Exploiting Unverified Control of Organization Namespaces on Hugging Face

Report ID: 2737165

Hugging Face Response

- There doesn't seem to be any significant security impact so we will be closing this report as informative.
- If you can leverage this into a practical exploitation scenario, we will be happy to reevaluate this report.
    - My comment on this – Like backdooring a model?!?!?! As the org admin this would be trivial. Moving on.
- This will not have any impact on your Signal or Reputation score. We appreciate your effort and look forward to seeing more reports from you in the future.