TERMS OF SERVICE

TERMS OF SERVICE

Last Updated: December 31, 2025

Root.io, Inc.

1. ACCEPTANCE OF TERMS

By accessing or using the services provided by Root.io, Inc. ("Root," "we," "us," or "our"), including our website at www.root.io, the Root Platform, and any related services (collectively, the "Services"), you ("Customer" or "you") agree to be bound by these Terms of Service ("Terms").

If you are entering into these Terms on behalf of a company or other legal entity, you represent that you have the authority to bind such entities to these Terms.

If you do not agree to these Terms, you may not access or use the Services.

2. DEFINITIONS

"Authorized Users" means Customer's employees and contractors authorized by Customer to access and use the Services on Customer's behalf.

"Community Images" means container images designated by Root as available to Customer without a paid subscription. Community Images are provided without warranty or SLA.

"Customer Configuration Data" means information provided by Customer to enable the Services to be configured, including registry credentials, image tags, library specifications, and subscription selections.

"Customer Environment Data" means vulnerability scan results and metadata derived from Customer's subscribed images and libraries.

"Order Form" means a mutually executed ordering document specifying the Services, subscription term, fees, and any additional entitlements.

"Root Image Catalog (RIC)" means Root's catalog of hardened, continuously remediated container images.

"Root Library Catalog (RLC)" means Root's catalog of backported security fixes for application dependencies across supported language ecosystems (e.g., Python/PyPI, JavaScript/NPM, Java/Maven).

"Root Platform" means Root's proprietary software platform for vulnerability remediation, including access to RIC, RLC, associated APIs, and related documentation.

"Subscribed Images" and **"Subscribed Libraries"** mean the specific open source images and libraries to which Customer has subscribed, subject to the entitlements and the associated service level agreement (“SLA”) specified in the Order Form.

3. SERVICES

3.1 Description

The Services consist of container security and vulnerability remediation Services delivered through the Root Platform, including:

- **Root Image Catalog (RIC):** Access to hardened open source container images with continuous CVE remediation
- **Root Library Catalog (RLC):** Backported open source security fixes for application dependencies
- **Root proprietary documentation (the "Documentation"), APIs, and support services** as described in applicable Order Forms

3.2 Service Levels

Root will provide the Services in accordance with the Service Level Agreement ("SLA") available at https://www.root.io/service-level-agreement and incorporated herein by reference. Enhanced service levels and additional entitlements may be specified in an Order Form.

3.3 Order Form Hierarchy

The specific Services, entitlements, and terms applicable to Customer are determined by the Order Form. In the event of a conflict between these Terms and a fully executed Order Form , the Order Form shall control with respect to the specific subject matter addressed therein.

4. ACCOUNT AND ACCESS

4.1 Account Registration

To access the Services, Customer must create an account with accurate and complete information. Customer agrees to maintain and update account information as necessary.

4.2 Account Security

Customer is responsible for maintaining the confidentiality of account credentials and for all activities under Customer's account. Customer will notify Root immediately of any unauthorized access or security breach to Customer's account.

4.3 Authorized Users

Customer is responsible for Authorized Users' compliance with these Terms.

5. FEES AND PAYMENT

5.1 Fees

Customer agrees to pay all fees specified in the Order Form, including any fees specified for overages or additional usage. Fees are payable in United States dollars and except as expressly provided in these Terms or the SLA, are non-refundable.

5.2 Payment Terms

Unless otherwise specified in the Order Form, fees are due within thirty (30) days of invoice date. Late payments accrue interest at the lesser of 1.5% per month or the maximum rate permitted by law.

5.3 Taxes

Fees are exclusive of all taxes, duties, levies or similar governmental assessments of any nature (collectively, “Taxes”). Customer is responsible for all applicable Taxes, except taxes solely based on Root's net income.

6. ACCEPTABLE USE

6.1 Permitted Use

Customer and Authorized Users may use the Services for Customer's internal business purposes in accordance with these Terms and the applicable Order Form. Customer is responsible for all acts and omissions of its Authorized Users.

