Configuring Dependabot alerts

In this article

Enable Dependabot alerts to be generated when a new vulnerable dependency or malware is found in one of your repositories.

About Dependabot alerts for vulnerable dependencies and malware

A vulnerability is a problem in a project's code that could be exploited to damage the confidentiality, integrity, or availability of the project or other projects that use its code. Vulnerabilities vary in type, severity, and method of attack.

Dependabot scans code when a new advisory is added to the GitHub Advisory Database or the dependency graph for a repository changes. When vulnerable dependencies or malware are detected, Dependabot alerts are generated. For more information, see "About Dependabot alerts."

If you have enabled Dependabot security updates for your repository, the alert may also contain a link to a pull request to update the manifest or lock file to the minimum version that resolves the vulnerability. For more information, see "About Dependabot security updates."

You can enable or disable Dependabot alerts for:

- Your personal account
- Your repository
- Your organization
- Your enterprise

Managing Dependabot alerts for your personal account

Dependabot alerts for your repositories can be enabled or disabled by your enterprise owner. For more information, see "Enabling Dependabot for your enterprise."

Managing Dependabot alerts for your repository

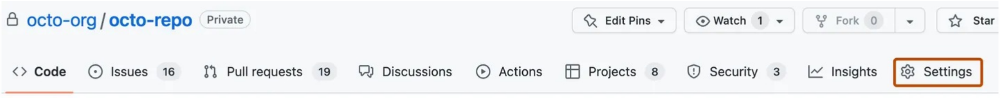
You can manage Dependabot alerts for your public, private or internal repository.

By default, we notify people with write, maintain, or admin permissions in the affected repositories about new Dependabot alerts. GitHub Enterprise Server never publicly discloses insecure dependencies for any repository. You can also make Dependabot alerts visible to additional people or teams working on repositories that you own or have admin permissions for.

An enterprise owner must first set up Dependabot for your enterprise before you can manage Dependabot alerts for your repository. For more information, see "Enabling Dependabot for your enterprise."

Enabling or disabling Dependabot alerts for a repository

1. On your GitHub Enterprise Server instance, 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** to enable alerts or **Disable** to disable alerts.

Managing Dependabot alerts for your organization

You can enable or disable Dependabot alerts for some or all repositories owned by your organization. For more information about enabling security features across an organization, see "Securing your organization."

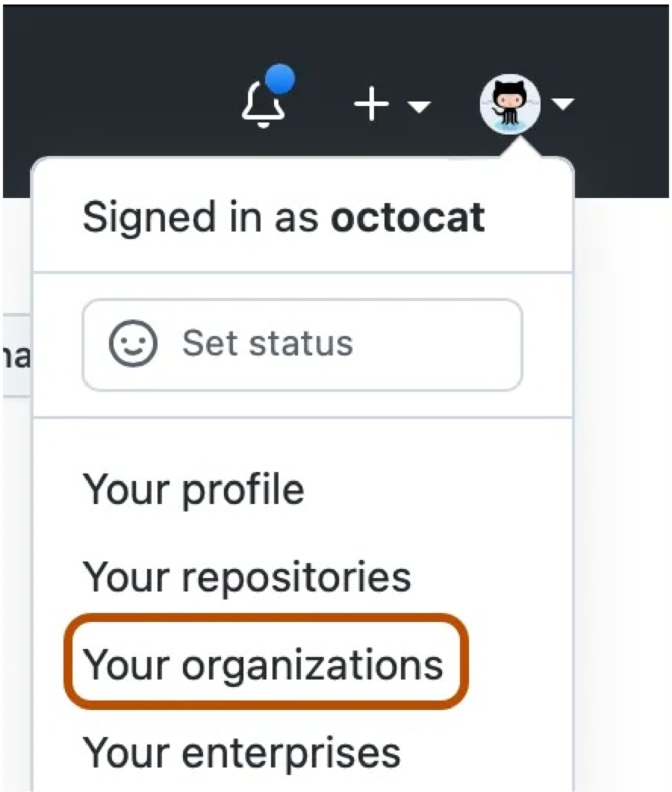
An enterprise owner must first set up Dependabot for your enterprise before you can manage Dependabot alerts for your repository. For more information, see "Enabling Dependabot for your enterprise."

Enabling or disabling Dependabot alerts for all existing repositories

You can use security overview to find a set of repositories and enable or disable Dependabot alerts for them all at the same time. For more information, see "Enabling security features for multiple repositories."

You can also use the organization settings page for "Code security and analysis" to enable or disable Dependabot alerts for all existing repositories in an organization.

1. In the top right corner of GitHub Enterprise Server, click your profile photo, then click **Your organizations**.

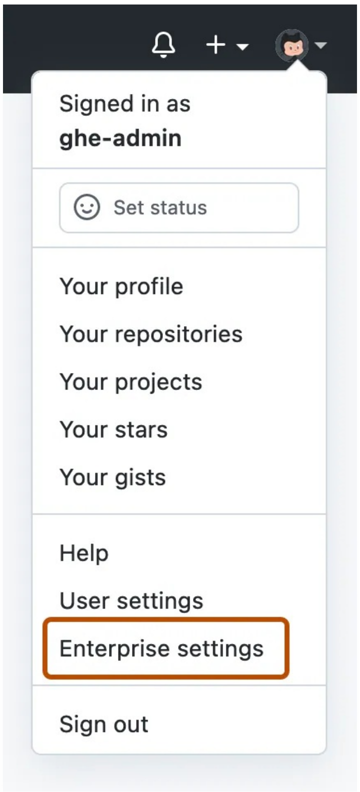


2. Next to the organization, click **Settings**.
3. In the "Security" section of the sidebar, click **Code security and analysis**.
4. Under "Code security and analysis", to the right of Dependabot alerts, click **Disable all** or **Enable all**.
5. Optionally, to enable Dependabot alerts by default for new repositories in your organization, in the dialog box, select "Enable by default for new repositories".
6. Click **Disable Dependabot alerts** or **Enable Dependabot alerts** to disable or enable Dependabot alerts for all the repositories in your organization.

Managing Dependabot alerts for your enterprise

You can enable or disable Dependabot alerts for all current and future repositories owned by organizations in your enterprise. Your changes affect all repositories.

1. In the top-right corner of GitHub Enterprise Server, click your profile photo, then click **Enterprise settings**.



2. In the enterprise account sidebar, click **Settings**.

3. In the left sidebar, click **Code security and analysis**.

4. In the "Dependabot" section, to the right of Dependabot alerts, click **Disable all** or **Enable all**.

5. Optionally, select **Automatically enable for new repositories** to enable Dependabot alerts by default for your organizations' new repositories.