TL;DR

The Ethereum <> Harmony bridge has been exploited and as consequence, Aave V3 Harmony is potentially affected. We open this thread for the community to discuss and decide about different aspects, and for us (BGD) to help with all different technical details being/to-be considered.

Context

Around ~48h ago, an exploit was executed on the Harmony Horizon ERC20 bridge, allowing users on the Ethereum mainnet to bridge their assets to Harmony One.

~36h ago, the Harmony team publicly notified the existence of such an attack on the following tweet https://twitter.com/harmonyprotocol/status/1540110924400324608, certifying a loss on the bridge of approximately $100'000'000.

[

harmony-exploit-erc20

1920×723 116 KB

](https://europe1.discourse-cdn.com/business20/uploads/aave/original/2X/3/340dcd31338d06440b9f2d9cfff9daa6e52505a9.jpeg)

ERC20s exploited

Given that some of the assets exploited are listed on Aave V3 Harmony (specifically DAI, USDC, USDT, and AAVE), some dynamics of the protocol have been disrupted.

Aave on Harmony, same as on other networks, uses Chainlink as the main source of oracle prices. In order to consider the market-wide price (not only on/in-chain) of well-adopted assets, Chainlink reports/reported similar prices on the Harmony assets as on other networks: 1 USDC as ~1 USD, 1 ETH as ~ 1'155 USD, etc. This is expected behavior from Chainlink.

Going back to the Harmony bridge exploit, what this type of attack means in practice is that for X amount of an asset locked on a contract on Ethereum L1 there is not exactly

X supply of the bridged asset on the connected Harmony One chain, but X - Y locked, with Y being the exploited amount. Consequently, the X supply of the asset of Harmony One is backed only by X-Y assets, so it is trivial to understand that each unit of bridge asset has less value than it should and consequently lower price.

Some accounts on Aave V3 Harmony have taken advantage of this arbitrage opportunity, trusting that the assets on mainnet will not be restored back, making the potentially temporary price divergence, completely permanent. To execute this arbitrage on Aave some accounts (probably the attacker of the bridge, but not necessarily) did the following hours ago:

- They deposited one of the assets with currently less value (1USDC) enabled as collateral on Aave V3 Harmony.
- They borrowed assets not exploited: at the moment we can fully confirm ONE, but highly probable LINK too.

The key to this arbitrage is the price divergence on the "real" value of the bridged-exploited asset, compared with the value reported by the oracle, not aware of the exploit itself.

Current situation

At the moment, even if for the protocol the positions with USDC-collateral/ ONE-borrowed are perfectly healthy, in reality, if the assets backing the 1Tokens are not restored by any party on mainnet, they should be under liquidation. This creates an obvious problem for the Aave V3 Harmony pool, same as with any other instance, as one of the main requirements is that all positions under 1 HF should not be opened, and in this case, they factually are.

The specific nature of this problem leads to different aspects to be analysed before taking any decision, in parallel with other measures that can (have) be taken to protect as much as possible without creating potential harm.

What we are taking into account in the analysis is:

- The priority is to find solutions for all users (apart from people doing the aforementioned arbitrage) that could be affected, and keep protocol-wide health, meaning no bad debt.
- The market is currently under control of the community Guardian, elected by AAVE holders via Snapshot and strictly following the mandates from this forum and Snapshot. In our opinion, the red line to not cross for the Aave community

decisions should be doing “forced” modifications of an account position on Aave. Users are in full control of their funds.

- There are 1…N entities that maliciously did an arbitrage on Aave V3 Harmony. The system worked as intended and the community should not assume that the entities are the same as the bridge attacker. That being said, we think is legitimate to not try to protect the positions of these users, if they are indirectly affected by pool-wide protections.
- If funds of the bridge are not backed by return-of-funds or the Harmony Network itself, the Aave community should start an analysis and a discussion if the Safety Module was supposed to cover Aave V3 Harmony or not yet.

