNT_ROLE**
Auth type	**custom-acl-oz-fork**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role sets the new value for the max **maxNodeOperatorsPerExtraDataItemCount**.

Impact description

The role can change the **maxNodeOperatorsPerExtraDataItemCount** to allow too many node operators which is improper because of NOR allowance and can cause out-of-gas. Can be too low not allowing to report of proper data.

Owners

Owner type	**Unassigned**
Owner address	**N/A**
Attack complexity	**HIGH**

Attack scenario

The owner is not assigned, so the attack complexity is equal to the attack complexity of **APP_MANAGER_ROLE**. The **APP_MANAGER_ROLE** is controlled by Aragon Voting, so the attacker has to execute a malicious proposal to compromise this role.

Domain	**Staking pool**
Contract	**OracleReportSanityChecker**
Role name	**REQUEST_TIMESTAMP_MARGIN_MANAGER_ROLE**
Auth type	**custom-acl-oz-fork**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role sets the new value for the **requestTimestampMargin**.

Impact description

The role can change the **requestTimestampMargin** to be too low which allows finalization manipulations or too high preventing withdrawals finalization at all.

Owners

Owner type	**Unassigned**
Owner address	**N/A**
Attack complexity	**HIGH**

Attack scenario

The owner is not assigned, so the attack complexity is equal to the attack complexity of **APP_MANAGER_ROLE**. The **APP_MANAGER_ROLE** is controlled by Aragon Voting, so the attacker has to execute a malicious proposal to compromise this role.

Domain	**Staking pool**
Contract	**OracleReportSanityChecker**
Role name	**MAX_POSITIVE_TOKEN_REBASE_MANAGER_ROLE**
Auth type	**custom-acl-oz-fork**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role sets max positive token rebase allowed per single oracle report.

Impact description

The role can change the maxPositiveTokenRebase to be too low and lower the token APR temporarily or too high which allows price manipulations.

Owners

Owner type	**Unassigned**
Owner address	**N/A**
Attack complexity	**HIGH**

Attack scenario

The owner is not assigned, so the attack complexity is equal to the attack complexity of **APP_MANAGER_ROLE**. The **APP_MANAGER_ROLE** is controlled by Aragon Voting, so the attacker has to execute a malicious proposal to compromise this role.

Domain	**Staking pool**
Contract	**OracleDaemonConfig**
Role name	**DEFAULT_ADMIN_ROLE**
Auth type	**custom-acl-oz-fork**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role is able to grant or revoke all roles.

Impact description

The impact is a cumulative impact from all the roles of this contract. Also may affect the bunker mode activation params.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**Staking pool**
Contract	**OracleDaemonConfig**
Role name	**CONFIG_MANAGER_ROLE**
Auth type	**custom-acl-oz-fork**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role sets, updates, unsets data.

Impact description

The role can set improper values to parameters and for some time make oracle daemons check and submit data inaccurately. Also may affect the bunker mode activation params.

Owners

Owner type	**Unassigned**
Owner address	**N/A**
Attack complexity	**HIGH**

Attack scenario

The owner is not assigned, so the attack complexity is equal to the attack complexity of **APP_MANAGER_ROLE**. The **APP_MANAGER_ROLE** is controlled by Aragon Voting, so the attacker has to execute a malicious proposal to compromise this role.

Domain	**Staking pool**
Contract	**Legacy Oracle (Implementation)**
Role name	**Lido**
Auth type	**custom-acl**
Role impact severity	**MEDIUM**
Attack complexity cumulative	**HIGH**

Role description

The role handles token rebase.

Impact description

The role can violate daily rebase and APR calculation at old LidoOracle APIs.

Owners

Owner type	**Lido and stETH token**
Owner address	**0xae7ab96520DE3A18E5e111B5EaAb095312D7fE84**
Attack complexity	**HIGH**

Attack scenario

The method at AccountingOracle can be executed only by **AccountingOracle:SUBMIT_DATA_ROLE** or by anyone from **AccountingOracle:HashConsensus:QuorumMembers**. However, there is no owner for **SUBMIT_DATA_ROLE**. So it is needed to get the private key of some quorum members.

Domain	**Staking pool**
Contract	**Legacy Oracle (Implementation)**
Role name	**AccountingOracle**
Auth type	**custom-acl**
Role impact severity	**MEDIUM**
Attack complexity cumulative	**HIGH**

Role description

The role handles consensus layer reports.

Impact description

The role can violate daily rebase and APR calculation at old LidoOracle APIs given that the quorum submitted the wrong data before.

Owners

Owner type	**Accounting Oracle**
Owner address	**0x852deD011285fe67063a08005c71a85690503Cee**
Attack complexity	**HIGH**

Attack scenario

The method at AccountingOracle can be executed only by **AccountingOracle:SUBMIT_DATA_ROLE** or by anyone from **AccountingOracle:HashConsensus:QuorumMembers**. However, there is no owner for **SUBMIT_DATA_ROLE**. So it is needed to get the private key of some quorum members.

Domain	**DAO Aragon**
Contract	**Lido DAO (Implementation) – Kernel**
Role name	**APP_MANAGER_ROLE**
Auth type	**aragon-acl**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**HIGH**

Role description

The role allows creating, registering, and removing implementation addresses that contain the business logic of contracts.

Impact description

The role can replace the logic address of the contract via update exist Aragon app or to create a new inside kernel. Cumulative impact depends on apps registered in Kernel. Updating contracts:

- **Node Operators registry (Proxy) – 0x55032650b14df07b85bF18A3a3eC8E0Af2e028d5** Loss of new deposits cause of incorrect keys from obtainDepositData method.
- **Lido and stETH token (Proxy) – 0xae7ab96520DE3A18E5e111B5EaAb095312D7fE84** So, the attacker can steal/block all funds from the main core contract of the protocol, and block all functions in the protocol.
- **Legacy Oracle (Proxy) – 0x442af784A788A5bd6F42A01Ebe9F287a871243fb** So, attacker can manipulate APIs that use these contracts. Also, can break rewards distribution (rebasings).
- **KernelProxy – 0xb8FFC3Cd6e7Cf5a098A1c92F48009765B24088Dc (Lido DAO), 0x468efc7aceb906c7923fb7180144cf21ddf5f5c1 (NOT-Lido DAO)** If an attacker is the owner of **APP_MANAGER_ROLE** and changes Kernel implementation, it's equivalent to a total loss of control over Lido Aragon DAO.
- **KernelProxy – 0x468efc7aceb906c7923fb7180144cf21ddf5f5c1 (NOT-Lido DAO)** If an attacker is the owner of **APP_MANAGER_ROLE** and changes Kernel implementation, it's equivalent to losing control over Repos and APM registry and other information-providing contracts.
- **Aragon ACL (Proxy) – 0x9895f0f17cc1d1891b6f18ee0b483b6f221b37bb (Lido DAO), 0x40757238D800e0C1D88cdbD3331669d36B6C53A1 (NOT-Lido DAO)** So, an attacker can create/add/revoke any role for controlled addresses.
- **Aragon Agent (Proxy) – 0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c** So, the attacker can steal funds from Lido Aragon DAO, and execute any action from other roles Aragon Agent. Details in the description of every role.
- **Aragon Voting (Proxy) – 0x2e59A20f205bB85a89C53f1936454680651E618e** So, the attacker can create, vote, and execute any votes without voting tokens on their own balance.
- **Aragon Token Manager (Proxy) – 0xf73a1260d222f447210581DDf212D915c09a3249** So, the attacker can block votes creation, because Token Manager is **CREATE_VOTES_ROLE** owner. Also, the attacker can mint, or burn any amount of LDO.
- **Aragon Finance (Proxy) – 0xB9E5CBB9CA5b0d659238807E84D0176930753d86** So, the attacker can block any operation for Aragon Finance. Also, the attacker can steal funds from the vault contract.
- **Voting Repo (Proxy) – 0x4ee3118e3858e8d7164a634825bfe0f73d99c792**
- **Lido App Repo (Proxy) – 0xF5Dc67E54FC96F993CD06073f71ca732C1E654B1**
- **Lido Oracle Repo (Proxy) – 0xF9339DE629973c60c4d2b76749c81E6F40960E3A**
- **Node Operators Registry Repo (Proxy) – 0x0D97E876ad14DB2b183CFeEB8aa1A5C788eB1831**
- **UnknownRepo (Proxy) – 0x1EcBaa265104CD337E409d42986a58d1259aE8bc**
- **Aragon Finance Repo (Proxy) – 0x24782eac7E9eF6e34819b0a5C77311a7aD3558D6**
- **Aragon Token Manager Repo (Proxy) – 0x5f53411436704B95CBE7F65663fd1C14a32848D2**
- **Repo Repo (Proxy) – 0x96017c9d16F14cA24B6BAcfc36F1bA806bb07DD2**

- APMRegistry Repo (Proxy) – 0xBc9eD4f82D98cCcb0738c64eDbC12E8b771E7605
- Aragon Agent Repo (Proxy) – 0xC132877BAe6021F319F2288e03668A1C494D13B8 So, the attacker can block or fake providing info about the version. The impact may depend on the use of the contract by an external system.
- APMRegistry (Proxy) – 0x0cb113890b04B49455DfE06554e2D784598A29C9 APMRegistry has CREATE_PERMISSIONS_ROLE, because it grants permissions during creating repo contracts. So, the attacker can issue any new or existing role without the permission manager.

Owners

Owner type	Aragon Voting
Owner address	0x2e59A20f205bB85a89C53f1936454680651E618e
Attack complexity	HIGH

Attack scenario

This role is protected by the Aragon Voting contract and doesn't contain other significant conditions. Thus, the compromisation complexity is equivalent to a vote with a malicious script. The implementation update for the Aragon proxy contracts is possible only after the role is captured.

Domain	**DAO Aragon**
Contract	**Aragon ACL (Implementation)**
Role name	**CREATE_PERMISSIONS_ROLE**
Auth type	**aragon-acl**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**HIGH**

Role description

The role allows the creation of new(non existing and non managed) roles and setting permission manager to new roles.

Impact description

The role can occupy all roles with an unregistered entity and set a manager for it.

Owners

Owner type	**Aragon Voting**
Owner address	**0x2e59A20f205bB85a89C53f1936454680651E618e**
Attack complexity	**HIGH**

Attack scenario

This role is protected by the Aragon Voting contract and doesn't contain other significant conditions. Thus, the compromisation complexity is equivalent to a vote with a malicious script.

Domain	**DAO Aragon**
Contract	**Aragon ACL (Implementation)**
Role name	**PERMISSION_MANAGER**
Auth type	**aragon-acl**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**HIGH**

Role description

The role allows granting and revoking new addresses to roles that are assigned to the permission manager. Also, the role can update/remove the address of the permission manager.

