Publishing a repository security advisory

In this article

You can publish a security advisory to alert your community about a security vulnerability in your project.

Anyone with admin permissions to a security advisory can publish the security advisory.

> **Note**: This article applies to editing repository-level advisories as a repository owner.
>
> Users who are not repository owners can contribute to global security advisories in the GitHub Advisory Database at github.com/advisories. Edits to global advisories will not change or affect how the advisory appears on the repository. For more information, see "Editing security advisories in the GitHub Advisory Database."

Prerequisites

Before you can publish a security advisory or request a CVE identification number, you must create a draft security advisory and provide information about the versions of your project affected by the security vulnerability. For more information, see "Creating a repository security advisory."

If you've created a security advisory but haven't yet provided details about the versions of your project that the security vulnerability affects, you can edit the security advisory. For more information, see "Editing a repository security advisory."

About publishing a security advisory

When you publish a security advisory, you notify your community about the security vulnerability that the security advisory addresses. Publishing a security advisory makes it easier for your community to update package dependencies and research the impact of the security vulnerability.

You can also use repository security advisories to republish the details of a security vulnerability that you have already disclosed elsewhere by copying and pasting the details of the vulnerability into a new security advisory.

Before you publish a security advisory, you can privately collaborate to fix the vulnerability in a temporary private fork. For more information, see "Collaborating in a temporary private fork to resolve a repository security vulnerability."

Warning: Whenever possible, you should always add a fix version to a security advisory prior to publishing the advisory. If you don't, the advisory will be published without a fixed version, and Dependabot will alert your users about the issue, without offering any safe version to update to.

We recommend you take the following steps in these different situations:

- If a fix version is imminently available, and you are able to, wait to disclose the issue when the fix is ready.
- If a fix version is in development but not yet available, mention this in the advisory, and edit the advisory later, after publication.
- If you are not planning to fix the issue, be clear about it in the advisory so that your users don't contact you to ask when a fix will be made. In this case, it is helpful to include steps users can take to mitigate the issue.

When you publish a draft advisory from a public repository, everyone is able to see:

- The current version of the advisory data.
- Any advisory credits that the credited users have accepted.

Note: The general public will never have access to the edit history of the advisory, and will only see the published version.

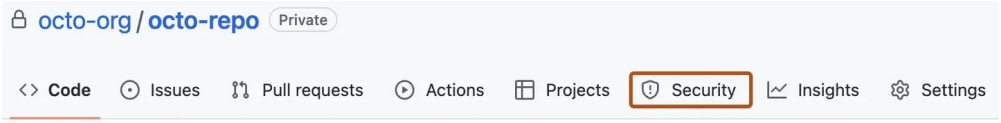
After you publish a security advisory, the URL for the security advisory will remain the same as before you published the security advisory. Anyone with read access to the repository can see the security advisory. Collaborators on the security advisory can continue to view past conversations, including the full comment stream, in the security advisory unless someone with admin permissions removes the collaborator from the security advisory.

If you need to update or correct information in a security advisory that you've published, you can edit the security advisory. For more information, see "Editing a repository security advisory."

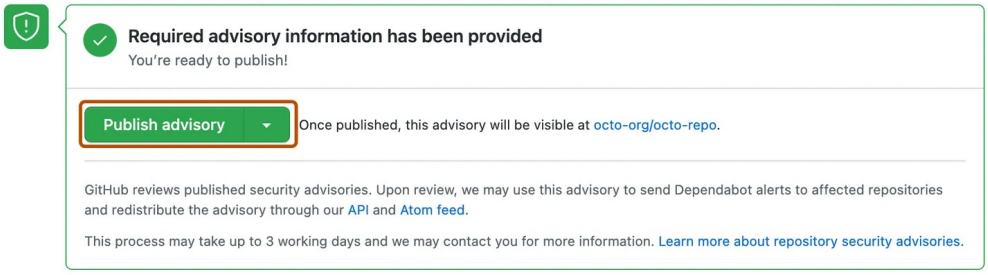
Publishing a security advisory

Publishing a security advisory deletes the temporary private fork for the security advisory.

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. In the "Security Advisories" list, click the name of the security advisory you'd like to publish.
5. Scroll to the bottom of the advisory form and click **Publish advisory**.



Note: If you selected "Request CVE ID later", you will see a **Request CVE** button in place of the **Publish advisory** button. For more information, see "Requesting a CVE identification number (Optional)" below.

Dependabot alerts for published security advisories

GitHub will review each published security advisory, add it to the GitHub Advisory Database, and may use the security advisory to send Dependabot alerts to affected repositories. If the security advisory comes from a fork, we'll only send an alert if the fork owns a package, published under a unique name, on a public package registry. This process can take up to 72 hours and GitHub may contact you for more information.

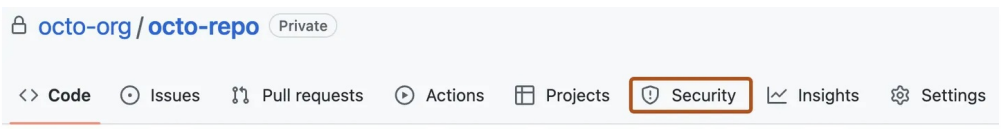
For more information about Dependabot alerts, see "About Dependabot alerts" and "About Dependabot security updates." For more information about GitHub Advisory Database, see "Browsing security advisories in the GitHub Advisory Database."

Requesting a CVE identification number (Optional)

If you want a CVE identification number for the security vulnerability in your project, and don't already have one, you can request a CVE identification number from GitHub. GitHub usually reviews the request within 72 hours. Requesting a CVE identification number doesn't make your security advisory public. If your security advisory is eligible for a CVE, GitHub will reserve a CVE identification number for your advisory. We'll then publish the CVE details after you make your security advisory public. Anyone with admin permissions to a security advisory can request a CVE identification number.

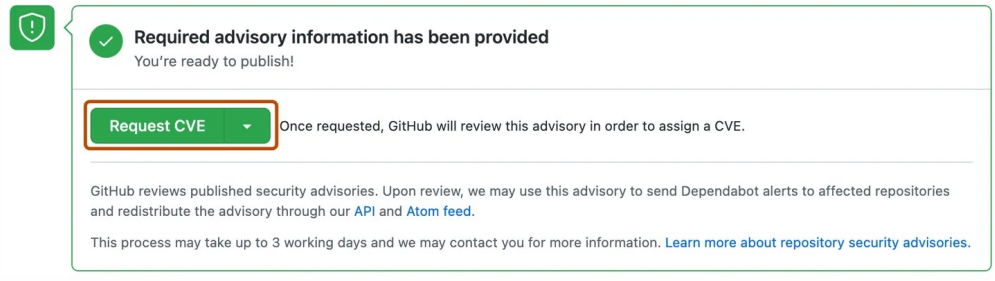
If you already have a CVE you want to use, for example, if you use a CVE Numbering Authority (CNA) other than GitHub, add the CVE to the security advisory form. This may happen, for example, if you want to get the advisory consistent with other communications you plan to send out at publication time. GitHub cannot assign CVEs to your project if it is covered by another CNA. For more information, see "About repository security advisories."

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. In the "Security Advisories" list, click the name of the security advisory you'd like to request a CVE identification number for.
5. Scroll to the bottom of the advisory form and click **Request CVE**.



Further reading

- "Withdrawing a repository security advisory"