About Dependabot security updates

In this article

Dependabot can fix vulnerable dependencies for you by raising pull requests with security updates.

Dependabot security updates are free to use for all repositories on GitHub.com.

About Dependabot security updates

Dependabot security updates make it easier for you to fix vulnerable dependencies in your repository. If you enable this feature, when a Dependabot alert is raised for a vulnerable dependency in the dependency graph of your repository, Dependabot automatically tries to fix it. For more information, see "About Dependabot alerts" and "Configuring Dependabot security updates."

GitHub may send Dependabot alerts to repositories affected by a vulnerability disclosed by a recently published GitHub security advisory. For more information, see "Browsing security advisories in the GitHub Advisory Database."

Dependabot checks whether it's possible to upgrade the vulnerable dependency to a fixed version without disrupting the dependency graph for the repository. Then Dependabot raises a pull request to update the dependency to the minimum version that includes the patch and links the pull request to the Dependabot alert, or reports an error on the alert. For more information, see "Troubleshooting Dependabot errors."

The Dependabot security updates feature is available for repositories where you have enabled the dependency graph and Dependabot alerts. You will see a Dependabot alert for every vulnerable dependency identified in your full dependency graph. However, security updates are triggered only for dependencies that are specified in a manifest or lock file. For more information, see "About the dependency graph."

Note: For npm, Dependabot will raise a pull request to update an explicitly defined dependency to a secure version, even if it means updating the parent dependency or dependencies, or even removing a sub-dependency that is no longer needed by the parent. For other ecosystems, Dependabot is unable to update an indirect or transitive dependency if it would also require an update to the parent dependency. For more information, see "Troubleshooting Dependabot errors."

You can enable a related feature, Dependabot version updates, so that Dependabot raises pull requests to update the manifest to the latest version of the dependency, whenever it detects an outdated dependency. For more information, see "About

Dependabot version updates."

When Dependabot raises pull requests, these pull requests could be for *security* or *version* updates:

- *Dependabot security updates* are automated pull requests that help you update dependencies with known vulnerabilities.
- *Dependabot version updates* are automated pull requests that keep your dependencies updated, even when they don’t have any vulnerabilities. To check the status of version updates, navigate to the Insights tab of your repository, then Dependency Graph, and Dependabot.

GitHub Actions is not required for Dependabot version updates and Dependabot security updates to run on GitHub Enterprise Cloud. However, pull requests opened by Dependabot can trigger workflows that run actions. For more information, see "Automating Dependabot with GitHub Actions."

Dependabot security updates can fix vulnerable dependencies in GitHub Actions. When security updates are enabled, Dependabot will automatically raise a pull request to update vulnerable GitHub Actions used in your workflows to the minimum patched version.

About pull requests for security updates

Each pull request contains everything you need to quickly and safely review and merge a proposed fix into your project. This includes information about the vulnerability like release notes, changelog entries, and commit details. Details of which vulnerability a pull request resolves are hidden from anyone who does not have access to Dependabot alerts for the repository.

When you merge a pull request that contains a security update, the corresponding Dependabot alert is marked as resolved for your repository. For more information about Dependabot pull requests, see "Managing pull requests for dependency updates."

Note: It's good practice to have automated tests and acceptance processes in place so that checks are carried out before the pull request is merged. This is particularly important if the suggested version to upgrade to contains additional functionality, or a change that breaks your project's code. For more information about continuous integration, see "About continuous integration."

About compatibility scores

Dependabot security updates may include compatibility scores to let you know whether updating a dependency could cause breaking changes to your project. These are calculated from CI tests in other public repositories where the same security update has been generated. An update's compatibility score is the percentage of CI runs that passed when updating between specific versions of the dependency.

About automatic deactivation of Dependabot updates

When maintainers of a repository stop interacting with Dependabot pull requests, Dependabot temporarily pauses its updates and lets you know. This automatic opt-out behavior reduces noise because Dependabot doesn't create pull requests for version and security updates, and doesn't rebase Dependabot pull requests for inactive repositories.

The automatic deactivation of Dependabot updates only applies to repositories where

Dependabot has opened pull requests but the pull requests remain untouched. If Dependabot hasn't opened any pull requests, Dependabot will never become paused.

An active repository is a repository for which a user (not Dependabot) has carried out *any* of the actions below in the last 90 days:

- Merge or close a Dependabot pull request on the repository.
- Make a change to the `dependabot.yml` file for the repository.
- Manually trigger a security update or a version update.
- Enable Dependabot security updates for the repository.
- Use `@dependabot` commands on pull requests.

An inactive repository is a repository that has at least one Dependabot pull request open for more than 90 days, has been enabled for the full period, and where none of the actions listed above has been taken by a user.

When Dependabot is paused, GitHub adds a notice to the body of all open Dependabot pull requests, and assigns a `dependabot-paused` label to these pull requests. You'll also see a banner notice in the UI of the **Settings** tab of the repository (under **Code security and analysis**, then **Dependabot**), as well in the list of Dependabot alerts (if Dependabot security updates are affected). Additionally, you will be able to see whether Dependabot is paused at the organization-level in the security overview. The `paused` status will also be visible via the API. For more information, see "Repositories" in the REST API documentation.

As soon as a maintainer interacts with a Dependabot pull request again, Dependabot will unpause itself:

- Security updates are automatically resumed for Dependabot alerts.
- Version updates are automatically resumed with the schedule specified in the `dependabot.yml` file.

About notifications for Dependabot security updates

You can filter your notifications on GitHub to show Dependabot security updates. For more information, see "Managing notifications from your inbox."