Impact description

The role can block all functions of the protocol which has authentication via roles that are managed by the permission manager. Bypass the authentication mechanism for roles, because the permission manager can set any addresses to roles.

Owners

Owner type	**Aragon Voting**
Owner address	**0x2e59A20f205bB85a89C53f1936454680651E618e**
Attack complexity	**HIGH**

Attack scenario

This role is protected by the Aragon Voting contract and doesn't contain other significant conditions. Thus, the compromisation complexity is equivalent to a vote with a malicious script.

Domain	**DAO Aragon**
Contract	**EVMScriptRegistry (Implementation)**
Role name	**REGISTRY_ADD_EXECUTOR_ROLE**
Auth type	**aragon-acl**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**HIGH**

Role description

The role allows adding a new EVM script executor.

Impact description

The role can register a malicious script executor. If a victim doesn't check the executor's implementation, so malicious executor can execute any code when the victim tries to run their own script.

Owners

Owner type	**Aragon Voting**
Owner address	**0x2e59A20f205bB85a89C53f1936454680651E618e**
Attack complexity	**HIGH**

Attack scenario

This role is protected by the Aragon Voting contract and doesn't contain other significant conditions. Thus, the compromisation complexity is equivalent to a vote with a malicious script.

Domain	**DAO Aragon**
Contract	**EVMScriptRegistry (Implementation)**
Role name	**REGISTRY_MANAGER_ROLE**
Auth type	**aragon-acl**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role allows disabling/enabling status for the EVM script executor.

Impact description

The role can disable all executors, get script executors, and run their scripts.

Owners

Owner type	**Aragon Voting**
Owner address	**0x2e59A20f205bB85a89C53f1936454680651E618e**
Attack complexity	**HIGH**

Attack scenario

This role is protected by the Aragon Voting contract and doesn't contain other significant conditions. Thus, the compromisation complexity is equivalent to a vote with a malicious script.

Domain	**DAO Aragon**
Contract	**Aragon Agent (Implementation)**
Role name	**EXECUTE_ROLE**
Auth type	**aragon-acl**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**HIGH**

Role description

The role executes any data and can spend any tokens from the treasury.

Impact description

The role can steal all the funds (any tokens and ETH). Also, it can call any function at other contracts, where it has a needed role.

Owners

Owner type	**Aragon Voting**
Owner address	**0x2e59A20f205bB85a89C53f1936454680651E618e**
Attack complexity	**HIGH**

Attack scenario

Aragon Agent allows direct call external contracts using Agent:execute function. This role is protected by the Aragon Voting Contract and doesn't contain any other significant conditions. Thus, the compromisation complexity is equivalent to acceptance of voting with malicious script.

Domain	**DAO Aragon**
Contract	**Aragon Agent (Implementation)**
Role name	**TRANSFER_ROLE**
Auth type	**aragon-acl**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**HIGH**

Role description

Transfer tokens from the Vault.

Impact description

The role can steal any ERC20 token and ETH.

Owners

Owner type	**Aragon Finance**
Owner address	**0xB9E5CBB9CA5b0d659238807E84D0176930753d86**
Attack complexity	**HIGH**

Attack scenario

It can be compromised by compromising **Aragon Finance:CREATE_PAYMENTS_ROLE** or **Aragon Finance:EXECUTE_PAYMENTS_ROLE**.

Domain	**DAO Aragon**
Contract	**Aragon Agent (Implementation)**
Role name	**SAFE_EXECUTE_ROLE**
Auth type	**aragon-acl**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**HIGH**

Role description

The role executes any data without spending protected tokens

Impact description

The role can steal any token except protected ones. Also, it can call any function at other contracts, where it has a needed role.

Owners

Owner type	**Unassigned**
Owner address	**N/A**
Attack complexity	**HIGH**

Attack scenario

The owner is not assigned, so the attack complexity is equal to the attack complexity of APP_MANAGER_ROLE. The APP_MANAGER_ROLE is controlled by Aragon Voting, so the attacker has to execute a malicious proposal to compromise this role.

Domain	**DAO Aragon**
Contract	**Aragon Agent (Implementation)**
Role name	**ADD_PROTECTED_TOKEN_ROLE**
Auth type	**aragon-acl**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

Add some tokens to the list of protected tokens

Impact description

The role can add protected tokens. Therefore, having SAFE_EXECUTE_ROLE enables to steal any token.

Owners

Owner type	**Unassigned**
Owner address	**N/A**
Attack complexity	**HIGH**

Attack scenario

The owner is not assigned, so the attack complexity is equal to the attack complexity of APP_MANAGER_ROLE. The APP_MANAGER_ROLE is controlled by Aragon Voting, so the attacker has to execute a malicious proposal to compromise this role.

Domain	**DAO Aragon**
Contract	**Aragon Agent (Implementation)**
Role name	**REMOVE_PROTECTED_TOKEN_ROLE**
Auth type	**aragon-acl**
Role impact severity	**MEDIUM**
Attack complexity cumulative	**HIGH**

Role description

Remove some tokens from the list of protected tokens

Impact description

If the last protected token was removed, the array will have the dirty bytes at the first slot (the implementation of **_removeProtectedToken()** isn't fully correct).

Owners

Owner type	**Unassigned**
Owner address	**N/A**
Attack complexity	**HIGH**

Attack scenario

The owner is not assigned, so the attack complexity is equal to the attack complexity of **APP_MANAGER_ROLE**. The **APP_MANAGER_ROLE** is controlled by Aragon Voting, so the attacker has to execute a malicious proposal to compromise this role.

Domain	**DAO Aragon**
Contract	**Aragon Agent (Implementation)**
Role name	**ADD_PRESIGNED_HASH_ROLE**
Auth type	**aragon-acl**
Role impact severity	**MEDIUM**
Attack complexity cumulative	**HIGH**

Role description

Pre-sign hash

Impact description

The role can make any signature/hash valid through ERC-1271. It could result in a lack of authentication.

Owners

Owner type	**Unassigned**
Owner address	**N/A**
Attack complexity	**HIGH**

Attack scenario

The owner is not assigned, so the attack complexity is equal to the attack complexity of APP_MANAGER_ROLE. The APP_MANAGER_ROLE is controlled by Aragon Voting, so the attacker has to execute a malicious proposal to compromise this role.

Domain	**DAO Aragon**
Contract	**Aragon Agent (Implementation)**
Role name	**DESIGNATE_SIGNER_ROLE**
Auth type	**aragon-acl**
Role impact severity	**MEDIUM**
Attack complexity cumulative	**HIGH**

Role description

Set any non-zero designatedSigner to validate the signatures for ERC-1271.

Impact description

The role can make any signature/hash valid (via malicious designatedSigner) through ERC-1271. It could result in a lack of authentication.

Owners

Owner type	**Unassigned**
Owner address	**N/A**
Attack complexity	**HIGH**

Attack scenario

The owner is not assigned, so the attack complexity is equal to the attack complexity of **APP_MANAGER_ROLE**. The **APP_MANAGER_ROLE** is controlled by Aragon Voting, so the attacker has to execute a malicious proposal to compromise this role.

Domain	**DAO Aragon**
Contract	**Aragon Agent (Implementation)**
Role name	**RUN_SCRIPT_ROLE**
Auth type	**aragon-acl**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**HIGH**

Role description

Execute the script as the Agent app

Impact description

The role can steal any tokens. Also, it can call any function at other contracts, where it has a needed role.

Owners

Owner type	**Aragon Voting**
Owner address	**0x2e59A20f205bB85a89C53f1936454680651E618e**
Attack complexity	**HIGH**

Attack scenario

Aragon Agent allows the execution of EVM scripts using Agent:forward function. However, **msg.sender** should have RUN_SCRIPT_ROLE(Aragon Voting) for the execution script. This role is protected by Aragon Voting Contract, so read the compromisation complexity for Aragon Voting Contract.

Domain	**DAO Aragon**
Contract	**LDO token**
Role name	**Controller**
Auth type	**custom-acl**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**HIGH**

Role description

The role generates, and destroys LDO tokens. Enable, and disable transfers. Claim tokens

Impact description

The role can unlimited mint/burn LDO tokens and transfer any tokens from the token contract. Also, the controller can permanently block token transferring for all LDO tokens. LDO token used for voting.

Owners

Owner type	**Aragon Token Manager**
Owner address	**0xf73a1260d222f447210581DDf212D915c09a3249**
Attack complexity	**HIGH**

Attack scenario

LDO tokens are managed by several roles in Aragon Token Management contracts. EVMScriptRegistry has only a single CallScript contract for script execution which reverts if target contract addresses contain blacklist addresses. Token Manager adds LDO token as a blacklisted address when executing a script.

1. If REGISTRY_ADD_EXECUTOR_ROLE adds a new executor implementation without blacklisting the attacker can unlimited mint, burn, and transfer LDO tokens.
2. If REGISTRY_ADD_EXECUTOR_ROLE adds a new executor which uses DELEGATE_CALL opcode it can corrupt Token Manager storage during the execution script. The attacker can execute the script via DELEGATE_CALL executor and change the token storage variable to a fake token in the Token Manager contract. In the next step, execute a malicious script for minting/burning LDO tokens, because the blacklist will contain the address of the fake token.

Domain	**DAO Aragon**
Contract	**Aragon Voting (Implementation)**
Role name	**CREATE_VOTES_ROLE**
Auth type	**aragon-acl**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

Create a new vote and register an EVM script that is to be executed on approval

Impact description

The role can spam the voting contract with useless votes or block creating new votes. Also, the role can create dummy votes with correct metadata but contains a malicious execution script.

Owners

Owner type	**Aragon Token Manager**
Owner address	**0xf73a1260d222f447210581DDf212D915c09a3249**
Attack complexity	**HIGH**

Attack scenario

Anyone who has an LDO token on balance can create a new proposal using TokenManager:forward function. So, an attacker has no reason to compromise this role.

Domain	**DAO Aragon**
Contract	**Aragon Voting (Implementation)**
Role name	**MODIFY_SUPPORT_ROLE**
Auth type	**aragon-acl**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**HIGH**

Role description

Change the percentage of "yes" in cast votes for a vote to succeed

Impact description

The role can decrease the percentage of "yes" in cast votes. So, the attacker can try to approve and execute an existing vote that does not have enough "yes" votes. Vote examples can be anything.

Owners

Owner type	**Aragon Voting**
Owner address	**0x2e59A20f205bB85a89C53f1936454680651E618e**
Attack complexity	**HIGH**

Attack scenario

The compromisation complexity is equivalent to to acceptance of voting with malicious script.

