

Troubleshooting Dependabot errors

In this article

- About Dependabot errors
 - Investigating errors with Dependabot security updates
 - Investigating errors with Dependabot version updates
 - Understanding Dependabot errors
 - Triggering a Dependabot pull request manually
 - Further reading
-

Sometimes Dependabot is unable to raise a pull request to update your dependencies. You can review the error and unblock Dependabot.

Note: Your site administrator must set up Dependabot updates for your GitHub Enterprise Server instance before you can use this feature. For more information, see "[Enabling Dependabot for your enterprise](#)."

You may not be able to enable or disable Dependabot updates if an enterprise owner has set a policy at the enterprise level. For more information, see "[Enforcing policies for code security and analysis for your enterprise](#)."

About Dependabot errors

Dependabot raises pull requests to update dependencies. Depending on how your repository is configured, Dependabot may raise pull requests for version updates and/or for security updates. You manage these pull requests in the same way as any other pull request, but there are also some extra commands available. For information about enabling Dependabot dependency updates, see "[Configuring Dependabot security updates](#)" and "[Configuring Dependabot version updates](#)."

If anything prevents Dependabot from raising a pull request, this is reported as an error.

Note: Dependabot doesn't create pull requests for inactive repositories. For information about inactivity criteria, see "[About Dependabot security updates](#)" and "[About Dependabot version updates](#)," for security and version updates, respectively.

Investigating errors with Dependabot security updates

When Dependabot is blocked from creating a pull request to fix a Dependabot alert, it posts the error message on the alert. The Dependabot alerts view shows a list of any alerts that have not been resolved yet. To access the alerts view, click **Dependabot alerts** on the **Security** tab for the repository. Where a pull request that will fix the vulnerable dependency has been generated, the alert includes a link to that pull request.

is:open

91 Open 22 Closed

Package

Ecosystem

Manifest

Severity

Sort

High resource usage when parsing multipart form data with many fields High

#125 opened 3 weeks ago · Detected in Werkzeug (pip) · pip-compile/requirements.txt

#353

High resource usage when parsing multipart form data with many fields High

#124 opened 3 weeks ago · Detected in Werkzeug (pip) · poetry/poetry.lock

There are several reasons why an alert may have no pull request link:

- 1 Dependabot security updates are not enabled for the repository.
- 2 The alert is for malware and there is no secure version of the package.
- 3 The alert is for an indirect or transitive dependency that is not explicitly defined in a lock file.
- 4 An error blocked Dependabot from creating a pull request.

If an error blocked Dependabot from creating a pull request, you can display details of the error by clicking the alert.

Investigating errors with Dependabot version updates

When Dependabot is blocked from creating a pull request to update a dependency in an ecosystem, it posts the error icon on the manifest file.

The manifest files that are managed by Dependabot are listed on the Dependabot tab. To access this tab, on the **Insights** tab for the repository click **Dependency graph**, and then click the **Dependabot** tab.

Dependency graph

Dependencies

Dependents

Dependabot

go.mod

Last checked 10 hours ago

To see the logs for any manifest file, click the **Last checked TIME ago** link, and then click **View logs**.

Understanding Dependabot errors

Pull requests for security updates act to upgrade a vulnerable dependency to the minimum version that includes a fix for the vulnerability. In contrast, pull requests for version updates act to upgrade a dependency to the latest version allowed by the package manifest and Dependabot configuration files. Consequently, some errors are specific to one type of update.

Dependabot cannot update DEPENDENCY to a non-vulnerable version

Security updates only. Dependabot cannot create a pull request to update the

vulnerable dependency to a secure version without breaking other dependencies in the dependency graph for this repository.

Every application that has dependencies has a dependency graph, that is, a directed acyclic graph of every package version that the application directly or indirectly depends on. Every time a dependency is updated, this graph must resolve otherwise the application won't build. When an ecosystem has a deep and complex dependency graph, for example, npm and RubyGems, it is often impossible to upgrade a single dependency without upgrading the whole ecosystem.

The best way to avoid this problem is to stay up to date with the most recently released versions, for example, by enabling version updates. This increases the likelihood that a vulnerability in one dependency can be resolved by a simple upgrade that doesn't break the dependency graph. For more information, see "[Configuring Dependabot version updates](#)."

Dependabot tries to update dependencies without an alert

Security updates only. Dependabot updates explicitly defined transitive dependencies that are vulnerable for all ecosystems. For npm, Dependabot will raise a pull request that also updates the parent dependency if it's the only way to fix the transitive dependency.

