**Popsicle Finance Bug**

Popsicle finance is an investment platform that acts and liquidity provider at several liquidity pools and manage to optimize gained fees for the benefit of the investor. The protocol had a bug that led to 25M$ loss of funds.

In short, the bug is that the popsicle finance team forgot to override their default ERC20 transfer function, which decrease tokens for user and increase tokens to user . The problem was that every user had different amount of fees to collect, depends on the time he invests at the platform.

This bug let an investor that just join and buy shares, transfer its shares to a friend that joint an year ago and can collect fees per share but had only one share. Now the fried can collect the fees reward for the tokens that he now holds. Which is a bug since this user deserve fees per share only for its share and not for the shares its friend sent him.

The way popsicle finance records the fees the user can collect is by two fields:

* **Popsicle debt field** (in the code “token0Rewards” / “token1Rewards”) – this field is not “per share” but is how much popsicle finance owns this user for different reasons. One reason might be a withdraw without claiming the earned fees.
* **Fees earned per share** **paid** (in the code “token0PerSharePaid” / “token1PerSharePaid”) – Popsicle finance would rather prefer to maintain the field **Fees earned per share**, which is how many fees are earned for this user per share from the day it entered.   
  But, since maintaining this field requires update for all users at every earn – it costs a lot of gas. Therefore, we add the “**paid”** and actually   
    
  That means we only maintain the fees earned at the day we enter and at the time we collect the fees we get the difference per share and update this field to the current fees earned.

At deposit the popsicle finance code put the total earned by the user at the dept field and update **Fees earned per share** **paid** to the current earned fees per share which is correct for the new deposited shares.

But at transfer the popsicle finance team forgot doing that, and just transferred the tokens and let the user to claim the fees per share for much larger amount of tokens.

To fix the bug – follow at transfer the same logic as in deposit and update the **Fees earned per share** **paid** into a valid value.

Another bug that the attacker exploited, allows him not to have this friend who invested a year ago, but send the tokens to an address that not exists – and therefore its **Fees earned per share** **paid** is at the initial value which is 0. So, the attacker claim fees per share earned from the very beginning of the popsicle finance platform.

**This summary is written assuming the attacker is a man, although I don’t know if it’s true.**