BlockSec Follow
Dec 3, 2020 · 3 min read · Listen

Loopring(LRC) Protocol Incident

The blog is published by BlockSec Team, Zhejiang University, China

In November 2020, lots of DeFi platforms in Ethereum encounters a security incident, such as Pickle Finance, 88mph.

To detect the security incidents that happened in DeFi, we developed the **ThunderForecast** system. When analyzing recent transactions, it discovers a class of transactions that are extremely suspicious. First of all, there exists a pair of trades, which has a trade rate difference of more than a thousand times. Secondly, the caller(EOA) can always gain a few Ether at the end of each transaction. We used the EthScope system developed by our research team to analyze these transactions and discovered that this is an attack leveraging a vulnerability of Loopring's vault protocol for the arbitrage purpose.

LRC Protocol Fee Vault

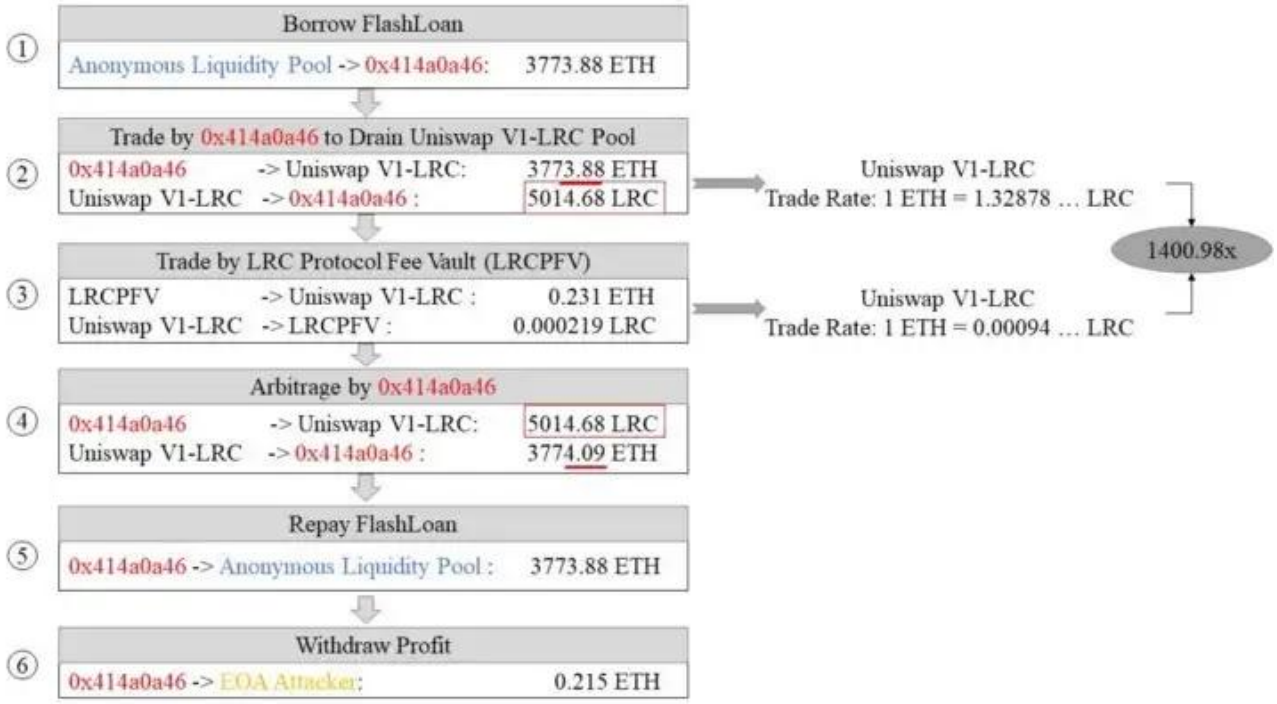
Loopring is an open-source protocol for decentralized exchange(DEX) on the Ethereum blockchain. Correspondingly, LRC is the token(ERC-20) of Loopring. Furthermore, Loopring has a specific vault protocol(LRC Protocol Fee Vault) to store protocol fee. We will use the short term LRCPFV for the analysis below.

```
function sellTokenForLRC(
        address token,
        uint    amount
        )
        external
        nonReentrant
    {
        require(amount > 0, "ZERO_AMOUNT");
        require(token != lrcAddress, "PROHIBITED");

        address recipient = tokenSellerAddress == address(0) ? owner : tokenSellerAddress;

        if (token == address(0)) {
            recipient.sendETHAndVerify(amount, gasleft());
        } else {
            token.safeTransferAndVerify(recipient, amount);
        }

        require(
            tokenSellerAddress == address(0) ||
            ITokenSeller(tokenSellerAddress).sellToken(token, lrcAddress),
            "SELL_FAILURE"
        );

        emit TokenSold(token, amount);
    }
```

