MythX

Analysis df09fb12-025d-4ab1-9604-524451d1e269 MythX

Started	Wed Apr 26 2023 04:06:21 GMT+0000 (Coordinated Universal Time)
Finished	Wed Apr 26 2023 04:08:30 GMT+0000 (Coordinated Universal Time)
Mode	Quick
Client Tool	Mythx-Cli-0.7.3
Main Source File	Contracts/Oracle/Oracle.Sol

DETECTED VULNERABILITIES

HIGH	MEDIUM	LOW
0	0	53

ISSUES

LOW

SWC-103

A floating pragma is set.

The current pragma Solidity directive is ""^0.8.0"". It is recommended to specify a fixed compiler version to ensure that the bytecode produced does not vary between builds. This is especially important if you rely on bytecode-level verification of the code.

Source file
contracts/oracle/Oracle.sol
Locations

```
1 // SPDX-License-Identifier: BUSL-1.1
2
3 pragma solidity ^0.8.0;
4
5 import "../libraries/math/SafeCast.sol";
```

LOW

SWC-108

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "EmptyTokens" is internal. Other possible visibility settings are public and private.

Source file
contracts/oracle/Oracle.sol
Locations

```
97  mapping (address => uint256) public maxOracleBlockNumbers;
98
99  error EmptyTokens();
100 error InvalidBlockNumber(uint256 blockNumber);
101 error InvalidMinMaxBlockNumber(uint256 minOracleBlockNumber, uint256 maxOracleBlockNumber);
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "InvalidBlockNumber" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

contracts/oracle/Oracle.sol

Locations

```
98
99  error EmptyTokens();
100 error InvalidBlockNumber(uint256 blockNumber);
101 error InvalidMinMaxBlockNumber(uint256 minOracleBlockNumber, uint256 maxOracleBlockNumber);
102 error MaxPriceAgeExceeded(uint256 oracleTimestamp);
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "blockNumber" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

contracts/oracle/Oracle.sol

Locations

```
98
99  error EmptyTokens();
100 error InvalidBlockNumber(uint256 blockNumber);
101 error InvalidMinMaxBlockNumber(uint256 minOracleBlockNumber, uint256 maxOracleBlockNumber);
102 error MaxPriceAgeExceeded(uint256 oracleTimestamp);
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "InvalidMinMaxBlockNumber" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

contracts/oracle/Oracle.sol

Locations

```
99  error EmptyTokens();
100 error InvalidBlockNumber(uint256 blockNumber);
101 error InvalidMinMaxBlockNumber(uint256 minOracleBlockNumber, uint256 maxOracleBlockNumber);
102 error MaxPriceAgeExceeded(uint256 oracleTimestamp);
103 error MinOracleSigners(uint256 oracleSigners, uint256 minOracleSigners);
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "minOracleBlockNumber" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

contracts/oracle/Oracle.sol

Locations

```
99  error EmptyTokens();
100 error InvalidBlockNumber(uint256 blockNumber);
101 error InvalidMinMaxBlockNumber(uint256 minOracleBlockNumber, uint256 maxOracleBlockNumber);
102 error MaxPriceAgeExceeded(uint256 oracleTimestamp);
103 error MinOracleSigners(uint256 oracleSigners, uint256 minOracleSigners);
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "maxOracleBlockNumber" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

contracts/oracle/Oracle.sol

Locations

```
99  error EmptyTokens();
100 error InvalidBlockNumber(uint256 blockNumber);
101 error InvalidMinMaxBlockNumber(uint256 minOracleBlockNumber, uint256 maxOracleBlockNumber);
102 error MaxPriceAgeExceeded(uint256 oracleTimestamp);
103 error MinOracleSigners(uint256 oracleSigners, uint256 minOracleSigners);
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "MaxPriceAgeExceeded" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

contracts/oracle/Oracle.sol

Locations

```
100 error InvalidBlockNumber(uint256 blockNumber);
101 error InvalidMinMaxBlockNumber(uint256 minOracleBlockNumber, uint256 maxOracleBlockNumber);
102 error MaxPriceAgeExceeded(uint256 oracleTimestamp);
103 error MinOracleSigners(uint256 oracleSigners, uint256 minOracleSigners);
104 error MaxOracleSigners(uint256 oracleSigners, uint256 maxOracleSigners);
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "oracleTimestamp" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

contracts/oracle/Oracle.sol

Locations

