Understanding your software supply chain

About supply chain security

GitHub Enterprise Cloud helps you secure your supply chain, from understanding the dependencies in your environment, to knowing about vulnerabilities in those dependencies, and patching them.

About the dependency graph

You can use the dependency graph to identify all your project's dependencies. The dependency graph supports a range of popular package ecosystems.

Configuring the dependency graph

You can allow users to identify their projects' dependencies by enabling the dependency graph.

Exporting a software bill of materials for your repository

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.

Using the Dependency submission API

You can use the Dependency submission API to submit dependencies for projects, such as the dependencies resolved when a project is built or compiled.

About dependency review

Dependency review lets you catch insecure dependencies before you introduce them to your environment, and provides information on license, dependents, and age of dependencies.

Configuring dependency review

You can use dependency review to catch vulnerabilities before they are added to your project.

Exploring the dependencies of a repository

You can use the dependency graph to see the packages your project depends on and the repositories that depend on it. In addition, you can see any vulnerabilities detected in its dependencies.

Troubleshooting the dependency graph

If the dependency information reported by the dependency graph is not what you expected, there are a number of points to consider, and various things you can check.