6.2 Restrictions

In connection with Customer’s use of the Services or the Root Platform, Customer agrees not to:

(a) Use the Services for unlawful purposes or in violation of applicable laws.
(b) Infringe or misappropriate intellectual property rights.
(c) Transmit malicious code or interfere with Service operations.
(d) Attempt unauthorized access to the Root Platform, Services, systems, or data.
(e) Use the Services to develop a competing product or service.
(f) Resell, redistribute, or sublicense the Services or Root Platform without written authorization.
(g) Remove or modify proprietary notices or markings.
(h) Redistribute Root-provided images or libraries outside Customer's organization. except as necessary for the sale or license of Customer's products and services.
(i) Engage in pull rates or access patterns that in Root’s sole reasonable discretion indicate abuse, misconfiguration, or unauthorized redistribution.
(j) Use the Services in a service bureau or application service provider environment, in a commercial time share arrangement, or for purposes of providing services to a third party.
(k) Create derivative works from the Services.
(l) Otherwise use the Services for any purpose beyond the scope of rights granted in this Agreement.

6.3 Suspension

Root may suspend Customer's access for violation of these Terms with prior notice, or immediately when necessary to protect Service integrity or to comply with law.

7. INTELLECTUAL PROPERTY

7.1 Root Ownership

Except as set forth in Section 7.2 (“License to Services”) Root and its licensors retain all rights, title, and interest in and to the Root Platform, the Services, and all related Deliverables, formats, tooling, ideas, concepts, know-how, and methodologies, including but not limited to all intellectual property and other proprietary rights therein and all derivatives thereof. These Terms do not grant Customer any rights except the limited licenses expressly stated herein.

7.2 License to Services

Subject to these Terms and payment of all applicable fees, Root grants Customer and its Authorized Users, a limited, non-exclusive, non-transferable, non-sublicensable right and license during the subscription term to use the Services to:

(a) Access and use the Root Platform for its internal business purposes.
(b) Pull, deploy, and use Subscribed Images and Subscribed Libraries in Customer's environments.
(c) Redistribute Root-provided images and libraries solely as incorporated into Customer's products and services.

7.3 Third Party Products/Open Source Licensing

Root’s Services are limited to patching and maintaining open source dependencies within container images. In connection with the Services, Root may make available certain third party patches, products or services, including but not limited to publicly available or open source software. Root does not offer, modify, host, or operate the functionality of any third party code on behalf Customer. Customer retains sole responsibility for compliance with all third party licensing terms. Use of Root-provided images and libraries, including Community Images and those provided in the RIC, are subject to their underlying open source licenses. Root publishes patches, including those in the RLC, in compliance with applicable open source license requirements. More information on Root’s commitment to open source license compliance and software transparency can be found here.

7.4 Deliverables License

Upon full payment, Root grants Customer a perpetual, non-exclusive, irrevocable, royalty-free license to use SBOMs, VEX statements, diff files, and related Documentation delivered as part of the Services under this Agreement (the “Deliverables”) for Customer's internal compliance, audit, and security purposes.

7.5 Feedback

Customer grants Root a perpetual, royalty-free, irrevocable, worldwide license to use any feedback, suggestions, or ideas provided by Customer, for any purpose without obligation or compensation.

8. DATA

8.1 Customer Configuration Data

Customer retains ownership of Customer Configuration Data. Customer grants Root a license to use Customer Configuration Data solely in connection with the provision of Services.

8.2 Customer Environment Data

Root may process Customer Environment Data in connection with the operation and delivery of Services, including vulnerability scanning and remediation. Root does not acquire ownership of Customer's Environment Data or any underlying software or source code.

8.3 Aggregated Data

Root may collect and use aggregated, anonymized data derived from Service usage for product improvement, research, analytics, and benchmarking, provided such data does not identify Customer.

8.4 Usage Data

Root may collect diagnostic, technical, and usage information to operate, maintain, and improve the Services.