Domain	**DAO Aragon**
Contract	**Aragon Voting (Implementation)**
Role name	**MODIFY_QUORUM_ROLE**
Auth type	**aragon-acl**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**HIGH**

Role description

Change the percentage of yes in total possible votes for a vote to succeed

Impact description

The role can decrease the percentage of "yes" in total possible votes for a vote to succeed. So, the attacker can try to approve and execute an existing vote that does not have enough "yes" votes. Vote examples can be anything. If the attacker has MODIFY_SUPPORT_ROLE and MODIFY_QUORUM_ROLE he can execute any votes without a sufficient balance of voting tokens.

Owners

Owner type	**Aragon Voting**
Owner address	**0x2e59A20f205bB85a89C53f1936454680651E618e**
Attack complexity	**HIGH**

Attack scenario

The compromisation complexity is equivalent to to acceptance of voting with malicious script.

Domain	**DAO Aragon**
Contract	**Aragon Voting (Implementation)**
Role name	**UNSAFELY_MODIFY_VOTE_TIME_ROLE**
Auth type	**aragon-acl**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**HIGH**

Role description

Change vote time. Change the objection phase duration. The change affects all existing unexecuted votes

Impact description

The role can set short voting time or objection phase duration. So, the vote will not have enough time to get the required number of votes and will not pass. The role can set infinite voting time or objection phase duration. So, the approved vote can't be executed.

Owners

Owner type	**Unassigned**
Owner address	**N/A**
Attack complexity	**HIGH**

Attack scenario

The owner is not assigned, so the attack complexity is equal to the attack complexity of APP_MANAGER_ROLE. The APP_MANAGER_ROLE is controlled by Aragon Voting, so the attacker has to execute a malicious proposal to compromise this role.

Domain	**DAO Aragon**
Contract	**Aragon Token Manager (Implementation)**
Role name	**MINT_ROLE**
Auth type	**aragon-acl**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**HIGH**

Role description

The role mints tokens to anyone except the Token Manager

Impact description

The role can mint any amount of LDO tokens to anyone (except the Token Manager). Therefore, it can destroy the whole ecosystem through proposals. Extra tokens can be burned with BURN_ROLE (if its owner is not the same).

Owners

Owner type	**Unassigned**
Owner address	**N/A**
Attack complexity	**HIGH**

Attack scenario

The owner is not assigned, so the attack complexity is equal to the attack complexity of APP_MANAGER_ROLE. The APP_MANAGER_ROLE is controlled by Aragon Voting, so the attacker has to execute a malicious proposal to compromise this role.

Domain	**DAO Aragon**
Contract	**Aragon Token Manager (Implementation)**
Role name	**ISSUE_ROLE**
Auth type	**aragon-acl**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role can mint tokens for the Token Manager

Impact description

The role can mint any amount of LDO tokens to the Token Manager. So, new votes can be always rejected, because getting min quorum of votes is impossible. Also, unauthorized minting impacts LDO price and trust in the protocol.

Owners

Owner type	**Unassigned**
Owner address	**N/A**
Attack complexity	**HIGH**

Attack scenario

The owner is not assigned, so the attack complexity is equal to the attack complexity of **APP_MANAGER_ROLE**. The **APP_MANAGER_ROLE** is controlled by Aragon Voting, so the attacker has to execute a malicious proposal to compromise this role.

Domain	**DAO Aragon**
Contract	**Aragon Token Manager (Implementation)**
Role name	**ASSIGN_ROLE**
Auth type	**aragon-acl**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**HIGH**

Role description

The role assigns tokens to anyone from the Token Manager's holdings (can be via vesting)

Impact description

The role can transfer any amount of LDO tokens from the Token Manager to anyone. Also, **TokenManager:assignVested** it is assumed that the receiver is vesting contract. However, a role owner can just transfer the tokens to EOA receiver. Impact actual only when Token Manager has LDO token in own balance.

Owners

Owner type	**Aragon Voting**
Owner address	**0x2e59A20f205bB85a89C53f1936454680651E618e**
Attack complexity	**HIGH**

Attack scenario

LDO tokens are managed by several roles in Aragon Token Management contracts. **EVMScriptRegistry** has only a single CallScript contract for script execution which reverts if target contract addresses contain blacklist addresses. Token Manager adds LDO token as a blacklisted address when executing a script. If **REGISTRY_ADD_EXECUTOR_ROLE** adds a new executor implementation without a blacklist it is equivalent to a role capture. So, an attacker can transfer the LDO token from the Token Manager.

Domain	**DAO Aragon**
Contract	**Aragon Token Manager (Implementation)**
Role name	**REVOKE_VESTINGS_ROLE**
Auth type	**aragon-acl**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role revokes vesting, returning unvested tokens to the Token Manager

Impact description

The role can grief users with revokable vestings.

Owners

Owner type	**Unassigned**
Owner address	**N/A**
Attack complexity	**HIGH**

Attack scenario

The owner is not assigned, so the attack complexity is equal to the attack complexity of APP_MANAGER_ROLE. The APP_MANAGER_ROLE is controlled by Aragon Voting, so the attacker has to execute a malicious proposal to compromise this role.

Domain	**DAO Aragon**
Contract	**Aragon Token Manager (Implementation)**
Role name	**BURN_ROLE**
Auth type	**aragon-acl**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**HIGH**

Role description

The role burns LDO tokens from anyone

Impact description

The role can burn tokens from anyone. Therefore, it can destroy the whole ecosystem's economy. Tokens can be minted again via MINT_ROLE (if its owner is not the same), and ISSUE_ROLE.

Owners

Owner type	**Unassigned**
Owner address	**N/A**
Attack complexity	**HIGH**

Attack scenario

The owner is not assigned, so the attack complexity is equal to the attack complexity of APP_MANAGER_ROLE. The APP_MANAGER_ROLE is controlled by Aragon Voting, so the attacker has to execute a malicious proposal to compromise this role.

Domain	**DAO Aragon**
Contract	**Aragon Finance (Implementation)**
Role name	**CREATE_PAYMENTS_ROLE**
Auth type	**aragon-acl**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**HIGH**

Role description

This creates new immediate or scheduled payments. Immediate payment transfers funds from the vault to a recipient as part of the creation transaction. Scheduled payment executes transfers of funds from the vault to a recipient as part of the creation transaction depending on schedule parameters.

Impact description

The role can create immediate or scheduled payments. However, stealing funds from the vault by payments is possible if the proxy has TRANSFER_ROLE in the vault contract. Otherwise, the role owner can create fake payments, but can't execute them. At the time of the report, this vault had funds.

Owners

Owner type	**Aragon Voting**
Owner address	**0x2e59A20f205bB85a89C53f1936454680651E618e**
Attack complexity	**HIGH**

Attack scenario

The Finance contract must be the owner of TRANSFER_ROLE, and Vault contract should have tokens on balance. This role is protected by Aragon Voting Contract, so check the compromisation complexity for Aragon Voting Contract.

Owner type	**EVMScriptExecutor**
Owner address	**0xFE5986E06210aC1eCC1aDCafc0cc7f8D63B3F977**
Attack complexity	**HIGH**

Attack scenario

Aragon voting can be compromised in the following cases:

1. The undiscovered bug in the implementation of **EVMScriptExecutor** contract. However, EasyTrack contracts(including **EVMScriptExecutor**) successfully passed several audits and battle-tested in production, so the probability of this kind of bug can be considered low.
2. Accepts malicious proposals in EasyTrack.

Domain	**DAO Aragon**
Contract	**Aragon Finance (Implementation)**
Role name	**CHANGE_PERIOD_ROLE**
Auth type	**aragon-acl**
Role impact severity	**MEDIUM**
Attack complexity cumulative	**HIGH**

Role description

The role changes the period duration for internal accounting of the Finance contract. Operations such as depositing, creation and execution payments, managing budget and duration required making in actual period. So, the contract checks the current period timestamp and creates a new period if the timestamp expires.

Impact description

The role can set min period that is restricted to 1 day. If there is a timestamp difference between the end time of the last period and the current timestamp contract try fast-forwarding to an actual period. If there are too many periods, there may not be enough gas in a transaction. However, any participant can fast-forward using **Finance:tryTransitionAccountingPeriod** function. The role can set an infinite period duration, but it has no negative impact.

Owners

Owner type	**Unassigned**
Owner address	**N/A**
Attack complexity	**HIGH**

Attack scenario

The owner is not assigned, so the attack complexity is equal to the attack complexity of **APP_MANAGER_ROLE**. The **APP_MANAGER_ROLE** is controlled by Aragon Voting, so the attacker has to execute a malicious proposal to compromise this role.

Domain	**DAO Aragon**
Contract	**Aragon Finance (Implementation)**
Role name	**CHANGE_BUDGETS_ROLE**
Auth type	**aragon-acl**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role sets or removes the spending limit for some token, effective immediately. New payments can not be created and existing payments can't be executed if the limit is not enough.

Impact description

The role can block the creation of new payments and execution of existing payments via a setting 0 limit for any token.

Owners

Owner type	**Unassigned**
Owner address	**N/A**
Attack complexity	**HIGH**

Attack scenario

The owner is not assigned, so the attack complexity is equal to the attack complexity of APP_MANAGER_ROLE. The APP_MANAGER_ROLE is controlled by Aragon Voting, so the attacker has to execute a malicious proposal to compromise this role.

Domain	**DAO Aragon**
Contract	**Aragon Finance (Implementation)**
Role name	**EXECUTE_PAYMENTS_ROLE**
Auth type	**aragon-acl**
Role impact severity	**NO IMPACT**
Attack complexity cumulative	**HIGH**

Role description

The role executes a pending payment, which is limited by the payment schedule settings.

Impact description

The role can execute any existing scheduled payment. If the finance contract has no active fake payments then there is no impact. Also, the role can block the execution of payments for existing scheduled payments.

Owners

Owner type	**Aragon Voting**
Owner address	**0x2e59A20f205bB85a89C53f1936454680651E618e**
Attack complexity	**HIGH**

Attack scenario

The Finance contract must be the owner of TRANSFER_ROLE, and the Vault contract should have tokens on balance. This role is protected by the Aragon Voting Contract, so check the compromisation complexity for the Aragon Voting Contract.

Domain	DAO Aragon
Contract	Aragon Finance (Implementation)
Role name	MANAGE_PAYMENTS_ROLE
Auth type	aragon-acl
Role impact severity	HIGH
Attack complexity cumulative	HIGH

Role description

The role activates/disables any existing scheduled payment

Impact description

The role can block all existing scheduled payments. Also, the role can unblock existing scheduled payments that were blocked earlier for any reason.

Owners

Owner type	Aragon Voting
Owner address	0x2e59A20f205bB85a89C53f1936454680651E618e
Attack complexity	HIGH

Attack scenario

The Finance contract must be the owner of TRANSFER_ROLE, and the Vault contract should have tokens on balance. This role is protected by the Aragon Voting Contract, so check the compromisation complexity for the Aragon Voting Contract.

