About Dependabot alerts

In this article

About Dependabot alerts
Detection of insecure dependencies
Configuration of Dependabot alerts
Access to Dependabot alerts
Further reading

GitHub Enterprise Server sends Dependabot alerts when we detect that your repository uses a vulnerable dependency or malware.

Dependabot alerts are free to use for repositories (user-owned and organization-owned) on GitHub Enterprise Server, provided enterprise administrators enable the feature for your enterprise.

About Dependabot alerts

Note: Advisories for malware are currently in beta and subject to change.

Dependabot alerts tell you that your code depends on a package that is insecure.

If your code depends on a package with a security vulnerability, this can cause a range of problems for your project or the people who use it. You should upgrade to a secure version of the package as soon as possible. If your code uses malware, you need to replace the package with a secure alternative.

For an overview of the different features offered by Dependabot and instructions on how to get started, see "Dependabot quickstart guide."

Detection of insecure dependencies

Dependabot performs a scan of the default branch of your repository to detect insecure dependencies, and sends Dependabot alerts when:

- New advisory data is synchronized to your GitHub Enterprise Server instance each hour from GitHub.com. For more information, see "Browsing security advisories in the GitHub Advisory Database."

  Note: Only advisories that have been reviewed by GitHub will trigger Dependabot alerts.

- The dependency graph for a repository changes. For example, when a contributor pushes a commit to change the packages or versions it depends on. For more information, see "About the dependency graph."

Note: Dependabot doesn't scan archived repositories.

Additionally, GitHub can review any dependencies added, updated, or removed in a pull request made against the default branch of a repository, and flag any changes that would reduce the security of your project. This allows you to spot and deal with vulnerable dependencies or malware before, rather than after, they reach your codebase. For more information, see "Reviewing dependency changes in a pull request."

As Dependabot alerts rely on the dependency graph, the ecosystems that are supported by Dependabot alerts are the same as those supported by the dependency graph. For a list of these ecosystems, see "About the dependency graph."

Note: It is important to keep your manifest and lock files up to date. If the dependency graph doesn't accurately reflect your current dependencies and versions, then you could miss alerts for insecure dependencies that you use. You may also get alerts for dependencies that you no longer use.

Dependabot will only create Dependabot alerts for vulnerable GitHub Actions that use semantic versioning. You will not receive alerts for a vulnerable action that uses SHA versioning. If you use GitHub Actions with SHA versioning, we recommend enabling Dependabot version updates for your repository or organization to keep the actions you use updated to the latest versions.

Configuration of Dependabot alerts

Enterprise owners must enable Dependabot alerts for your GitHub Enterprise Server instance before you can use this feature. For more information, see "Enabling Dependabot for your enterprise."

When GitHub Enterprise Server identifies a vulnerable dependency or malware, we generate a Dependabot alert and display it on the **Security** tab for the repository and in the repository's dependency graph. The alert includes a link to the affected file in the project, and information about a fixed version.

GitHub Enterprise Server may also notify the maintainers of affected repositories about new alerts according to their notification preferences. For more information, see "Configuring notifications for 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."

Note: GitHub Enterprise Server's security features do not claim to catch all vulnerabilities and malware. We actively maintain GitHub Advisory Database and generate alerts with the most up-to-date information. However, we cannot catch everything or tell you about known vulnerabilities within a guaranteed time frame. These features are not substitutes for human review of each dependency for potential vulnerabilities or any other issues, and we recommend consulting with a security service or conducting a thorough dependency review when necessary.

Access to Dependabot alerts

You can see all of the alerts that affect a particular project in the repository's dependency graph. For more information, see "Viewing and updating Dependabot alerts."

By default, we notify people with write, maintain, or admin permissions in the affected repositories about new Dependabot alerts.

To receive notifications about Dependabot alerts on repositories, you need to watch these repositories, and subscribe to receive "All Activity" notifications or configure custom settings to include "Security alerts." 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. For more information, see "Configuring notifications for Dependabot alerts."

You can also see all the Dependabot alerts that correspond to a particular advisory in the GitHub Advisory Database. For more information, see "Browsing security advisories in the GitHub Advisory Database."

Further reading

- "About Dependabot security updates"
- "Viewing and updating Dependabot alerts"
- "Auditing security alerts"