

CASE STUDY

Sourcegraph reaches “inbox zero” for CVEs with Chainguard Images

The growing use of open-source components and dependencies can create security vulnerabilities. This case study explains how Sourcegraph streamlined Common Vulnerabilities and Exposures (CVEs) detection and remediation with Chainguard Images, significantly reducing known vulnerabilities.

Challenge

CVEs are a long-standing reality in software development. As more companies leverage open-source components, dependencies, and libraries to accelerate product creation and development, developers have less control over the security of their release pipelines and artifact sources. Sourcegraph helps developers stay secure and in control through a code search and intelligence tool to index and analyze large code bases that incorporate commercial open-source, local, and cloud-based repositories.

When the Sourcegraph team detected a CVE, reviewing and remediating the issue was a lengthy process, involving everything from triaging the components and patching the code to creating an exception for the issue and documenting it. It was incredibly timeconsuming — the equivalent of a full-time engineer spending 25% of their time detecting and remediating vulnerabilities. The complexity of identifying and resolving CVEs also had a negative effect on their sales and customer success divisions, who fielded calls from frustrated customers who couldn't leverage the latest version of Sourcegraph software because it had known vulnerabilities. When looking for a solution to detect and eliminate CVEs, Sourcegraph's top priority was a product that avoided unnecessary packages in dependencies, employing and securing the fewest possible pieces needed to build working images.



About

Sourcegraph is the leading Code AI platform revolutionizing how developers understand, fix, and automate their code. Over one million engineers use Sourcegraph to improve code security, efficiently onboard developers, promote code reuse, resolve incidents, and boost code health.

Industry

Software Development

Products

[Chainguard Images](#)

Cloud Platform

Google Cloud

The scratch and distroless image solutions lacked adequate support, and the Sourcegraph team needed something that combined the wisdom of the open-source community and the stability and resources of an enterprise-level commercial product.

“

We had a lot of discussions with customers who weren't happy because they were not able to use the latest releases that we distributed. And then suddenly, as the customers were using the new releases with Wolfi OS and Chainguard Images, there was not that friction. It was really impressive.

Diego Comas

Head of Security, Sourcegraph

Solution

Sourcegraph found the right combination of security and support in Chainguard Images, a collection of container base images that eliminates complexity and reduces security risks by shrinking the number of components needed to compile an image to the bare minimum. The platform was an overnight success: where the team previously struggled with minimizing and triaging CVEs in their most critical customerfacing images, they adopted Chainguard Images and reached inbox zero — zero-known CVEs — for the first time in two years. Chainguard Images eliminated the daily headache of vulnerability maintenance and freed engineers and customer success teams to focus on customer innovation, new security controls, and other improvements.

Chainguard Images helps to streamline and improve customer conversations and interactions, creating friction-free deployments for users. Customers previously had to wait weeks before they were comfortable using Sourcegraph's latest release, and it took 10–15 business days to approve and review exceptions and issue patches. Now, the containers within their control ship CVE-free. Chainguard resolves any issues as part of its daily patching process, so there's never more than a two- or three-day delay. It's a massive improvement for Sourcegraph's business, and they can operate with more confidence knowing their software is developed with components free of known vulnerabilities.