



# **Code Security Audit Report**

For

**ChiliSwap**

Oct 24th 2023

# Table of Contents

## Summary

## Overview

Audit Summary

Result Summary

## Audit Result

ChiliSwap-01(Low): Pragma allows old versions(^0.4.18)

## About

## Summary

This report has been prepared for ChiliSwap to discover issues and vulnerabilities in the source code of the ChiliSwap project as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing Static Analysis and Manual Review techniques.

The auditing process pays special attention to the following consideration:

- Testing the smart contracts against both common and uncommon attack vectors.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

# Overview

## Audit Scope

Contract Name	ChiliSwapContract
Platform	Etherum
Language	Solidity
Code Base	<a href="https://github.com/ChiliSwap/chili-swap-contract">https://github.com/ChiliSwap/chili-swap-contract</a>
Commit	44683f475a6a9a5b531717d2b226bb5b7fc2952a

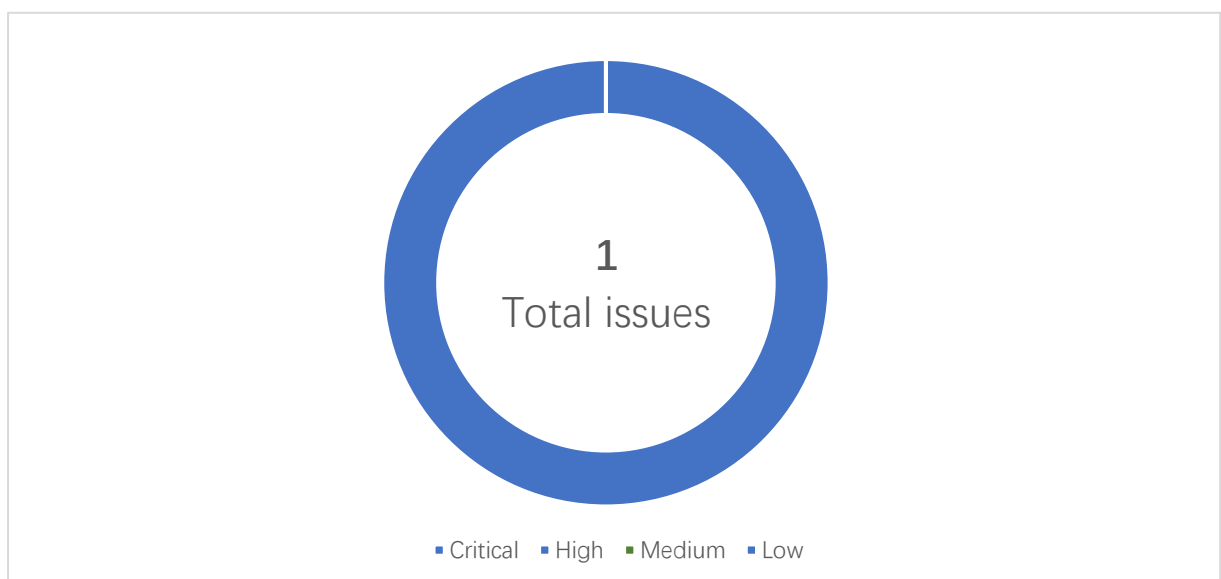
## Audit File Scope

ProjectERC721NFTMarket.sol	44683f475a6a9a5b531717d2b226bb5b7fc2952a
ProjectFactory.sol	44683f475a6a9a5b531717d2b226bb5b7fc2952a
ProjectFarm.sol	44683f475a6a9a5b531717d2b226bb5b7fc2952a
ProjectIFODeployer.sol	44683f475a6a9a5b531717d2b226bb5b7fc2952a
ProjectMerkleDistributor.sol	44683f475a6a9a5b531717d2b226bb5b7fc2952a
ProjectMulticall.sol	44683f475a6a9a5b531717d2b226bb5b7fc2952a
ProjectOracle.sol	44683f475a6a9a5b531717d2b226bb5b7fc2952a
ProjectPool.sol	44683f475a6a9a5b531717d2b226bb5b7fc2952a
ProjectProfile.sol	44683f475a6a9a5b531717d2b226bb5b7fc2952a
ProjectRolling.sol	44683f475a6a9a5b531717d2b226bb5b7fc2952a
ProjectRouter.sol	44683f475a6a9a5b531717d2b226bb5b7fc2952a
ProjectSimpleRewarderPerBlock.sol	44683f475a6a9a5b531717d2b226bb5b7fc2952a
ProjectTicket.sol	44683f475a6a9a5b531717d2b226bb5b7fc2952a
ProjectTicketFactory.sol	44683f475a6a9a5b531717d2b226bb5b7fc2952a
ProjectToken.sol	44683f475a6a9a5b531717d2b226bb5b7fc2952a
ProjectTrading.sol	44683f475a6a9a5b531717d2b226bb5b7fc2952a
ProjectWChain.sol	44683f475a6a9a5b531717d2b226bb5b7fc2952a
ProjectPegFactory.sol	44683f475a6a9a5b531717d2b226bb5b7fc2952a

## Result Summary

Vulnerability Level	Total	Pending	Solved	Acknowledged
Critical	0	0	0	0
High	0	0	0	0
Medium	0	0	0	0
Low	1	0	1	0

## Audit Result



### WChain-01 |Pragma allows old versions(^0.4.18)

Category	Severity	Location	Status
Incorrect Version	Low	ProjectWChain.sol:3	<b>Pending</b>

## Description

Solc frequently releases new compiler versions. Using an old version prevents access to new Solidity security checks. We also recommend avoiding complex pragma statement. However, the current version is not recommended.

## Recommendation

Deploy with any of the following Solidity versions:

- 0.8.18

The recommendations take into account:

- Risks related to recent releases
- Risks of complex code generation changes
- Risks of new language features
- Risks of known bugs

Use a simple pragma version that allows any of these versions. Consider using the latest version of Solidity for testing.

## About

Damocles is a 2023 web3 security company specializing in online security services, including smart contract audit, Product audit, penetration testing, GameFi security audit and cheat detection.

Main Web: <https://damocleslabs.com/>

Medium: <https://damocleslabs.medium.com/>

Twitter: <https://twitter.com/DamoclesLabs>

Email: [support@damocleslabs.com](mailto:support@damocleslabs.com)