About supply chain security

In this article

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

About supply chain security at GitHub

With the accelerated use of open source, most projects depend on hundreds of open-source dependencies. This poses a security problem: what if the dependencies you're using are vulnerable? You could be putting your users at risk of a supply chain attack. One of the most important things you can do to protect your supply chain is to patch your vulnerable dependencies and replace any malware.

You add dependencies directly to your supply chain when you specify them in a manifest file or a lockfile. Dependencies can also be included transitively, that is, even if you don’t specify a particular dependency, but a dependency of yours uses it, then you’re also dependent on that dependency.

GitHub Enterprise Server offers a range of features to help you understand the dependencies in your environment, know about vulnerabilities in those dependencies, and patch them.

The supply chain features on GitHub Enterprise Server are:

- **Dependency graph**
- **Dependency review**
- **Dependabot alerts**
- **Dependabot updates**
  - **Dependabot security updates**
  - **Dependabot version updates**

The dependency graph is central to supply chain security. The dependency graph identifies all upstream dependencies and public downstream dependents of a repository or package. You can see your repository’s dependencies and some of their properties, like vulnerability information, on the dependency graph for the repository.

Other supply chain features on GitHub rely on the information provided by the dependency graph.

- Dependency review uses the dependency graph to identify dependency changes and help you understand the security impact of these changes when you review pull requests.

- Dependabot cross-references dependency data provided by the dependency graph with the list of advisories published in the GitHub Advisory Database, scans your dependencies and generates Dependabot alerts when a potential vulnerability or malware is detected.
- Dependabot security updates use the dependency graph and Dependabot alerts to help you update dependencies with known vulnerabilities in your repository.

Dependabot version updates don't use the dependency graph and rely on the semantic versioning of dependencies instead. Dependabot version updates help you keep your dependencies updated, even when they don’t have any vulnerabilities.

For best practice guides on end-to-end supply chain security including the protection of personal accounts, code, and build processes, see "Securing your end-to-end supply chain."

Feature overview

What is the dependency graph

To generate the dependency graph, GitHub looks at a repository’s explicit dependencies declared in the manifest and lockfiles. When enabled, the dependency graph automatically parses all known package manifest files in the repository, and uses this to construct a graph with known dependency names and versions.

- The dependency graph includes information on your *direct* dependencies and *transitive* dependencies.
- The dependency graph is automatically updated when you push a commit to GitHub that changes or adds a supported manifest or lock file to the default branch, and when anyone pushes a change to the repository of one of your dependencies.
- You can see the dependency graph by opening the repository's main page on GitHub Enterprise Server, and navigating to the **Insights** tab.
- If you have at least read access to the repository, you can export the dependency graph for the repository as an SPDX-compatible, Software Bill of Materials (SBOM), via the GitHub UI or GitHub REST API. For more information, see "Exporting a software bill of materials for your repository."

Additionally, you can use the Dependency submission API (beta) to submit dependencies from the package manager or ecosystem of your choice, even if the ecosystem is not supported by dependency graph for manifest or lock file analysis. The dependency graph will display the submitted dependencies grouped by ecosystem, but separately from the dependencies parsed from manifest or lock files. For more information on the Dependency submission API, see "Using the Dependency submission API."

For more information about the dependency graph, see "About the dependency graph."

What is dependency review

Dependency review helps reviewers and contributors understand dependency changes and their security impact in every pull request.

- Dependency review tells you which dependencies were added, removed, or updated, in a pull request. You can use the release dates, popularity of dependencies, and vulnerability information to help you decide whether to accept the change.
- You can see the dependency review for a pull request by showing the rich diff on the **Files Changed** tab.

For more information about dependency review, see "About dependency review."

What is Dependabot

Dependabot keeps your dependencies up to date by informing you of any security vulnerabilities in your dependencies, and automatically opens pull requests to upgrade your dependencies to the next available secure version when a Dependabot alert is triggered, or to the latest version when a release is published.

The term "Dependabot" encompasses the following features:

- Dependabot alerts—Displayed notification on the **Security** tab for the repository, and in the repository's dependency graph. The alert includes a link to the affected file in the project, and information about a fixed version.
- Dependabot updates:
    - Dependabot security updates—Triggered updates to upgrade your dependencies to a secure version when an alert is triggered.
    - Dependabot version updates—Scheduled updates to keep your dependencies up to date with the latest version.

Dependabot security updates and Dependabot version updates require GitHub Actions to run on GitHub Enterprise Server. Dependabot alerts do not require GitHub Actions. For more information, see "Enabling Dependabot for your enterprise."

Dependabot security updates can fix vulnerable dependencies in GitHub Actions. When security updates are enabled, Dependabot will automatically raise a pull request to update vulnerable GitHub Actions used in your workflows to the minimum patched version. For more information, see "About Dependabot security updates."

What are Dependabot alerts

Dependabot alerts highlight repositories affected by a newly discovered vulnerability based on the dependency graph and the GitHub Advisory Database, which contains advisories for known vulnerabilities and malware.

- Dependabot performs a scan to detect insecure dependencies and sends Dependabot alerts when:
    - New advisory data is synchronized to your GitHub Enterprise Server instance each hour from GitHub.com. For more information, see "Browsing security advisories in the GitHub Advisory Database."
    - The dependency graph for the repository changes.
- Dependabot alerts are displayed on the **Security** tab for the repository and in the repository's dependency graph. The alert includes a link to the affected file in the project, and information about a fixed version.

For more information, see "About Dependabot alerts."

What are Dependabot updates

There are two types of Dependabot updates: Dependabot *security* updates and *version* updates. Dependabot generates automatic pull requests to update your dependencies in both cases, but there are several differences.

Dependabot security updates:

- Triggered by a Dependabot alert
- Update dependencies to the minimum version that resolves a known vulnerability
- Supported for ecosystems the dependency graph supports
- Does not require a configuration file, but you can use one to override the default behavior

Dependabot version updates:

- Requires a configuration file
- Run on a schedule you configure
- Update dependencies to the latest version that matches the configuration
- Supported for a different group of ecosystems

For more information about Dependabot updates, see "About Dependabot security updates" and "About Dependabot version updates."

Feature availability

- **Dependency graph** and **Dependabot alerts**—not enabled by default. Both features are configured at an enterprise level by the enterprise owner. For more information, see "Enabling the dependency graph for your enterprise" and "Enabling Dependabot for your enterprise."

- **Dependency review**—available when dependency graph is enabled for your GitHub Enterprise Server instance and Advanced Security is enabled for the organization or repository. For more information, see "About GitHub Advanced Security."

- **Dependabot security updates**—not enabled by default. You can enable Dependabot security updates for any repository that uses Dependabot alerts and the dependency graph. For information about enabling security updates, see "Configuring Dependabot security updates."

- **Dependabot version updates**—not enabled by default. People with write permissions to a repository can enable Dependabot version updates. For information about enabling version updates, see "Configuring Dependabot version updates."