```
# Dependency Review Action
#
# This Action will scan dependency manifest files that change as part of a Pull Request,
# surfacing known-vulnerable versions of the packages declared or updated in the PR.
# Once installed, if the workflow run is marked as required, PRs introducing known-vulnerable
# packages will be blocked from merging.
#
# Source repository: https://github.com/actions/dependency-review-action
# Public documentation:
https://docs.github.com/en/code-security/supply-chain-security/understanding-your-software-supply-
chain/about-dependency-review#dependency-review-enforcement
name: 'Dependency review'
on:
  pull_request:
    branches: [ "master" ]

# If using a dependency submission action in this workflow this permission will need to be set to:
#
# permissions:
#   contents: write
#
#
https://docs.github.com/en/enterprise-cloud@latest/code-security/supply-chain-security/understandi
ng-your-software-supply-chain/using-the-dependency-submission-api
permissions:
  contents: read
```

```
  # Write permissions for pull-requests are required for using the `comment-summary-in-pr` option, comment out if you aren't using this option
  pull-requests: write

jobs:
  dependency-review:
    runs-on: ubuntu-latest
    steps:
      - name: 'Checkout repository'
        uses: actions/checkout@v4
      - name: 'Dependency Review'
        uses: actions/dependency-review-action@v4
                                                # Commonly enabled options, see https://github.com/actions/dependency-review-action#configuration-options for all available options.
        with:
          comment-summary-in-pr: always
        #   fail-on-severity: moderate
        #   deny-licenses: GPL-1.0-or-later, LGPL-2.0-or-later
        #   retry-on-snapshot-warnings: true
```