Privately reporting a security vulnerability

In this article

About privately reporting a security vulnerability

Privately reporting a security vulnerability

Some public repositories configure security advisories so that anyone can report security vulnerabilities directly and privately to the maintainers.

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."

Notes:

- If you have admin or security permissions for a public repository, you don't need to submit a vulnerability report. Instead, you can create a draft security advisory directly. For more information, see "Creating a repository security advisory."
- The ability to privately report a vulnerability in a repository is not related to the presence of a `SECURITY.md` file in that repository's root or `docs` directory.
  - The `SECURITY.md` file contains the security policy for the repository. Repository administrators can add and use this file to provide *public* instructions for how to report a security vulnerability in their repository. For more information, see "Adding a security policy to your repository."
  - You can only report a vulnerability privately for repositories where private vulnerability reporting is enabled, and you don't have to follow the instructions in the `SECURITY.md` file. This reporting process is fully private, and GitHub notifies the repository administrators directly about your submission.

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 repository maintainer using a simple form.

For security researchers, the benefits of using private vulnerability reporting are:

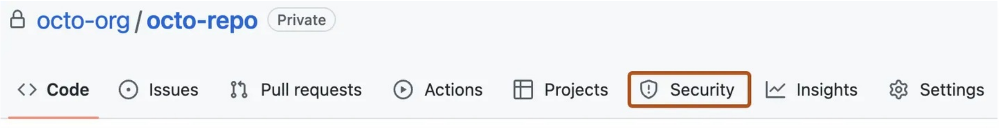
- Less frustration, and less time spent trying to figure out how to contact the maintainer.
- A smoother process for disclosing and discussing vulnerability details.
- The opportunity to discuss vulnerability details privately with repository maintainer.

Note: If the repository doesn't have private vulnerability reporting enabled, you need to initiate the reporting process by following the instructions in the security policy for the repository, or create an issue asking the maintainers for a preferred security contact. For more information, see "About coordinated disclosure of security vulnerabilities."

Privately reporting a security vulnerability

If you do not have admin or security permissions for a public repository, you can still privately report a security vulnerability to repository maintainers. You can also evaluate the general security of a public repository and suggest a security policy. For more information, see "Evaluating the security settings of 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. Click **Report a vulnerability** to open the advisory form.
4. Fill in the advisory details form.

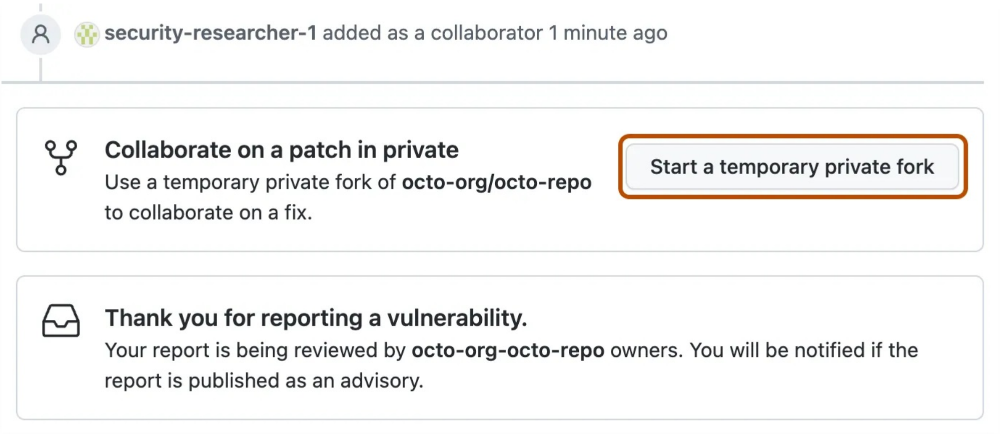
   Tip: In this form, only the title and description are mandatory. (In the general draft security advisory form, which the repository maintainer initiates, specifying the ecosystem is also required.) However, we recommend security researchers provide as much information as possible on the form so that the maintainers can make an informed decision about the submitted report. You can adopt the template used by our security researchers from the GitHub Security Lab, which is available on the `github/securitylab` repository."

   For more information about the fields available and guidance on filling in the form, see "Creating a repository security advisory" and "Best practices for writing repository security advisories."

5. At the bottom of the form, click **Submit report**. GitHub will display a message letting you know that maintainers have been notified and that you have a pending credit for this security advisory.

   Tip: When the report is submitted, GitHub automatically adds the reporter of the vulnerability as a collaborator and as a credited user on the proposed advisory.

6. Optionally, click **Start a temporary private fork** if you want to start to fix the issue. Note that only the repository maintainer can merge changes from that private fork into the parent repository.



security-researcher-1 added as a collaborator 1 minute ago

Collaborate on a patch in private
Use a temporary private fork of **octo-org/octo-repo** to collaborate on a fix.

Thank you for reporting a vulnerability.
Your report is being reviewed by **octo-org-octo-repo** owners. You will be notified if the report is published as an advisory.

The next steps depend on the action taken by the repository maintainer. For more information, see "Managing privately reported security vulnerabilities."