MythX

Analysis c9a05782-cd2c-4787-8075-a283403afe75 MythX

Started	Sat Nov 05 2022 13:44:58 GMT+0000 (Coordinated Universal Time)
Finished	Sat Nov 05 2022 14:30:50 GMT+0000 (Coordinated Universal Time)
Mode	Deep
Client Tool	Mythx-Vscode-Extension
Main Source File	/Flattenedcontracts/Flattened_nobleswap.Sol

DETECTED VULNERABILITIES

HIGH	MEDIUM	LOW
0	0	2

ISSUES

LOW

SWC-120

Potential use of "block.number" as source of randonmness.

The environment variable "block.number" looks like it might be used as a source of randomness. Note that the values of variables like coinbase, gaslimit, block number and timestamp are predictable and can be manipulated by a malicious miner. Also keep in mind that attackers know hashes of earlier blocks. Don't use any of those environment variables as sources of randomness and be aware that use of these variables introduces a certain level of trust into miners.

Source file

/flattenedcontracts/flattened_nobleswap.sol

Locations

```
1262 function getPriorVotes(address account, uint blockNumber) external view returns (uint256) {
1263
1264 require(blockNumber < block.number, "NOBLE: getPriorVotes: not yet determined");
1265
1266 uint32 nCheckpoints = numCheckpoints[account];
```

LOW

SWC-120

Potential use of "block.number" as source of randonmness.

The environment variable "block.number" looks like it might be used as a source of randomness. Note that the values of variables like coinbase, gaslimit, block number and timestamp are predictable and can be manipulated by a malicious miner. Also keep in mind that attackers know hashes of earlier blocks. Don't use any of those environment variables as sources of randomness and be aware that use of these variables introduces a certain level of trust into miners.

Source file

/flattenedcontracts/flattened_nobleswap.sol

Locations

```
1374 function _writeCheckpoint(address delegatee, uint32 nCheckpoints, uint256 oldVotes, uint256 newVotes) internal {
1375
1376 uint32 blockNumber = _safe32(block.number, "NOBLE: _writeCheckpoint: block number exceeds 32 bits");
1377
1378 if (nCheckpoints > 0 && checkpoints[delegatee][nCheckpoints - 1].fromBlock == blockNumber) {
```