

Configuring private vulnerability reporting for a repository

In this article

About privately reporting a security vulnerability

Enabling or disabling private vulnerability reporting for a repository

Configuring notifications for private vulnerability reporting

Owners and administrators of public repositories can allow security researchers to report vulnerabilities securely in the repository by enabling private vulnerability reporting.

Who can use this feature

Anyone with admin permissions to a public repository can enable and disable private vulnerability reporting for the repository.

About privately reporting a security vulnerability

Security researchers often feel responsible for alerting users to a vulnerability that could be exploited. If there are no clear instructions about contacting maintainers of the repository containing the vulnerability, security researchers may have no other choice but to post about the vulnerability on social media, send direct messages to the maintainer, or even create public issues. This situation can potentially lead to a public disclosure of the vulnerability details.

Private vulnerability reporting makes it easy for security researchers to report vulnerabilities directly to you using a simple form.


When a security researcher reports a vulnerability privately, you are notified and can choose to either accept it, ask more questions, or reject it. If you accept the report, you're ready to collaborate on a fix for the vulnerability in private with the security researcher.

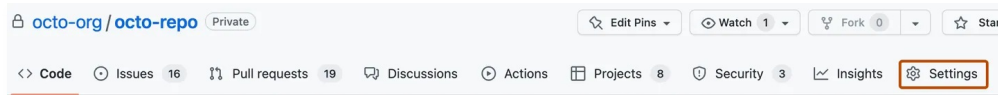
For maintainers, the benefits of using private vulnerability reporting are:


- Less risk of being contacted publicly, or via undesired means.
- Receive reports in the same platform you resolve them in for simplicity
- The security researcher creates or at least initiates the advisory report on the behalf of maintainers.
- Maintainers receive reports in the same platform as the one used to discuss and resolve the advisories.
- Vulnerability less likely to be in the public eye.
- The opportunity to discuss vulnerability details privately with security researchers and collaborate on the patch.

The instructions in this article refer to enablement at repository level. For information about enabling the feature at organization level, see "[Configuring private vulnerability reporting for an organization](#)."

Enabling or disabling private vulnerability reporting for a repository

- 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 "Code security and analysis", to the right of "Private vulnerability reporting", click **Enable** or **Disable**, to enable or disable the feature, respectively.

Code security and analysis

Security and analysis features help keep your repository secure and updated. By enabling these features, you're granting us permission to perform read-only analysis on your repository.

Private vulnerability reporting Beta

Allow your community to privately report potential security vulnerabilities to maintainers and repository owners. [Learn more about private vulnerability reporting.](#)

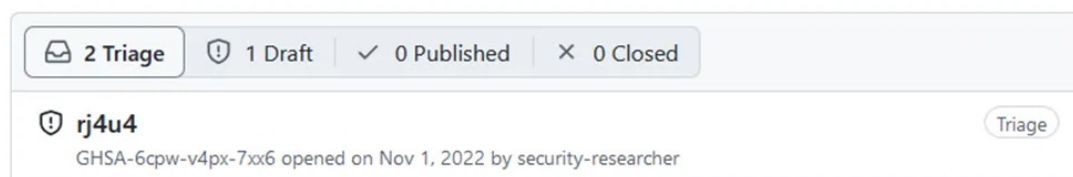
Enable

When private vulnerability reporting is enabled for a repository, security researchers will see a new button in the **Advisories** page of the repository. The security researcher can click this button to privately report a security vulnerability to the repository maintainer.

Security Advisories

Report a vulnerability

View known security vulnerabilities and report new vulnerabilities privately to maintainers.



Security researchers can also use the REST API to privately report security vulnerabilities. For more information, see "[Privately report a security vulnerability](#)" in the REST API documentation.

Configuring notifications for private vulnerability reporting


When a new vulnerability is privately reported on a repository where private vulnerability reporting is enabled, GitHub Enterprise Cloud notifies repository maintainers and security managers if:

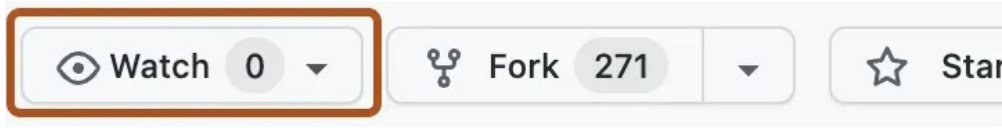
- They're watching the repository for all activity.
- They have notifications enabled for the repository.

Notifications depend on the user's notification preferences. You will receive an email notification if:

- You are watching the repository.
- You have enabled notifications for "All Activity".
- In your notification settings, under "Subscriptions", then under "Watching", you have selected to receive notifications by email.

1 On GitHub.com, navigate to the main page of the repository.

2 To start watching the repository, select  **Watch**.



3 In the dropdown menu, click **All Activity**.

4 Navigate to the notification settings for your personal account. These are available at <https://github.com/settings/notifications>.

5 On your notification settings page, under "Subscriptions," then under "Watching," select the **Notify me** dropdown.

6 Select "Email" as a notification option, then click **Save**.

Subscriptions

Watching

Notifications for all repositories, teams, or conversations you're watching. [View watched repositories](#)

Notify me: on GitHub ▾

☒ On GitHub
 ☒ Email

Custom

Notifications you are participating in, or if someone cites you with an @mention. Also for all specific events.

Cancel Save

Ignored repositories

You'll never be notified. [View ignored repositories](#)

For more information about setting up notification preferences, see "[Managing security and analysis settings for your repository](#)" and "[Configuring your watch settings for an individual repository](#)."

Legal

© 2023 GitHub, Inc. [Terms](#) [Privacy](#) [Status](#) [Pricing](#) [Expert services](#) [Blog](#)