9. CONFIDENTIALITY

9.1 Definition

"Confidential Information" means non-public information disclosed by either party that is designated as confidential or reasonably should be understood to be confidential given its nature and circumstances of disclosure.

9.2 Obligations

Each party agrees to: (a) use Confidential Information only as necessary to exercise rights or perform obligations under these Terms; (b) protect Confidential Information using at least the same degree of care used to protect its own confidential information, but no less than reasonable care; (c) not disclose Confidential Information except to employees, contractors, and agents with a need to know who are bound by confidentiality obligations at least as protective as these Terms.

9.3 Exclusions. Information will not be deemed Confidential Information hereunder if such information: (i) is known prior to receipt from the disclosing party, without any obligation of confidentiality; (ii) becomes known to the receiving party directly or indirectly from a source other than one having an obligation of confidentiality to the disclosing party; (iii) becomes publicly known or otherwise publicly available, except through a breach of this Agreement; or (iv) is independently developed by the receiving party without use of or reference to the disclosing party’s Confidential Information or breach of this Agreement. The receiving party may disclose Confidential Information pursuant to the requirements of applicable law (including without limitation applicable state or federal regulations which may require you to make disclosure pursuant to and as limited by such regulations, such as freedom of information regulations), legal process or government regulation, provided that it gives the disclosing party reasonable

prior written notice to permit the disclosing party to contest such disclosure, and such disclosure is otherwise limited to the required disclosure.

9.4 Specific Performance. If the receiving party discloses or uses (or threatens to disclose or use) any Confidential Information in breach of this Section 9, the disclosing party shall have the right, in addition to any other remedies available to it, to seek injunctive relief to enjoin such acts, it being specifically acknowledged by the parties that any other available remedies are inadequate.

10. WARRANTIES AND DISCLAIMERS

10.1 Customer Representations and Warranties

Customer hereby represents and warrants that its use of the Services will comply with all applicable laws.

10.2 Root Warranties

Root warrants that:

(a) The Services will be performed in a professional and workmanlike manner and materially as described in the Documentation.
(b) Root has the authority to enter into these Terms and grant the licenses herein.
(c) Root-provided fixes will be built from source in accordance with SLSA standards.

Your exclusive remedy for Root's breach of the foregoing warranties is that Root will, at its option and at no cost to you, either (a) provide remedial services necessary to enable the Services to conform to the warranty, or (b) replace any defective Services. If neither of the foregoing options is commercially feasible within a reasonable period of time, Root will refund all prepaid fees for the unused remainder of the applicable Term following the date of termination for the affected Service and this Agreement and any associated Order Forms for the affected Service will immediately terminate without further action of the parties. You agree to provide Root with a reasonable opportunity to remedy any breach and reasonable assistance in remedying any nonconformities.

10.3 Disclaimer

EXCEPT AS EXPRESSLY PROVIDED IN THESE TERMS, THE SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE." ROOT DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT.

ROOT DOES NOT WARRANT THAT THE SERVICES WILL BE UNINTERRUPTED, ERROR-FREE, OR COMPLETELY SECURE, OR THAT ALL VULNERABILITIES WILL BE REMEDIATED.

10.4 Security Disclaimer

CUSTOMER ACKNOWLEDGES THAT VULNERABILITY REMEDIATION CANNOT GUARANTEE ELIMINATION OF ALL SECURITY RISKS. ROOT'S SERVICES ARE ONE COMPONENT OF A COMPREHENSIVE SECURITY PROGRAM AND DO NOT REPLACE CUSTOMER'S RESPONSIBILITY FOR OVERALL SECURITY.

11. LIMITATION OF LIABILITY

11.1 Liability Cap

EXCEPT FOR EXCLUDED CLAIMS, NEITHER PARTY'S TOTAL AGGREGATE LIABILITY ARISING UNDER OR RELATED TO THESE TERMS SHALL EXCEED THE FEES PAID OR PAYABLE BY CUSTOMER TO ROOT DURING THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO LIABILITY.