Domain	**DAO Aragon**
Contract	**Repo (Implementation)**
Role name	**CREATE_VERSION_ROLE**
Auth type	**aragon-acl**
Role impact severity	**NO IMPACT**
Attack complexity cumulative	**HIGH**

Role description

The role creates a new version with a contract and content

Impact description

The role can provide fake information about the version and contract address. The impact may depend on the use of the contract by an external system. No impacts, because Lido has already upgraded with **LidoTemplate**.

Owners

Owner type	**Aragon Voting**
Owner address	**0x2e59A20f205bB85a89C53f1936454680651E618e**
Attack complexity	**HIGH**

Attack scenario

This role is protected by the Aragon Voting contract and doesn't contain other significant conditions. Thus, the compromisation complexity is equivalent to a vote with a malicious script.

Domain	**DAO Aragon**
Contract	**Insurance Fund**
Role name	**Owner**
Auth type	**oz-ownable**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**HIGH**

Role description

Transfers ether, ERC20, ERC721, ERC1155 from this contract.

Impact description

The role can steal any native, ERC tokens from the contract.

Owners

Owner type	**Aragon Agent**
Owner address	**0xFE5986E06210aC1eCC1aDCafc0cc7f8D63B3F977**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**DAO Aragon**
Contract	**GateSeal**
Role name	**SEALING_COMMITTEE**
Auth type	**custom-acl-immutable**
Role impact severity	**HIGH**
Attack complexity cumulative	**MEDIUM**

Role description

The role pauses all sealable contracts.

Impact description

The role can temporarily block core contracts of the protocol. The currently deployed GateSeal 0x1ad5cb2955940f998081c1ef5f5f00875431aa90 contract can pause only for 6 days. However, based on the limitations of the source code future instances of GateSeal can be paused for 6–14 days after the current instance expires.

Owners

Owner type	**Multisig (Safe-Gnosis)**
Owner address	**0x8772E3a2D86B9347A2688f9bc1808A6d8917760C**
Attack complexity	**MEDIUM**

Attack scenario

Need to have signatures of txn hash for 3 owners out of 6. All owners are EOA, and 4 of them are historically active on-chain, causing a higher probability of receiving their signatures.

Domain	**DAO EasyTrack**
Contract	**EasyTrack**
Role name	**DEFAULT_ADMIN_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**HIGH**

Role description

The role is able to grant or revoke all roles. Sets the minimal time required (259200 seconds for the deployed instance) to pass before enacting of motion. Sets percent from total supply of governance tokens required to reject motion. Sets max count of active motions. Adds new EVMScript Factory to the list of allowed EVMScript factories. Sets new EVMScriptExecutor.

Impact description

The role can DoS motions, lose rewards, create fake payments, and possibly lose funds from AragonFinance, also interrupt Curated Staking Module work.

Owners

Owner type	**Aragon Voting**
Owner address	**0x2e59A20f205bB85a89C53f1936454680651E618e**
Attack complexity	**HIGH**

Attack scenario

This role is protected by the Aragon Voting Contract and doesn't contain any other significant conditions. Thus, the compromisation complexity is equivalent to acceptance of voting with malicious script.

Domain	**DAO EasyTrack**
Contract	**EasyTrack**
Role name	**PAUSE_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**MEDIUM**
Attack complexity cumulative	**MEDIUM**

Role description

The role pauses if it isn't paused. Paused functions: createMotion(), enactMotion()

Impact description

The role can DoS motions.

Owners

Owner type	**Multisig (Safe-Gnosis)**
Owner address	**0x73b047fe6337183A454c5217241D780a932777bD**
Attack complexity	**MEDIUM**

Attack scenario

Need to have signatures of txn hash for 3 owners out of 5. This multisig also pauses L2 bridges for Arbitrum/Optimism on Ethereum.

Domain	DAO EasyTrack
Contract	EasyTrack
Role name	UNPAUSE_ROLE
Auth type	oz-accesscontrol
Role impact severity	HIGH
Attack complexity cumulative	HIGH

Role description

The role unpauses if it is paused.

Impact description

The role can unpause the contract when it needs to be paused.

Owners

Owner type	Aragon Voting
Owner address	0x2e59A20f205bB85a89C53f1936454680651E618e
Attack complexity	HIGH

Attack scenario

This role is protected by the Aragon Voting Contract and doesn't contain any other significant conditions. Thus, the compromisation complexity is equivalent to acceptance of voting with malicious script.

Domain	**DAO EasyTrack**
Contract	**EasyTrack**
Role name	**CANCEL_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**MEDIUM**
Attack complexity cumulative	**HIGH**

Role description

The role cancels any motions.

Impact description

The role can DoS motions.

Owners

Owner type	**Aragon Voting**
Owner address	**0x2e59A20f205bB85a89C53f1936454680651E618e**
Attack complexity	**HIGH**

Attack scenario

This role is protected by the Aragon Voting Contract and doesn't contain any other significant conditions. Thus, the compromisation complexity is equivalent to acceptance of voting with malicious script.

Domain	DAO EasyTrack
Contract	EVMScriptExecutor
Role name	Owner
Auth type	oz-ownable
Role impact severity	CRITICAL
Attack complexity cumulative	HIGH

Role description

The role sets the EasyTrack role and manages the owner role.

Impact description

The role can set its own contract to Easy Track role. So, the role can run EVM scripts. An attacker can create different EVM scripts that allow calling functions protected by authorization. At the moment, the executor has many permissions, therefore, the potential impact is cumulative from all assigned roles.

Owners

Owner type	Aragon Voting
Owner address	0x2e59A20f205bB85a89C53f1936454680651E618e
Attack complexity	HIGH

Attack scenario

This role is protected by the Aragon Voting Contract and doesn't contain any other significant conditions. Thus, the compromisation complexity is equivalent to acceptance of voting with malicious script.

Domain	**DAO EasyTrack**
Contract	**EVMScriptExecutor**
Role name	**EasyTrack**
Auth type	**custom-acl**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**HIGH**

Role description

The role executes EVM scripts provided by Easy Track via delegate call Aragon's **CallsScript.sol** contract. CallScript use call for execution script.

Impact description

The role can run any EVM scripts. The main impact is the calls of contracts in which the **EVMExecutor** is the owner of the role. Stealing funds from **Insurance Fund** contract, executing a malicious payment in **Aragon Finance**, adding a malicious authorized user to the register, etc.

Owners

Owner type	**EasyTrack**
Owner address	**0xF0211b7660680B49De1A7E9f25C65660F0a13Fea**
Attack complexity	**HIGH**

Attack scenario

The role is managed by the owner of the **Owner** role. The compromisation complexity of this role is equivalent to compromising the **Owner** role, which is protected by the Aragon Voting. Thus, the compromisation complexity is equivalent to acceptance of voting with malicious script.

Domain	**DAO EasyTrack**
Contract	**reWARDS stETH:AllowedRecipientsRegistry**
Role name	**DEFAULT_ADMIN_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role grants or revokes all roles in **AllowedRecipientsRegistry**.

Impact description

The role has a cumulative impact on other roles in the contract.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**DAO EasyTrack**
Contract	**reWARDS stETH:AllowedRecipientsRegistry**
Role name	**SET_PARAMETERS_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role updates the spending total limit to any amount. Replaces **IBokkyPooBahsDateTimeContract** that makes conversion between date and timestamp. Updates current payout total amount without checks.

Impact description

The role can set an unlimited total amount. However, only fair registered recipients can get payouts. Also, unsafe increasing setting payment amount == total limit can block future payments.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	DAO EasyTrack
Contract	reWARDS stETH:AllowedRecipientsRegistry
Role name	UPDATE_SPENT_AMOUNT_ROLE
Auth type	oz-accesscontrol
Role impact severity	HIGH
Attack complexity cumulative	HIGH

Role description

The role checks the current payout total amount and total limits and updates the payout amount in the current period.

Impact description

The role can spend the payout amount in the current period without real spending and block any future proposal in this period.

Owners

Owner type	Aragon Agent
Owner address	0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c
Attack complexity	HIGH

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Owner type	EVMScriptExecutor
Owner address	0xFE5986E06210aC1eCC1aDCafc0cc7f8D63B3F977
Attack complexity	HIGH

Attack scenario

Aragon voting can be compromised in the following cases:

1. The undiscovered bug in the implementation of **EVMScriptExecutor** contract. However, EasyTrack contracts(including **EVMScriptExecutor**) successfully passed several audits and battle-tested in production, so the probability of this kind of bug can be considered low.
2. Accepts malicious proposals in EasyTrack.

Domain	**DAO EasyTrack**
Contract	**reWARDS stETH:AllowedRecipientsRegistry**
Role name	**ADD_RECIPIENT_TO_ALLOWED_LIST_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role adds a new recipient to a registry. So, EVM script builder contracts check a recipient when building EVM script. It excludes malicious recipients.

Impact description

The role can add a malicious recipient. So, the attacker can try to create and execute a proposal that transfers funds to a malicious recipient.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**DAO EasyTrack**
Contract	**reWARDS stETH:AllowedRecipientsRegistry**
Role name	**REMOVE_RECIPIENT_FROM_ALLOWED_LIST_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**MEDIUM**
Attack complexity cumulative	**HIGH**

Role description

The role removes an existing recipient from a registry. So, EVM script builder contracts fail to check if it is an unknown recipient.

Impact description

The role can remove a fair recipient and block creating a proposal via EasyTrack for payment to the recipient.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**DAO EasyTrack**
Contract	**Rewards Share stETH:AllowedRecipientsRegistry**
Role name	**DEFAULT_ADMIN_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role grants or revokes all roles in **AllowedRecipientsRegistry**.

Impact description

The role has a cumulative impact on other roles in the contract.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**DAO EasyTrack**
Contract	**Rewards Share stETH:AllowedRecipientsRegistry**
Role name	**SET_PARAMETERS_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role updates the spending total limit to any amount. Replaces **IBokkyPooBahsDateTimeContract**that makes conversion between date and timestamp. Updates current payout total amount without checks.

Impact description

The role can set an unlimited total amount. However, only fair registered recipients can get payouts. Also, unsafe increasing setting payment amount == total limit can block future payments.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	DAO EasyTrack
Contract	Rewards Share stETH:AllowedRecipientsRegistry
Role name	UPDATE_SPENT_AMOUNT_ROLE
Auth type	oz-accesscontrol
Role impact severity	HIGH
Attack complexity cumulative	HIGH

Role description

The role checks the current payout total amount and total limits and updates the payout amount in the current period.

Impact description

The role can spend the payout amount in the current period without real spending and block any future proposal in this period.

