Filtering alerts in security overview

In this article

Use filters to view specific categories of alerts

> **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 you will see additional information. For more information, see "About GitHub Advanced Security."

About filtering security overview

You can use filters in a security overview to narrow your focus based on a range of factors, like alert risk level, alert type, and feature enablement. Different filters are available depending on the specific view and whether you are viewing data at the enterprise or organization level.

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."

Filter by repository

Security overview supports free text search for repositories. With free text search, you can search for a keyword, and repositories with names containing that keyword will be displayed. For example, if you search for "test", your search results would include both "test-repository" and "octocat-testing".

To perform an exact search for a single repository, use the `repo` qualifier. If you do not type the name of the repository exactly as it appears, the repository will not be found.

Qualifier	Description
`repo:REPOSITORY-NAME`	Displays data for the specified repository.

Filter by organization

In the enterprise-level views, you can filter the data by organization.

Qualifier	Description
`org:ORGANIZATION-NAME`	Displays data for the specified organization.

Filter by whether security features are enabled

In the examples below, replace `:enabled` with `:not-enabled` to see repositories where security features are not enabled. These qualifiers are available in the main summary views.

Qualifier	Description
`code-scanning:enabled`	Display repositories that have configured code scanning.
`dependabot:enabled`	Display repositories that have enabled Dependabot alerts.
`secret-scanning:enabled`	Display repositories that have enabled secret scanning alerts.
`any-feature:enabled`	Display repositories where at least one security feature is enabled.

The organization-level "Security coverage" view includes extra filters.

> **Note:** The "Security risk" and "Security coverage" views are currently in beta and subject to change.

Qualifier	Description
`advanced-security:enabled`	Display repositories that have enabled GitHub Advanced Security.
`code-scanning-pull-request-alerts:enabled`	Display repositories that have configured code scanning to run on pull requests.
`dependabot-security-updates:enabled`	Display repositories that have enabled Dependabot security updates.
`secret-scanning-push-protection:enabled`	Display repositories that have enabled push protection for secret scanning.

Filter by repository type

These qualifiers are available in the main summary views.

Qualifier	Description
`is:public`	Display public repositories.
`is:internal`	Display internal repositories.
`is:private`	Display private repositories.
`archived:true`	Display archived repositories.
`archived:false`	Omit archived repositories.

Filter by number of alerts

These qualifiers are available in the "Security risk" view.

Qualifier	Description
`code-scanning-alerts:NUMBER`	Display repositories that have NUMBER code scanning alerts. This qualifier can use `=`, `>` and `<` comparison operators.
`secret-scanning-alerts:NUMBER`	Display repositories that have NUMBER secret scanning alerts. This qualifier can use `=`, `>` and `<` comparison operators.
`dependabot-alerts:NUMBER`	Display repositories that have NUMBER Dependabot alerts. This qualifier can use `=`, `>` and `<` comparison operators.

Filter by team

These qualifiers are available in the main summary views and the alert-centric views for Dependabot, code scanning, and secret scanning.

Qualifier	Description
`team:TEAM-NAME`	Displays repositories that TEAM-NAME has write access or admin access to.

Filter by topic

These qualifiers are available in the main summary views and the alert-centric views for Dependabot, code scanning, and secret scanning.

Qualifier	Description
`topic:TOPIC-NAME`	Displays repositories that are classified with TOPIC-NAME. For more information on repository topics, see "Classifying your repository with topics."

Additional filters for Dependabot alert views

You can filter the view to show Dependabot alerts that are ready to fix or where additional information about exposure is available. You can click any result to see full details of the alert.