11.2 Exclusion of Damages

EXCEPT FOR EXCLUDED CLAIMS, NEITHER PARTY SHALL BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES, INCLUDING LOST PROFITS, REVENUE, DATA, BUSINESS OPPORTUNITIES, OR COSTS OF PROCUREMENT OF SUBSTITUTE SERVICES, REGARDLESS OF FORESEEABILITY OR WHETHER ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

11.3 Excluded Claims

As used in this Agreement, "Excluded Claims" means: (a) Customer's breach of Section 6 (Acceptable Use); (b) either party's breach of its confidentiality obligations under Section 9; (c) either party's indemnification obligations under Section 12; (provided that in no event shall Root's liability in connection with such obligations exceed three times (3X) the amount paid or payable by Customer to Root during the one (1) year period immediately prior to the event giving rise to the liability); and (d) the gross negligence or willful misconduct of either party or its agents.

11.4 Allocation of Risk

THE LIMITATIONS IN THIS SECTION REFLECT AN INFORMED, VOLUNTARY ALLOCATION OF RISK AND ARE AN ESSENTIAL BASIS OF THE BARGAIN BETWEEN THE PARTIES.

12. INDEMNIFICATION

12.1 By Root

Root will defend, indemnify, and hold Customer harmless from third-party claims alleging that the Services (excluding open source components provided under their own licenses) infringe such third party's intellectual property rights, and pay resulting damages and costs awarded by a court of competent jurisdiction or agreed to in a signed settlement agreement, provided Customer: (a) promptly notifies Root of the claim; (b) gives Root sole control of the defense and settlement; (c) provides reasonable cooperation.

Root's obligations do not apply to claims arising from: (a) Customer's modifications to the Services; (b) combination of the Services with products not provided by Root; (c) use in violation of these Terms; (d) open source components governed by their own licenses.

Further, if Root has a reasonable belief that the Service is infringing or may become infringing, Root will, at its sole cost and expense, either (a) obtain for Customer a license to continue using the Service, or (b) modify the Service so that it is no longer infringing without any material loss of functionality; provided that if neither option is commercially feasible within a reasonable period of time, either party may elect to terminate this Agreement upon written notice to the other party and Root will refund all prepaid fees for the unused remainder of the Subscription Term following the termination date with respect to the Service. This Section 12.1 states Root's sole liability and Customer's exclusive remedy for claims of infringement or misappropriation of third-party intellectual property rights.

12.2 By Customer

Customer will defend, indemnify, and hold Root harmless from third-party claims arising from: (a) Customer or its Authorized Users' use of the Services in violation of these Terms; (b) Customer or its Authorized Users' use or misuse of third party data in a manner which infringes the rights of, or causes harm to, a third party, or (c) any violation of applicable laws.

---

13. TERM AND TERMINATION

13.1 Term

These Terms are effective upon Customer's first access to the Services and continue until terminated in accordance with these Terms. The subscription term for paid Services is specified in the Order Form (the "Subscription Term").

13.2 Renewal

Unless otherwise specified in the Order Form, subscriptions automatically renew for successive periods equal to the initial term unless either party provides written notice of non-renewal at least thirty (30) days before the renewal date.

13.3 Termination for Cause

Either party may terminate: a) for material breach if the breach is not cured within thirty (30) days of written notice specifying the breach or immediately if the breach is not capable of being cured within such period; or b) if the other party becomes insolvent, resolves to file bankruptcy, is adjudicated as bankrupt, or if a petition in bankruptcy is filed against the other party and such petition is not discharged within sixty (60) days of such filing.

13.4 Termination for SLA Failure

Customer may terminate for material SLA failure as provided in the SLA, subject to the conditions and cure periods specified therein.

13.5 Termination by Root

Root may suspend or terminate Customer's access immediately upon notice for: (a) violation of Acceptable Use provisions; (b) non-payment exceeding thirty (30) days; (c) as required by law.

