SOOHO

c6590e4bf4007d280a2faf8c0e6bde74b98bc7c08eaa0be6a23ebea512a92469

File: TheVault.sol | Language:solidity | Size:15137 bytes | Date:2022-01-21T11:42:04.186Z

Critical	High	Medium	Low	Note
0	0	0	1	3

Issues

Severity	Issue	Analyzer	Code Lines
Low	SWC-103	Achilles	2
Note	SWC-116	Achilles	137, 318, 379

Code

1. SWC-103 / lines: 2 Low Achilles

A security vulnerability has been detected.

```
1  // SPDX-License-Identifier: MIT
2  pragma solidity ^0.8.0;
3
```

In detail

Contracts should be deployed with the same compiler version and flags that they have been tested with thoroughly. Locking the pragma helps to ensure that contracts do not accidentally get deployed using, for example, an outdated compiler version that might introduce bugs that affect the contract system negatively.

2. SWC-116 / lines: 137 Note Achilles

A security vulnerability has been detected.

```
136         require(
137             _lastInteraction[msg.sender] + INTERACTION_DELAY <= block.number,
138             "< DELAY"
```

In detail

Contracts often need access to the current timestamp to trigger time-dependent events. As Ethereum is decentralized, nodes can synchronize time only to some degree. Moreover, malicious miners can alter the timestamp of their blocks, especially if they can gain advantages by doing so. However, miners can't set timestamp smaller than the previous one (otherwise the block will be rejected), nor can they set the timestamp too far ahead in the future. Taking all of the above into consideration, developers can't rely on the preciseness of the provided timestamp.

3. SWC-116 / lines: 318 Note Achilles

A security vulnerability has been detected.

```
317             address(this),
318             block.timestamp
319         );
```

In detail

Contracts often need access to the current timestamp to trigger time-dependent events. As Ethereum is decentralized, nodes can synchronize time only to some degree. Moreover, malicious miners can alter the timestamp of their blocks, especially if they can gain advantages by doing so. However, miners can't set timestamp smaller than the previous one (otherwise the block will be rejected), nor can they set the timestamp too far ahead in the future. Taking all of the above into

consideration, developers can't rely on the preciseness of the provided timestamp.

4. SWC-116 / lines: 379 Note Achilles

A security vulnerability has been detected.

```
378
379         _lastInteraction[msg.sender] = block.number;
380
```

In detail

Contracts often need access to the current timestamp to trigger time-dependent events. As Ethereum is decentralized, nodes can synchronize time only to some degree. Moreover, malicious miners can alter the timestamp of their blocks, especially if they can gain advantages by doing so. However, miners can't set timestamp smaller than the previous one (otherwise the block will be rejected), nor can they set the timestamp too far ahead in the future. Taking all of the above into consideration, developers can't rely on the preciseness of the provided timestamp.