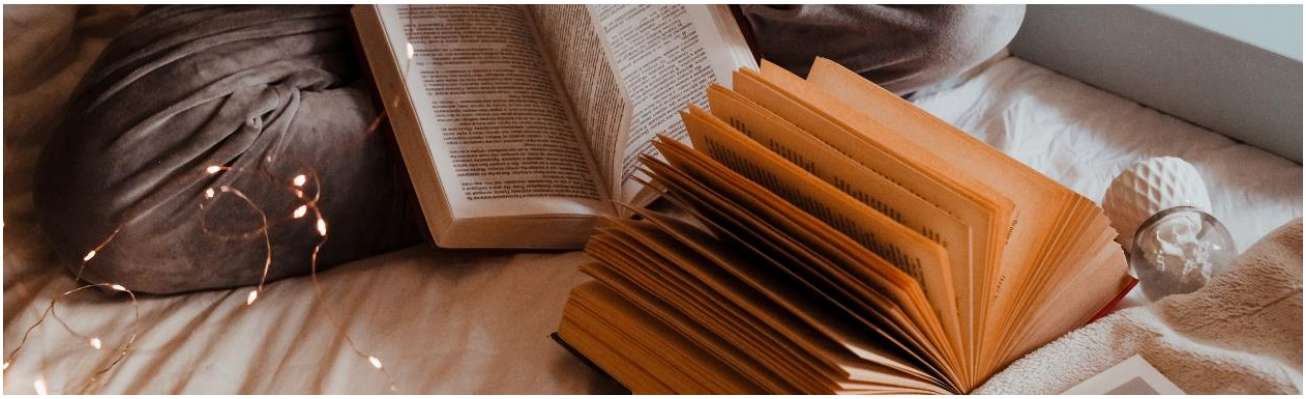

MythX Report
For Galxe Campaign Pool

Overview

Project Name	zkSwap Finance - Galxe Campaign Pool
Auditor	MythX.io
Source Code	https://github.com/ZkSwapFinance/galxe-lge
Mode	Deep
Time	Fri Jun 30th 2023
DETECTED VULNERABILITIES	**2 (Low Risk Issues)**

Summary

Done	Contract	High Risk Issues	Medium Risk Issues	Low Risk Issues
☑	ZFGalxePool.sol	0	0	2

Reference

MythX Passed Badge on Github mainnet-contracts ZkSwap Finance Mainnet contracts MythX passed	https://github.com/ZkSwapFinance/galxe-lge

MythX

REPORT 649E4AD5A9CECA001ABF33C3

Created	Fri Jun 30 2023 03:24:05 GMT+0000 (Coordinated Universal Time)
Number of analyses	1
User	648fc02af4bf584372592643

REPORT SUMMARY

Analyses ID	Main source file	Detected vulnerabilities
4c9277ab-af3a-43fe-8f46-657f6e89cc38	/farm/zfgalxepool.sol	2

Analysis 4c9277ab-af3a-43fe-8f46-657f6e89cc38 MythX

Started	Fri Jun 30 2023 03:24:08 GMT+0000 (Coordinated Universal Time)
Finished	Fri Jun 30 2023 04:09:20 GMT+0000 (Coordinated Universal Time)
Mode	Deep
Client Tool	Mythx-Vscode-Extension
Main Source File	/Farm/Zfgalxepool.Sol

DETECTED VULNERABILITIES

HIGH	MEDIUM	LOW
0	0	2

ISSUES

LOW

SWC-116

A control flow decision is made based on The block.timestamp environment variable.

The block.timestamp environment variable is used to determine a control flow decision. 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

/farm/zfgalxepool.sol

Locations

```
62
63  if (_amount > user.amount) {
64  _amount = user.amount;
65  }
66
67  lpToken.safeTransfer(address(msg.sender), _amount);
68
69  // Update user info
```

LOW

SWC-116

A control flow decision is made based on The block.timestamp environment variable.

The block.timestamp environment variable is used to determine a control flow decision. 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

`/farm/zfgalxepool.sol`

Locations

```
43 IERC20(lpToken).safeTransferFrom(
44 address(msg.sender),
45 address(this),
46 _amount
47 );
48 // Update user amount
49 user.amount = user.amount.add(_amount);
50 user.lastTimeAction = block.timestamp;
```