```
100 error InvalidBlockNumber(uint256 blockNumber);
101 error InvalidMinMaxBlockNumber(uint256 minOracleBlockNumber, uint256 maxOracleBlockNumber);
102 error MaxPriceAgeExceeded(uint256 oracleTimestamp);
103 error MinOracleSigners(uint256 oracleSigners, uint256 minOracleSigners);
104 error MaxOracleSigners(uint256 oracleSigners, uint256 maxOracleSigners);
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "MinOracleSigners" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

contracts/oracle/Oracle.sol

Locations

```
101 error InvalidMinMaxBlockNumber(uint256 minOracleBlockNumber, uint256 maxOracleBlockNumber);
102 error MaxPriceAgeExceeded(uint256 oracleTimestamp);
103 error MinOracleSigners(uint256 oracleSigners, uint256 minOracleSigners);
104 error MaxOracleSigners(uint256 oracleSigners, uint256 maxOracleSigners);
105 error BlockNumbersNotSorted(uint256 minOracleBlockNumber, uint256 prevMinOracleBlockNumber);
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "oracleSigners" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

contracts/oracle/Oracle.sol

Locations

```
101 error InvalidMinMaxBlockNumber(uint256 minOracleBlockNumber, uint256 maxOracleBlockNumber);
102 error MaxPriceAgeExceeded(uint256 oracleTimestamp);
103 error MinOracleSigners(uint256 oracleSigners, uint256 minOracleSigners);
104 error MaxOracleSigners(uint256 oracleSigners, uint256 maxOracleSigners);
105 error BlockNumbersNotSorted(uint256 minOracleBlockNumber, uint256 prevMinOracleBlockNumber);
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "minOracleSigners" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

contracts/oracle/Oracle.sol

Locations

```
101 error InvalidMinMaxBlockNumber(uint256 minOracleBlockNumber, uint256 maxOracleBlockNumber);
102 error MaxPriceAgeExceeded(uint256 oracleTimestamp);
103 error MinOracleSigners(uint256 oracleSigners, uint256 minOracleSigners);
104 error MaxOracleSigners(uint256 oracleSigners, uint256 maxOracleSigners);
105 error BlockNumbersNotSorted(uint256 minOracleBlockNumber, uint256 prevMinOracleBlockNumber);
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "MaxOracleSigners" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

contracts/oracle/Oracle.sol

Locations

```
102 error MaxPriceAgeExceeded(uint256 oracleTimestamp);
103 error MinOracleSigners(uint256 oracleSigners, uint256 minOracleSigners);
104 error MaxOracleSigners(uint256 oracleSigners, uint256 maxOracleSigners);
105 error BlockNumbersNotSorted(uint256 minOracleBlockNumber, uint256 prevMinOracleBlockNumber);
106 error MinPricesNotSorted(address token, uint256 price, uint256 prevPrice);
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "oracleSigners" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

contracts/oracle/Oracle.sol

Locations

```
102 error MaxPriceAgeExceeded(uint256 oracleTimestamp);
103 error MinOracleSigners(uint256 oracleSigners, uint256 minOracleSigners);
104 error MaxOracleSigners(uint256 oracleSigners, uint256 maxOracleSigners);
105 error BlockNumbersNotSorted(uint256 minOracleBlockNumber, uint256 prevMinOracleBlockNumber);
106 error MinPricesNotSorted(address token, uint256 price, uint256 prevPrice);
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "maxOracleSigners" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

contracts/oracle/Oracle.sol

Locations

```
102 error MaxPriceAgeExceeded(uint256 oracleTimestamp);
103 error MinOracleSigners(uint256 oracleSigners, uint256 minOracleSigners);
104 error MaxOracleSigners(uint256 oracleSigners, uint256 maxOracleSigners);
105 error BlockNumbersNotSorted(uint256 minOracleBlockNumber, uint256 prevMinOracleBlockNumber);
106 error MinPricesNotSorted(address token, uint256 price, uint256 prevPrice);
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "BlockNumbersNotSorted" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

contracts/oracle/Oracle.sol

Locations

```
103 error MinOracleSigners(uint256 oracleSigners, uint256 minOracleSigners);
104 error MaxOracleSigners(uint256 oracleSigners, uint256 maxOracleSigners);
105 error BlockNumbersNotSorted(uint256 minOracleBlockNumber, uint256 prevMinOracleBlockNumber);
106 error MinPricesNotSorted(address token, uint256 price, uint256 prevPrice);
107 error MaxPricesNotSorted(address token, uint256 price, uint256 prevPrice);
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "minOracleBlockNumber" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

contracts/oracle/Oracle.sol

Locations

