This version of GitHub Enterprise was discontinued on 2023-03-15. No patch releases will be made, even for critical security issues. For better performance, improved security, and new features, upgrade to the latest version of GitHub Enterprise. For help with the upgrade, contact GitHub Enterprise support.

Automatically scanning your code for vulnerabilities and errors

You can find vulnerabilities and errors in your project's code on GitHub, as well as view, triage, understand, and resolve the related code scanning alerts.

Code scanning is available for organization-owned repositories in GitHub Enterprise Server. This feature requires a license for GitHub Advanced Security. For more information, see "About GitHub Advanced Security."

About code scanning with CodeQL

You can use CodeQL to identify vulnerabilities and errors in your code. The results are shown as code scanning alerts in GitHub.

Recommended hardware resources for running CodeQL

Recommended specifications (RAM, CPU cores, and disk) for running CodeQL analysis on self-hosted machines, based on the size of your codebase.

Configuring the CodeQL workflow for compiled languages

You can configure how GitHub uses the CodeQL analysis workflow to scan code written in compiled languages for vulnerabilities and errors.

Troubleshooting the CodeQL workflow

If you're having problems with code scanning setup, you can troubleshoot by using these tips for resolving issues.

Running CodeQL code scanning in a container

You can run code scanning in a container by ensuring that all processes run in the same container.

Viewing code scanning logs

You can view the output generated during code scanning analysis in your GitHub Enterprise Server instance.