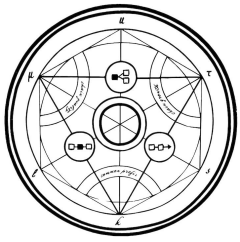
FLR Finance

FLRLoans Price-Feed Oracle Attack Post-Mortem

July 4th, 2022

Common Prefix



Post-Mortem

The post-mortem report was written by three members of the Common Prefix team and reviewed by the FLR Finance team.

Incident Response

The incident was handled by five members of the FLR Finance team and two members of the Common Prefix team.

Incident Overview

At the time of the incident, the FLRLoans protocol had one large, undercollateralized open nest with ~7.6 million EXFI of collateral and ~3.5 million CAND of debt, so a collateral ratio of ~80% at a market price of ~$0.37 per EXFI. The total collateral ratio of the protocol was thus ~80%, and its stability pool had a limited capital of ~$150,000 CAND.

As the protocol only had one big undercollateralized nest, if anyone opened a new nest, it would immediately 'absorb' the existing one. In other words, all the collateral and debt of this existing nest would be added automatically to the new one. The adversary opened a small nest that absorbed the big undercollateralized position.

Since the protocol's total collateral ratio was less than 150%, it was in *recovery mode*, meaning that no open nest could lower its collateral or increase its debt. Hence, even though the adversary's nest inherited the collateral and debt of the larger one, they could not do anything with it. Given that this large position was undercollateralized, paying off its debt to recover the underlying collateral would not be profitable.

To exit recovery mode, the price of EXFI had to exceed ~$0.7. An implementation error in the FLRLoans Price Feed oracle permitted the adversary to artificially inflate the price of EXFI to a high of ~$2.0 from the oracle's perspective. This action not only took the protocol out of recovery mode but also allowed the adversary to mint ~6.785 million CAND of 'bad' debt without forcing the system back into recovery mode.

Incident Timeline

On June 9th, at ~11:05 PM UTC, a small, sudden spike was observed in the Bitrue exchange's EXFI/USDT market activity, temporarily driving the price of EXFI up to ~0.55 USDT (from a stable price of ~0.41-0.44 USDT). At around the same time, similar activity occurred on the MEXC exchange's EXFI/USDT market, with an EXFI high price of ~0.47 USDT (similarly, from ~0.41-0.44 USDT). We suspect that the individual who controlled account `0xba1d` (whom we will refer to as *the adversary*) caused these momentary spikes to test the feasibility of the attack that they would carry out a few days later. However, there is no clear evidence to suggest that the adversary caused these price manipulations.

On June 11th, at 05:01 PM UTC, the adversary's account opened a nest in the FLRLoans protocol with 7,197.692 EXFI as collateral (worth ~$2,879 at $0.4 per EXFI) for 1,800 CAND debt.

At 7:55 PM UTC of the same day, the one remaining nest in the system with ~7,624,953.245 (~7.6 million) EXFI as collateral (worth ~$2,821,232 at $0.37 per EXFI) and 3,466,966.393 (~3.5 million) CAND of debt was liquidated (by what we believe to be a liquidation bot). The nest belonged to account `0x4c6f`.

The liquidated position's collateral and debt were redistributed to the adversary's nest, as it was the only open nest at the time. However, the adversary could not extract that EXFI in any way until the system was out of recovery mode. Exiting recovery mode required an EXFI price of ~$0.7, while the reported price was ~$0.37 at the time (yielding a collateral ratio of ~81.6%).

Between 11:20 and 11:30 PM UTC, the adversary bought at least ~$70,000 worth of EXFI (assuming that the adversary caused all of the trading volumes in that period) via the EXFI/USDT market on the Bitrue exchange. As a result of Bitrue's thin market, the price of EXFI, as reported by Bitrue, increased to as high as 4.43 USDT.