```
103 error MinOracleSigners(uint256 oracleSigners, uint256 minOracleSigners);
104 error MaxOracleSigners(uint256 oracleSigners, uint256 maxOracleSigners);
105 error BlockNumbersNotSorted(uint256 minOracleBlockNumber, uint256 prevMinOracleBlockNumber);
106 error MinPricesNotSorted(address token, uint256 price, uint256 prevPrice);
107 error MaxPricesNotSorted(address token, uint256 price, uint256 prevPrice);
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "prevMinOracleBlockNumber" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

contracts/oracle/Oracle.sol

Locations

```
103 error MinOracleSigners(uint256 oracleSigners, uint256 minOracleSigners);
104 error MaxOracleSigners(uint256 oracleSigners, uint256 maxOracleSigners);
105 error BlockNumbersNotSorted(uint256 minOracleBlockNumber, uint256 prevMinOracleBlockNumber);
106 error MinPricesNotSorted(address token, uint256 price, uint256 prevPrice);
107 error MaxPricesNotSorted(address token, uint256 price, uint256 prevPrice);
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "MinPricesNotSorted" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

contracts/oracle/Oracle.sol

Locations

```
104 error MaxOracleSigners(uint256 oracleSigners, uint256 maxOracleSigners);
105 error BlockNumbersNotSorted(uint256 minOracleBlockNumber, uint256 prevMinOracleBlockNumber);
106 error MinPricesNotSorted(address token, uint256 price, uint256 prevPrice);
107 error MaxPricesNotSorted(address token, uint256 price, uint256 prevPrice);
108 error EmptyPriceFeedMultiplier(address token);
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "token" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

contracts/oracle/Oracle.sol

Locations

```
104 error MaxOracleSigners(uint256 oracleSigners, uint256 maxOracleSigners);
105 error BlockNumbersNotSorted(uint256 minOracleBlockNumber, uint256 prevMinOracleBlockNumber);
106 error MinPricesNotSorted(address token, uint256 price, uint256 prevPrice);
107 error MaxPricesNotSorted(address token, uint256 price, uint256 prevPrice);
108 error EmptyPriceFeedMultiplier(address token);
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "price" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

contracts/oracle/Oracle.sol

Locations

```
104 error MaxOracleSigners(uint256 oracleSigners, uint256 maxOracleSigners);
105 error BlockNumbersNotSorted(uint256 minOracleBlockNumber, uint256 prevMinOracleBlockNumber);
106 error MinPricesNotSorted(address token, uint256 price, uint256 prevPrice);
107 error MaxPricesNotSorted(address token, uint256 price, uint256 prevPrice);
108 error EmptyPriceFeedMultiplier(address token);
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "prevPrice" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

contracts/oracle/Oracle.sol

Locations

```
104 error MaxOracleSigners(uint256 oracleSigners, uint256 maxOracleSigners);
105 error BlockNumbersNotSorted(uint256 minOracleBlockNumber, uint256 prevMinOracleBlockNumber);
106 error MinPricesNotSorted(address token, uint256 price, uint256 prevPrice);
107 error MaxPricesNotSorted(address token, uint256 price, uint256 prevPrice);
108 error EmptyPriceFeedMultiplier(address token);
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "MaxPricesNotSorted" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

contracts/oracle/Oracle.sol

Locations

