Do not trust all actions, they are created by anyone.

Your pipeline has critical deploy information, be aware of what kind of actions you use.

Don’t trust third party GitHub Actions

The Evil GitHub Actions!

CodeCov: https://www.wolfe.id.au/2021/04/26/github-actions-supply-chain-attacks/

The Evil GitHub Actions!

- Do not trust all actions, they are created by anyone.
- Your pipeline has critical deploy information, be aware of what kind of actions you use.

Don’t trust third party GitHub Actions

CodeCov:
https://www.wolfe.id.au/2021/04/26/github-actions-supply-chain-attacks/

The mighty CI BOT

- Is your CI/CD executed as root?
- There is only one all mighty bot user?
- Your bot user has admin permissions over production?

Unchecked Privileges: https://portswigger.net/daily-swig/unresolved-github-actions-flaw-allows-code-to-be-approved-without-review