13.6 Effect of Termination

Upon termination:

(a) Customer's license to access the Services terminates.
(b) Customer shall pay all outstanding fees.
(c) Each party shall return or destroy Confidential Information upon request.
(d) Root will provide reasonable transition assistance for thirty (30) days following termination.
(e) Provisions that by their nature should survive will survive, including Sections 7.4, 8.3, 9, 10.3, 10.4, 11, 12, and 14

14. GENERAL PROVISIONS

14.1 Governing Law and Jurisdiction

These Terms are governed by the laws of the State of Delaware, without regard to conflict of laws principles.Any dispute shall be resolved in the state or federal courts located in Delaware. Each party consents to personal jurisdiction in such courts. In each case these Terms of Use shall be construed and enforced without regard to the United Nations Convention on the International Sale of Goods and without regard to the Uniform Computer Information Transactions Act. To the fullest extent permitted, each party waives the right to trial by jury in any legal proceeding arising out of or relating to this Agreement or the transactions contemplated hereby.

14.2 Third Party Beneficiaries.

The parties agree that there are no third party beneficiaries to this Agreement. Neither party shall be deemed to be an employee, agent, or other legal representative of the other party for any purpose whatsoever, or have the right or authority to assume or otherwise create any obligation or responsibility, express or implied, on behalf of the other party or to bind the other party in any manner whatsoever.

14.3 Entire Agreement

These Terms, together with the SLA, Privacy Policy, and any Order Forms, constitute the entire agreement (the “Agreement”) between the parties regarding the subject matter hereof and supersede all prior agreements and understandings.

14.4 Amendments

Root may modify these Terms by posting updated terms at https://www.root.io/terms-of-service. Material changes will be communicated with at least thirty (30) days notice. Continued use after the effective date constitutes acceptance.

14.5 Assignment

Customer may not assign these Terms without Root's prior written consent. Root may assign these Terms in connection with a merger, acquisition, or sale of substantially all its assets. Any attempted assignment in violation hereof is void.

14.6 Waiver

Failure to enforce any provision is not a waiver of that provision or any other provision.

14.7 Severability

If any provision is held unenforceable, the remaining provisions continue in full force and effect.

14.8 Export Compliance

Customer may not export or re-export the Services except in compliance with applicable export control laws. Customer represents it is not located in, or a national of, any embargoed country or on any restricted party list.

14.9 Notices

Notices to Root: legal@root.io

Notices to Customer: The email address associated with Customer's account

14.10 Independent Contractors

The parties are independent contractors. Nothing creates an employment, agency, or partnership relationship.

14.11 US Government Users

Software and Documentation provided in connection with the Services are "Commercial items," "Commercial computer software" and "Computer software documentation" as defined by the Federal Acquisition Regulations (“FAR”) and Defense Federal Acquisition Regulations Supplement (“DFARS”). Pursuant to FAR 12.211, FAR 12.212, DFARS, 227.7202-1 through 227.7202-4, and their successors, the U.S. Government acquires the Software and its Documentation subject to the terms of this Agreement.

SERVICE LEVEL AGREEMENT

SERVICE LEVEL AGREEMENT

Last Updated: December 31, 2025

Root.io, Inc.

1. OVERVIEW

This Service Level Agreement ("SLA") describes Root's service level commitments for customers with paid subscriptions to the Root Platform. This SLA is incorporated by reference into the Terms of Service and any applicable Order Form.

Capitalized terms not defined herein have the meanings set forth in the Terms of Service or the Order Form. In the event of a conflict between this SLA and an Order Form executed by Root's Chief Executive Officer, the Order Form shall control with respect to the specific commitments described therein.

Except as specifically excluded, Root will use commercially reasonable efforts to meet the specified SLA Target Timelines set forth below.

2. PLATFORM SERVICES

2.1 Root Image Catalog

Root Image Catalog provides access to hardened, continuously remediated container images. Customers may subscribe to images within the RIC for use in their environments.

