Referendum #164 ▸ Treasury #27

Immunefi report payout - Malicious users will steal LP shares cross-pool from liquidity-mining depositors

Jak-Pan · Treasurer · 4mos ago · 1

Executed

We have received a report via Hydration Immunefi bug bounty programme, labeled as "Critical", titled "Malicious users will steal LP shares cross-pool from liquidity-mining depositors".

Immunefi report summary:

```
A confused-deputy / cross-pool unlock in the withdrawal path will cause a direct loss of LP shares for LPs whose
```

We evaluated the report and acknowledged the severity of the vulnerability. The Technical Committee paused share withdrawals from XYK liquidity mining and performed a runtime upgrade with a fix. After the upgrade, the Technical Committee unpaused the share withdrawals and restored the full functionality of XYK liquidity mining.

The vulnerability

The root cause of the vulnerability was the missing validation of the `AssetPair` provided by the user. In XYK liquidity mining, the `AssetPair` is used to derive the `amm_pool_id`, which identifies the AMM pool and determines which LP shares to unlock.

The fix

We added a cross-check between the `amm_pool_id` derived from the `AssetPair` and the `amm_pool_id` saved in the `deposit`.

```
ensure!(amm_pool_id == deposit.amm_pool_id, Error::<T, I>::AmmPoolIdMismatch);
```

https://github.com/galacticcouncil/hydration-node/commit/2fb7430d615c4c50a6905c8218b01649423714f7

Economic assessment

At the time of the report, there were 2 XYK pools with farms running, this would make this attack possible to perform. The attacker would need to accrue "lower valued shares" from DOT<>MYTH pair and join LM to be able to extract "higher valued shares of DOT<>EWT". By doing so, he would lock these shares forever.

There is roughly 200k$ worth of DOT <> EWT in LM. We have calculated that an attacker would need to accrue roughly 40k$ worth of DOT <> MYTH to empty DOT <> EWT pool not considering the slippage and other problems attacker would face with low liquidity pools, it is safe to say the total NET extracted value would be under 200k$.

As such, minimum payout for “Critical” issue is 20k$ under our Immunefi bug bounty programme paid out in HDX with 7 day EMA price of 0.0088

Edited

Request

≈ 2.27M HDX

Status

Decision	7d
Confirmation	12hrs
Attempts	1

Tally

99.4% Aye	50.0% Threshold	0.6% Nay

Aye (255)	≈ 1.54B HDX
Nay (10)	≈ 9.87M HDX

0.0%	0.0% Threshold	14.2%

Support 11.4%	≈ 507.65M HDX
Issuance	≈ 4.46B HDX

Votes Nested Flattened Actions

Check how referenda works **here**.

Call **Metadata** **Timeline** 6 **Votes Bubble** **Curves** **Statistics**

Proposal Hash	0xd49dc36e1209a926b285c4e9061be46544a6e8dffa850d4cbae101707dd9a709	
Call	Treasury SpendLocal	
Request	≈ 2.27M HDX to 0x005A...9e22	immediately

Comments

Filter 1

0x005A...9e22 4mos ago

Thanks for the bug bounty

Reply Up

Login