About Dependabot alert rules

In this article

You can use Dependabot alert rules to auto-triage alerts, so you can reduce false positives and better prioritize the alerts that you're interested in.

> **Who can use this feature**
> People with write permissions can view Dependabot alert rules for the repository. People with with admin permissions to a repository, or the security manager role for the repository, can enable or disable Dependabot alert rules for the repository, as well as create custom alert rules.

Note: Dependabot alert rules are currently in beta and are subject to change.

About Dependabot alert rules

Dependabot alert rules allow you to instruct Dependabot to automatically dismiss or reopen certain alerts, based on complex logic from a variety of contextual criteria.

There are two types of Dependabot alert rules:

- A GitHub-curated rule, called `Dismiss low impact alerts`
- User-created custom rules

The GitHub-curated rule, `Dismiss low impact alerts`, auto-dismisses certain types of vulnerabilities that are found in npm dependencies used in development. The rule has been curated to reduce false positives and reduce alert fatigue. The rule is enabled by default for public repositories and can be opted into for private repositories. However, you cannot modify GitHub-curated rules. For more information, see "Using GitHub-curated alert rules to prioritize Dependabot alerts."

With user-created custom rules, you can create your own rules to automatically dismiss or reopen alerts based on your own criteria, such as severity, package name, CWE, and more. For more information, see "Customizing alert rules to prioritize Dependabot alerts."

Whilst you may find it useful to auto-dismiss alerts, you can still reopen auto-dismissed alerts and filter to see which alerts have been auto-dismissed. For more information, see "Managing alerts that have been automatically dismissed by an alert rule."

Additionally, auto-dismissed alerts are still available for reporting and reviewing, and can be auto-reopened if the alert metadata changes, for example:

- If you change the scope of a dependency from development to production.
- If GitHub modifies certain metadata for the related advisory.

Auto-dismissed alerts are defined by the `resolution:auto-dismiss` close reason.

Automatic dismissal activity is included in alert webhooks, REST and GraphQL APIs, and the audit log. For more information, see "Dependabot alerts" in the REST API documentation, and the "`repository_vulnerability_alert`" section in "Reviewing the audit log for your organization."

Further reading

- Using GitHub-curated alert rules to prioritize Dependabot alerts
- Customizing alert rules to prioritize Dependabot alerts