About dependency review

In this article

Dependency review lets you catch insecure dependencies before you introduce them to your environment, and provides information on license, dependents, and age of dependencies.

Dependency review is available for organization-owned repositories in GitHub Enterprise Server. This feature requires a license for GitHub Advanced Security. For more information, see "About GitHub Advanced Security."

About dependency review

Dependency review helps you understand dependency changes and the security impact of these changes at every pull request. It provides an easily understandable visualization of dependency changes with a rich diff on the "Files Changed" tab of a pull request. Dependency review informs you of:

- Which dependencies were added, removed, or updated, along with the release dates.
- How many projects use these components.
- Vulnerability data for these dependencies.

If a pull request targets your repository's default branch and contains changes to package manifests or lock files, you can display a dependency review to see what has changed. The dependency review includes details of changes to indirect dependencies in lock files, and it tells you if any of the added or updated dependencies contain known vulnerabilities.

Sometimes you might just want to update the version of one dependency in a manifest and generate a pull request. However, if the updated version of this direct dependency also has updated dependencies, your pull request may have more changes than you expected. The dependency review for each manifest and lock file provides an easy way to see what has changed, and whether any of the new dependency versions contain known vulnerabilities.

By checking the dependency reviews in a pull request, and changing any dependencies that are flagged as vulnerable, you can avoid vulnerabilities being added to your project. For more information about how dependency review works, see "Reviewing dependency changes in a pull request."

For more information about configuring dependency review, see "Configuring dependency review."

Dependabot alerts will find vulnerabilities that are already in your dependencies, but it's

much better to avoid introducing potential problems than to fix problems at a later date. For more information about Dependabot alerts, see "About Dependabot alerts."

Dependency review supports the same languages and package management ecosystems as the dependency graph. For more information, see "About the dependency graph."

For more information on supply chain features available on GitHub Enterprise Server, see "About supply chain security."

Enabling dependency review

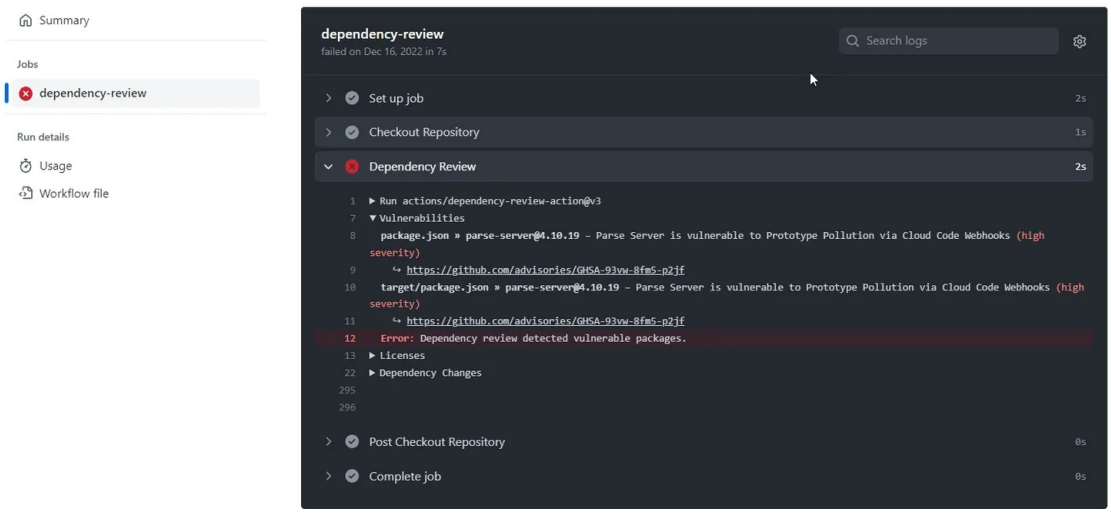
The dependency review feature becomes available when you enable the dependency graph. For more information, see "Enabling the dependency graph for your enterprise."

Dependency review enforcement

The action is available for all repositories that have GitHub Advanced Security enabled.

Enterprise owners and people with admin access to a repository can add the dependency review action to their enterprise and repository, respectively.

You can use the dependency review action in your repository to enforce dependency reviews on your pull requests. The action scans for vulnerable versions of dependencies introduced by package version changes in pull requests, and warns you about the associated security vulnerabilities. This gives you better visibility of what's changing in a pull request, and helps prevent vulnerabilities being added to your repository. For more information, see `dependency-review-action`.



By default, the dependency review action check will fail if it discovers any vulnerable packages. A failed check blocks a pull request from being merged when the repository owner requires the dependency review check to pass. For more information, see "About protected branches."

The action uses the dependency review REST API to get the diff of dependency changes between the base commit and head commit. You can use the dependency review API to get the diff of dependency changes, including vulnerability data, between any two commits on a repository. For more information, see "Dependency Graph."

You can configure the dependency review action to better suit your needs. For example, you can specify the severity level that will make the action fail. For more information, see "Configuring dependency review."

Legal

© 2023 GitHub, Inc.