Creating a repository security advisory

In this article

Creating a security advisory

Next steps

You can create a draft security advisory to privately discuss and fix a security vulnerability in your open source project.
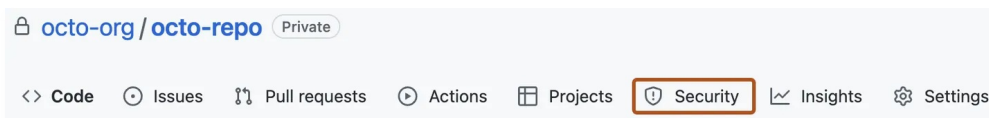
Who can use this feature
Anyone with admin permissions to a repository, or with a security manager role within the repository, can create a security advisory.

> **Note:** If you are a security researcher, you should directly contact maintainers to ask them to create security advisories or issue CVEs on your behalf in repositories that you don't administer. However, if private vulnerabiliy reporting is enabled for the repository, you can *privately* report a vulnerability yourself. For more information, see "Privately reporting a security vulnerability."

Creating a security advisory 🔗

You can also use the REST API to create 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**.

   🔒 octo-org / **octo-repo** ⸤Private⸣

   ⟨⟩ **Code**   ⊙ Issues   ⑂ Pull requests   ⊙ Actions   ⊞ Projects   ⓘ Security   ⬚ Insights   ⚙ Settings

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

4. Click **New draft security advisory** to open the draft advisory form. The fields marked with an asterisk are required.

5. In the **Title** field, type a title for your security advisory.

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", add credits by searching for a GitHub username, the email address associated with their GitHub account, or their full name.

    - 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 the About credits for repository security advisories section.

    Credits

    🔍 Add a user by username, full name, or email

    ○ 🐱 **octocat** The Octocat | Choose a credit type ⇕ | ✕

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

12. Click **Create draft 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.

About credits for repository security advisories 🔗

You can credit people who helped discover, report, or fix a security vulnerability. If you credit someone, they can choose to accept or decline credit.

You can assign different types of credit to people.

Credit type	Reason
Finder	Identifies the vulnerability
Reporter	Notifies the vendor of the vulnerability to a CNA
Analyst	Validates the vulnerability to ensure accuracy or severity
Coordinator	Facilitates the coordinated response process
Remediation developer	Prepares a code change or other remediation plans

Remediation reviewer	Reviews vulnerability remediation plans or code changes for effectiveness and completeness
Remediation verifier	Tests and verifies the vulnerability or its remediation
Tool	Names of tools used in vulnerability discovery or identification
Sponsor	Supports the vulnerability identification or remediation activities

If someone accepts credit, the person's username appears in the "Credits" section of the security advisory. Anyone with read access to the repository can see the advisory and the people who accepted credit for it.

> **Note:** If you believe you should be credited for a security advisory, please contact the creator of the advisory and to ask for the advisory to be edited to include your credit. Only the creator of the advisory can credit you, so please don't contact GitHub Support about credits for security advisories.

Next steps ⚲

- Comment on the draft security advisory to discuss the vulnerability with your team.
- Add collaborators to the security advisory. For more information, see "Adding a collaborator to a repository security advisory."
- 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."
- Add individuals who should receive credit for contributing to the security advisory. For more information, see "Editing a repository security advisory."
- Publish the security advisory to notify your community of the security vulnerability. For more information, see "Publishing a repository security advisory."