

# Configuring notifications for Dependabot alerts

## In this article

About notifications for Dependabot alerts

Configuring notifications for Dependabot alerts

How to reduce the noise from notifications for Dependabot alerts

Further reading

---

Optimize how you receive notifications about Dependabot alerts.

## About notifications for Dependabot alerts

When Dependabot detects vulnerable dependencies or malware in your repositories, we generate a Dependabot alert and display it on the **Security** tab for the repository.

GitHub Enterprise Cloud notifies the maintainers of affected repositories about the new alert according to their notification preferences. Dependabot is enabled by default on all public repositories, and needs to be enabled on private repositories. By default, you will receive Dependabot alerts by email. You can override the default overall behavior by choosing the type of notifications you want to receive, or switching notifications off altogether in the settings page for your user notifications at


<https://github.com/settings/notifications>.

Regardless of your notification preferences, when Dependabot is first enabled, GitHub Enterprise Cloud does not send notifications for all vulnerable dependencies found in your repository. Instead, you will receive notifications for new vulnerable dependencies identified after Dependabot is enabled, if your notification preferences allow it.

If you're an organization owner, you can enable or disable Dependabot alerts for all repositories in your organization with one click. You can also set whether Dependabot alerts will be enabled or disabled for newly-created repositories. For more information, see "[Managing security and analysis settings for your organization](#)."

## Configuring notifications for Dependabot alerts

When a new Dependabot alert is detected, GitHub Enterprise Cloud notifies all users with access to Dependabot alerts for the repository according to their notification preferences. You will receive alerts if you are watching the repository, have enabled notifications for security alerts or for all the activity on the repository, and are not ignoring the repository. For more information, see "[Configuring notifications](#)."

You can configure notification settings for yourself or your organization from the Manage notifications drop-down  shown at the top of each page. For more information, see "[Configuring notifications](#)."

You can choose the delivery method for notifications, as well as the frequency at which the notifications are sent to you. By default, you will receive notifications:

- in your inbox, as web notifications. A web notification is sent when Dependabot is

enabled for a repository, when a new manifest file is committed to the repository, and when a new vulnerability with a critical or high severity is found (**On GitHub** option).

- by email, an email is sent when Dependabot is enabled for a repository, when a new manifest file is committed to the repository, and when a new vulnerability with a critical or high severity is found (**Email** option).
- on the command line, warnings are displayed as callbacks when you push to repositories with any insecure dependencies (**CLI** option).
- on GitHub Mobile, as web notifications. For more information, see "[Configuring notifications](#)."

**Note:** The email and web/GitHub Mobile notifications are:

- *Per repository* when Dependabot is enabled on the repository, or when a new manifest file is committed to the repository.
- *Per organization* when a new vulnerability is discovered.
- Sent when a new vulnerability is discovered. GitHub doesn't send notifications when vulnerabilities are updated.

You can customize the way you are notified about Dependabot alerts. For example, you can receive a daily or weekly digest email summarizing alerts for up to 10 of your repositories using the **Email weekly digest** option.

**Dependabot alerts: New vulnerabilities**

When you're given access to [Dependabot alerts](#) automatically receive notifications when a new vulnerability is found in one of your dependencies.

Notify me: on GitHub, Email, CLI ▾

**Email weekly digest**

Email a weekly summary summarizing alerts for up to 10 of your repositories.

Send weekly ▾

Don't send

✓ Send weekly

Send daily

permissions to an organization, automatically receive notifications when a new deploy

**Note:** You can filter your notifications on GitHub to show Dependabot alerts. For more information, see "[Managing notifications from your inbox](#)."

Email notifications for Dependabot alerts that affect one or more repositories include the `X-GitHub-Severity` header field. You can use the value of the `X-GitHub-Severity` header field to filter email notifications for Dependabot alerts. For more information, see "[Configuring notifications](#)."

# How to reduce the noise from notifications for Dependabot alerts

If you are concerned about receiving too many notifications for Dependabot alerts, we recommend you opt into the weekly email digest, or turn off notifications while keeping Dependabot alerts enabled. You can still navigate to see your Dependabot alerts in your repository's **Security** tab. For more information, see "[Viewing and updating Dependabot alerts](#)."

## Further reading

---

- "[Configuring notifications](#)"
- "[Managing notifications from your inbox](#)"

### Legal

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