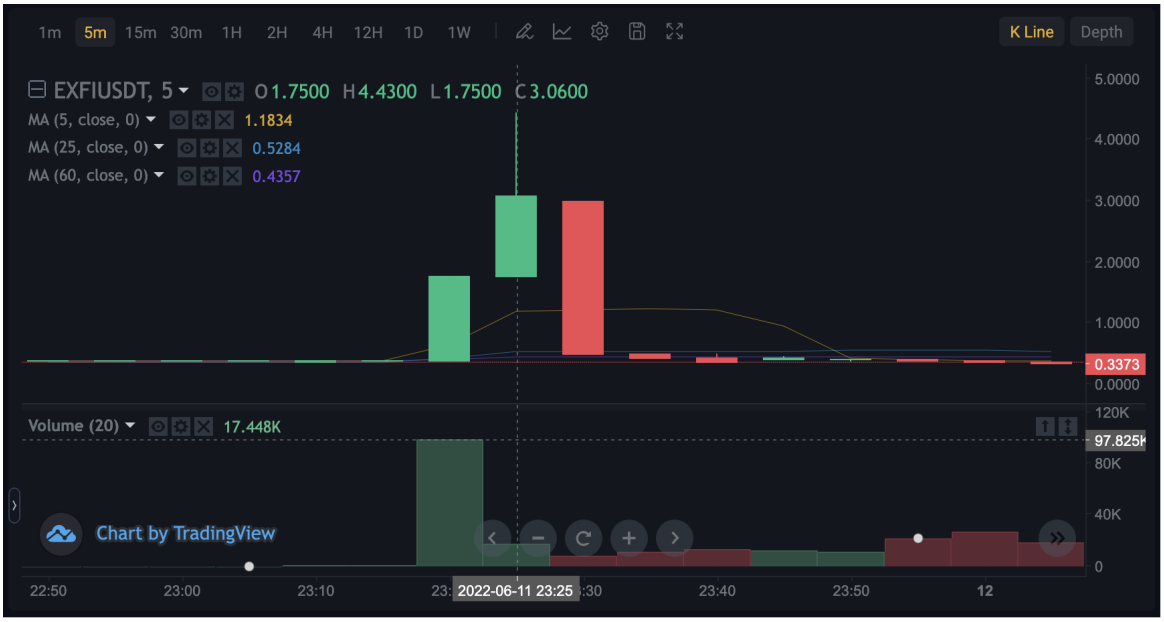


Figure 1: Large-volume trades temporarily inflated the EXFI market price on the Bitrue exchange.

The FLRLoans Price Feed should have used the exponential moving average (EMA) price calculation algorithm mentioned in Community Update 3. Instead, it erroneously provided the weighted average of the *real-time price* of EXFI (i.e., the price of the last trade) on the Bitrue and MEXC exchanges. This incident occurred because of a human implementation error in the off-chain Price Feed oracle's code that FLR Finance deployed before being audited.

As the off-chain oracle submitted the incorrect, inflated price on-chain, FLRLoans assumed a price of ~$2.03 per EXFI. The oracle calculated this number by taking the average between the price on Bitrue (3.5813 USDT) and the price on MEXC (0.486 USDT). Consequently, at about 11:30 PM UTC, the system came out of recovery mode, with the adversary's collateral ratio climbing to ~447%. The adversary was hence able to mint 6,784,988.95 (~6.785 million) CAND (effectively worth ~$6.785 million) from their nest (via three transactions, 1, 2, and 3) using the underlying ~8 million EXFI (momentarily worth ~$16.3 million) as collateral (which remained in the protocol). This new debt drove the collateral ratio of the adversary's nest down to ~150.87%, just enough to refrain the protocol from re-entering into recovery mode.

A timeline of the transactions that were performed during the attack has been documented in a spreadsheet.

Remediation Steps

Within 35 minutes after the attack, at ~12:05 AM UTC, the FLRLoans platform was disabled by the FLR Finance team (via two transactions, 1 and 2) to prevent any similar attacks from taking place. The protocol was disabled by updating the proxy contract to point to a logic contract that reverted on all relevant function calls.

