Summary

Today 4th November 2023, we received a report on the Aave bug bounty program about a high vulnerability affecting Aave v2, which afterwards was raised to a critical.

After some coordination with the Aave Guardian, protection measurements that completely stop the attack vector on the whole Aave protocol have been applied, and all Aave pools are perfectly safe

.

The reported vulnerability

Currently, all Aave pools are protected with the measures taken, but given Aave v2/v3 is a protocol “forked” by multiple third parties, we don’t think it is responsible to give full details of the vulnerability yet.

However, to provide maximum tranquility and transparency to the community, we have compiled the following FAQ.

What pools were affected by the vulnerability?

Some assets of Aave v2 Ethereum and Aave v3 Optimism/Arbitrum/Avalanche/Polygon were potential targets of the attack vector.

What exactly is the vulnerability?

As commented before, we don’t think it is responsible to disclose the details surrounding the vulnerability, but we can say that by disabling stable rate mode borrowing, it is not exploitable

.

Was the vulnerability exploited?

No, we simply received a bug report and protected against it.

Any funds at risk?

There are no funds at risk at the moment.

What are the next steps?

1. We are creating a governance proposal to remove the current freezing protections, and apply a more specific one: disable the stable rate mode for all assets which have it.

2. In parallel, we are designing a plan for the unpausing of the affected pools.

Once we think it is responsible, we will publish an extensive explainer of the vulnerability and how was the course of action from disclosure to fix.

Updates

→ Nov 8th

For transparency with the community, now that all the major planned governance proposals of protection remediation have been created, the estimated timeline for every item is the following.

IMPORTANT

.

- This assumes the community votes for YES on all the proposals.

- Due to how governance proposals work, execution timing can vary slightly, but in the order of low hours/minutes.

Proposal 358 Disable Stable Borrows

- Created

: November 04,10:30 PM UTC

- Estimated execution time

: November 10, 15:18 UTC

- The goal was?

: the first line of protection, stopping the reported vulnerability

- What unblocks?

: in practice nothing; v2 Ethereum will keep being paused as the following proposals are required before unpausing (for security reasons).

Proposal 359 Multichain Stable Debt Token Upgrades

- Created

: November 06, 2023, 09:30 PM UTC

- Estimated execution time

: November 12th, 2023, 07:30-09:30 PM UTC

- The goal was?

: full protection for the vulnerability of all assets being upgraded

- What does it unblock?

: it will be possible to unpause all assets on v3 Polygon, v3 Avalanche, v3 Optimism and v3 Arbitrum. CRV on v3 Polygon can’t be unpaused.

Proposal 361 Liquidations Grace Sentinel Activation

- Created

: November 07, 2023, 05:20 PM UTC

- Estimated execution time

: November 13th, 2023, 03-20-05:20 PM UTC

- The goal was?

: activation of the Liquidations Grace Sentinel feature for Aave v2, which risk providers can recommend using to give a grace period for previously paused assets. Additionally, upgrading implementation of extra v2 Ethereum assets and CRV on v3 Polygon.

- What does it unblock?

: Full return to operations on all pending Aave instances and assets (v2 Ethereum and CRV on v3 Polygon). If the risk providers recommend adding a liquidations grace period for any asset, the unpause of v2 Ethereum will happen just after that grace period for that specific asset only.

→ Nov 10th

As an update for the community, proposal 358 has been executed early today, following the timeline. This doesn’t create any meaningful effect on users, as all affected assets are still paused.

The next event will be on Sunday November 12th, 2023, 07:30-09:30 PM UTC

, when assets on v3 Optimism/Arbitrum/Optimism/Polygon will be unpaused.

P.S. To keep clarity on this highly populated thread, we will move all BGD updates to the 1 post, with the time of publication.

→ Nov 11th

An update for the community, proposal 359 has entered into the last timelock of 24 hours and will be ready for final execution on all networks tomorrow Sunday, 12th.

As previously described, this will mean the following:

- All assets on Aave v3 Polygon, Arbitrum, Optimism, and Avalanche will be eligible for unpause by the Guardian

.

- The unpause by the Guardian will happen slightly later than the final proposal execution.

We will try to support them to be as close as possible once the proposal has been executed on each network.

- Aave v3 has no Liquidations Grace Sentinel, so immediately after unpause, all operations will re-start.

We recommend users closely monitor their positions if they need to take any actions on the unpaused assets.

- Aave v2 Ethereum and CRV on Aave v3 Polygon will remain paused for 1 day more

.

The estimated execution times for each payload (automated by Aave Robot) are the following:

Polygon

14:25 UTC

Optimism

14:04 UTC

Arbitrum

14:17 UTC

Avalanche

14:08 UTC

Unpausing can happen anytime after execution, whenever the Guardian can process the transaction.

→ Nov 12th

All Aave v3 instances (Arbitrum, Avalanche, Optimism, Polygon) have been unpaused by the Aave Guardian, after the successful execution of proposal 359.

Depending on operational aspects (recommendations of grace periods, and Guardian coordination), v2 Ethereum is estimated for tomorrow morning UTC, earlier than initially communicated due to block times on voting.

→ Nov 13th

As an update to the community, the liquidations grace period on Aave v2 Ethereum has been set by Guardian to 14:30 UTC , slightly more than the 3 hours recommended by risk providers from now.

Unpause of v2 Ethereum will follow, which will mean that v2 Ethereum will be fully operational again, but users with WETH will have a 3-hour grace period to protect their positions.

→ Nov 13th

Aave v2 Ethereum has been unpaused by the Aave Guardian. Again, if you are a WETH user, it is possible to protect your position.

→ Nov 16th

As the last step in the set of planned actions, we can confirm that Guardian has unpaused CRV on Aave v3 Polygon.

This means that all Aave v2 and v3 pools operate normally, without exception.