Owners

Owner type	Aragon Agent
Owner address	0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c
Attack complexity	HIGH

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Owner type	EVMScriptExecutor
Owner address	0xFE5986E06210aC1eCC1aDCafc0cc7f8D63B3F977
Attack complexity	HIGH

Attack scenario

Aragon voting can be compromised in the following cases:

1. The undiscovered bug in the implementation of **EVMScriptExecutor** contract. However, EasyTrack contracts(including **EVMScriptExecutor**) successfully passed several audits and battle-tested in production, so the probability of this kind of bug can be considered low.
2. Accepts malicious proposals in EasyTrack.

Domain	**DAO EasyTrack**
Contract	**Rewards Share stETH:AllowedRecipientsRegistry**
Role name	**ADD_RECIPIENT_TO_ALLOWED_LIST_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role adds a new recipient to a registry. So, EVM script builder contracts check a recipient when building EVM script. It excludes malicious recipients.

Impact description

The role can add a malicious recipient. So, the attacker can try to create and execute a proposal that transfers funds to a malicious recipient.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**DAO EasyTrack**
Contract	**Rewards Share stETH:AllowedRecipientsRegistry**
Role name	**REMOVE_RECIPIENT_FROM_ALLOWED_LIST_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**MEDIUM**
Attack complexity cumulative	**HIGH**

Role description

The role removes an existing recipient from a registry. So, EVM script builder contracts fail to check if it is an unknown recipient.

Impact description

The role can remove a fair recipient and block creating a proposal via EasyTrack for payment to the recipient.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**DAO EasyTrack**
Contract	**TRP LDO:AllowedRecipientsRegistry**
Role name	**DEFAULT_ADMIN_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role grants or revokes all roles in **AllowedRecipientsRegistry**.

Impact description

The role has a cumulative impact on other roles in the contract.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**DAO EasyTrack**
Contract	**TRP LDO:AllowedRecipientsRegistry**
Role name	**SET_PARAMETERS_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role updates the spending total limit to any amount. Replaces **IBokkyPooBahsDateTimeContract**that makes conversion between date and timestamp. Updates current payout total amount without checks.

Impact description

The role can set an unlimited total amount. However, only fair registered recipients can get payouts. Also, unsafe increasing setting payment amount == total limit can block future payments.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**DAO EasyTrack**
Contract	**TRP LDO:AllowedRecipientsRegistry**
Role name	**UPDATE_SPENT_AMOUNT_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role checks the current payout total amount and total limits and updates the payout amount in the current period.

Impact description

The role can spend the payout amount in the current period without real spending and block any future proposal in this period.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Owner type	**EVMScriptExecutor**
Owner address	**0xFE5986E06210aC1eCC1aDCafc0cc7f8D63B3F977**
Attack complexity	**HIGH**

Attack scenario

Aragon voting can be compromised in the following cases:

1. The undiscovered bug in the implementation of **EVMScriptExecutor** contract. However, EasyTrack contracts(including **EVMScriptExecutor**) successfully passed several audits and battle-tested in production, so the probability of this kind of bug can be considered low.
2. Accepts malicious proposals in EasyTrack.

Domain	**DAO EasyTrack**
Contract	**TRP LDO:AllowedRecipientsRegistry**
Role name	**ADD_RECIPIENT_TO_ALLOWED_LIST_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role adds a new recipient to a registry. So, EVM script builder contracts check a recipient when building EVM script. It excludes malicious recipients.

Impact description

The role can add a malicious recipient. So, the attacker can try to create and execute a proposal that transfers funds to a malicious recipient.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**DAO EasyTrack**
Contract	**TRP LDO:AllowedRecipientsRegistry**
Role name	**REMOVE_RECIPIENT_FROM_ALLOWED_LIST_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**MEDIUM**
Attack complexity cumulative	**HIGH**

Role description

The role removes an existing recipient from a registry. So, EVM script builder contracts fail to check if it is an unknown recipient.

Impact description

The role can remove a fair recipient and block creating a proposal via EasyTrack for payment to the recipient.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**DAO EasyTrack**
Contract	**ATC DAI:AllowedRecipientsRegistry**
Role name	**DEFAULT_ADMIN_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role grants or revokes all roles in **AllowedRecipientsRegistry**.

Impact description

The role has a cumulative impact on other roles in the contract.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**DAO EasyTrack**
Contract	**ATC DAI:AllowedRecipientsRegistry**
Role name	**SET_PARAMETERS_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role updates the spending total limit to any amount. Replaces **IBokkyPooBahsDateTimeContract**that makes conversion between date and timestamp. Updates current payout total amount without checks.

Impact description

The role can set an unlimited total amount. However, only fair registered recipients can get payouts. Also, unsafe increasing setting payment amount == total limit can block future payments.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**DAO EasyTrack**
Contract	**ATC DAI:AllowedRecipientsRegistry**
Role name	**UPDATE_SPENT_AMOUNT_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role checks the current payout total amount and total limits and updates the payout amount in the current period.

Impact description

The role can spend the payout amount in the current period without real spending and block any future proposal in this period.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Owner type	**EVMScriptExecutor**
Owner address	**0xFE5986E06210aC1eCC1aDCafc0cc7f8D63B3F977**
Attack complexity	**HIGH**

Attack scenario

Aragon voting can be compromised in the following cases:

1. The undiscovered bug in the implementation of **EVMScriptExecutor** contract. However, EasyTrack contracts(including **EVMScriptExecutor**) successfully passed several audits and battle-tested in production, so the probability of this kind of bug can be considered low.
2. Accepts malicious proposals in EasyTrack.

Domain	**DAO EasyTrack**
Contract	**ATC DAI:AllowedRecipientsRegistry**
Role name	**ADD_RECIPIENT_TO_ALLOWED_LIST_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role adds a new recipient to a registry. So, EVM script builder contracts check a recipient when building EVM script. It excludes malicious recipients.

Impact description

The role can add a malicious recipient. So, the attacker can try to create and execute a proposal that transfers funds to a malicious recipient.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**DAO EasyTrack**
Contract	**ATC DAI:AllowedRecipientsRegistry**
Role name	**REMOVE_RECIPIENT_FROM_ALLOWED_LIST_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**MEDIUM**
Attack complexity cumulative	**HIGH**

Role description

The role removes an existing recipient from a registry. So, EVM script builder contracts fail to check if it is an unknown recipient.

Impact description

The role can remove a fair recipient and block creating a proposal via EasyTrack for payment to the recipient.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**DAO EasyTrack**
Contract	**LEGO LDO:AllowedRecipientsRegistry**
Role name	**DEFAULT_ADMIN_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role grants or revokes all roles in **AllowedRecipientsRegistry**.

Impact description

The role has a cumulative impact on other roles in the contract.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**DAO EasyTrack**
Contract	**LEGO LDO:AllowedRecipientsRegistry**
Role name	**SET_PARAMETERS_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role updates the spending total limit to any amount. Replaces **IBokkyPooBahsDateTimeContract**that makes conversion between date and timestamp. Updates current payout total amount without checks.

Impact description

The role can set an unlimited total amount. However, only fair registered recipients can get payouts. Also, unsafe increasing setting payment amount == total limit can block future payments.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**DAO EasyTrack**
Contract	**LEGO LDO:AllowedRecipientsRegistry**
Role name	**UPDATE_SPENT_AMOUNT_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role checks the current payout total amount and total limits and updates the payout amount in the current period.

Impact description

The role can spend the payout amount in the current period without real spending and block any future proposal in this period.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Owner type	**EVMScriptExecutor**
Owner address	**0xFE5986E06210aC1eCC1aDCafc0cc7f8D63B3F977**
Attack complexity	**HIGH**

Attack scenario

Aragon voting can be compromised in the following cases:

1. The undiscovered bug in the implementation of **EVMScriptExecutor** contract. However, EasyTrack contracts(including **EVMScriptExecutor**) successfully passed several audits and battle-tested in production, so the probability of this kind of bug can be considered low.
2. Accepts malicious proposals in EasyTrack.

Domain	**DAO EasyTrack**
Contract	**LEGO LDO:AllowedRecipientsRegistry**
Role name	**ADD_RECIPIENT_TO_ALLOWED_LIST_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role adds a new recipient to a registry. So, EVM script builder contracts check a recipient when building EVM script. It excludes malicious recipients.

Impact description

The role can add a malicious recipient. So, the attacker can try to create and execute a proposal that transfers funds to a malicious recipient.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**DAO EasyTrack**
Contract	**LEGO LDO:AllowedRecipientsRegistry**
Role name	**REMOVE_RECIPIENT_FROM_ALLOWED_LIST_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**MEDIUM**
Attack complexity cumulative	**HIGH**

Role description

The role removes an existing recipient from a registry. So, EVM script builder contracts fail to check if it is an unknown recipient.

Impact description

The role can remove a fair recipient and block creating a proposal via EasyTrack for payment to the recipient.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**DAO EasyTrack**
Contract	**LEGO DAI:AllowedRecipientsRegistry**
Role name	**DEFAULT_ADMIN_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role grants or revokes all roles in **AllowedRecipientsRegistry**.

Impact description

The role has a cumulative impact on other roles in the contract.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**DAO EasyTrack**
Contract	**LEGO DAI:AllowedRecipientsRegistry**
Role name	**SET_PARAMETERS_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role updates the spending total limit to any amount. Replaces **IBokkyPooBahsDateTimeContract** that makes conversion between date and timestamp. Updates current payout total amount without checks.

Impact description

The role can set an unlimited total amount. However, only fair registered recipients can get payouts. Also, unsafe increasing setting payment amount == total limit can block future payments.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	DAO EasyTrack
Contract	LEGO DAI:AllowedRecipientsRegistry
Role name	UPDATE_SPENT_AMOUNT_ROLE
Auth type	oz-accesscontrol
Role impact severity	HIGH
Attack complexity cumulative	HIGH

Role description

The role checks the current payout total amount and total limits and updates the payout amount in the current period.

Impact description

The role can spend the payout amount in the current period without real spending and block any future proposal in this period.

Owners

Owner type	Aragon Agent
Owner address	0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c
Attack complexity	HIGH

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Owner type	EVMScriptExecutor
Owner address	0xFE5986E06210aC1eCC1aDCafc0cc7f8D63B3F977
Attack complexity	HIGH

Attack scenario

Aragon voting can be compromised in the following cases:

1. The undiscovered bug in the implementation of **EVMScriptExecutor** contract. However, EasyTrack contracts(including **EVMScriptExecutor**) successfully passed several audits and battle-tested in production, so the probability of this kind of bug can be considered low.
2. Accepts malicious proposals in EasyTrack.

