Assessing your code security risk

In this article

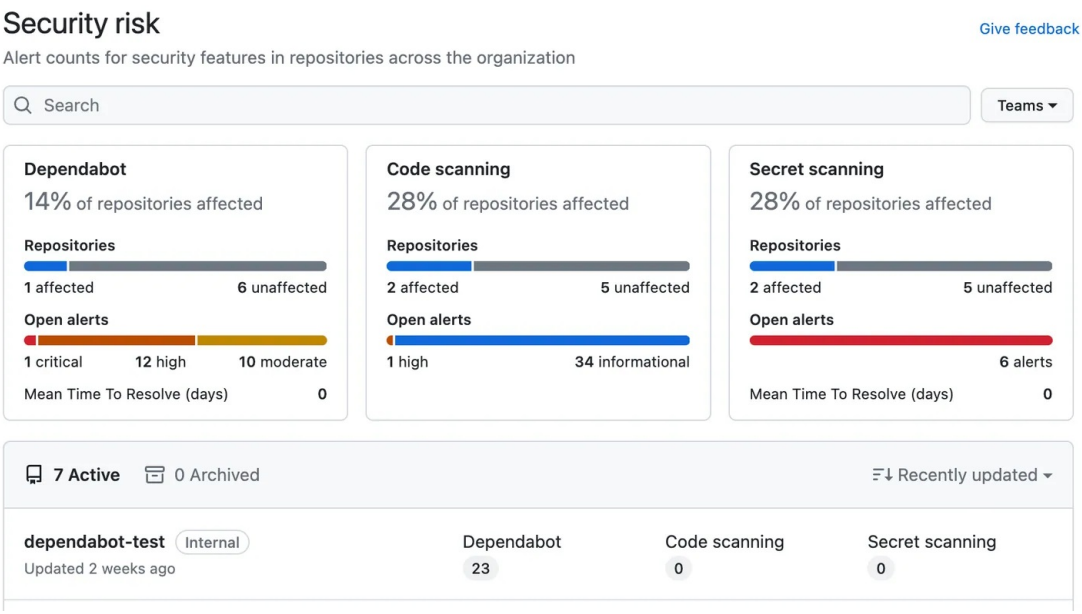
You can use security overview to see which teams and repositories are affected by security alerts, and identify repositories for urgent remedial action.

> **Who can use this feature**
> Security overview for an organization is available to all members of the organization. The views and data displayed are determined by your role in the organization, and by your permissions for individual repositories within the organization. For more information, see "About security overview."
>
> Security overview for an enterprise shows organization owners and security managers data for the organizations they have access to. Enterprise owners can only view data for organizations where they are added as an organization owner or security manager. For more information, see "Managing your role in an organization owned by your enterprise."

All enterprises and their organizations have a security overview. If you use GitHub Advanced Security features, which are free for public repositories, you will see additional information. For more information, see "About GitHub Advanced Security."

About security risks in your code

You can use security overview to see which repositories and teams are free from any security alerts and which have unresolved security alerts. The "Security risk" page shows a summary and detailed information on which repositories in an organization or enterprise are affected by security alerts, with a breakdown of alert by severity. You can filter the view to show a subset of repositories using the "affected" and "unaffected" links, the links under "Open alerts", the "Teams" dropdown menu, and a search field in the page header. This view is a great way to understand the broader picture for a repository, team, or group of repositories because you can see security alerts of all types in one view.



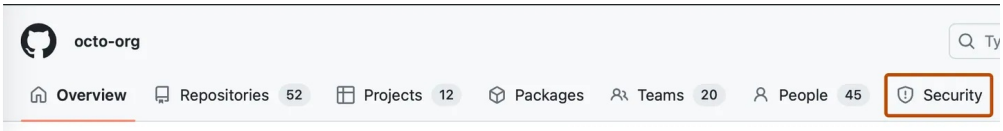
You can download a CSV file of the data displayed on the "Security risk" page. This data file can be used for efforts like security research and in-depth data analysis, and can integrate easily with external datasets. For more information, see "Exporting data from the risk and coverage pages."

Note: It's important to understand that all repositories without open alerts are included in the set of unaffected repositories. That is, unaffected repositories include any repositories where the feature is not enabled, in addition to repositories that have been scanned and any alerts identified have been closed.

