MythX

REPORT 6195B840DDE18F0019C88E24

Created	Thu Nov 18 2021 02:19:44 GMT+0000 (Coordinated Universal Time)
Number of analyses	1
User	5f50e9c4f992e6001848d9db

REPORT SUMMARY

Analyses ID	Main source file	Detected vulnerabilities
31489c10-b3ec-4c14-be8c-5e571b6d5c24	buckpool.sol	13

Analysis 31489c10-b3ec-4c14-be8c-5e571b6d5c24

MythX

Started	Thu Nov 18 2021 02:19:52 GMT+0000 (Coordinated Universal Time)
Finished	Thu Nov 18 2021 03:04:57 GMT+0000 (Coordinated Universal Time)
Mode	Deep
Client Tool	Remythx
Main Source File	`Buckpool.Sol`

DETECTED VULNERABILITIES

HIGH	MEDIUM	LOW
0	0	13

ISSUES

LOW

SWC-103

A floating pragma is set.

The current pragma Solidity directive is ""^0.7.0"". 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

`buckpool.sol`

Locations

```
// SPDX-License-Identifier: MIT

pragma solidity ^0.7.0;

/*
```

LOW

SWC-103

A floating pragma is set.

The current pragma Solidity directive is ""^0.7.0"". 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

`buckpool.sol`

Locations

```


pragma solidity ^0.7.0;

/**
```

LOW

SWC-103

A floating pragma is set.

The current pragma Solidity directive is ""^0.7.0"". 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

`buckpool.sol`

Locations

```


pragma solidity ^0.7.0;

/**
```

LOW

SWC-103

A floating pragma is set.

The current pragma Solidity directive is ""^0.7.0"". 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

`buckpool.sol`

Locations

```


pragma solidity ^0.7.0;

/**
```

LOW

SWC-103

A floating pragma is set.

The current pragma Solidity directive is ""^0.7.0"". 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

`buckpool.sol`

Locations

```


pragma solidity ^0.7.0;

// Due to compiling issues, _name, _symbol, and _decimals were removed
```

LOW

SWC-103

A floating pragma is set.

The current pragma Solidity directive is ""^0.7.0"". 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

`buckpool.sol`

Locations

```


pragma solidity ^0.7.0;

/**
```

LOW

SWC-103

A floating pragma is set.

The current pragma Solidity directive is "">=0.6.7"". 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

`buckpool.sol`

Locations

```


pragma solidity >=0.6.7;

interface AggregatorV3Interface {
```

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

`buckpool.sol`

Locations

```
*/
function getPriorVotes(address account, uint blockNumber) public view returns (uint96) {
require(blockNumber < block.number, "BEVY::getPriorVotes: not yet determined");

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

buckpool.sol

Locations

```

function _writeCheckpoint(address voter, uint32 nCheckpoints, uint96 oldVotes, uint96 newVotes) internal {
uint32 blockNumber = safe32(block.number, "BEVY::_writeCheckpoint: block number exceeds 32 bits");

if (nCheckpoints > 0 && checkpoints[voter][nCheckpoints - 1].fromBlock == blockNumber) {
```

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

buckpool.sol

Locations

```
redeemCollateralBalances[msg.sender] = redeemCollateralBalances[msg.sender].add(collateral_needed);
unclaimedPoolCollateral = unclaimedPoolCollateral.add(collateral_needed);
lastRedeemed[msg.sender] = block.number;

// Move all external functions to the end
```

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

buckpool.sol

Locations

```
unclaimedPoolBEVY = unclaimedPoolBEVY.add(bevy_amount);

lastRedeemed[msg.sender] = block.number;

// Move all external functions to the end
```

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

`buckpool.sol`

Locations

```
unclaimedPoolBEVY = unclaimedPoolBEVY.add(bevy_amount);

lastRedeemed[msg.sender] = block.number;

require(BEVY_out_min <= bevy_amount, "Slippage limit reached");
```

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

`buckpool.sol`

Locations

```
// to take out BUCK/collateral from the system, use an AMM to trade the new price, and then mint back into the system.
function collectRedemption() external {
require((lastRedeemed[msg.sender].add(redemption_delay)) <= block.number, "Must wait for redemption_delay blocks before collecting redemption");
bool sendBEVY = false;
bool sendCollateral = false;
```