GitHub security features

In this article

An overview of GitHub security features.

About GitHub's security features

GitHub has security features that help keep code and secrets secure in repositories and across organizations. Some features are available for repositories on all plans. Additional features are available to enterprises that use GitHub Advanced Security. GitHub Advanced Security features are also enabled for all public repositories on GitHub.com. For more information, see "About GitHub Advanced Security."

The GitHub Advisory Database contains a curated list of security vulnerabilities that you can view, search, and filter. For more information, see "Browsing security advisories in the GitHub Advisory Database."

Available for all repositories

Security policy

Make it easy for your users to confidentially report security vulnerabilities they've found in your repository. For more information, see "Adding a security policy to your repository."

Security advisories

Privately discuss and fix security vulnerabilities in your repository's code. You can then publish a security advisory to alert your community to the vulnerability and encourage community members to upgrade. For more information, see "About repository security advisories."

Dependabot alerts and security updates

View alerts about dependencies that are known to contain security vulnerabilities, and choose whether to have pull requests generated automatically to update these dependencies. For more information, see "About Dependabot alerts" and "About Dependabot security updates."

Additionally, you can use Dependabot alert rules to filter out false positive alerts or alerts you're not interested in, based on complex logic from a variety of contextual criteria. For more information, see "About Dependabot alert rules."

For an overview of the different features offered by Dependabot and instructions on how to get started, see "Dependabot quickstart guide."

Dependabot version updates

Use Dependabot to automatically raise pull requests to keep your dependencies up-to-date. This helps reduce your exposure to older versions of dependencies. Using newer versions makes it easier to apply patches if security vulnerabilities are discovered, and also makes it easier for Dependabot security updates to successfully raise pull requests to upgrade vulnerable dependencies. You can also customize Dependabot version updates to streamline their integration into your repositories. For more information, see "About Dependabot version updates."

Dependency graph

The dependency graph allows you to explore the ecosystems and packages that your repository depends on and the repositories and packages that depend on your repository.

You can find the dependency graph on the **Insights** tab for your repository. For more information, see "About the dependency graph."

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."

Security overview for repositories

Security overview shows which security features are enabled for the repository, and lets you configure any available security features that are not already enabled.

Available for free public repositories

Secret scanning alerts for partners

Automatically detect leaked secrets across all public repositories, as well as public npm packages. GitHub informs the relevant service provider that the secret may be compromised. For details of the supported secrets and service providers, see "Secret scanning patterns."

Available with GitHub Advanced Security

The following GitHub Advanced Security features are available and free of charge for public repositories on GitHub.com. Organizations that use GitHub Enterprise Cloud with a license for GitHub Advanced Security can use the full set of features in any of their repositories. For a list of the features available with GitHub Enterprise Cloud, see the GitHub Enterprise Cloud documentation.

Code scanning

Automatically detect security vulnerabilities and coding errors in new or modified code. Potential problems are highlighted, with detailed information, allowing you to fix the code before it's merged into your default branch. For more information, see "About code scanning."

Secret scanning alerts for users

Automatically detect tokens or credentials that have been checked into a repository. You can view alerts for any secrets that GitHub finds in your code, in the **Security** tab of the repository, so that you know which tokens or credentials to treat as compromised. For more information, see "About secret scanning."

Dependency review

Show the full impact of changes to dependencies and see details of any vulnerable versions before you merge a pull request. For more information, see "About dependency review."

Further reading

- "GitHub's plans"
- "GitHub language support"