Included in RIC:

- Access to all standard catalog images
- Subscription to any number of images (subject to Acceptable Use guidelines in the Terms of Service)
- SBOMs, VEX statements, and build provenance for all images
- CVE remediation per applicable SLA tier

Not Included in RIC (Separate Entitlement Required):

- FIPS-validated images
- STIG-hardened images
- Other specialized compliance images as specified in an Order Form

Image Request Entitlement: Where specified in an Order Form, Customer may request to add new images to the catalog. Root will use commercially reasonable efforts to add requested images within thirty (30) days of request if and as specified in the Order Form, subject to technical feasibility. Image request entitlements do not guarantee addition of any specific image.

Community Images: Root may offer certain images designated as "Community Images" at no charge or at a reduced subscription cost. Community Images are provided "AS IS" without warranty or SLA commitment.

2.2 Root Library Catalog (RLC)

Root Library Catalog provides backported security fixes for application dependencies across supported language ecosystems (e.g., Python/PyPI, JavaScript/NPM, Java/Maven).

Scope of RLC SLA:

- Applies only to new CVEs discovered after Customer's Subscription has commenced.
- Applies only to libraries explicitly designated as "Subscribed Libraries" in the Order Form or Root Platform.
- Does not apply to pre-existing CVE debt in existence at commencement date of Subscription.

CVE Burn Down: Remediation of pre-existing vulnerabilities in Customer's pinned library versions may be available as a separate entitlement ("CVE Burn Down Credits") if and as specified in the Order Form.

2.3 Deliverables

All Root-delivered fixes include:

- Full source code build in accordance with SLSA standards
- Software Bill of Materials (SBOM)
- VEX (Vulnerability Exploitability eXchange) statements
- Diff files and provenance documentation
- Patch efficacy testing against proof-of-concept exploits where available

Root maintains underlying open source licensing for all images and publishes patches in compliance with applicable license requirements as provided in the Terms of Service.

3. PLATFORM AVAILABILITY

3.1 Uptime Target

Root targets 99.9% monthly Platform Availability for the Root Platform, including registry services and API access ("Platform Availability").

3.2 Calculation

```
Platform Availability % = ((Total Minutes - Downtime Minutes) / Total Minutes) × 100
```

Where:

- **Total Minutes** = Total minutes in the calendar month
- **Downtime Minutes** = Minutes where Platform was unavailable, excluding Exclusions

3.3 Exclusions

Downtime does not include unavailability due to:

(a) **Scheduled Maintenance:** Planned maintenance with at least twenty-four (24) hours advance notice via email or Platform notification.
(b) **Third-Party Infrastructure:** Outages of underlying infrastructure providers (e.g., AWS, Google Cloud, Cloudflare) outside Root's reasonable control.
(c) **Force Majeure:** Events beyond Root's reasonable control, including natural disasters, acts of war, terrorism, pandemic, or government action.
(d) **Customer-Caused Issues:** Unavailability resulting from Customer's acts, omissions, equipment, software, or network connectivity.
(e) **Suspension:** Service suspension due to Customer's breach of the Terms of Service, including non-payment.

3.4 Scanning Frequency

Root targets vulnerability scanning of Subscribed Images and Subscribed Libraries at least once every twenty-four (24) hours when utilizing Root-controlled registries. Scanning frequency for Customer-controlled registries depends on Customer's CI/CD configuration and API integration.

3.5 Pull Rate Limits

To ensure fair use and to prevent service degradation, Root may implement reasonable pull-rate limits on registry access. Customers experiencing rate limiting due to suspected misconfiguration will be notified and Root will use reasonable commercial efforts to assist such Customers in remediation of service degradation issues .

4. VULNERABILITY REMEDIATION SLA

SLA Tiers

This SLA defines Standard remediation timelines included with all paid subscriptions. Enhanced SLA tiers with accelerated timelines may be available at an additional charge for customers who require more aggressive remediation timelines. Enhanced SLA terms, eligibility, and pricing are specified in the Order Form.

4.1 General Definitions

"CVE" means a vulnerability with an assigned Common Vulnerabilities and Exposures identifier.

"CISA KEV" means a vulnerability listed in CISA's Known Exploited Vulnerabilities catalog.