Domain	**DAO EasyTrack**
Contract	**LEGO DAI:AllowedRecipientsRegistry**
Role name	**ADD_RECIPIENT_TO_ALLOWED_LIST_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role adds a new recipient to a registry. So, EVM script builder contracts check a recipient when building EVM script. It excludes malicious recipients.

Impact description

The role can add a malicious recipient. So, the attacker can try to create and execute a proposal that transfers funds to a malicious recipient.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**DAO EasyTrack**
Contract	**LEGO DAI:AllowedRecipientsRegistry**
Role name	**REMOVE_RECIPIENT_FROM_ALLOWED_LIST_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**MEDIUM**
Attack complexity cumulative	**HIGH**

Role description

The role removes an existing recipient from a registry. So, EVM script builder contracts fail to check if it is an unknown recipient.

Impact description

The role can remove a fair recipient and block creating a proposal via EasyTrack for payment to the recipient.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**DAO EasyTrack**
Contract	**RCC DAI:AllowedRecipientsRegistry**
Role name	**DEFAULT_ADMIN_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role grants or revokes all roles in **AllowedRecipientsRegistry**.

Impact description

The role has a cumulative impact on other roles in the contract.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**DAO EasyTrack**
Contract	**RCC DAI:AllowedRecipientsRegistry**
Role name	**SET_PARAMETERS_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role updates the spending total limit to any amount. Replaces **IBokkyPooBahsDateTimeContract**that makes conversion between date and timestamp. Updates current payout total amount without checks.

Impact description

The role can set an unlimited total amount. However, only fair registered recipients can get payouts. Also, unsafe increasing setting payment amount == total limit can block future payments.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**DAO EasyTrack**
Contract	**RCC DAI:AllowedRecipientsRegistry**
Role name	**UPDATE_SPENT_AMOUNT_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role checks the current payout total amount and total limits and updates the payout amount in the current period.

Impact description

The role can spend the payout amount in the current period without real spending and block any future proposal in this period.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Owner type	**EVMScriptExecutor**
Owner address	**0xFE5986E06210aC1eCC1aDCafc0cc7f8D63B3F977**
Attack complexity	**HIGH**

Attack scenario

Aragon voting can be compromised in the following cases:

1. The undiscovered bug in the implementation of **EVMScriptExecutor** contract. However, EasyTrack contracts(including **EVMScriptExecutor**) successfully passed several audits and battle-tested in production, so the probability of this kind of bug can be considered low.
2. Accepts malicious proposals in EasyTrack.

Domain	**DAO EasyTrack**
Contract	**RCC DAI:AllowedRecipientsRegistry**
Role name	**ADD_RECIPIENT_TO_ALLOWED_LIST_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role adds a new recipient to a registry. So, EVM script builder contracts check a recipient when building EVM script. It excludes malicious recipients.

Impact description

The role can add a malicious recipient. So, the attacker can try to create and execute a proposal that transfers funds to a malicious recipient.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**DAO EasyTrack**
Contract	**RCC DAI:AllowedRecipientsRegistry**
Role name	**REMOVE_RECIPIENT_FROM_ALLOWED_LIST_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**MEDIUM**
Attack complexity cumulative	**HIGH**

Role description

The role removes an existing recipient from a registry. So, EVM script builder contracts fail to check if it is an unknown recipient.

Impact description

The role can remove a fair recipient and block creating a proposal via EasyTrack for payment to the recipient.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**DAO EasyTrack**
Contract	**PML DAI:AllowedRecipientsRegistry**
Role name	**DEFAULT_ADMIN_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role grants or revokes all roles in **AllowedRecipientsRegistry**.

Impact description

The role has a cumulative impact on other roles in the contract.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**DAO EasyTrack**
Contract	**PML DAI:AllowedRecipientsRegistry**
Role name	**SET_PARAMETERS_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role updates the spending total limit to any amount. Replaces **IBokkyPooBahsDateTimeContract**that makes conversion between date and timestamp. Updates current payout total amount without checks.

Impact description

The role can set an unlimited total amount. However, only fair registered recipients can get payouts. Also, unsafe increasing setting payment amount == total limit can block future payments.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**DAO EasyTrack**
Contract	**PML DAI:AllowedRecipientsRegistry**
Role name	**UPDATE_SPENT_AMOUNT_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role checks the current payout total amount and total limits and updates the payout amount in the current period.

Impact description

The role can spend the payout amount in the current period without real spending and block any future proposal in this period.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Owner type	**EVMScriptExecutor**
Owner address	**0xFE5986E06210aC1eCC1aDCafc0cc7f8D63B3F977**
Attack complexity	**HIGH**

Attack scenario

Aragon voting can be compromised in the following cases:

1. The undiscovered bug in the implementation of **EVMScriptExecutor** contract. However, EasyTrack contracts(including **EVMScriptExecutor**) successfully passed several audits and battle-tested in production, so the probability of this kind of bug can be considered low.
2. Accepts malicious proposals in EasyTrack.

Domain	**DAO EasyTrack**
Contract	**PML DAI:AllowedRecipientsRegistry**
Role name	**ADD_RECIPIENT_TO_ALLOWED_LIST_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role adds a new recipient to a registry. So, EVM script builder contracts check a recipient when building EVM script. It excludes malicious recipients.

Impact description

The role can add a malicious recipient. So, the attacker can try to create and execute a proposal that transfers funds to a malicious recipient.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**DAO EasyTrack**
Contract	**PML DAI:AllowedRecipientsRegistry**
Role name	**REMOVE_RECIPIENT_FROM_ALLOWED_LIST_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**MEDIUM**
Attack complexity cumulative	**HIGH**

Role description

The role removes an existing recipient from a registry. So, EVM script builder contracts fail to check if it is an unknown recipient.

Impact description

The role can remove a fair recipient and block creating a proposal via EasyTrack for payment to the recipient.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**DAO EasyTrack**
Contract	**Gas Supply stETH:AllowedRecipientsRegistry**
Role name	**DEFAULT_ADMIN_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role grants or revokes all roles in **AllowedRecipientsRegistry**.

Impact description

The role has a cumulative impact on other roles in the contract.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**DAO EasyTrack**
Contract	**Gas Supply stETH:AllowedRecipientsRegistry**
Role name	**SET_PARAMETERS_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role updates the spending total limit to any amount. Replaces **IBokkyPooBahsDateTimeContract**that makes conversion between date and timestamp. Updates current payout total amount without checks.

Impact description

The role can set an unlimited total amount. However, only fair registered recipients can get payouts. Also, unsafe increasing setting payment amount == total limit can block future payments.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	DAO EasyTrack
Contract	Gas Supply stETH:AllowedRecipientsRegistry
Role name	UPDATE_SPENT_AMOUNT_ROLE
Auth type	oz-accesscontrol
Role impact severity	HIGH
Attack complexity cumulative	HIGH

Role description

The role checks the current payout total amount and total limits and updates the payout amount in the current period.

Impact description

The role can spend the payout amount in the current period without real spending and block any future proposal in this period.

Owners

Owner type	Aragon Agent
Owner address	0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c
Attack complexity	HIGH

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Owner type	EVMScriptExecutor
Owner address	0xFE5986E06210aC1eCC1aDCafc0cc7f8D63B3F977
Attack complexity	HIGH

Attack scenario

Aragon voting can be compromised in the following cases:

1. The undiscovered bug in the implementation of **EVMScriptExecutor** contract. However, EasyTrack contracts(including **EVMScriptExecutor**) successfully passed several audits and battle-tested in production, so the probability of this kind of bug can be considered low.
2. Accepts malicious proposals in EasyTrack.

Domain	**DAO EasyTrack**
Contract	**Gas Supply stETH:AllowedRecipientsRegistry**
Role name	**ADD_RECIPIENT_TO_ALLOWED_LIST_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**HIGH**
Attack complexity cumulative	**HIGH**

Role description

The role adds a new recipient to a registry. So, EVM script builder contracts check a recipient when building EVM script. It excludes malicious recipients.

Impact description

The role can add a malicious recipient. So, the attacker can try to create and execute a proposal that transfers funds to a malicious recipient.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Owner type	**EVMScriptExecutor**
Owner address	**0xFE5986E06210aC1eCC1aDCafc0cc7f8D63B3F977**
Attack complexity	**HIGH**

Attack scenario

Aragon voting can be compromised in the following cases:

1. **The undiscovered bug in the implementation of EVMScriptExecutor contract. However, EasyTrack contracts(including EVMScriptExecutor) successfully passed several audits and battle-tested in production, so the probability of this kind of bug can be considered low.**
2. **Accepts malicious proposals in EasyTrack.**

Domain	**DAO EasyTrack**
Contract	**Gas Supply stETH:AllowedRecipientsRegistry**
Role name	**REMOVE_RECIPIENT_FROM_ALLOWED_LIST_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**MEDIUM**
Attack complexity cumulative	**HIGH**

Role description

The role removes an existing recipient from a registry. So, EVM script builder contracts fail to check if it is an unknown recipient.

Impact description

The role can remove a fair recipient and block creating a proposal via EasyTrack for payment to the recipient.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Owner type	**EVMScriptExecutor**
Owner address	**0xFE5986E06210aC1eCC1aDCafc0cc7f8D63B3F977**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**DAO EasyTrack**
Contract	**LEGO DAI:TopUpAllowedRecipients**
Role name	**Trusted Caller**
Auth type	**custom-acl-immutable**
Role impact severity	**MEDIUM**
Attack complexity cumulative	**MEDIUM**

Role description

The role creates EVMScript to top up allowed recipients' addresses. The created script can transfer only **DAI** token, the total amount of transfer is limited for each period, and is stored in **AllowedRecipientsRegistry**.

Impact description

The contract has a stateless architecture and allows **TrustedCaller** to create a script that has no impact without Easy Track. Therefore, it is necessary to consider factory contracts in combination with Easy Track. **TrustedCaller** can create a malicious script, but the script can send **DAI** only to allowed addresses within the period limit. Also, malicious motion can be rejected by an objection, and the factory is excluded by voting using Aragon DAO.

Owners

Owner type	**Multisig (Safe-Gnosis)**
Owner address	**0x12a43b049A7D330cB8aEAB5113032D18AE9a9030**
Attack complexity	**MEDIUM**

Attack scenario

Need to have signatures of txn hash for 4 owners out of 8. All owners are EOA, and 3 of them are historically active on-chain, causing a higher probability of receiving their signatures.

Domain	**DAO EasyTrack**
Contract	**ATC DAI:TopUpAllowedRecipients**
Role name	**Trusted Caller**
Auth type	**custom-acl-immutable**
Role impact severity	**MEDIUM**
Attack complexity cumulative	**MEDIUM**

Role description

The role creates EVMScript to top up allowed recipients' addresses. The created script can transfer only **DAI** token, the total amount of transfer is limited for each period, and is stored in **AllowedRecipientsRegistry**.

