MythX

Analysis 1469d1ae-ea2a-41e0-ac87-7904e1ec6a48 MythX

Started	Mon Sep 06 2021 11:10:41 GMT+0000 (Coordinated Universal Time)
Finished	Mon Sep 06 2021 11:10:50 GMT+0000 (Coordinated Universal Time)
Mode	Deep
Client Tool	Mythx-Vscode-Extension
Main Source File	/Contracts/Vault.Sol

DETECTED VULNERABILITIES

HIGH	MEDIUM	LOW
0	0	1

ISSUES

UNKNOWN SWC-101 Arithmetic operation "**" discovered

This plugin produces issues to support false positive discovery within MythX.

Source file
/contracts/vault.sol
Locations

```
uint256 excessAmount = isToken0Excess ? token0Converted.sub(amount1).mulDiv(factor, ratio) : amount1.sub(token0Converted);
uint256 amountOut;
uint256 amountIn = isToken0Excess
? excessAmount.mulDiv(ratio, price.add(ratio))
: excessAmount.mulDiv(price, price.add(ratio));
```

UNKNOWN SWC-101 Arithmetic operation "*" discovered

This plugin produces issues to support false positive discovery within MythX.

Source file
/contracts/vault.sol
Locations

```

token0AfterSwap = isToken0Excess
? amount0.sub(amountIn)
: amount0.add(amountOut);
```

UNKNOWN

SWC-101

Arithmetic operation "**" discovered

This plugin produces issues to support false positive discovery within MythX.

Source file

/contracts/vault.sol

Locations

```

} else {
mintLiquidity(
_lowerTick,
_upperTick,
```

UNKNOWN

SWC-101

Arithmetic operation "**" discovered

This plugin produces issues to support false positive discovery within MythX.

Source file

/contracts/vault.sol

Locations

```

} else {
mintLiquidity(
_lowerTick,
_upperTick,
_liquidityForAmounts(
```

UNKNOWN

SWC-101

Arithmetic operation "+" discovered

This plugin produces issues to support false positive discovery within MythX.

Source file

/contracts/vault.sol

Locations

```
accruedProtocolFees1 = accruedProtocolFees1.sub(amount1);
if (amount0 > 0) token0.safeTransfer(to, amount0);
if (amount1 > 0) token1.safeTransfer(to, amount1);
}
```

UNKNOWN

SWC-101

Arithmetic operation "%" discovered

This plugin produces issues to support false positive discovery within MythX.

Source file

`/contracts/vault.sol`

Locations

```
/// @dev Callback for Uniswap V3 pool.
function uniswapV3SwapCallback(
int256 amount0Delta,
int256 amount1Delta,
bytes calldata data
) public override {
```

UNKNOWN

SWC-101

Arithmetic operation "%" discovered

This plugin produces issues to support false positive discovery within MythX.

Source file

`/contracts/vault.sol`

Locations

```
int256 amount1Delta,
bytes calldata data
) public override {
require(msg.sender == address(pool));

if (amount0Delta > 0)
```

LOW

SWC-103

A floating pragma is set.

The current pragma Solidity directive is "">=0.7.5"". 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/vault.sol`

Locations

```
pragma solidity >=0.7.5;
pragma abicoder v2;
```