```
105 error BlockNumbersNotSorted(uint256 minOracleBlockNumber, uint256 prevMinOracleBlockNumber);
106 error MinPricesNotSorted(address token, uint256 price, uint256 prevPrice);
107 error MaxPricesNotSorted(address token, uint256 price, uint256 prevPrice);
108 error EmptyPriceFeedMultiplier(address token);
109 error EmptyFeedPrice(address token);
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "token" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

contracts/oracle/Oracle.sol

Locations

```
105 error BlockNumbersNotSorted(uint256 minOracleBlockNumber, uint256 prevMinOracleBlockNumber);
106 error MinPricesNotSorted(address token, uint256 price, uint256 prevPrice);
107 error MaxPricesNotSorted(address token, uint256 price, uint256 prevPrice);
108 error EmptyPriceFeedMultiplier(address token);
109 error EmptyFeedPrice(address token);
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "price" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

contracts/oracle/Oracle.sol

Locations

```
105 error BlockNumbersNotSorted(uint256 minOracleBlockNumber, uint256 prevMinOracleBlockNumber);
106 error MinPricesNotSorted(address token, uint256 price, uint256 prevPrice);
107 error MaxPricesNotSorted(address token, uint256 price, uint256 prevPrice);
108 error EmptyPriceFeedMultiplier(address token);
109 error EmptyFeedPrice(address token);
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "prevPrice" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

contracts/oracle/Oracle.sol

Locations

```
105 error BlockNumbersNotSorted(uint256 minOracleBlockNumber, uint256 prevMinOracleBlockNumber);
106 error MinPricesNotSorted(address token, uint256 price, uint256 prevPrice);
107 error MaxPricesNotSorted(address token, uint256 price, uint256 prevPrice);
108 error EmptyPriceFeedMultiplier(address token);
109 error EmptyFeedPrice(address token);
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "EmptyPriceFeedMultiplier" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

contracts/oracle/Oracle.sol

Locations

```
106 error MinPricesNotSorted(address token, uint256 price, uint256 prevPrice);
107 error MaxPricesNotSorted(address token, uint256 price, uint256 prevPrice);
108 error EmptyPriceFeedMultiplier(address token);
109 error EmptyFeedPrice(address token);
110 error MaxSignerIndex(uint256 signerIndex, uint256 maxSignerIndex);
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "token" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

contracts/oracle/Oracle.sol

Locations

```
106 error MinPricesNotSorted(address token, uint256 price, uint256 prevPrice);
107 error MaxPricesNotSorted(address token, uint256 price, uint256 prevPrice);
108 error EmptyPriceFeedMultiplier(address token);
109 error EmptyFeedPrice(address token);
110 error MaxSignerIndex(uint256 signerIndex, uint256 maxSignerIndex);
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "EmptyFeedPrice" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

contracts/oracle/Oracle.sol

Locations

```
107 error MaxPricesNotSorted(address token, uint256 price, uint256 prevPrice);
108 error EmptyPriceFeedMultiplier(address token);
109 error EmptyFeedPrice(address token);
110 error MaxSignerIndex(uint256 signerIndex, uint256 maxSignerIndex);
111 error DuplicateSigner(uint256 signerIndex);
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "token" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

contracts/oracle/Oracle.sol

Locations

```
107 error MaxPricesNotSorted(address token, uint256 price, uint256 prevPrice);
108 error EmptyPriceFeedMultiplier(address token);
109 error EmptyFeedPrice(address token);
110 error MaxSignerIndex(uint256 signerIndex, uint256 maxSignerIndex);
111 error DuplicateSigner(uint256 signerIndex);
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "MaxSignerIndex" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

contracts/oracle/Oracle.sol

Locations

```
108 error EmptyPriceFeedMultiplier(address token);
109 error EmptyFeedPrice(address token);
110 error MaxSignerIndex(uint256 signerIndex, uint256 maxSignerIndex);
111 error DuplicateSigner(uint256 signerIndex);
112 error InvalidOraclePrice(address token);
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "signerIndex" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

contracts/oracle/Oracle.sol

Locations

```
108 error EmptyPriceFeedMultiplier(address token);
109 error EmptyFeedPrice(address token);
110 error MaxSignerIndex(uint256 signerIndex, uint256 maxSignerIndex);
111 error DuplicateSigner(uint256 signerIndex);
112 error InvalidOraclePrice(address token);
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "maxSignerIndex" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

contracts/oracle/Oracle.sol

Locations

