# Editing a repository security advisory

**In this article**

You can edit the metadata and description for a repository security advisory if you need to update details or correct errors.

**Who can use this feature**
Anyone with admin permissions to a repository security advisory, or with a security manager role within the repository, can edit 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."

## Editing a security advisory 🔗

You can also use the REST API to edit repository security advisories. For more information, see "Repository security advisories" in the REST API documentation.

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**.
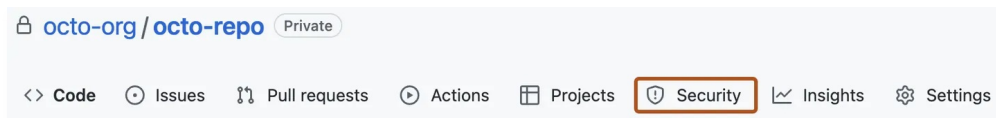
   

3. In the left sidebar, under "Reporting", click ⊕ **Advisories**.

4. In the "Security Advisories" list, click the name of the security advisory you'd like to edit.

5. In the upper-right corner of the details for the security advisory, click **Edit advisory**. This will open the security advisory form in edit mode.

6. Use the **CVE identifier** dropdown menu to specify whether you already have a CVE identifier or plan to request one from GitHub later. If you have an existing CVE identifier, select **I have an existing CVE identifier** to display an **Existing CVE** field, and type the CVE identifier in the field. For more information, see "About repository security advisories."

7. In the **Description** field, type a description of the security vulnerability including its

impact, any patches or workarounds available, and any references.

8. Under "Affected products", define the ecosystem, package name, affected/patched versions, and vulnerable functions for the security vulnerability that this security advisory describes. If applicable, you can add multiple affected products to the same advisory by clicking **Add another affected product**.

   For information about how to specify information on the form, including affected versions, see "[Best practices for writing repository security advisories](#)."

9. Define the severity of the security vulnerability using the **Severity** dropdown menu. If you want to calculate a CVSS score, select **Assess severity using CVSS** and then select the appropriate values in the **Calculator**. The GitHub Enterprise Cloud calculates the score according to the [Common Vulnerability Scoring System Calculator](#).

10. Under "Weaknesses", in the **Common weakness enumerator** field, type common weakness enumerators (CWEs) that describe the kinds of security weaknesses that this security advisory reports. For a full list of CWEs, see the "[Common Weakness Enumeration](#)" from MITRE.

11. Optionally, under "Credits", remove existing credits, or use the search box to find additional people you want to credit on the security advisory, then click their username to add them.

    - Use the dropdown menu next to the name of the person you're crediting to assign a credit type. For more information about credit types, see "[Creating a repository security advisory](#)."

    

    - Optionally, to remove someone, click the ✕ next to the credit type.

12. Click **Update security advisory**.

The people listed in the "Credits" section will receive an email or web notification inviting them to accept credit. If a person accepts, their username will be publicly visible once the security advisory is published.

## Further reading 🔗

- "[Withdrawing a repository security advisory](#)"