Pancake Bunny遭遇闪电贷攻击

背景

简介：基于BCS链的DeFi收益聚合器Pancake Bunny Finance损失了4500万美元。这是由于使用了PancakeSwap来检索PancakeSwap流动性提供者价格的协议中的一个错误。8笔闪电贷被用来操纵各种PancakeSwap池的价格，从而从VaultFliptoFlip保险库中创建了Bunny的倾斜计算。这导致了铸造了697000个Bunny代币，然后被出售，导致价格从146美元跌至6美元。

PancakeBunny的代币发行方式是，每产生1BNB的税费，即发行10BUNNY分配给相应用户。

慢雾科技认为关键点在于WBNB-BUNNY LP的价格计算存在缺陷，而BunnyMinterV2合约铸造的BUNNY数量依赖此存在缺陷的LP价格计算方式，最总导致了攻击者利用闪电贷操控了WBNB-BUNNY池子从而拉高了LP的价格。使得BunnyMinterV2合约铸造了大量的BUNNY代币给攻击者。

分析

术语

流动资金矿池：流动性指的是一种资产转换成另一种资产的容易程度，而不会对价格产生太大影响。AMM平台通过智能合约将资金汇集到一个流动性池，以促进去中心化交易、借贷和其他金融功能。对于Uniswap或PancakeSwap这样去中心化的交易所，流动资金矿池使平台能够平稳运行。
流动性提供者和LP代币：鼓励流动性提供者向流动性矿池提供资产，以便可以轻松地在平台上交易代币。 例如，通过矿池内交易产生的部分费用可用于“偿还”流动性提供者。 此外，当流动性提供者向资产矿池中投入资产时，AMM平台将自动生成LP代币，然后该LP代币也可用于其他功能（在其本机平台或其他DeFi应用程序上），以便流动性提供者甚至可以收到更高的回报。
自动做市商AMMs: 尽管并非所有去中心化交易所都是AMM平台，但一些最受欢迎的DEX还是。 AMM平台允许使用编程的流动资金矿池而不是将买卖双方聚集在一起的传统订单簿来自动进行加密货币交易。

攻击过程

攻击利用了两个东西：闪电贷款，和DeFi平台上的软件漏洞。

1. 为了发起攻击，先将价值一个BNB的USDT存入Bunny的USDT-WBNB Vault，进行一次抵押，产生了9.725个LP代币的抵押奖励。

```
function getReward() external override {
    uint amount = earned(msg.sender);
    uint shares = Math.min(amount.mul(totalShares).div(balance()), _shares[msg.sender]);
    totalShares = totalShares.sub(shares);
    _shares[msg.sender] = _shares[msg.sender].sub(shares);
    _cleanupIfDustShares();

    amount = _withdrawTokenWithCorrection(amount);
    uint depositTimestamp = _depositedAt[msg.sender];
    uint performanceFee = canMint() ? _minter.performanceFee(amount) : 0;
    if (performanceFee > DUST) {
        _minter.mintForV2(address(_stakingToken), 0, performanceFee, msg.sender, depositTimestamp);
        amount = amount.sub(performanceFee);
    }

    _stakingToken.safeTransfer(msg.sender, amount);
    emit ProfitPaid(msg.sender, amount, performanceFee);
}
```

2. 用闪贷从7个Pancake Swap矿池中借了230万BNB（7.04亿美元），并从ForTube Bank借了290万USDT。

The first seven flashloans are taken from various PancakeSwap pools while the last comes from Fortube Bank.

1.05M WBNB from WBNB+CAKE pool

522.52K WBNB from WBNB+BUSD pool

210.16K WBNB from WBNB+ETH pool

133.50K WBNB from WBNB+BTCB pool

241.02K WBNB from WBNB+SAFEMOON pool

98.519K WBNB from WBNB+BELT pool

66.29K WBNB from WBNB+DOT pool

2.96M USDT from Fortube Bank.

3. 向PancakeSwap USDT-WBNB矿池中再存入7,700 BNB和290万USDT的流动性，获得了14.4万LP代币。
4. 通过PancakeSwap USDT-WBNB V1矿池将230万BNB兑换为USDT提走，池子BNB的注入，而池中USDT数量显著减少。
5. 因为在Pancake Swap USDT-WBNB矿池中还有额外LP代币，Bunny Finance认为，该「开采者」（攻击者）已向系统中添加了大量BNB，从而开始印制奖励的700万Bunny代币的资金（10亿美元）。调用 getReward() 从 VaultFlipToFlip 领取奖励。凭借较高的 LP 代币估值，攻击者能够获得 697 万 BUNNY 的奖励（价值约 1 美元+ B）。请注意，开发团队会获得单独的 1.05M BUNNY。

```
function getReward() external override {
    uint amount = earned(msg.sender);
    uint shares = Math.min(amount.mul(totalShares).div(balance()), _shares[msg.sender]);
    totalShares = totalShares.sub(shares);
    _shares[msg.sender] = _shares[msg.sender].sub(shares);
    _cleanupIfDustShares();

    amount = _withdrawTokenWithCorrection(amount);
    uint depositTimestamp = _depositedAt[msg.sender];
    uint performanceFee = canMint() ? _minter.performanceFee(amount) : 0;
    if (performanceFee > DUST) {
        _minter.mintForV2(address(_stakingToken), 0, performanceFee, msg.sender, depositTimestamp);
        amount = amount.sub(performanceFee);
    }

    _stakingToken.safeTransfer(msg.sender, amount);
    emit ProfitPaid(msg.sender, amount, performanceFee);
}
```

6. 然后，攻击者出售了480万Bunny代币获得230万美元的WBNB和290万美元的USDT，然后用来偿还第2步中借入的闪电贷款。

结论

此次事件的最大受害者是BUNNY。凭空创造了700万枚BUNNY代币，现有代币被稀释，使BUNNY的价格下跌，由于BUNNY代币在市场上的销售，BUNNY的流动性已被彻底破坏。

本次攻击事件中，攻击者在一笔交易中完成了一系列借用、兑换、获取奖励、归还闪电贷等操作，主要原因还是在项目计算抵押奖励时获取lp价格出现了逻辑问题，导致黑客进行了一系列利用。

参考链接

https://www.bihai123.com/info/ywqkl/15364.html

https://new.qq.com/omn/20210520/20210520A0E74700.html