`sellTokenForLRC` is a function in LRCPFV. This function allows users to swap the fee to the LRC token from the pool. However, there is no access control designed in `sellTokenForLRC` by their developer so that anybody can invoke this function. Finally, through leveraging this vulnerability, the attacker gains an opportunity to launch a series of attacks with the same logic. The details of the attack will be analysed below.

Details

We now start revealing more details of this attack with one attacking transaction 0x00b2c...



There are six steps involved :

- Step 1: Take a flash loan of **3773.88** ETH from 0xEB7e...
- Step 2: Swap **3773.88** ETH to **5014.68** LRC at Uniswap V1-LRC. And the rate in this trade is: **1** ETH = **1.32878** LRC
- Step 3: Swap **0.231** ETH fee stored at LRCFV to **0.000219** LRC at Uniswap V1-LRC pool by invoking `sellTokenForLRC` (As mentioned previously, the attacker is not supposed to invoke `sellTokenForLRC`). However, based on the price calculation algorithm used at Uniswap V1-LRC, the price of LRC against ETH at Uniswap V1-LRC increases dramatically. And this rate of this trade is: **1** ETH = **0.00094** LRC
- Step 4: Swap **5014.68** LRC to **3774.09** ETH at Uniswap V1-LRC. Based on step 3, only a few of LRC is swapped at Uniswap V1-LRC. This action makes LRC more valuable against ETH at Uniswap V1-LRC. Therefore, compared to step 1, the attacker gets **3773.88** ETH by swapping **5014.68** LRC at Uniswap V1-LRC and gains extra **0.215** ETH as a profit
- Step 5: Return **3773.88** ETH flash loan
- Step 6: Send **0.215** ETH to attacker's address(EOA)

Gain & Loss

The transaction analysed above is launched on 13th Oct 2020. To calculate the rough but accountable gain and loss for both the attacker and victim, we utilize coingecko to obtain LRC's price, which is **0.0005175** ETH. On the other hand, LRCPFV.

The attacker manipulates the price in Step 4, and gain a profit of **0.215** ETH through two trades.

The scale of the attack

Based on the feature of the attack, we detect **3** deployed malicious contracts(0xa896..., 0x414a..., 0xd91d...) and **90** transactions launched by the attacker 0x81e8... since 9644449th block(where LRCPFV is deployed (The largest profit gained in transaction 0x33eab... even reaches 9.89 ETH.). In the end, the attacker arb out a total of 80.97 ETH, which is equivalent to 48,849.2 USD based on the price on 1st Oct 2020.

The end

With the development of DeFi eco-system in Ethereum, various security problems are gradually pop out. However, the community might easily be attracted by an attack causing a vast financial loss instead of some inconspicuous attacks. In fact, the root cause, which is **access control**, behind the attack also causes a considerable loss(80.97ETH) for Loopring through launching 90 transactions.

Timeline

- 2020/11/30： Suspicious transactions were found.
- 2020/12/01: Finished the analysis.
- 2020/12/02: Reported to loopring.
- 2020/12/03: Vulnerability was confirmed and the fix is online.
- 2020/12/03: Details were released.
- 2021/01/03: CVE-2020–35962 is assigned.

Defi Loopring Attack

Connect with BlockSec Team

Your email

Subscribe