"Severity" is determined by CVSS score from the NIST National Vulnerability Database:

- **Critical:** CVSS 9.0–10.0
- **High:** CVSS 7.0–8.9
- **Medium:** CVSS 4.0–6.9
- **Low:** CVSS 0.1–3.9

"Fix Candidate" means a proposed remediation existing within the trusted ecosystem, including upstream maintainer releases, sibling distributions, forks, or validated unmerged pull requests.

"Remediation Complete" means Root has delivered a fix that is fully tested, validated against proof-of-concept exploits where available, and includes diff file and provenance documentation.

"Subscription Date" means the effective date of Customer's subscription for the applicable service (RIC or RLC) as specified in the Order Form.

4.2 SLA Timeline Commencement (Both RIC and RLC)

SLA timelines begin upon the later of:

(f) CVE publication in a recognized vulnerability database (NVD, vendor advisory, etc.); **AND**

(g) Availability of a Fix Candidate within the trusted ecosystem

Subsequent severity reclassification (e.g., addition to CISA KEV) triggers the more stringent timeline from the time of reclassification.

4.3 Remediation Delivery Standards (Both RIC and RLC)

All Root-delivered fixes include:

- Source builds in accordance with SLSA standards
- Software Bill of Materials (SBOM)
- VEX statements
- Diff files and provenance documentation
- Patch efficacy testing and PoC validation where available

Root maintains underlying open source licensing and publishes patches in compliance with applicable license requirements as provided in the Terms of Service.

4A. ROOT IMAGE CATALOG (RIC) — SLA SPECIFICS

4A.1 Scope of RIC SLA Coverage

The RIC Remediation SLA applies to:

(h) **Subscribed Images:** Container images explicitly subscribed to by Customer within the Root Platform.

(i) **All CVEs:** Both new and pre-existing vulnerabilities in Subscribed Images . There is no distinction between CVE Debt and new CVEs for RIC.

(j) **Supported Images:** Standard catalog images as available in the Root Platform. FIPS, STIG, and other specialized images require separate entitlement per Order Form.

4A.2 What RIC Covers vs. Excludes

Covered	Not Covered
All CVEs in Subscribed Images (new and existing)	Community Images (no SLA)

Critical, High, Medium severity per SLA tier	Low severity (commercially reasonable)
OS-level and package vulnerabilities	Customer-added layers or modifications
Standard catalog images	FIPS/STIG without entitlement

4A.3 RIC Standard SLA Target Timelines

Severity	Standard Timeline	CISA KEV
Critical	30 calendar days	72 hours
High	30 calendar days	72 hours
Medium	60 calendar days	—
Low	Commercially reasonable	—

4A.4 RIC Enhanced SLA Timelines

Enhanced SLA terms, eligibility, and pricing if and as specified in the Order Form.

Severity	Enhanced Timeline	CISA KEV
Critical	7 calendar days	48 hours
High	14 calendar days	48 hours
Medium	30 calendar days	—
Low	Commercially reasonable	—

5. CVE SURGE CONDITIONS

5.1 Surge Condition

A "CVE Surge Condition" exists when the rate of new Critical or High severity CVEs affecting a specific Subscribed Image or Subscribed Library version exceeds **2.5 times (2.5x)** the historical monthly average for that project or dependency, measured over the trailing twelve (12) months.

5.2 Effect of Surge Condition

Upon determination of a CVE Surge Condition:

(k) SLA timelines become advisory targets rather than commitments for the affected Subscribed Image or Subscribed Library.

(l) Root will notify Customer of the Surge Condition and collaborate on prioritization of critical fixes.

(m) Root will provide guidance on upgrade paths to more stable versions where available.

(n) Normal SLA commitments resume when the Surge Condition no longer exists.

5.3 Extended Life Support

For customers requiring continued support of end-of-life or high-CVE-volume versions, Extended Life Support may be available at additional cost if and as specified in the Order Form.

6. ESCALATION TO ROOTLABS

6.1 Triggering Escalation

In exceptional circumstances where standard AVR processes cannot remediate a CVE within SLA Timelines (typically due to extraordinary technical complexity or ecosystem-wide gaps) Customer will be notified and may request escalation to Root Labs.

