Dependabot quickstart guide

In this article

You can use Dependabot to alert you when your repository is using a software dependency with a known vulnerability. This guide will help get you started on enabling Dependabot for a repository, and exploring reported alerts.

Dependabot alerts are free to use for all repositories on GitHub.com. Advanced capabilities, like reachability analysis and the ability to create custom alert rules, are available on any public repositories (for free), and on any private repositories, when you have a license for GitHub Advanced Security.

About Dependabot

This quickstart guide walks you through setting up and enabling Dependabot and viewing Dependabot alerts and updates for a repository.

Dependabot consists of three different features that help you manage your dependencies:

- Dependabot alerts—inform you about vulnerabilities in the dependencies that you use in your repository.
- Dependabot security updates—automatically raise pull requests to update the dependencies you use that have known security vulnerabilities.
- Dependabot version updates—automatically raise pull requests to keep your dependencies up-to-date.

Prerequisites

For the purpose of this guide, we're going to use a demo repository to illustrate how Dependabot finds vulnerabilities in dependencies, where you can see Dependabot alerts on GitHub, and how you can explore, fix, or dismiss these alerts.

You need to start by forking the demo repository.

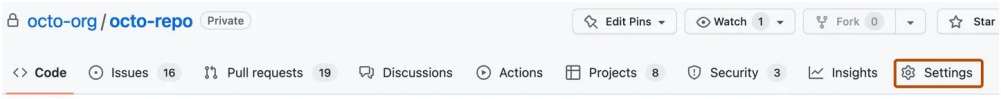
1. Navigate to https://github.com/dependabot/demo.
2. At the top of the page, on the right, click **Fork**.

3. Select an owner (you can select your GitHub personal account) and type a repository name. For more information about forking repositories, see "Fork a repo."
4. Click **Create fork**.

Enabling Dependabot for your repository

You need to follow the steps below on the repository you forked in "Prerequisites."

1. On GitHub.com, navigate to the main page of the repository.
2. Under your repository name, click **Settings**. If you cannot see the "Settings" tab, select the ··· dropdown menu, then click **Settings**.



3. In the "Security" section of the sidebar, click **Code security and analysis**.
4. Under "Code security and analysis", to the right of Dependabot alerts, click **Enable** for Dependabot alerts, Dependabot security updates, and Dependabot version updates.
5. Optionally, if you are interested in experimenting with Dependabot version updates, click **.github/dependabot.yml**. This will create a default `dependabot.yml` configuration file in the `/.github` directory of your repository. To enable Dependabot version updates for your repository, you typically configure this file to suit your needs by editing the default file, and committing your changes. You can refer to the snippet provided in "Configuring Dependabot version updates" for an example.

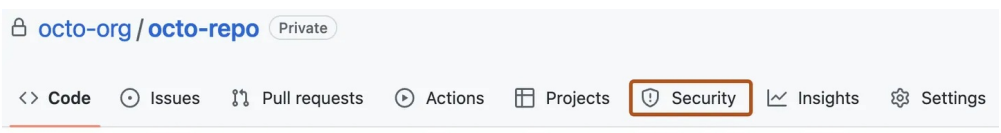
> **Note:** If the dependency graph is not already enabled for the repository, GitHub will enable it automatically when you enable Dependabot.

For more information about configuring each of these Dependabot features, see "Configuring Dependabot alerts," "Configuring Dependabot security updates," and "Configuring Dependabot version updates."

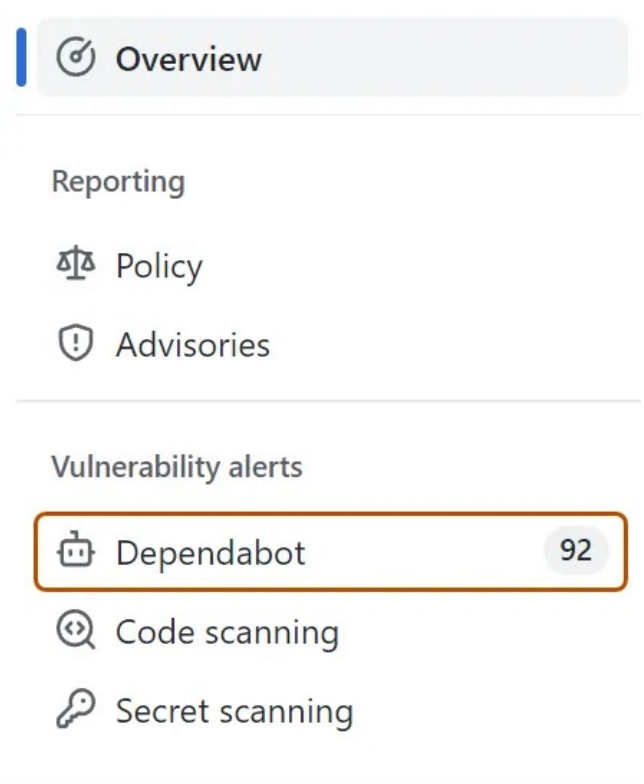
Viewing Dependabot alerts for your repository

