



MythX Report

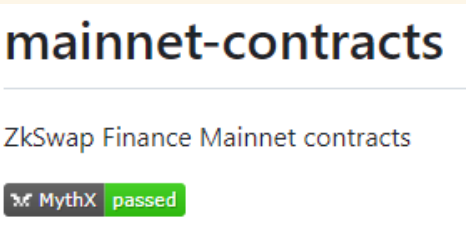
Overview

Project Name	zkSwap Finance
Auditor	MythX.io
Source Code	https://github.com/ZkSwapFinance/zf-periphery/tree/main/contracts/rewards
Mode	Deep
Time	Fri Dec 22 nd 2023
DETECTED VULNERABILITIES	2

Summary

Done	Contract	High Risk Issues	Medium Risk Issues	Low Risk Issues
<input checked="" type="checkbox"/>	ZFSwap2EarnRewarder.sol	0	0	2

Reference

ZFSwap2EarnRewarder.sol	Original MythX ZFSwap2EarnRewarder.pdf
<p>MythX Passed Badge on Github</p>  <p>mainnet-contracts</p> <p>ZkSwap Finance Mainnet contracts</p> <p>MythX passed</p>	https://github.com/ZkSwapFinance/zf-periphery

REPORT 65850142F1BCF1001A61D176




Created	Fri Dec 22 2023 03:23:46 GMT+0000 (Coordinated Universal Time)
Number of analyses	1
User	648fc02af4bf584372592643

REPORT SUMMARY

Analyses ID	Main source file	Detected vulnerabilities
107a3405-dac1-4c33-b319-6104b44d3fea	/vesting/zfswap2earnrewarder.sol	2

Started	Fri Dec 22 2023 03:23:50 GMT+0000 (Coordinated Universal Time)
Finished	Fri Dec 22 2023 04:09:16 GMT+0000 (Coordinated Universal Time)
Mode	Deep
Client Tool	Mythx-Vscode-Extension
Main Source File	/Vesting/Zfswap2earnrewarder.Sol

DETECTED VULNERABILITIES

 HIGH	 MEDIUM	 LOW
0	0	2

ISSUES

LOW

SWC-107

A call to a user-supplied address is executed.
An external message call to an address specified by the caller is executed. Note that the callee account might contain arbitrary code and could re-enter any function within this contract. Reentering the contract in an intermediate state may lead to unexpected behaviour. Make sure that no state modifications are executed after this call and/or reentrancy guards are in place.

Source file
/vesting/zfswap2earnrewarder.sol
Locations

```
126 | onlyOwner
127 | {
128 |     require(_cycleId < cycles, "editCycle: invalid cycleId");
129 |     merkleRoots[_cycleId] = _merkleRoot;
130 |
131 | }
```