Troubleshooting Dependabot errors

In this article

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

About Dependabot errors

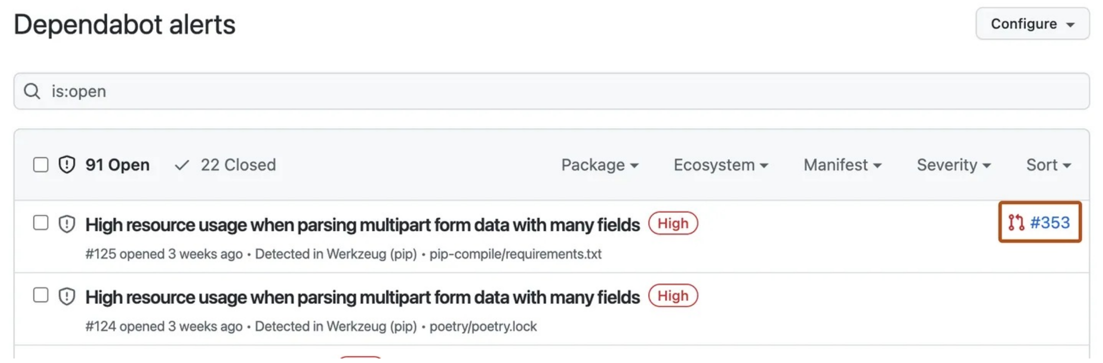
Dependabot raises pull requests to update dependencies. Depending on how your repository is configured, Dependabot may raise pull requests for version updates and/or for security updates. You manage these pull requests in the same way as any other pull request, but there are also some extra commands 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.



High resource usage when parsing multipart form data with many fields
#125 opened 3 weeks ago • Detected in Werkzeug (pip) • pip-compile/requirements.txt

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

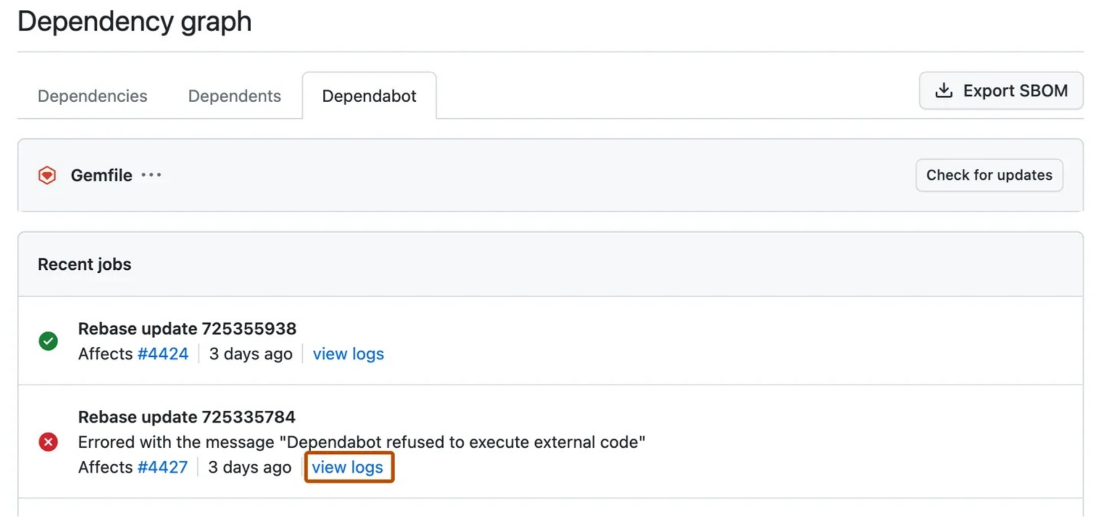
If an error blocked Dependabot from creating a pull request, you can display details of the error by clicking the alert.

Investigating errors with Dependabot version updates

When Dependabot is blocked from creating a pull request to update a dependency in an ecosystem, you can view the job logs list to find out more about the error .

The job logs list is accessible from the dependency graph of a repository. From the dependency graph, click the **Dependabot** tab, then to the right of the affected manifest file, click **Recent update jobs**.

To view the full logs files for a particular job, to the right of the log entry you are interested in, click **view logs**.



Rebase update 725355938
Affects #4424 | 3 days ago | view logs

Rebase update 725335784
Errored with the message "Dependabot refused to execute external code"
Affects #4427 | 3 days ago | view logs

For more information, see "Viewing Dependabot job 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."

Dependabot fails to group a set of dependencies into a single pull request

You can only create groups for Dependabot version updates. Dependabot security updates do not support grouped updates. In addition, if there is a grouped pull request for a vulnerable package, Dependabot security updates will always attempt to create a separate pull request, even if the existing group pull request is an update to the same, or a later, version.

You must configure groups per package ecosystem. To debug the problem, we recommend you look at the logs. For information about accessing the logs for a manifest, see "Investigating errors with Dependabot version updates" above.

You may have unintentionally created empty groups. This happens, for example, when you set a `dependency-type` in the `allow` key for the overall job.

```
allow:
  dependency-type: production
  # this restricts the entire job to production dependencies
  groups:
      development-dependencies:
        dependency-type: "development"
        # this group will always be empty
```

In this example, Dependabot will:

1. Look at your dependency list and restrict the job to dependencies used in `production` only.
2. Try to create a group called `development-dependencies` which is a subset of this reduced list.
3. Work out that the `development-dependencies` group is empty as all `development` dependencies were removed in step 1.
4. **Individually** update all the dependencies that are not in the group. As the group for dependencies in production is empty, Dependabot will ignore the group, and create a separate pull request for each dependency.

You need to ensure that configuration settings don't cancel each other, and update them appropriately in your configuration file.

For more information on how to configure groups for Dependabot version updates, see "Configuration options for the dependabot.yml file."

Dependabot fails to update one of the dependencies in a grouped pull request

Version updates only. Dependabot will show the failed update in your logs, as well as in the job summary at the end of your logs. You should use the `@dependabot recreate` comment on the pull request to build the group again. For more information, see "Managing pull requests for dependency updates."

If the dependency still fails to update, you should use the `exclude-patterns` configuration so that the dependency is excluded from the group. Dependabot will then raise a separate pull request to update the dependency.

If the dependency still fails to update, there may be a problem with the dependency itself, or with Dependabot for that specific ecosystem.

If you want to ignore version updates for the dependency, you must do one of the following.

- Configure an `ignore` rule for the dependency in the `dependabot.yml` file. For more information, see "Configuration options for the dependabot.yml file."
- Use the `@dependabot ignore` comment command for the dependency in the pull request for the grouped updates. For more information, see "Managing pull requests for dependency updates."

Continuous integration (CI) fails on my grouped pull request

Version updates only. If the failure is due to a single dependency, you should use the `exclude-patterns` configuration so that the dependency is excluded from the group. Dependabot will then raise a separate pull request to update the dependency.

If you want to ignore version updates for the dependency, you must do one of the following.

- Configure an `ignore` rule for the dependency in the `dependabot.yml` file. For more information, see "Configuration options for the dependabot.yml file."
- Use the `@dependabot ignore` comment command for the dependency in the pull request for the grouped updates. For more information, see "Managing pull requests for dependency updates."

If you continue to see CI failures, you should remove the group configuration so that Dependabot reverts to raising individual pull requests for each dependency. Then, you should check and confirm that the update works correctly for each individual pull request.

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