FLR Finance

PriceFeedFtsoConnector Contract Audit

April 18, 2022

Common Prefix

Overview

Introduction

Common Prefix was commissioned to perform a security audit on a smart contract of Flr Finance:
https://github.com/flrfinance/smartcontracts/commit/f5569431ee9976679b9f3e0a6610361997100f6a .
The file inspected is `PriceFeedFtsoConnector.sol`.

Description of the contract

`PriceFeedFtsoConnector` is a small contract, only ~20LoC, which requests a token's USD price from the corresponding FTSO oracle contract of Flare Network. The updated price values are used in several contracts within the LoansStable project.

Disclaimer

Note that this audit does not give any warranties on the bug-free status of the given smart contracts, i.e. the evaluation result does not guarantee the nonexistence of any further findings of security issues. This audit report is intended to be used for discussion purposes only. Functional correctness should not rely on human inspection but be verified through thorough testing. We always recommend proceeding with several independent audits and a public bug bounty program to ensure the security of the project.

Findings Severity Breakdown

The findings are classified under the following severity categories according to the impact and the likelihood of an attack.

Level	Description

Critical	Logical errors or implementation bugs that are easily exploited and may lead to any kind of loss of funds
High	Logical errors or implementation bugs that are likely to be exploited and may have disadvantageous economic impact or contract failure
Medium	Issues that may break the intended contract logic or lead to DoS attacks
Low	Issues harder to exploit (exploitable with low probability), issues that lead to poor contract performance, clumsy logic or seriously error-prone implementation
Informational	Advisory comments and recommendations that could help make the codebase clearer, more readable and easier to maintain

Findings

Critical

None found.

High

None found.

Medium

MEDIUM-1	Sloppines on the precision of the price value
Contract(s)	`PriceFeedFtsoConnector.sol`
Status	**Resolved**

Description

Price values returned from the FTSO oracle are multiplied with PRECISION.

```
    IFtso public immutable ftso;
    uint public immutable PRECISION;

    constructor(address _ftso, uint _precision) {
        //...
        PRECISION = _precision;
    }

    function fetchPrice() external view override returns (uint) {
        (uint price,) = ftso.getCurrentPrice();
        return price * PRECISION;
    }
```

However, the returned price value is already considering precision of 5 decimals and this should be taken into consideration when constructing the contract.

Recommendation

We suggest fetching the decimal precision value of the FTSO contract at construction and set the PRECISION variable by subtracting it from the final desired precision (18 decimals throughout the FlareLoans project).

Alleviation

The issue has been resolved by the FLR Finance team. The updated contract can be found in https://github.com/flrfinance/price-feed-ftso-connector/commit/0fafb60a2baeccefb414a7f1b841eaa41a865d30 .

Low

None found.

About Common Prefix

Common Prefix is a blockchain research, development, and consulting company consisting of a small number of scientists and engineers specializing in many aspects of blockchain science. We work with industry partners who are looking to advance the state-of-the-art in our field to help them analyze and design simple but rigorous protocols from first principles, with provable security in mind.

Our consulting and audits pertain to theoretical cryptographic protocol analyses as well as the pragmatic auditing of implementations in both core consensus technologies and application layer smart contracts.