Chainguard

Chainguard Libraries

Combat malware attacks without compromising developer experience and productivity with language dependencies built securely from source in SLSA-hardened infrastructure.

Enterprise reliance on open source language libraries from public registries like Maven Central, PyPI, and npm has become ubiquitous. But these registries are designed for frictionless publishing, not secure enterprise consumption. As a result, language libraries are a complex and critical attack vector for enterprises to lock down as malware attacks become pervasive, particularly at the package build and distribution stages of the software supply chain.

Chainguard Libraries helps organizations prevent malware and supply chain attacks by offering a secure, trusted set of libraries built entirely from source. This offering provides a single standardized endpoint for developers to pull libraries, ensuring enterprises protect themselves against software supply chain attacks at the build and distribution stages without compromising developer experience and productivity.

Chainguard Libraries offers the following benefits:

Hardening against supply chain attacks

Eliminate risks from compromised build systems and hijacked package distribution mechanisms to prevent attacks like XZ-Utils, MavenGate, and npm Shai-Hulud. Chainguard Libraries provide trusted, verifiable packages that ensure end-to-end integrity, giving developers a secure and reliable foundation to build. Chainguard Libraries contains significantly fewer CVEs and features a minimized attack surface, substantially reducing security risk.

Improved developer experience and velocity

Free up developers to ship faster by eliminating toil, complexity, and overhead that slow down operations. Chainguard Libraries replaces time-consuming, manual, and policy-based package curation with a single, trusted source of truth for libraries.

Simplify dynamic dependencies

Offload the hard work of building the required system libraries by dynamically linking dependencies to Chainguard Libraries. Reduce manual developer effort to decouple language libraries from the OS to ensure that shared libraries are readily available and updated.

Features of Chainguard Libraries:

1. **Continuously built from source:** Continuously built from source in Chainguard's SLSA Level 2 build infrastructure, eliminating supply chain attacks at the build and distribution phases of the package lifecycle.

2. **CVE remediation:** Chainguard Libraries provides built-in CVE remediation to protect organizations from high and critical vulnerabilities by offering patch versions of older Python Libraries, supporting organizations that rely on older versions of libraries, where maintainers are no longer providing fixes before they're able to upgrade.

3. **Use anywhere; better with Chainguard images:** Use anywhere code is developed and deployed. Or use with Chainguard Containers or VMs for complete protection over the entire stack.

4. **One secure, standardized source for all dependencies:** Chainguard Libraries is a single source of safe and secure language dependencies for Java, Python, and JavaScript with a signature from Chainguard and a build receipt describing the source of the library artifact, including the build infrastructure and tooling.

5. **Integration with common artifact managers:** Chainguard Libraries ensures consistency in existing dev workflows by integrating with common artifact managers like JFrog Artifactory, Cloudsmith, and Sonatype Nexus so that developers can pull trusted dependencies without any disruption in experience.

Our customers

ANDURIL Canva DELL Technologies Domino elastic GitLab Hewlett Packard Enterprise snowflake