Impact description

The contract has a stateless architecture and allows **TrustedCaller** to create a script that has no impact without Easy Track. Therefore, it is necessary to consider factory contracts in combination with Easy Track. **TrustedCaller** can create a malicious script, but the script can send **DAI** only to allowed addresses within the period limit. Also, malicious motion can be rejected by an objection, and the factory is excluded by voting using Aragon DAO.

Owners

Owner type	**Multisig (Safe-Gnosis)**
Owner address	**0x9B1cebF7616f2BC73b47D226f90b01a7c9F86956**
Attack complexity	**MEDIUM**

Attack scenario

Need to have signatures of txn hash for 4 owners out of 6. All owners are EOA, and 2 of them are historically active on-chain, causing a higher probability of receiving their signatures.

Domain	**DAO EasyTrack**
Contract	**TRP LDO:TopUpAllowedRecipients**
Role name	**Trusted Caller**
Auth type	**custom-acl-immutable**
Role impact severity	**MEDIUM**
Attack complexity cumulative	**MEDIUM**

Role description

The role creates EVMScript to top up allowed recipients' addresses. The created script can transfer only LDO token, the total amount of transfer is limited for each period, and is stored in AllowedRecipientsRegistry.

Impact description

The contract has a stateless architecture and allows TrustedCaller to create a script that has no impact without Easy Track. Therefore, it is necessary to consider factory contracts in combination with Easy Track. TrustedCaller can create a malicious script, but the script can send LDO only to allowed addresses within the period limit. Also, malicious motion can be rejected by an objection, and the factory is excluded by voting using Aragon DAO.

Owners

Owner type	**Multisig (Safe-Gnosis)**
Owner address	**0x834560F580764Bc2e0B16925F8bF229bb00cB759**
Attack complexity	**MEDIUM**

Attack scenario

Need to have signatures of txn hash for 4 owners out of 7.

Domain	**DAO EasyTrack**
Contract	**LEGO LDO:TopUpAllowedRecipients**
Role name	**Trusted Caller**
Auth type	**custom-acl-immutable**
Role impact severity	**MEDIUM**
Attack complexity cumulative	**MEDIUM**

Role description

The role creates EVMScript to top up allowed recipients' addresses. The created script can transfer only LDO token, the total amount of transfer is limited for each period, and is stored in AllowedRecipientsRegistry.

Impact description

The contract has a stateless architecture and allows TrustedCaller to create a script that has no impact without Easy Track. Therefore, it is necessary to consider factory contracts in combination with Easy Track. TrustedCaller can create a malicious script, but the script can send LDO only to allowed addresses within the period limit. Also, malicious motion can be rejected by an objection, and the factory is excluded by voting using Aragon DAO.

Owners

Owner type	**Multisig (Safe-Gnosis)**
Owner address	**0x12a43b049A7D330cB8aEAB5113032D18AE9a9030**
Attack complexity	**MEDIUM**

Attack scenario

Need to have signatures of txn hash for 4 owners out of 8. All owners are EOA, 3 of them are historically active on-chain, causing higher probability of receiving their signatures.

Domain	**DAO EasyTrack**
Contract	**RCC DAI:TopUpAllowedRecipients**
Role name	**Trusted Caller**
Auth type	**custom-acl-immutable**
Role impact severity	**MEDIUM**
Attack complexity cumulative	**MEDIUM**

Role description

The role creates EVMScript to top up allowed recipients' addresses. The created script can transfer only **DAI** token, the total amount of transfer is limited for each period, and is stored in **AllowedRecipientsRegistry**.

Impact description

The contract has a stateless architecture and allows **TrustedCaller** to create a script that has no impact without Easy Track. Therefore, it is necessary to consider factory contracts in combination with Easy Track. **TrustedCaller** can create a malicious script, but the script can send **DAI** only to allowed addresses within the period limit. Also, malicious motion can be rejected by an objection, and the factory is excluded by voting using Aragon DAO.

Owners

Owner type	**Multisig (Safe-Gnosis)**
Owner address	**0xDE06d17Db9295Fa8c4082D4f73Ff81592A3aC437**
Attack complexity	**MEDIUM**

Attack scenario

Need to have signatures of txn hash for 4 owners out of 7. All owners are EOA, 1 of them is historically active on-chain, causing higher probability of receiving their signatures.

Domain	**DAO EasyTrack**
Contract	**PML DAI:TopUpAllowedRecipients**
Role name	**Trusted Caller**
Auth type	**custom-acl-immutable**
Role impact severity	**MEDIUM**
Attack complexity cumulative	**MEDIUM**

Role description

The role creates EVMScript to top up allowed recipients' addresses. The created script can transfer only **DAI** token, the total amount of transfer is limited for each period, and is stored in **AllowedRecipientsRegistry**.

Impact description

The contract has a stateless architecture and allows **TrustedCaller** to create a script that has no impact without Easy Track. Therefore, it is necessary to consider factory contracts in combination with Easy Track. **TrustedCaller** can create a malicious script, but the script can send **DAI** only to allowed addresses within the period limit. Also, malicious motion can be rejected by an objection, and the factory is excluded by voting using Aragon DAO.

Owners

Owner type	**Multisig (Safe-Gnosis)**
Owner address	**0x17F6b2C738a63a8D3A113a228cfd0b373244633D**
Attack complexity	**MEDIUM**

Attack scenario

Need to have signatures of txn hash for 4 owners out of 7. All owners are EOA, 1 of them is historically active on-chain, causing a higher probability of receiving their signatures.

Domain	**DAO EasyTrack**
Contract	**Gas Supply stETH:TopUpAllowedRecipients**
Role name	**Trusted Caller**
Auth type	**custom-acl-immutable**
Role impact severity	**MEDIUM**
Attack complexity cumulative	**MEDIUM**

Role description

The role creates EVMScript to top up allowed recipients' addresses. The created script can transfer only **stETH** token, the total amount of transfer is limited for each period, and is stored in **AllowedRecipientsRegistry**.

Impact description

The contract has a stateless architecture and allows **TrustedCaller** to create a script that has no impact without Easy Track. Therefore, it is necessary to consider factory contracts in combination with Easy Track. **TrustedCaller** can create a malicious script, but the script can send **stETH** only to allowed addresses within the period limit. Also, malicious motion can be rejected by an objection, and the factory is excluded by voting using Aragon DAO.

Owners

Owner type	**Multisig (Safe-Gnosis)**
Owner address	**0x5181d5D56Af4f823b96FE05f062D7a09761a5a53**
Attack complexity	**MEDIUM**

Attack scenario

Need to have signatures of txn hash for 3 owners out of 5.

Domain	**DAO EasyTrack**
Contract	**reWARDS stETH:TopUpAllowedRecipients**
Role name	**Trusted Caller**
Auth type	**custom-acl-immutable**
Role impact severity	**MEDIUM**
Attack complexity cumulative	**MEDIUM**

Role description

The role creates EVMScript to top up allowed recipients' addresses. The created script can transfer only **stETH** token, the total amount of transfer is limited for each period, and is stored in **AllowedRecipientsRegistry**.

Impact description

The contract has a stateless architecture and allows **TrustedCaller** to create a script that has no impact without Easy Track. Therefore, it is necessary to consider factory contracts in combination with Easy Track. **TrustedCaller** can create a malicious script, but the script can send **stETH** only to allowed addresses within the period limit. Also, malicious motion can be rejected by an objection, and the factory is excluded by voting using Aragon DAO.

Owners

Owner type	**Multisig (Safe-Gnosis)**
Owner address	**0x87D93d9B2C672bf9c9642d853a8682546a5012B5**
Attack complexity	**MEDIUM**

Attack scenario

Need to have signatures of txn hash for 4 owners out of 8.

Domain	**DAO EasyTrack**
Contract	**Rewards Share stETH:TopUpAllowedRecipients**
Role name	**Trusted Caller**
Auth type	**custom-acl-immutable**
Role impact severity	**MEDIUM**
Attack complexity cumulative	**MEDIUM**

Role description

The role creates EVMScript to top up allowed recipients' addresses. The created script can transfer only **stETH** token, the total amount of transfer is limited for each period, and is stored in **AllowedRecipientsRegistry**.

Impact description

The contract has a stateless architecture and allows **TrustedCaller** to create a script that has no impact without Easy Track. Therefore, it is necessary to consider factory contracts in combination with Easy Track. **TrustedCaller** can create a malicious script, but the script can send **stETH** only to allowed addresses within the period limit. Also, malicious motion can be rejected by an objection, and the factory is excluded by voting using Aragon DAO.

Owners

Owner type	**Multisig (Safe-Gnosis)**
Owner address	**0xe2A682A9722354D825d1BbDF372cC86B2ea82c8C**
Attack complexity	**MEDIUM**

Attack scenario

Need to have signatures of txn hash for 4 owners out of 7.

Domain	**DAO EasyTrack**
Contract	**reWARDS stETH:AddAllowedRecipient**
Role name	**Trusted Caller**
Auth type	**custom-acl-immutable**
Role impact severity	**LOW**
Attack complexity cumulative	**MEDIUM**

Role description

The role creates EVMScript to add a new allowed recipient address to **AllowedRecipientsRegistry** contract.

Impact description

The contract has a stateless architecture and allows **TrustedCaller** to create a script that has no impact without Easy Track. Therefore, it is necessary to consider factory contracts in combination with Easy Track. **TrustedCaller** can create a malicious script, that can add the attacker's address to the allowed list, but this does not lead to a loss of funds, because the attacker needs to execute another malicious script to transfer funds to the added address. Also, malicious motion can be rejected by an objection, and the factory is excluded by voting using Aragon DAO.

Owners

Owner type	**Multisig (Safe-Gnosis)**
Owner address	**0x87D93d9B2C672bf9c9642d853a8682546a5012B5**
Attack complexity	**MEDIUM**

Attack scenario

Need to have signatures of txn hash for 4 owners out of 8.

Domain	**DAO EasyTrack**
Contract	**Rewards Share stETH:AddAllowedRecipient**
Role name	**Trusted Caller**
Auth type	**custom-acl-immutable**
Role impact severity	**LOW**
Attack complexity cumulative	**MEDIUM**

Role description

The role creates EVMScript to add a new allowed recipient address to **AllowedRecipientsRegistry** contract.

Impact description

The contract has a stateless architecture and allows **TrustedCaller** to create a script that has no impact without Easy Track. Therefore, it is necessary to consider factory contracts in combination with Easy Track. **TrustedCaller** can create a malicious script, that can add the attacker's address to the allowed list, but this does not lead to a loss of funds, because the attacker needs to execute another malicious script to transfer funds to the added address. Also, malicious motion can be rejected by an objection, and the factory is excluded by voting using Aragon DAO.