For example, a project with a dependency on `A` version `~2.0.0` which has a transitive dependency on `B` version `~1.0.0` which has resolved to `1.0.1`.

```
my project
|
--> A (2.0.0) [~2.0.0]
    |
    --> B (1.0.1) [~1.0.0]
```

If a security vulnerability is released for `B` versions `<2.0.0` and a patch is available at `2.0.0` then Dependabot will attempt to update `B` but will find that it's not possible due to the restriction in place by `A` which only allows lower vulnerable versions. To fix the vulnerability, Dependabot will look for updates to dependency `A` which allow the fixed version of `B` to be used.

Dependabot automatically generates a pull request that upgrades both the locked parent and child transitive dependencies.

Dependabot cannot update to the required version as there is already an open pull request for the latest version

Security updates only. Dependabot will not create a pull request to update the vulnerable dependency to a secure version because there is already an open pull request to update this dependency. You will see this error when a vulnerability is detected in a single dependency and there's already an open pull request to update the dependency to the latest version.

There are two options: you can review the open pull request and merge it as soon as you are confident that the change is safe, or close that pull request and trigger a new security update pull request. For more information, see "[Triggering a Dependabot pull request manually](#)."

Dependabot timed out during its update

Dependabot took longer than the maximum time allowed to assess the update required and prepare a pull request. This error is usually seen only for large repositories with many manifest files, for example, npm or yarn monorepo projects with hundreds of `package.json` files. Updates to the Composer ecosystem also take longer to assess and

may time out.

This error is difficult to address. If a version update times out, you could specify the most important dependencies to update using the `allow` parameter or, alternatively, use the `ignore` parameter to exclude some dependencies from updates. Updating your configuration might allow Dependabot to review the version update and generate the pull request in the time available.

If a security update times out, you can reduce the chances of this happening by keeping the dependencies updated, for example, by enabling version updates. For more information, see "[Configuring Dependabot version updates](#)."

Dependabot cannot open any more pull requests

There's a limit on the number of open pull requests Dependabot will generate. When this limit is reached, no new pull requests are opened and this error is reported. The best way to resolve this error is to review and merge some of the open pull requests.

There are separate limits for security and version update pull requests, so that open version update pull requests cannot block the creation of a security update pull request. The limit for security update pull requests is 10. By default, the limit for version updates is 5 but you can change this using the `open-pull-requests-limit` parameter in the configuration file. For more information, see "[Configuration options for the dependabot.yml file](#)."

The best way to resolve this error is to merge or close some of the existing pull requests and trigger a new pull request manually. For more information, see "[Triggering a Dependabot pull request manually](#)."

Dependabot can't resolve or access your dependencies

If Dependabot attempts to check whether dependency references need to be updated in a repository, but can't access one or more of the referenced files, the operation will fail with the error message "Dependabot can't resolve your LANGUAGE dependency files." The API error type is `git_dependencies_not_reachable`.

Similarly, if Dependabot can't access a private package registry in which a dependency is located, one of the following errors is generated:

- "Dependabot can't reach a dependency in a private package registry"
(API error type: `private_source_not_reachable`)
- "Dependabot can't authenticate to a private package registry"
(API error type: `private_source_authentication_failure`)
- "Dependabot timed out while waiting for a private package registry"
(API error type: `private_source_timed_out`)
- "Dependabot couldn't validate the certificate for a private package registry"
(API error type: `private_source_certificate_failure`)

To allow Dependabot to update the dependency references successfully, make sure that all of the referenced dependencies are hosted at accessible locations.

Version updates only. When running security or version updates, some ecosystems must be able to resolve all dependencies from their source to verify that updates have been successful. If your manifest or lock files contain any private dependencies, Dependabot must be able to access the location at which those dependencies are hosted. Organization owners can grant Dependabot access to private repositories containing dependencies for a project within the same organization. For more information, see "[Managing security and analysis settings for your organization](#)." You can configure access to private registries in a repository's `dependabot.yml` configuration file. For more information, see "[Configuration options for the dependabot.yml file](#)."

Additionally, Dependabot doesn't support private GitHub dependencies for all package managers. For more information, see "[About Dependabot version updates](#)."

Triggering a Dependabot pull request manually

If you unblock Dependabot, you can manually trigger a fresh attempt to create a pull request.

- **Security updates**—display the Dependabot alert that shows the error you have fixed and click **Create Dependabot security update**.
- **Version updates**—on the **Insights** tab for the repository click **Dependency graph**, and then click the **Dependabot** tab. Click **Last checked *TIME* ago** to see the log file that Dependabot generated during the last check for version updates. Click **Check for updates**.

Further reading

- "[Troubleshooting the dependency graph](#)"
- "[Troubleshooting the detection of vulnerable dependencies](#)"

Legal

© 2023 GitHub, Inc. [Terms](#) [Privacy](#) [Status](#) [Pricing](#) [Expert services](#) [Blog](#)