Soon after, the adversary contacted an FLR Finance team member via a direct message on Discord (using the account *cryptoreturn123321*), and they willingly returned 5.5 million CAND tokens to the team. FLR Finance negotiated to have the remaining tokens returned in return for a bug bounty reward, but the adversary has yet to agree to those terms.

The adversary has been an active member of the FLR Finance ecosystem since its Songbird launch, with transactions dating back as early as September of 2021. They did not use a fresh wallet to perform the attack. FLR Finance has contacted its legal team to evaluate the possibility of taking legal action against the adversary. The team has not notified the authorities about the attack.

In the meantime, the FLR Finance team notified the community (via Twitter, at 1:57 AM UTC) and worked on ensuring that the FLRLoans Price Feed oracle returned the correct exponential moving average (EMA) price calculation of EXFI. The oracle fix was committed, audited, and deployed to production on June 14th, at 1:29 PM UTC. Under the correct EMA oracle implementation, the price manipulation attack would have resulted in a reported price of ~$0.66 rather than ~$2.03. The adversary's collateral ratio would have increased to 145.53% instead of 447.26%.

Damage Assessment

The attack left behind ~6.785 million CAND worth of bad debt in the FLRLoans protocol. The 5.5 million CAND the adversary returned has since been repaid, leaving a total of ~1,284,988.95 (~1.3 million) CAND worth of unhealthy debt. Therefore, all new positions will automatically absorb this debt until it has been fully repaid.

Additionally, the attack caused the CAND stablecoin to lose its peg, falling to as low as 0.48 USDT per CAND on the MEXC CAND/USDT trading pair.

Figure 2: The price of CAND on the MEXC exchange.

Had the adversary inflated the price of EXFI on the MEXC exchange, too, they would have been able to carry out an even larger attack by increasing the price reported by the Price Feed oracle even further. Given MEXC's substantial depth, price manipulation would have been more expensive for the adversary.

The CAND tokens that the adversary still possesses are theoretically worth ~$1.285 million, but there is not enough liquidity to directly trade it for the equivalent USD. Most of the adversary's CAND has been swapped for WSGB and EXFI, staked, or transferred to other accounts (some of which could be exchange wallets).

Since FLRLoans was disabled while the FLR Finance team worked on repairing the Price Feed oracle, users could not interact with their nests or open new ones during this time. Farming SFIN in the stability pool was the only component that remained operational. Before making FLRLoans fully functional again, FLR Finance partially restored the system to allow users who wanted to manage their nests or exit the platform to be able to do so safely.

Incident Causes

The major causes of the incident were:

- The incorrect calculation of price estimates based on erroneously averaged data.
- The deployment of incorrect code due to human error.

The contributing causes were:

- The system was in an unhealthy state, with a large, single undercollateralized nest.
- The stability pool had limited capital.
- The amount of capital across all nests in the protocol was limited.
- The liquidity of EXFI across exchanges was thin.
- The lack of unit and regression tests with significant coverage to ensure that all components are working as expected.
- The deployment of unreviewed and unaudited code. The oracle code changes were committed directly to the master branch without being reviewed via a pull request. The code was not audited before being deployed.

Security Roadmap

To avoid such an incident from reoccurring, the FLR Finance team is enforcing the following internal policies:

1. **Auditing & Testing**: Before any new code can be deployed to production, it will need to be *audited by an external auditor* and have a *testing coverage score of at least 95%*.
2. **Development & Deployment Procedures**: Code must go through a pull request with at least one approval and have a minimum of 95% testing coverage before being merged into the master branch. Only code in the master branch can be deployed to production.
3. **Tracking Deployments**: Every time a new deployment is made, the commit hash of the deployed code will be recorded in a document within the repo to keep track of the exact code that has made it to production.

In the meantime, FLR Finance is working closely with Common Prefix to get all the existing code audited and tested. The goal is to reach a minimum testing coverage score of 95% on the entire codebase.

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.