Exporting a software bill of materials for your repository

In this article

You can export a software bill of materials or SBOM for your repository from the dependency graph. SBOMs allow transparency into your open source usage and help expose supply chain vulnerabilities, reducing supply chain risks.

> **Who can use this feature**
> Anyone can export the dependency graph of a repository as a software bill of materials. The SBOM export will contain a list of the dependencies that are used in the repository.

About the dependency graph and SBOM exports

The dependency graph is a summary of the manifest and lock files stored in a repository and any dependencies that are submitted for the repository using the Dependency submission API (beta). For each repository, it shows:

- Dependencies, the ecosystems and packages it depends on
- Dependents, the repositories and packages that depend on it

For each dependency, you can see the license information and vulnerability severity. You can also search for a specific dependency using the search bar. Dependencies are sorted automatically by vulnerability severity.

You can export the current state of the dependency graph for your repository as a Software Bill of Materials (SBOM) using the industry standard SPDX format:

- Via the GitHub UI
- Using the REST API

An SBOM is a formal, machine-readable inventory of a project's dependencies and associated information (such as versions, package identifiers, and licenses). SBOMs help reduced supply chain risks by:

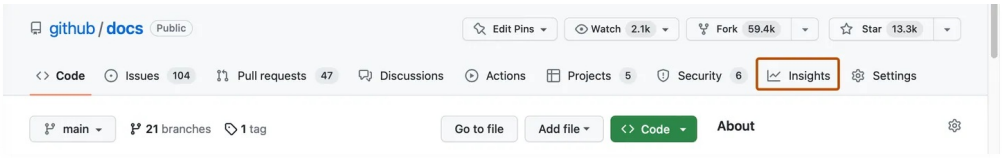
- providing transparency about the dependencies used by your repository
- allowing vulnerabilities to be identified early in the process
- providing insights in the license compliance, security, or quality issues that may exist in your codebase
- enabling you to better comply with various data protection standards

If your company provides software to the US federal government per Executive Order 14028, you will need to provide an SBOM for your product. You can also use SBOMs as part of your audit process and use them to comply with regulatory and legal

requirements.

Exporting a software bill of material for your repository from the UI

1. On GitHub.com, navigate to the main page of the repository.
2. Under your repository name, click **Insights**.



3. In the left sidebar, click **Dependency graph**.
4. On the top right side of the **Dependencies** tab, click **Export SBOM** to generate an SBOM file for download from your browser.

Exporting a software bill of material for your repository using the REST API

If you want to use the REST API to export an SBOM for your repository, see Software bill of materials (SBOM) in the REST API documentation for more information.