STATE MIND

MEV-Boost relay allowlist

05-09-2022 - 09-09-2022

Table of contents

1. Project Brief

Title	Description
Client	Lido
Project name	MEV-Boost relay allowlist
Timeline	05-09-2022 - 09-09-2022
Number of auditors	7
Initial commit	26ec6791c2466e784a894b8867db71d8de620745

Short Overview

The on-chain relays allowed list is planned to be used by Node Operators participating in the Lido protocol after the Merge to extract MEV according to the expected Lido policies.

Context

Lido needs to adopt a clear and public strategy with regards to MEV extraction on Ethereum. From a rewards perspective, Lido has already outlined a plan and technical approach on how both priority fees as well as possible MEV rewards can be (re)-distributed between stakers, node operators, and the protocol.

It's proposed that Node Operators should use MEV-Boost infrastructure developed by Flashbots to support MEV extraction through the open market mechanics as a current PBS solution that has a market fit.

Usage and purpose

The proposed allowed list is intended to be a source of truth for the set of possible relays allowed to be used by Node Operators. In particular, Node Operators would use the contract to keep their software configuration up-to-date (setting the necessary relays once Lido DAO updates the set).

Project Scope

The audit covered the following files:

MEVBoostRelayAllowedList.vy

2. Finding Severity breakdown

All vulnerabilities discovered during the audit are classified based on its potential severity and has the following classification:

Severity	Description
Critical	Bugs leading to assets theft, fund access locking, or any other loss funds to be transferred to any party.
High	Bugs that can trigger a contract failure. Further recovery is possible only by manual modification of the contract state or replacement.
Medium	Bugs that can break the intended contract logic or expose it to DoS attacks, but do not cause direct loss funds.
Informational	Bugs that do not have a significant immediate impact and could be easily fixed.

Based on the feedback received from the Customer regarding the list of findings discovered by the Contractor, they are assigned the following statuses:

Status	Description
Fixed	Recommended fixes have been made to the project code and no longer affect its security.
Acknowledged	The Customer is aware of the finding. Recommendations for the finding are planned to be resolved in the future.

3. Summary of findings

Severity	# of Findings
Critical	0
High	0
Medium	0
Informational	7

4. Conclusion

Commit with all fixes: `912f4143387ab04a7042b4887df67d3eecc97179`
No critical or high severity issues were found, fixed 5 out of 7 issues, 2 acknowledged.

Deployment

File name	Contract deployed on mainnet
contracts/MEVBoostRelayAllowedList.vy	0xf95f069f9ad107938f6ba802a3da87892298610e

5. Findings report

Informational

Gas optimisation	Fixed at 293636

Description

In add_relay function in case of adding more relays than `MAX_NUM_RELAYS` execution reverts only at the end at Line 155.

Recommendation

It is recommended to check a number of relays right after the `msg.sender` check.

```
assert len(self.relays) < MAX_NUM_RELAYS
```

Redundant check	Acknowledged

Description

At Line 271 `msg.sender` is checked for zero address.

Recommendation

Remove zero address check for `msg.sender`, because it is impossible to make a call from zero address.

Client's comments

> Zero address is used as a special value denoting manager absence, so this check carries mostly semantical meaning. Also although it is negligibly likely, in theory, someone could own a private key associated with the zero address. Just being paranoid.

Function _safe_erc20_transfer() doesn't revert if token is not a contract	Fixed at 293636

Description

At the line MEVBoostRelayAllowedList.vy#L288

The function `_safe_erc20_transfer()` takes address `token` as argument, but it doesn't check if that address is a contract. A low-level call to an EOA address returns `True` with no return data. This can lead to an emitting of the event `ERC20Recovered()` even though no tokens were transferred.

Recommendation

It is recommended to check if `token` address is a contract in the function `_safe_erc20_transfer()`.

Inaccurate NatSpec comments	Fixed at 293636

Description

At the line MEVBoostRelayAllowedList.vy#L164 it should be "Remove relay" instead of "Add relay".
At the line MEVBoostRelayAllowedList.vy#L189 it should be "Address of the new owner".
At the line MEVBoostRelayAllowedList.vy#L232 the `recipient` address is not necessarily the DAO treasury. The comment should reflect that.

Recommendation

It is recommended to fix these comments.

Event name RelaysUpdated is ambiguous	Fixed at 293636

Description

At the line MEVBoostRelayAllowedList.vy#L21 the event name `RelaysUpdated` can be interpreted as some relays in the list were updated. It is recommended to name the event `AllowedListUpdated` or `RelayAllowedListUpdated`.

Recommendation

Consider changing the name of this event to better reflect the state change.

Address of a recipient in ERC20Recovered might be indexed.	Fixed at 293636

Description

In order to simlify and facilitate interaction with venets logs, it makes sense to change recipient address in ERC20Recovered event to `indexed`.

Recommendation

Add `indexed` keword.

Inefficient storage of relays	Acknowledged

Description

Relays are stored in an array so to the value by URI you need to do a linear search. It can be optimized to O(1) asymptotic.

Recommendation

In addition to the array, use mapping that maps URI to index of relay in the array. In function `add_relay` you need to add value `len(self.relays) - 1` for key `uri` in mapping. In function `remove_relay` you need to update indexes for swapping elements in mapping.

Client's comments

> The solution is optimized in favor of storage structure simplicity and straightforwardness.

8. Appendix C. Tests

Tests result

```
38 passed in 46.90s
```

Tests coverage

Function	Stmts	Coverage
tests/test_ownership.py	61	100%
tests/test_recovery.py	53	100%
tests/test_relay_allowed_list.py	137	100%

STATE
MIND