MythX

REPORT 5F562488D144D30018DC0CE9

Created Mon Sep 07 2020 12:16:08 GMT+0000 (Coordinated Universal Time)

Number of analyses 1

## REPORT SUMMARY

| Analyses ID | Main source file | Detected vulnerabilities |
|---|---|---|
| 3c64bdd6-3cbf-4beb-ba63-bf5355009d5f | browser/Octo_Yield.sol | 2 |

Analysis 3c64bdd6-3cbf-4beb-ba63-bf5355009d5f MythX

| | |
|---|---|
| Started | Mon Sep 07 2020 12:16:10 GMT+0000 (Coordinated Universal Time) |
| Finished | Mon Sep 07 2020 13:01:21 GMT+0000 (Coordinated Universal Time) |
| Mode | Deep |
| Client Tool | Remythx |
| Main Source File | Browser/Octo_Yield.Sol |

## DETECTED VULNERABILITIES

| HIGH | MEDIUM | LOW |
|---|---|---|
| 0 | 1 | 1 |

## ISSUES

MEDIUM

SWC-128

### Loop over unbounded data structure.

Gas consumption in function "triggerWithdrawAll" in contract "YieldContract" depends on the size of data structures or values that may grow unboundedly. If the data structure grows too large, the gas required to execute the code will exceed the block gas limit, effectively causing a denial-of-service condition. Consider that an attacker might attempt to cause this condition on purpose.

Source file

browser/Octo_Yield.sol

Locations

```
631 // Helper function to release everything
632 function triggerWithdrawAll() public {
633 for (uint256 i = 0; i < lockBoxStructs.length; ++i) {
634 if (lockBoxStructs[i].releaseTime <= now && lockBoxStructs[i].balance > 0) {
635 withdraw(i);
```

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 "token" is internal. Other possible visibility settings are public and private.

Source file

browser/Octo_Yield.sol

Locations

```
530 contract YieldContract is YieldRoles {
531 using SafeERC20 for IERC20;
532 IERC20 token;
533
534 // Timeframe in which it it possible to deposit tokens
```