

Configuring private vulnerability reporting for an organization

In this article

About privately reporting a security vulnerability

Enabling or disabling private vulnerability reporting for all the existing public repositories in an organization

Enabling or disabling private vulnerability reporting for new public repositories added to the organization

What having private vulnerability reporting enabled for a repository looks like for a security researcher

Organization owners and security managers can allow security researchers to report vulnerabilities securely in repositories within the organization by enabling private vulnerability reporting for all its public repositories.

Who can use this feature

Anyone with admin permissions to an organization, or with a security manager role within the organization, can enable and disable private vulnerability reporting for that organization.

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 organization owners and security managers, 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 below refer to enablement at organization level. For information about enabling the feature for a repository, see "[Configuring private vulnerability reporting for a repository](#)."

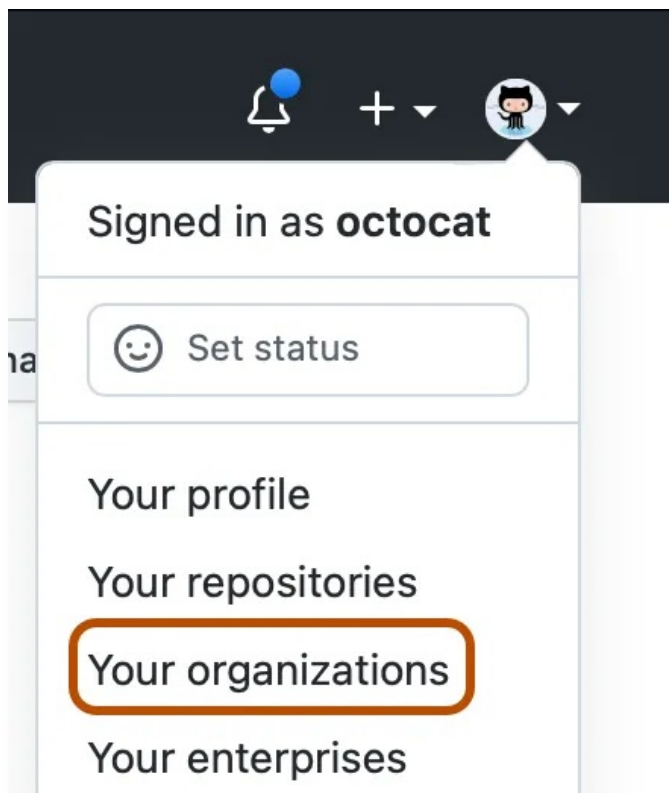
When a new vulnerability is privately reported on a repository where private vulnerability reporting is enabled, GitHub Enterprise Cloud notifies repository maintainers and security managers if:


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

For more information about configuring notification preferences, see "[Configuring private vulnerability reporting for a repository](#)."

Enabling or disabling private vulnerability reporting for all the existing public repositories in an organization [↗](#)

- 1 In the top right corner of GitHub.com, click your profile photo, then click  **Your organizations**.



- 2 Next to the organization, 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 all** or **Disable all**, to enable or disable the feature for all the public repositories within the organization, respectively.

Code security and analysis

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

Private vulnerability reporting Beta


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

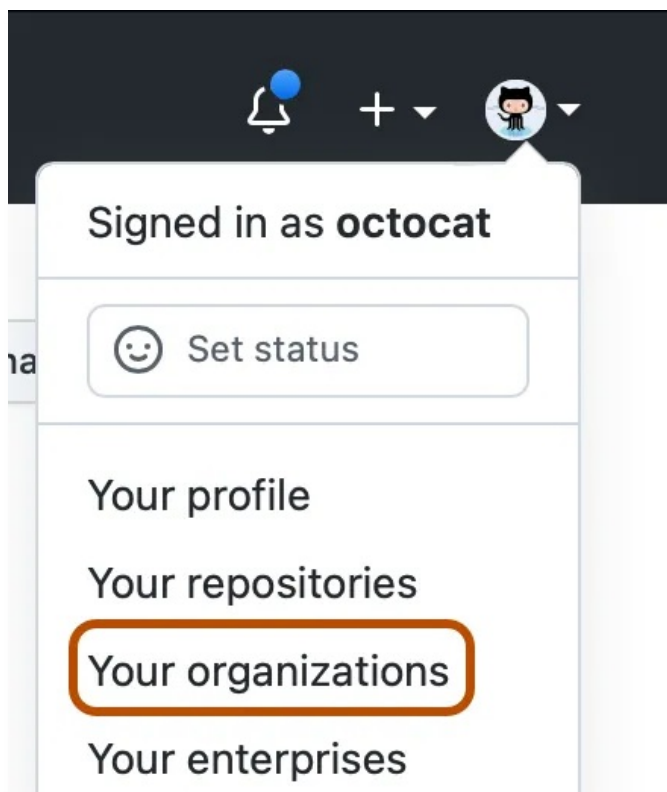
Disable all


Enable all

☐ Automatically enable for new public repositories

Enabling or disabling private vulnerability reporting for new public repositories added to the organization [🔗](#)

- 1 In the top right corner of GitHub.com, click your profile photo, then click  **Your organizations**.



- 2 Next to the organization, 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 the feature, click **Automatically enable for new public repositories**.

Code security and analysis

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

Private vulnerability reporting Beta

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

Disable all

Enable all

☒ Automatically enable for new public repositories ✓

- 5 To the right of "Private vulnerability reporting", click **Enable all** or **Disable all**, to enable or disable the feature for all new public repositories that will be added to the organization, respectively.

What having private vulnerability reporting enabled for a repository looks like for a security researcher [↗](#)

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.

2 Triage

1 Draft

0 Published

0 Closed

! **rj4u4**

GHSA-6cpw-v4px-7xx6 opened on Nov 1, 2022 by security-researcher

Triage

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.

Legal

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