If Dependabot alerts are enabled for a repository, you can view Dependabot alerts on the "Security" tab for the repository. You can use the forked repository that you enabled Dependabot alerts on in the previous section.

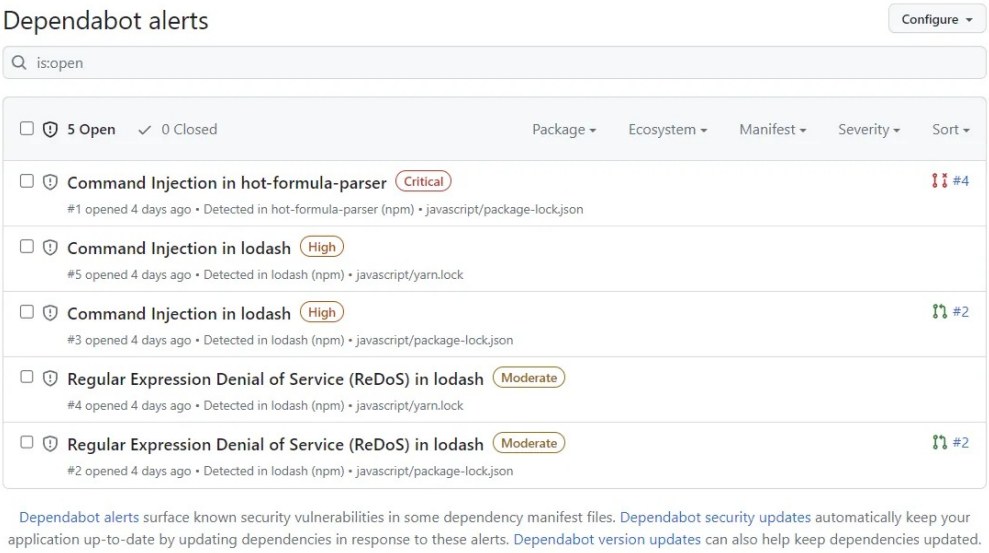
1. On GitHub.com, navigate to the main page of the repository.
2. Under the repository name, click **Security**. If you cannot see the "Security" tab, select the ··· dropdown menu, and then click **Security**.



3. In the "Vulnerability alerts" sidebar of security overview, click **Dependabot**. If this option is missing, it means you don't have access to security alerts and need to be given access. For more information, see "Managing security and analysis settings for your repository."



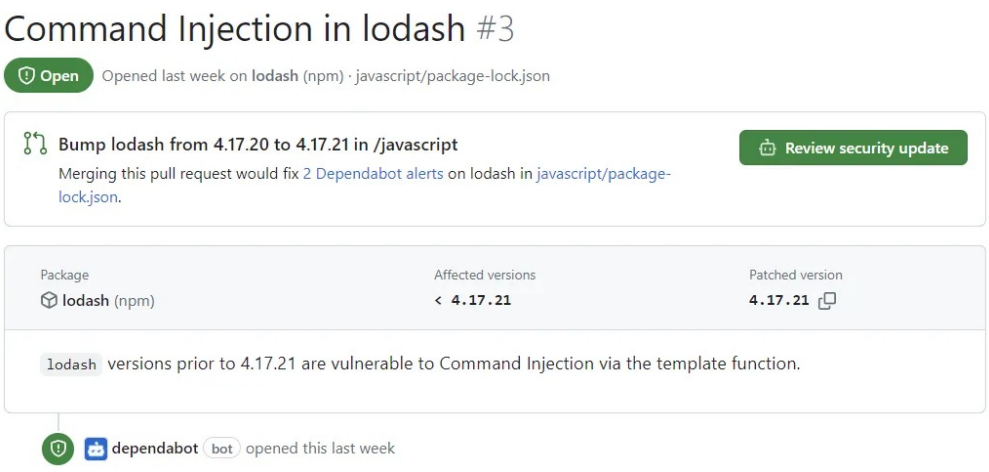
4. Review the open alerts on the Dependabot alerts page. By default, the page displays the **Open** tab, listing the open alerts. (You'll be able to view any closed alerts by clicking **Closed**.)