```
108 error EmptyPriceFeedMultiplier(address token);
109 error EmptyFeedPrice(address token);
110 error MaxSignerIndex(uint256 signerIndex, uint256 maxSignerIndex);
111 error DuplicateSigner(uint256 signerIndex);
112 error InvalidOraclePrice(address token);
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "DuplicateSigner" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

contracts/oracle/Oracle.sol

Locations

```
109 error EmptyFeedPrice(address token);
110 error MaxSignerIndex(uint256 signerIndex, uint256 maxSignerIndex);
111 error DuplicateSigner(uint256 signerIndex);
112 error InvalidOraclePrice(address token);
113 error InvalidSignerMinMaxPrice(uint256 minPrice, uint256 maxPrice);
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "signerIndex" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

contracts/oracle/Oracle.sol

Locations

```
109 error EmptyFeedPrice(address token);
110 error MaxSignerIndex(uint256 signerIndex, uint256 maxSignerIndex);
111 error DuplicateSigner(uint256 signerIndex);
112 error InvalidOraclePrice(address token);
113 error InvalidSignerMinMaxPrice(uint256 minPrice, uint256 maxPrice);
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "InvalidOraclePrice" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

contracts/oracle/Oracle.sol

Locations

```
110 error MaxSignerIndex(uint256 signerIndex, uint256 maxSignerIndex);
111 error DuplicateSigner(uint256 signerIndex);
112 error InvalidOraclePrice(address token);
113 error InvalidSignerMinMaxPrice(uint256 minPrice, uint256 maxPrice);
114 error InvalidMedianMinMaxPrice(uint256 minPrice, uint256 maxPrice);
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "token" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

contracts/oracle/Oracle.sol

Locations

```
110 error MaxSignerIndex(uint256 signerIndex, uint256 maxSignerIndex);
111 error DuplicateSigner(uint256 signerIndex);
112 error InvalidOraclePrice(address token);
113 error InvalidSignerMinMaxPrice(uint256 minPrice, uint256 maxPrice);
114 error InvalidMedianMinMaxPrice(uint256 minPrice, uint256 maxPrice);
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "InvalidSignerMinMaxPrice" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

contracts/oracle/Oracle.sol

Locations

```
111 error DuplicateSigner(uint256 signerIndex);
112 error InvalidOraclePrice(address token);
113 error InvalidSignerMinMaxPrice(uint256 minPrice, uint256 maxPrice);
114 error InvalidMedianMinMaxPrice(uint256 minPrice, uint256 maxPrice);
115 error NonEmptyTokensWithPrices(uint256 tokensWithPricesLength);
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "minPrice" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

contracts/oracle/Oracle.sol

Locations

```
111 error DuplicateSigner(uint256 signerIndex);
112 error InvalidOraclePrice(address token);
113 error InvalidSignerMinMaxPrice(uint256 minPrice, uint256 maxPrice);
114 error InvalidMedianMinMaxPrice(uint256 minPrice, uint256 maxPrice);
115 error NonEmptyTokensWithPrices(uint256 tokensWithPricesLength);
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "maxPrice" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

contracts/oracle/Oracle.sol

Locations

```
111 error DuplicateSigner(uint256 signerIndex);
112 error InvalidOraclePrice(address token);
113 error InvalidSignerMinMaxPrice(uint256 minPrice, uint256 maxPrice);
114 error InvalidMedianMinMaxPrice(uint256 minPrice, uint256 maxPrice);
115 error NonEmptyTokensWithPrices(uint256 tokensWithPricesLength);
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "InvalidMedianMinMaxPrice" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

contracts/oracle/Oracle.sol

Locations

```
112 error InvalidOraclePrice(address token);
113 error InvalidSignerMinMaxPrice(uint256 minPrice, uint256 maxPrice);
114 error InvalidMedianMinMaxPrice(uint256 minPrice, uint256 maxPrice);
115 error NonEmptyTokensWithPrices(uint256 tokensWithPricesLength);
116 error EmptyPriceFeed(address token);
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "minPrice" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

contracts/oracle/Oracle.sol

Locations

```
112 error InvalidOraclePrice(address token);
113 error InvalidSignerMinMaxPrice(uint256 minPrice, uint256 maxPrice);
114 error InvalidMedianMinMaxPrice(uint256 minPrice, uint256 maxPrice);
115 error NonEmptyTokensWithPrices(uint256 tokensWithPricesLength);
116 error EmptyPriceFeed(address token);
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "maxPrice" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

contracts/oracle/Oracle.sol

Locations

