Multi-Strategy Vault Post-Mortem

It's the margins where smart contracts get exploited - those tiny percentage points between *high confidence* and ***absolute confidence.*** It was within these margins that, as we prepared for bed, approximately $1,700,000 was extracted from our Multi-Strategy vaults by an attacker. I'd like to start off saying that we are committed to returning user funds and will follow this post-mortem with a recovery plan after internal meetings. We were able to save approximately 10% of user funds by white-hatting our contracts and will redistribute those assets as soon as possible. Detailed writeup below:

On the evening of 8/1/2022, a hacker exploited our mis-implementation of the ERC-4626 interface to withdraw user funds into their account. It was a very simple mistake with dire consequences - validation of the receiver account was not accurate, allowing anyone to withdraw anyone else's funds. Considering the amount of scrutiny these vaults have had over the past couple of months, this exploit caught us way off guard and I will outline key factors below.

1. **Our team underestimated the nuance of ERC-4626**. After our security team pen-tested and secured our multi-strategy vaults, we decided to change the interface to abide by ERC-4626 standards. After the implementation was complete, we did not follow through with our security audit again and executed a typical code review. We should have respected this as a significant breaking change and put it through another internal audit.
2. **We confidently moved into production without 3rd party audits to back us up**. The contracts were still undergoing their external audit, and the time on our Pain.Finance staging environment was not enough to catch vulnerabilities. Our production testing also didn't discover the issue which leaves us with a lot of processes to scrutinize and improve upon.
3. **We did not advertise a new bug bounty for our Multi-Strategy crypts.** Though we have a 200k bounty available, we did not add our new crypts to its scope. This means our communications with the hacker were from a disadvantaged position, and we did not properly socialize the contracts within the hacker community. I believe a well-advertised bounty program would have resulted in this particular error being found before the exploit.

I believe any one of these failures would have resulted in the issue being found pre-exploit and will have a long series of meetings with our security engineers to ensure we mitigate risks of a future loss of funds occurring. This is a frustrating but recoverable event and we will meet internally and with advisors to determine a best path forward. We thank you for your patience.

Technical Breakdown:

User 0x5636e55e4a72299a0f194c001841e2ce75bb527a exploited our multi-strategies' lack of validation and drained user funds into their wallet. This was done in a rapid series of transactions on the Fantom network, most notable being https://ftmscan.com/tx/0xc929f3b9312ff26be0adb1c3ff832dbdafdcbcaad33d002744effd515e53c9d5.

This user's funds were bridged from Binance Smart Chain using O3 Network's cross-chain swap router. They received the BNB for this swap from Tornado cash, and https://tutela.xyz/ marks it 100% anonymous. We are exploring the possibility of tracking this user, but it's very unlikely it will yield results.

After the exploit, the user bridged funds to Ethereum to the following address: 0x2c177d20b1b1d68cc85d3215904a7bb6629ca954. The funds sat in that address for approximately 3 hours during which we white-hat hacked our vaults for the remaining assets and attempted to communicate with the attacker on the Ethereum blockchain. We waited in suspense for a response but never got one. The funds were promptly sent to Tornado Cash for laundering.

Suffice to say, this was not an acceptable outcome of our Multi-Strategy efforts. I'd like to apologize profusely to users affected by this exploit, and we will work on a recovery plan to ensure you are all made whole. We value the faith our community has put in us extremely highly and will not squander it. Expect further communication this week.