   You can filter Dependabot alerts in the list, using a variety of filters or labels. For more information, see "Viewing and updating Dependabot alerts." You can also use Dependabot alert rules to filter out false positive alerts or alerts you're not interested in. For more information, see "About Dependabot alert rules."

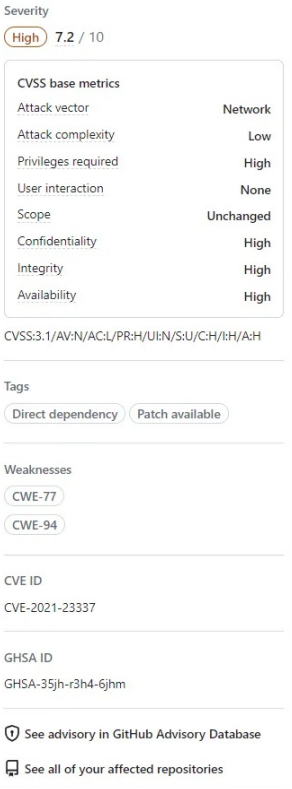
5. Click the "Command Injection in lodash" alert on the `javascript/package-lock.json` file. The details page for the alert will show the following information (note that some information may not apply to all alerts):

- Whether Dependabot created a pull request that will fix the vulnerability. You can review the suggested security update by clicking **Review security update**.
- Package involved
- Affected versions
- Patched version
- Brief description of the vulnerability



6. Optionally, you can also explore the information on the right-side of the page. Some of the information shown in the screenshot may not apply to every alert.

   - Severity
   - CVSS metrics—we use CVSS levels to assign severity levels. For more information, see "About the GitHub Advisory database."
   - Tags
   - Weaknesses—list of CWEs related to the vulnerability, if applicable
   - CVE ID—unique CVE identifier for the vulnerability, if applicable
   - GHSA ID—unique identifier of the corresponding advisory on the GitHub Advisory Database. For more information, see "About the GitHub Advisory database."
   - Option to navigate to the advisory on the GitHub Advisory Database
   - Option to see all of your repositories that are affected by this vulnerability
   - Option to suggest improvements for this advisory on the GitHub Advisory Database

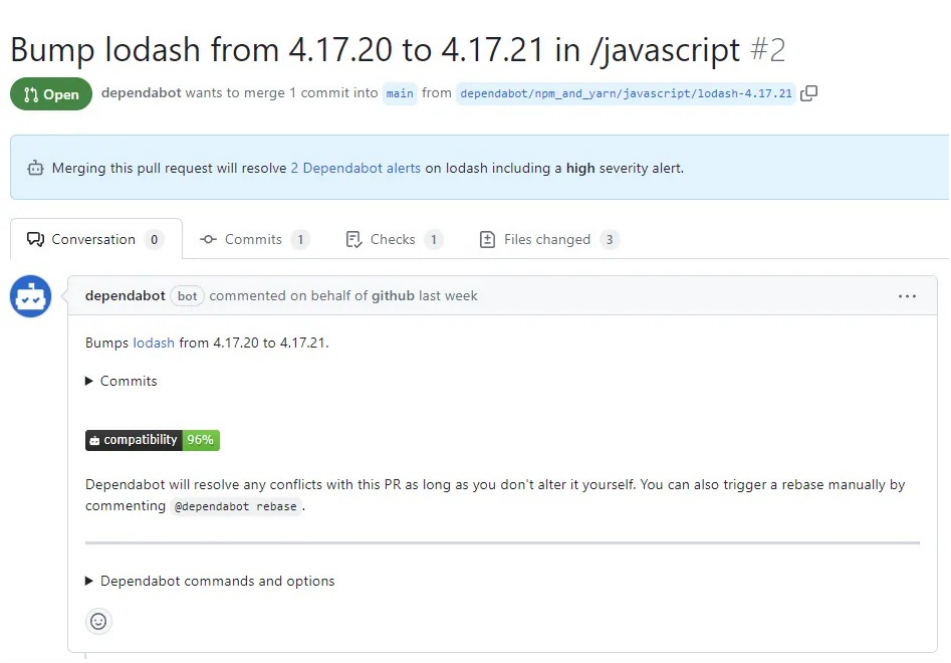


For more information about viewing, prioritizing, and sorting Dependabot alerts, see "Viewing and updating Dependabot alerts."

