## Summary

Block builder submissions with incorrect timestamp

and prev_randao

values were sent in bids to proposers, resulting in the beacon node rejecting the bid and falling back to local block production.

By sending specially crafted payloads to exploit this, attackers could prevent any MEV-Boost block from landing on chain, forcing proposers to fallback to local block production. However, there was no risk of proposers missing slots.

The Manifold team responsibly disclosed the issue, with tests in goerli. In close collaboration with EF security, consensus client, and relay operators teams, we identified the root cause of the issue, an incomplete builder submission validation, and deployed a solution to all networks.

A malicious builder sent bids to the Flashbots Mainnet relay, leading to a drop in MEV-Boost blocks between 12:00 and 16:00 UTC on Nov. 10:

[

chart showing drop in mev-boost transactions

1558×438 24.3 KB

](https://collective.flashbots.net/uploads/default/original/1X/95e6c168b620ed3ed7d3589825b1a06e3b83ab88.png)

Once we noticed and identified the builder as [0xab847b...91921b

](https://boost-relay.flashbots.net/relay/v1/data/bidtraces/builder_blocks_received?builder_pubkey=0xab847befe59b5effffa12f47acf44cbf8ef875e7c891a4ee9e9c483254cf9a55f5ed688e43ff5bc6cd9276e99091921b), we briefly blacklisted him at 15:30 UTC while implementing a solution, and unblocked him again afterwards. At the time of writing, there are no blacklisted builders on the Flashbots relay.

## Timeline

(all times in UTC)

Thursday, Nov. 10, 2022

1. We've received a high-level report from Manifold about a possible relay DoS vector at 7:39.
2. Started the investigation.
3. At 12:18, engineers from Manifold provided an example payload that triggers the issue, and we asked them to continuously cause the DoS vector on the Goerli relay.
4. Tried to reproduce the issue by running the payloads through MEV-Boost, which did not show any errors. What was needed to diagnose the behavior further were logs from MEV-Boost and Beacon nodes on Goerli.
5. At 14:21, we asked engineers from the Teku and Prysm whether they run Goerli validators that may have received bids where local fallback was triggered.
6. At 14:34 Enrico and Stefan from Teku found logs showing that an incorrect timestamp was causing the local fallback.
7. A solution for the timestamp validation was implemented in https://github.com/flashbots/mev-boost-relay/pull/241 and deployed at around 15:19.
8. The cross-org engineering team worked on figuring out the best way to check the prev_randao

field in the relay API. We arrived athttps://github.com/flashbots/mev-boost-relay/pull/242 using a new (and not yet documented) beacon-node API (/eth/v1/beacon/states//randao

).

1. The prev_randao

validation solution was tested, and deployed to mainnet at 22:00.

Friday, Nov 11, 2022

1. The BlockSec security team, contracted by Manifold, notified us at 7:44 that there may also be a missing validation of gas_limit

.

1. After confirming the report, we fixed the gas_limit

validation logic in the validation nodes [1] [2].

1. The update was deployed to Mainnet at 9:35.

## Impact

Around 350 locally built blocks were proposed instead of mev-boost blocks between 12:00 UTC and 16:00 UTC on Nov. 10. There was no risk of proposers missing slots.

Big thanks to @justintraglia, @tbenr, @stefanbratanov, @terencechain, @dickmanben, @realbigsean and several others who helped investigating, diagnosing and resolving!

We thank Manifold in particular for the responsible disclosure.