Managing privately reported security vulnerabilities

In this article

About privately reporting a security vulnerability

Managing security vulnerabilities that are privately reported

---

Repository maintainers can manage security vulnerabilities that have been privately reported to them by security reseachers for repositories where private vulnerability reporting is enabled.

> **Who can use this feature**
> Anyone with admin permissions to a repository can see, review, and manage privately-reported vulnerabilities for the repository.

Owners and administrators of public repositories can enable private vulnerability reporting on their repositories. For more information, see "[Configuring private vulnerability reporting for a repository](#)."

About privately reporting a security vulnerability 🔗

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.

Managing security vulnerabilities that are privately reported 🔗

When a new vulnerability is privately reported on a repository where private vulnerability reporting is enabled, GitHub 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](#)."

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

2. Under the repository name, click 🛡️ **Security**. If you cannot see the "Security" tab, select the ••• dropdown menu, and then click **Security**.

3 In the left sidebar, under "Reporting", click 🛡 **Advisories**.

4 Click the advisory you want to review. An advisory that was reported privately has a status of `Triage`.

5 Carefully review the report, then choose how to proceed.

- To collaborate on a patch in private, click **Start a temporary private fork** to create a place for further discussions with the contributor. This does not change the status of the proposed advisory from `Triage`.

- To accept the reported vulnerability, click **Accept and open as draft** to accept the vulnerability report as a draft advisory on GitHub. If you choose this option:

  - This doesn't make the report public.
  - The report becomes a draft repository security advisory and you can work on it in the same way as any draft advisory that you create. For more information on security advisories, see "[About repository security advisories](#)."

- To ask for more information, or to open a discussion with the reporter, you can comment on the advisory. Any comments are visible only to the reporter and to any collaborators on the advisory.

- If you have enough information to determine that the problem the reporter describes is not a security risk, click **Close security advisory**. Where possible, you should add a comment explaining why you don't consider the report a security risk before you close the advisory.

Legal

Terms   Privacy   Status   Pricing   Expert services   Blog