Qualifier	Description
`has:patch`	Displays Dependabot alerts for vulnerabilities where a secure version is already available.
`has:vulnerable-calls`	Displays Dependabot alerts where at least one call from the repository to a vulnerable function is detected. For more information, see "Viewing and updating Dependabot alerts."
`ecosystem:ECOSYSTEM-NAME`	Displays Dependabot alerts detected in the specified ecosystem.
`is:open`	Displays open Dependabot alerts.
`is:closed`	Displays closed Dependabot alerts.
`package:PACKAGE-NAME`	Displays Dependabot alerts detected in the specified package.
`resolution:auto-dismissed`	Displays Dependabot alerts closed as "auto-dismissed."
`resolution:fix-started`	Displays Dependabot alerts closed as "a fix has already been started."
`resolution:fixed`	Displays Dependabot alerts closed as "fixed."
`resolution:inaccurate`	Displays Dependabot alerts closed as "this alert is inaccurate or incorrect."
`resolution:no-bandwidth`	Displays Dependabot alerts closed as "no bandwidth to fix this."
`resolution:not-used`	Displays Dependabot alerts closed as "vulnerable code is not actually used."
`resolution:tolerable-risk`	Displays Dependabot alerts closed as "risk is tolerable to this project."
`scope:development`	Displays Dependabot alerts from the development dependency.
`scope:runtime`	Displays Dependabot alerts from the runtime dependency.
`sort:manifest-path`	Displays Dependabot alerts grouped by the manifest file path the alerts point to.
`sort:most-important`	Displays Dependabot alerts from most important to least important, as determined by CVSS score, vulnerability impact, relevancy, and actionability.
`sort:newest`	Displays Dependabot alerts from newest to oldest.

	oldest.
`sort:oldest`	Displays Dependabot alerts from oldest to newest.
`sort:package-name`	Displays Dependabot alerts grouped by the package in which the alert was detected.
`sort:severity`	Displays Dependabot alerts from most to least severe.

Additional filters for code scanning alert views

All code scanning alerts have one of the categories shown below. You can click any result to see full details of the relevant query and the line of code that triggered the alert.

Qualifier	Description
`is:open`	Displays open code scanning alerts.
`is:closed`	Displays closed code scanning alerts.
`resolution:false-positive`	Displays code scanning alerts closed as "false positive."
`resolution:fixed`	Displays code scanning alerts closed as "fixed."
`resolution:used-in-tests`	Displays code scanning alerts closed as "used in tests."
`resolution:wont-fix`	Displays code scanning alerts closed as "won't fix."
`rule:RULE-NAME`	Displays code scanning alerts opened for the specified rule.
`severity:critical`	Displays code scanning alerts categorized as critical.
`severity:high`	Displays code scanning alerts categorized as high.
`severity:medium`	Displays code scanning alerts categorized as medium.
`severity:low`	Displays code scanning alerts categorized as low.
`severity:error`	Displays code scanning alerts categorized as errors.
`severity:warning`	Displays code scanning alerts categorized as warnings.
`severity:note`	Displays code scanning alerts categorized as notes.
`sort:created-desc`	Displays code scanning alerts from newest to oldest.
`sort:created-asc`	Displays code scanning alerts from oldest to newest.

	newest.
`sort:updated-desc`	Displays code scanning alerts from most recently updated to least recently updated.
`sort:updated-asc`	Displays code scanning alerts from least recently updated to most recently updated.
`tool:TOOL-NAME`	Displays code scanning alerts detected by the specified tool.

Additional filters for secret scanning alert views

Qualifier	Description
`provider:PROVIDER-NAME`	Displays alerts for all secrets issues by the specified provider.
`secret-type:PROVIDER-PATTERN`	Displays alerts for the specified secret and provider.
`secret-type:CUSTOM-PATTERN`	Displays alerts for secrets matching the specified custom pattern.
`is:open`	Displays open secret scanning alerts.
`is:closed`	Displays closed secret scanning alerts.
`resolution:false-positive`	Displays secret scanning alerts closed as "false positive."
`resolution:pattern-deleted`	Displays secret scanning alerts closed as "pattern deleted."
`resolution:pattern-edited`	Displays secret scanning alerts closed as "pattern edited."
`resolution:revoked`	Displays secret scanning alerts closed as "revoked."
`resolution:used-in-tests`	Displays secret scanning alerts closed as "used in tests."
`resolution:wont-fix`	Displays secret scanning alerts closed as "won't fix."
`sort:created-desc`	Displays secret scanning alerts from newest to oldest.
`sort:created-asc`	Displays secret scanning alerts from oldest to newest.
`sort:updated-desc`	Displays secret scanning alerts from most recently updated to least recently updated.
`sort:updated-asc`	Displays secret scanning alerts from least recently updated to most recently updated.

For more information, see "Secret scanning patterns."