Using GitHub-curated alert rules to prioritize Dependabot alerts

In this article

You can use a GitHub-curated alert rule to auto-dismiss low impact development alerts for npm dependencies.

> **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.

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

About GitHub-curated alert rules 🔗

The GitHub-curated alert rule, `Dismiss low impact alerts`, auto-dismisses certain types of vulnerabilities that are found in npm dependencies used in development. These alerts cover cases that feel like false alarms to most developers as the associated vulnerabilities:

- Are unlikely to be exploitable in a developer (non-production or runtime) environment.
- May relate to resource management, programming and logic, and information disclosure issues.
- At worst, have limited effects like slow builds or long-running tests.
- Are not indicative of issues in production.

> **Note:** Automatic dismissal of low impact development alerts is currently only supported for npm.

The GitHub-curated `Dismiss low impact alerts` rule includes vulnerabilities relating to resource management, programming and logic, and information disclosure issues. For more information, see "Publicly disclosed CWEs used by the `Dismiss low impact alerts rule`."

Filtering out these low impact alerts allows you to focus on alerts that matter to you, without having to worry about missing potentially high-risk development-scoped alerts.

By default, GitHub-curated Dependabot alert rules are enabled on public repositories and disabled for private repositories. Administrators of private repositories can opt in by enabling alert rules for their repository.

Enabling the `Dismiss low impact alerts` rule for your private repository 🔗

You first need to enable Dependabot alerts for the repository. For more information, see "[Configuring Dependabot alerts](#)."

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**.
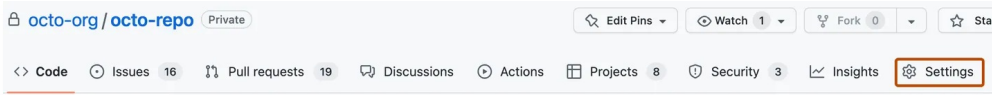
③ In the "Security" section of the sidebar, click ⊚ **Code security and analysis**.

④ Under "Dependabot alerts", click ⚙ close to "Dependabot rules".

⑤ Select **Dismiss low impact alerts**.

⑥ Click **Save rules**.

Publicly disclosed CWEs used by the `Dismiss low impact alerts` rule 🔗

Along with the `ecosystem:npm` and `scope:development` alert metadata, we use the following GitHub-curated Common Weakness Enumerations (CWEs) to filter out low impact alerts for the `Dismiss low impact alerts` rule. We regularly improve this list and vulnerability patterns covered by built-in rules.

Resource Management Issues 🔗

- CWE-400 Uncontrolled Resource Consumption
- CWE-770 Allocation of Resources Without Limits or Throttling
- CWE-409 Improper Handling of Highly Compressed Data (Data Amplification)
- CWE-908 Use of Uninitialized Resource
- CWE-1333 Inefficient Regular Expression Complexity
- CWE-835 Loop with Unreachable Exit Condition ('Infinite Loop')
- CWE-674 Uncontrolled Recursion
- CWE-1119 Excessive Use of Unconditional Branching

Programming and Logic Errors 🔗

- CWE-185 Incorrect Regular Expression
- CWE-754 Improper Check for Unusual or Exceptional Conditions

- CWE-755 Improper Handling of Exceptional Conditions
- CWE-248 Uncaught Exception
- CWE-252 Unchecked Return Value
- CWE-391 Unchecked Error Condition
- CWE-696 Incorrect Behavior Order
- CWE-1254 Incorrect Comparison Logic Granularity
- CWE-665 Improper Initialization
- CWE-703 Improper Check or Handling of Exceptional Conditions
- CWE-178 Improper Handling of Case Sensitivity

Information Disclosure Issues 🔗

- CWE-544 Missing Standardized Error Handling Mechanism
- CWE-377 Insecure Temporary File
- CWE-451 User Interface (UI) Misrepresentation of Critical Information
- CWE-668 Exposure of Resource to Wrong Sphere