Owners

Owner type	**Multisig (Safe-Gnosis)**
Owner address	**0xe2A682A9722354D825d1BbDF372cC86B2ea82c8C**
Attack complexity	**MEDIUM**

Attack scenario

Need to have signatures of txn hash for 4 owners out of 7.

Domain	**DAO EasyTrack**
Contract	**Gas Supply stETH:AddAllowedRecipient**
Role name	**Trusted Caller**
Auth type	**custom-acl-immutable**
Role impact severity	**LOW**
Attack complexity cumulative	**MEDIUM**

Role description

The role creates EVMScript to add a new allowed recipient address to **AllowedRecipientsRegistry** contract.

Impact description

The contract has a stateless architecture and allows **TrustedCaller** to create a script that has no impact without Easy Track. Therefore, it is necessary to consider factory contracts in combination with Easy Track. **TrustedCaller** can create a malicious script, that can add the attacker's address to the allowed list, but this does not lead to a loss of funds, because the attacker needs to execute another malicious script to transfer funds to the added address. Also, malicious motion can be rejected by an objection, and the factory is excluded by voting using Aragon DAO.

Owners

Owner type	**Multisig (Safe-Gnosis)**
Owner address	**0x5181d5D56Af4f823b96FE05f062D7a09761a5a53**
Attack complexity	**MEDIUM**

Attack scenario

Need to have signatures of txn hash for 3 owners out of 5.

Domain	**DAO EasyTrack**
Contract	**reWARDS stETH:RemoveAllowedRecipient**
Role name	**Trusted Caller**
Auth type	**custom-acl-immutable**
Role impact severity	**LOW**
Attack complexity cumulative	**MEDIUM**

Role description

The role creates EVMScript to remove the allowed recipient address from **AllowedRecipientsRegistry** contract.

Impact description

The contract has a stateless architecture and allows **TrustedCaller** to create a script that has no impact without Easy Track. Therefore, it is necessary to consider factory contracts in combination with Easy Track. **TrustedCaller** can create a malicious script, that can remove allowed recipient from list, but malicious motion can be rejected by an objection, and the factory is excluded by voting using Aragon DAO.

Owners

Owner type	**Multisig (Safe-Gnosis)**
Owner address	**0x87D93d9B2C672bf9c9642d853a8682546a5012B5**
Attack complexity	**MEDIUM**

Attack scenario

Need to have signatures of txn hash for 4 owners out of 8.

Domain	**DAO EasyTrack**
Contract	**Rewards Share stETH:RemoveAllowedRecipient**
Role name	**Trusted Caller**
Auth type	**custom-acl-immutable**
Role impact severity	**LOW**
Attack complexity cumulative	**MEDIUM**

Role description

The role creates EVMScript to remove the allowed recipient address from **AllowedRecipientsRegistry** contract.

Impact description

The contract has a stateless architecture and allows **TrustedCaller** to create a script that has no impact without Easy Track. Therefore, it is necessary to consider factory contracts in combination with Easy Track. **TrustedCaller** can create a malicious script, that can remove allowed recipient from list, but malicious motion can be rejected by an objection, and the factory is excluded by voting using Aragon DAO.

Owners

Owner type	**Multisig (Safe-Gnosis)**
Owner address	**0xe2A682A9722354D825d1BbDF372cC86B2ea82c8C**
Attack complexity	**MEDIUM**

Attack scenario

Need to have signatures of txn hash for 4 owners out of 7.

Domain	**DAO EasyTrack**
Contract	**Gas Supply stETH:RemoveAllowedRecipient**
Role name	**Trusted Caller**
Auth type	**custom-acl-immutable**
Role impact severity	**LOW**
Attack complexity cumulative	**MEDIUM**

Role description

The role creates EVMScript to remove the allowed recipient address from **AllowedRecipientsRegistry** contract.

Impact description

The contract has a stateless architecture and allows **TrustedCaller** to create a script that has no impact without Easy Track. Therefore, it is necessary to consider factory contracts in combination with Easy Track. **TrustedCaller** can create a malicious script, that can remove allowed recipient from list, but malicious motion can be rejected by an objection, and the factory is excluded by voting using Aragon DAO.

Owners

Owner type	**Multisig (Safe-Gnosis)**
Owner address	**0x5181d5D56Af4f823b96FE05f062D7a09761a5a53**
Attack complexity	**MEDIUM**

Attack scenario

Need to have signatures of txn hash for 3 owners out of 5.

Domain	**L2 Gateway**
Contract	**Arbitrum:L1ERC20TokenGateway (Proxy)**
Role name	**ADMIN**
Auth type	**custom-acl-over-oz-erc1967proxy**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**HIGH**

Role description

The role changes implementation, changes/resets ADMIN role owner.

Impact description

The role can upgrade contracts and break the connection between chains and steal the locked tokens.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**L2 Gateway**
Contract	**Arbitrum:L1ERC20TokenGateway (Implementation)**
Role name	**DEFAULT_ADMIN_ROLE**
Auth type	**custom-acl-oz-fork**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**HIGH**

Role description

The role is able to grant or revoke all roles.

Impact description

The role has a cumulative impact on all the roles of this contract. The worst case: the contract can accumulate the wstETH and stETH, while the claiming cannot be executed.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**L2 Gateway**
Contract	**Arbitrum:L1ERC20TokenGateway (Implementation)**
Role name	**DEPOSITS_ENABLER_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**HIGH**

Role description

The role unpauses token transfers L1 -> L2.

Impact description

The role can unblock forward bridging when not needed.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	L2 Gateway
Contract	Arbitrum:L1ERC20TokenGateway (Implementation)
Role name	DEPOSITS_DISABLER_ROLE
Auth type	oz-accesscontrol
Role impact severity	CRITICAL
Attack complexity cumulative	MEDIUM

Role description

The role pauses token transfers L1 -> L2.

Impact description

The role can block forward bridging.

Owners

Owner type	Multisig (Safe-Gnosis)
Owner address	0x73b047fe6337183A454c5217241D780a932777bD
Attack complexity	MEDIUM

Attack scenario

Need to have signatures of txn hash for 3 owners out of 5.

Domain	**L2 Gateway**
Contract	**Arbitrum:L1ERC20TokenGateway (Implementation)**
Role name	**WITHDRAWALS_ENABLER_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**HIGH**

Role description

The role unpauses token transfers L2 -> L1.

Impact description

The role can unblock backward bridging when not needed.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**L2 Gateway**
Contract	**Arbitrum:L1ERC20TokenGateway (Implementation)**
Role name	**WITHDRAWALS_DISABLER_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**MEDIUM**

Role description

The role pauses token transfers L2 -> L1.

Impact description

The role can block backward bridging.

Owners

Owner type	**Multisig (Safe-Gnosis)**
Owner address	**0x73b047fe6337183A454c5217241D780a932777bD**
Attack complexity	**MEDIUM**

Attack scenario

Need to have signatures of txn hash for 3 owners out of 5.

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**L2 Gateway**
Contract	**Optimism:L1ERC20TokenBridge (Proxy)**
Role name	**ADMIN**
Auth type	**custom-acl-over-oz-erc1967proxy**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**HIGH**

Role description

The role changes implementation, changes/resets ADMIN role owner.

Impact description

The role can upgrade contracts and break the connection between chains and steal the locked tokens.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**L2 Gateway**
Contract	**Optimism:L1ERC20TokenBridge (Implementation)**
Role name	**DEFAULT_ADMIN_ROLE**
Auth type	**custom-acl-oz-fork**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**HIGH**

Role description

The role is able to grant or revoke all roles.

Impact description

The role has a cumulative impact on all the roles of this contract. The worst case: the contract can accumulate the wstETH and stETH, while the claiming cannot be executed.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**L2 Gateway**
Contract	**Optimism:L1ERC20TokenBridge (Implementation)**
Role name	**DEPOSITS_ENABLER_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**HIGH**

Role description

The role unpauses token transfers L1 -> L2.

Impact description

The role can unblock forward bridging when not needed.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**L2 Gateway**
Contract	**Optimism:L1ERC20TokenBridge (Implementation)**
Role name	**DEPOSITS_DISABLER_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**MEDIUM**

Role description

The role pauses token transfers L1 -> L2.

Impact description

The role can block forward bridging.

Owners

Owner type	**Multisig (Safe-Gnosis)**
Owner address	**0x73b047fe6337183A454c5217241D780a932777bD**
Attack complexity	**MEDIUM**

Attack scenario

Need to have signatures of txn hash for 3 owners out of 5.

Domain	**L2 Gateway**
Contract	**Optimism:L1ERC20TokenBridge (Implementation)**
Role name	**WITHDRAWALS_ENABLER_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**HIGH**

Role description

The role unpauses token transfers L2 -> L1.

Impact description

The role can unblock backward bridging when not needed.

Owners

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

Domain	**L2 Gateway**
Contract	**Optimism:L1ERC20TokenBridge (Implementation)**
Role name	**WITHDRAWALS_DISABLER_ROLE**
Auth type	**oz-accesscontrol**
Role impact severity	**CRITICAL**
Attack complexity cumulative	**MEDIUM**

Role description

The role pauses token transfers L2 -> L1.

Impact description

The role can block backward bridging.

Owners

Owner type	**Multisig (Safe-Gnosis)**
Owner address	**0x73b047fe6337183A454c5217241D780a932777bD**
Attack complexity	**MEDIUM**

Attack scenario

Need to have signatures of txn hash for 3 owners out of 5.

Owner type	**Aragon Agent**
Owner address	**0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c**
Attack complexity	**HIGH**

Attack scenario

To execute the action for this role by Aragon Agent, the attacker must submit, pass, and execute a malicious proposal in Aragon Voting.

6. Limitations and use of the report

Security assessments may not uncover all vulnerabilities, but code assessments can reveal previously overlooked issues and highlight areas in need of additional security measures. Some vulnerabilities affect the entire application, while others are limited to specific areas. To address these issues, we conducted a source code assessment to identify necessary fixes within the timeframe agreed upon by the customer.

Our assessment focused on the code segments associated with items defined in the scope, assessing whether they conformed to user specifications and criteria established in the business specification. It's important to note that inherent limitations in software development and products may lead to undetected major failures or malfunctions. Uncertainties also exist in software products or applications used during development, which can contain errors or failures affecting the system's code, functions, and operation. We did not assess the underlying third-party infrastructure, which introduces inherent risks, as we rely on the proper functioning of third-party technology stacks. Additionally, changes in a software product's lifecycle or operational environment can lead to behaviors different from those initially specified in the business documentation.

The content of this report is not and shall not be construed as investment advice. This Information is meant to be informative and for general purposes only.

STATE
MIND