Fixing or dismissing a Dependabot alert

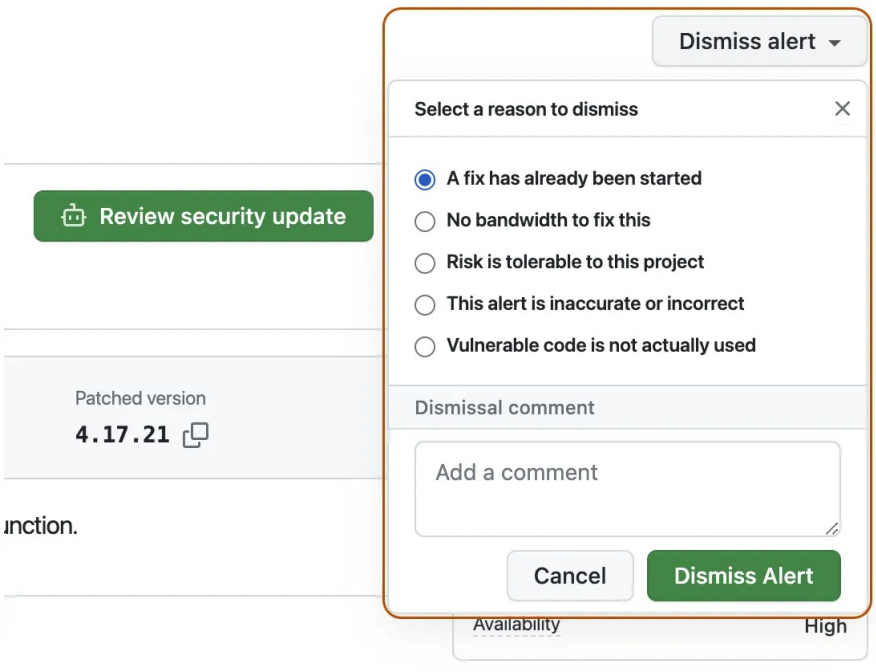
You can fix or dismiss Dependabot alerts on GitHub. Let's continue to use the forked repository as an example, and the "Command Injection in lodash" alert described in the previous section.

1. Navigate to the Dependabot alerts tab for the repository. For more information, see the "Viewing Dependabot alerts for your repository" section above.
2. Click an alert.
3. Click the "Command Injection in lodash" alert on the `javascript/package-lock.json` file.
4. Review the alert. You can:
    - Review the suggested security update by clicking **Review security update**. This will open the pull request generated by Dependabot with the security fix.



- On the pull request description, you can click **Commits** to explore the commits included in the pull request.
- You can also click **Dependabot commands and options** to learn about the commands that you can use to interact with the pull request.
- When you're ready to update your dependency and resolve the vulnerability, merge the pull request.

- If you decide that you want to dismiss the alert
  - Go back to the alert details page.
  - On the top-right corner, click **Dismiss alert**.



  - Select a reason for dismissing the alert.
  - Optionally, add a dismissal comment. The dismissal comment will be added to the alert timeline and can be used as justification during auditing and reporting.
  - Click **Dismiss alert**. The alert won't appear aymore in the **Open** tab of the alert list, and you are able to view it in the **Closed** tab.

For more information about reviewing and updating Dependabot alerts, see "Viewing and updating Dependabot alerts."

Troubleshooting

You may need to do some troubleshooting if:

- Dependabot is blocked from creating a pull request to fix an alert, or
- The information reported by Dependabot is not what you expect.

For more information, see "Troubleshooting Dependabot errors" and "Troubleshooting the detection of vulnerable dependencies," respectively.

Next steps

For more information about configuring Dependabot updates, see "Configuring Dependabot security updates" and "Configuring Dependabot version updates."

For more information about configuring Dependabot for an organization, see "Configuring Dependabot alerts.

For more information about viewing pull requests opened by Dependabot, see "Managing pull requests for dependency updates."

For more information about the security advisories that contribute to Dependabot alerts, see "Browsing security advisories in the GitHub Advisory Database."

For more information about configuring notifications about Dependabot alerts, see "Configuring notifications for Dependabot alerts."