Viewing organization-level code security risks

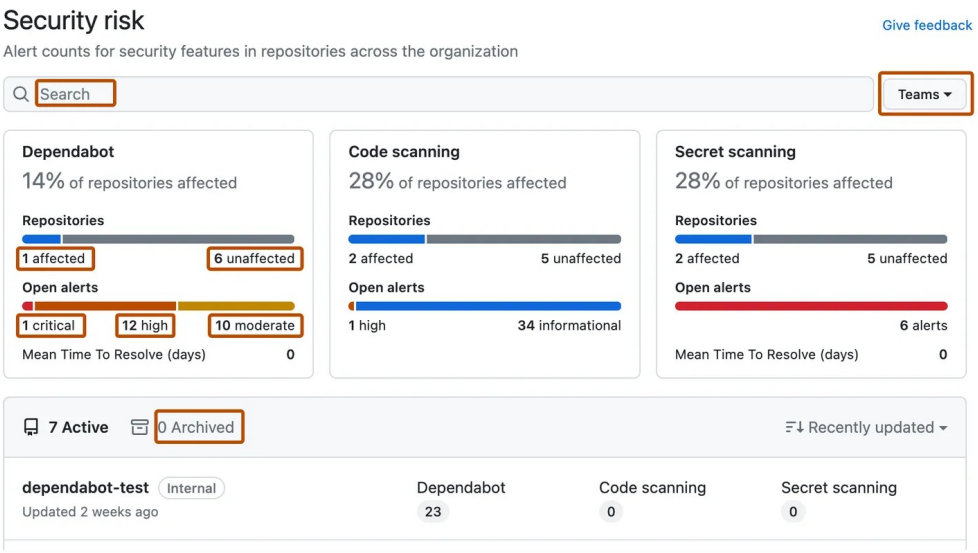
The information shown by security overview varies according to your access to repositories and organizations, and according to whether GitHub Advanced Security is used by those repositories and organizations. For more information, see "About security overview."

1. On GitHub.com, navigate to the main page of the organization.
2. Under your organization name, click **Security**.



3. To display the "Security risk" view, in the sidebar, click **Risk**.
4. Use options in the page summary to filter results to show the repositories you want to assess. The list of repositories and metrics displayed on the page automatically update to match your current selection. For more information on filtering, see "Filtering alerts in security overview."
    - Use the **Teams** dropdown to show information only for the repositories owned by one or more teams.
    - Click **NUMBER affected** or **NUMBER unaffected** in the header for any feature to show only the repositories with open alerts or no open alerts of that type.
    - Click any of the descriptions of "Open alerts" in the header to show only repositories with alerts of that type and category. For example, **1 critical** to show the repository with a critical alert for Dependabot.

- At the top of the list of repositories, click **NUMBER Archived** to show only repositories that are archived.
- Click in the search box to add further filters to the repositories displayed.



5. Optionally, use the sidebar on the left to explore alerts for a specific security feature in greater detail. On each page, you can use filters that are specific to that feature to refine your search. For more information about the available qualifiers, see "Filtering alerts in security overview."

Viewing enterprise-level code security risks

You can view data for security alerts across organizations in an enterprise. The information shown by security overview varies according to your access to repositories and organizations, and according to whether GitHub Advanced Security is used by those repositories and organizations. For more information, see "About security overview."

> **Tip:** You can use the `org:` filter in the search field to filter the data by organization. For more information, see "Filtering alerts in security overview."

1. Navigate to GitHub.com.
2. In the top-right corner of GitHub.com, click your profile photo, then click **Your enterprises**.
3. In the list of enterprises, click the enterprise you want to view.
4. In the left sidebar, click **Code Security**.
5. To display the "Security coverage" view, in the sidebar, click **Risk**.
6. Use options in the page summary to filter results to show the repositories you want to assess. The list of repositories and metrics displayed on the page automatically update to match your current selection. For more information on filtering, see "Filtering alerts in security overview."

   - Use the **Teams** dropdown to show information only for the repositories owned by one or more teams.
   - Click **NUMBER affected** or **NUMBER unaffected** in the header for any feature to show only the repositories with open alerts or no open alerts of that type.
   - Click any of the descriptions of "Open alerts" in the header to show only

repositories with alerts of that type and category. For example, **1 critical** to show the repository with a critical alert for Dependabot.

- At the top of the list of repositories, click **NUMBER Archived** to show only repositories that are archived.
- Click in the search box to add further filters to the repositories displayed.