Terms & Policies

Learn more about Chainguard policies and our legal documents.

Select legal document

Last Updated February 22, 2024

Chainguard SLA

Common Vulnerabilities and Exposures. Chainguard will use commercially reasonable efforts to address common vulnerabilities and exposures ("CVEs") for Chainguard's published collection of images (the "Guarded Images") as covered by this SLA, provided the CVEs meet all of the following requirements (a "Qualifying Patch"):

1. Chainguard's scanners identifies a CVE affecting a Guarded Image;
2. The CVE is independently fixable of any other bugs;
3. The CVE does not require the recompilation of more than one quarter (or 25%) of all Guarded Images (a "Major CVE Event"); and
4. Either (i) there is an upstream release version available which a credible and independent third party has verified fixes the CVE (i.e. the project maintainers have release notes or code commit message designating a fix to the CVE) or (ii) an affected Guarded Image can be rebuilt with updated compilers and/or libraries to remediate that CVE.

Severity Scoring. Chainguard may assign each CVE meeting the above criteria a severity score according to the Common Vulnerability Scoring System version 3, in accordance with the standards described at https://nvd.nist.gov/vuln-metrics/cvss. In addition, to the extent Customer requests a CVE severity score, Chainguard may elect to evaluate such CVE to determine, in good faith, the applicable CVE severity score.

Patching. Chainguard shall use commercially reasonable efforts to patch CVEs in Guarded Images within the estimated timeframe set forth below.

Critical Severity: 7 calendar days from the date a Qualifying Patch is publicly available.

High, Medium, and Low severity - 14 calendar days from the date a Qualifying Patch is publicly available.

In the event a CVE does not meet the requirements of a Qualifying Patch due to a Major CVE Event, Chainguard will use commercially reasonable efforts to rebuild all images promptly.

Remediation. A CVE will be considered patched when any of the following occur:

1. an Image or update to the Chainguard software is published to the Chainguard hosted registry; or
2. the CVE is either: a) not reported when passing the published image through Grype and Vexctl; or b) has been demonstrably added to the Chainguard security fixes feed.

In the event an image contains components that are FIPS validated, Chainguard will remediate any CVE in line with the above considerations, unless remediating would void the FIPS validation.

Resources

Light Dark

Media Kit →

Contact Us

Privacy Policy | Terms of Use