```
112 error InvalidOraclePrice(address token);
113 error InvalidSignerMinMaxPrice(uint256 minPrice, uint256 maxPrice);
114 error InvalidMedianMinMaxPrice(uint256 minPrice, uint256 maxPrice);
115 error NonEmptyTokensWithPrices(uint256 tokensWithPricesLength);
116 error EmptyPriceFeed(address token);
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "NonEmptyTokensWithPrices" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

contracts/oracle/Oracle.sol

Locations

```
113 error InvalidSignerMinMaxPrice(uint256 minPrice, uint256 maxPrice);
114 error InvalidMedianMinMaxPrice(uint256 minPrice, uint256 maxPrice);
115 error NonEmptyTokensWithPrices(uint256 tokensWithPricesLength);
116 error EmptyPriceFeed(address token);
117 error PriceAlreadySet(address token, uint256 minPrice, uint256 maxPrice);
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "tokensWithPricesLength" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

contracts/oracle/Oracle.sol

Locations

```
113 error InvalidSignerMinMaxPrice(uint256 minPrice, uint256 maxPrice);
114 error InvalidMedianMinMaxPrice(uint256 minPrice, uint256 maxPrice);
115 error NonEmptyTokensWithPrices(uint256 tokensWithPricesLength);
116 error EmptyPriceFeed(address token);
117 error PriceAlreadySet(address token, uint256 minPrice, uint256 maxPrice);
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "EmptyPriceFeed" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

contracts/oracle/Oracle.sol

Locations

```
114 error InvalidMedianMinMaxPrice(uint256 minPrice, uint256 maxPrice);
115 error NonEmptyTokensWithPrices(uint256 tokensWithPricesLength);
116 error EmptyPriceFeed(address token);
117 error PriceAlreadySet(address token, uint256 minPrice, uint256 maxPrice);
118
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "token" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

contracts/oracle/Oracle.sol

Locations

```
114 error InvalidMedianMinMaxPrice(uint256 minPrice, uint256 maxPrice);
115 error NonEmptyTokensWithPrices(uint256 tokensWithPricesLength);
116 error EmptyPriceFeed(address token);
117 error PriceAlreadySet(address token, uint256 minPrice, uint256 maxPrice);
118
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "PriceAlreadySet" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

contracts/oracle/Oracle.sol

Locations

```
115 error NonEmptyTokensWithPrices(uint256 tokensWithPricesLength);
116 error EmptyPriceFeed(address token);
117 error PriceAlreadySet(address token, uint256 minPrice, uint256 maxPrice);
118
119 event SetPositionManager(address indexed account, bool isActive);
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "token" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

contracts/oracle/Oracle.sol

Locations

```
115 error NonEmptyTokensWithPrices(uint256 tokensWithPricesLength);
116 error EmptyPriceFeed(address token);
117 error PriceAlreadySet(address token, uint256 minPrice, uint256 maxPrice);
118
119 event SetPositionManager(address indexed account, bool isActive);
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "minPrice" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

contracts/oracle/Oracle.sol

Locations

```
115 error NonEmptyTokensWithPrices(uint256 tokensWithPricesLength);
116 error EmptyPriceFeed(address token);
117 error PriceAlreadySet(address token, uint256 minPrice, uint256 maxPrice);
118
119 event SetPositionManager(address indexed account, bool isActive);
```

LOW

SWC-108

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "maxPrice" is internal. Other possible visibility settings are public and private.

Source file

contracts/oracle/Oracle.sol

Locations

```
115 error NonEmptyTokensWithPrices(uint256 tokensWithPricesLength);
116 error EmptyPriceFeed(address token);
117 error PriceAlreadySet(address token, uint256 minPrice, uint256 maxPrice);
118
119 event SetPositionManager(address indexed account, bool isActive);
```

LOW

SWC-120

Potential use of "blockhash" as source of randonmness.

The environment variable "blockhash" 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

contracts/libraries/chain/Chain.sol

Locations

```
37 }
38
39 return blockhash(blockNumber);
40 }
41 }
```

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

contracts/libraries/chain/Chain.sol

Locations

```
27 }
28
29 return block.number;
30 }
```