Potential actions in consideration

(In no particular order or priority)

1. Modification of oracles pool-wide.

This would be executed by forcing a “real” price of unbacked assets on the price feeds, via Chainlink or not. At the moment, the real price of the assets, as there is barely backing, is close to 0. Given that is not really possible to understand if the situation is permanent or not, this is a really extreme measure that actually will not help the pool: almost all positions would get instantaneously liquidated, but liquidators will probably not act, as collateral would not be liquid. Given the potential complexity of this, probably not advisable.

1. Minimize interest rates range, especially the ones on assets fully borrowed on the arbitrage.

Currently, ONE and LINK reserves are fully borrowed out, but this is because of the aforementioned arbitrage. What this means is that dynamics of interest rates to incentivize/de-incentivize assets’ entries/exits are not really applicable. In addition, the biggest borrowers of ONE are the arbitrators using un-backed assets as collateral, so if we assume the debt of those positions will not be repaid, this is only creating more potential protocol bad debt. We suggest reducing interest rates ranges to the minimum until the situation normalizes, as it can’t do any harm, but can save some minimal accruing of bad debt (we calculated in the order of approx. 30’000 USD per day).

1. Fully freeze the market, allowing only withdrawals and liquidations.

This is something to consider, but probably not a good idea at the moment. The rationale is that once borrowing of everything has been stopped, new deposits can’t be arbitraged by borrowing, but keeping the “door” open for the refilling of collateral or any protocol-wide intervention via deposit/injection of liquidity can be important.

1. Understand the probability of the Harmony network covering the unbacked assets, via recovering the funds or by covering the loss.

This is straightforward: if the attacker would return the funds to the bridge or the Harmony network itself would cover those assets, the Aave V3 Harmony pool would be completely fine.

1. Integration of Chainlink’s Proof-of-Reserve for bridged assets.

BGD had already introduced on its roadmap a proposal to integrate the Proof-of-Reserve into the Aave pools, but an event like that shows the need of it.

Actions executed

- Stop of borrowing on all assets of the pool

. Arbitrage by borrowing non-affected assets was the main vector on Aave V3 Harmony, we have recommended stopping borrowing of all assets, making the situation more controllable without doing any harm in the process.

- Coordination with Chainlink about historic oracle price last 24h

. As expected after our validations, Chainlink has confirmed that their oracle has been working as expected.

- Data analysis of everything surrounding Aave V3 Harmony and the exploit

.

Miscellaneous data/links

- Harmony Bridge: https://etherscan.io/address/0x2dccdb493827e15a5dc8f8b72147e6c4a5620857
- Exploiter: https://etherscan.io/address/0x0d043128146654c7683fbf30ac98d7b2285ded00
- Disclosures by the Harmony team:

- https://medium.com/harmony-one/harmonys-horizon-bridge-hack-1e8d283b6d66
- https://mobile.twitter.com/harmonyprotocol/status/1540110924400324608
- https://medium.com/harmony-one/harmonys-horizon-bridge-hack-1e8d283b6d66
- https://mobile.twitter.com/harmonyprotocol/status/1540110924400324608
- Aave V3 Harmony market https://app.aave.com/markets/?marketName=proto_harmony_v3
- The total market size of Aave V3 Harmony is ~$3'100'000 of which ~$1'560'000 is borrowed out.
- There is close to 100% utilization on ONE and LINK. ONE borrowings (~$1'220'000) accounting for ~78% of the total borrowings of the pool.
- Out of the ~$1'1180'000 ONE borrowed out, ~$398'000 were initiated after the Harmony bridge was exploited, by 25 different accounts.
- $438'000 of ONE+LINK has been borrowed out after the attack.
- If funds on the bridge would be restored, the bad debt of the Aave V3 Pool would be of approx. borrowings of LINK + borrowings of ONE = ~$40'000 + ~$1'180'000 = $1'240'000. It is important to highlight that this is LINK/ONE debt-denominated.
- There are ~1'900 active positions on Aave V3 Harmony.

Next steps

- From BGD we will keep monitoring the situation and adding information in this thread whenever there are updates, especially related to any remediation taken by the Harmony network.