Echo Images and Libraries SLA

Last updated on May 10, 2026

1. General

Subject to Customer's compliance with its obligations under the Subscription Agreement ("**Agreement**") entered between Customer and Echo Software Ltd. ("**Echo**"), during the term of the Agreement, Echo will use commercially reasonable efforts to address common vulnerabilities and exposures ("**CVEs**") affecting container images and libraries distributed via the Echo registry and repository (collectively referred to as the "**Clean Artifacts**"), by providing an applicable patch (each, a "**Patch**"), provided that the CVEs meet the requirements outlined below. Capitalized terms not defined herein, shall have the meaning ascribed to such terms in the Agreement. Echo reserves the right to change the terms of this SLA by posting an updated version on its website or by other reasonable means of notification, and such changes will become effective upon posting or notification. Any conflict between the terms of this SLA and the terms of Agreement regarding the description, delivery or specific requirements of the services under this SLA shall be resolved in favor of the terms of this SLA; all other conflicts between the terms of this SLA and the terms of the Agreement shall be resolved in favor of the Agreement.

2. Patch Eligibility Criteria

2.1 A CVE qualifies for remediation under this SLA if all of the following conditions are met:

1. **Detection:** The CVE is detected by security scanners currently in use by Echo. An up-to-date list of supported scanners is available on Echo's private documentation.
2. **Isolated Fix:** The CVE can be addressed independently and is not inherently linked to other bugs or systemic issues.
3. **Compatibility Preservation:** Applying the fix does not break backward compatibility of the affected Clean Artifact or introduce regressions.
4. **Official Fix Availability:** One of the following is available:
    1. An upstream release (with accompanying release notes or verified commit messages) that explicitly resolves the CVE.
    2. An updated version of the affected package or library that remediates the vulnerability.

2.2 Echo shall not be required to remediate any CVE that in Echo's reasonable discretion, results from:

1. Any modifications of the Service that have not been approved by Echo in writing;
2. Customer installation or set up adjustments;
3. Use of the Service other than as permitted in the Agreement;

4. Any fault in any equipment or programs used in conjunction with the Service, or other causes beyond the control of Echo; and/or
5. Customer's negligence or willful misconduct.

3. Patch Timelines

Echo will use commercially reasonable efforts to apply eligible Patches to Clean Artifacts within the following timeframes provided that all conditions detailed above are met:

1. Critical Severity and High Severity: within 7 business days
2. Medium Severity and Low Severity: within 10 business days

It is hereby clarified that the severity level will be determined based on automated results produced by Echo's scanners.

4. Remediation Completion Criteria

A CVE will be considered remediated when any one of the following conditions is met:

1. A new version of the affected image is published to the Echo platform with the vulnerability resolved.
2. An updated version of the affected library is published to the Echo platform with the vulnerability resolved.
3. The CVE is no longer detected by Echo's designated scanners.
4. The CVE is documented as resolved in Echo's public vulnerability remediation feed.

5. FIPS-Validated Components

For Clean Artifacts containing FIPS-validated components, Echo will remediate CVEs in accordance with the update stream of the validated module, regardless of timelines. However, Echo may defer or modify remediation efforts if applying the fix would invalidate the FIPS certification of the component.

6. Alternative Mitigations

In scenarios where no official fix is yet available, Echo may apply temporary mitigations (e.g., custom patching, backported fixes) to achieve a zero-detected-CVE state, subject to feasibility and scanner validation. Alternative Mitigations described under Section 6 are valid only in cases where the fix is isolated and compatibility preserved.