6.2 Root Labs Services

Upon Customer request, Root Labs may provide:

Risk Triage: Comprehensive analysis to determine actual applicability of the CVE to Customer's context, which may include:

- Reachability analysis of vulnerable code paths
- EPSS (Exploit Prediction Scoring System) evaluation
- Environmental context review (runtime, network exposure, access controls)
- Threat intelligence correlation
- Attack chain validation
- Proof-of-concept assessment

VEX Enforcement: When Root Labs determines, after Risk Triage, that the identified risk is low or does not exist:

- Standard VEX: SBOM with scanner-consumable VEX statements
- VEX-enforced image (at Customer discretion): Modified image enabling SCA tools to reflect corrected risk assessment

Custom Remediation: When CVE risk remains Critical or High and no viable ecosystem fix exists, Root Labs may use commercially reasonable efforts to engineer a novel fix, including:

- Developing targeted patches compatible with Customer's versions
- Validating fixes resolve the vulnerability without breaking functionality
- Providing supporting documentation for compliance records

6.3 Root Labs Timeline

While Root Labs prioritizes delivery within the SLA Timelines, complex research may extend up to thirty (30) days from escalation request.

6.4 Service Commitments

- **Parallel Processing:** Individual CVE escalations will not impact delivery timelines for other remediable CVEs.
- **Communication:** Root will provide regular status updates for all escalated issues.
- **Transparency:** If remediation is determined technically infeasible, Root Labs will provide written technical justification and support for alternative approaches.

6.5 Technical Infeasibility

If Root determines a CVE cannot be remediated, Root Labs will work with Customer to provide:

- Written technical justification for why a CVE cannot be remediated.
- Support for alternative workaround solutions (such as: "lowest lift" library or package-specific upgrades; collaboration with Customer engineering on alternative approaches; and alternative CVE-compliant image maintaining stability).

(q) Upon Customer request, additional technical review involving Root's CTO and/or VP of Engineering will be provided.

7. EXCLUSIONS

7.1 SLA Exclusions

Remediation SLA commitments do not apply when:

- No Fix Candidate exists within the Customer ecosystem.
- The vulnerability exists within Customer-provided code, configurations, or customizations.
- CVE is disputed, rejected, or withdrawn by NVD or the relevant authority.
- Customer has not provided required access, information, or timely response to Root inquiries.
- The Subscribed Image or the Subscribed Library is designated as Community (no SLA)
- A CVE Surge Condition applies (See Section 5).
- Vulnerability exists in a FIPS, STIG, or specialized image for which Customer does not have entitlement.
- Pre-existing CVE debt for RLC (covered by CVE Burn Down entitlement if applicable).

7.2 Force Majeure

Neither party shall be liable for failure to perform obligations due to events beyond reasonable control, including natural disasters, acts of war or terrorism, pandemic, government action, or failure of third-party infrastructure providers (a “Force Majeure” event).

8. SLA REMEDY AND ESCALATION

8.1 Escalation Path

Customer shall report SLA issues through Root's support organization as follows:

- **Level 1:** Account Manager
- **Level 2:** Head of Customer Success
- **Level 3:** Head of Field Engineering
- **Level 4:** CTO

Customer shall not escalate an SLA issue to the next Level of the support organization unless the prior level of support has failed to address and remedy an SLA issue within the timeframes provided for in this Service Level Agreement.

8.2 No Service Credits

SLA timelines represent Root's performance targets. Failure to meet SLA timelines does not entitle Customer to automatic service credits or financial remedies. Customer's remedy is escalation per Section 8.1 and, where applicable, termination rights per Section 9.

9. TERMINATION FOR SLA FAILURE

9.1 Conditions for Termination

Customer may terminate the Agreement for material SLA failure only if all of the following conditions are met:

- Root fails to remediate a Critical severity or CISA KEV vulnerability within two times (2x) the applicable SLA timeline;
- Customer has escalated to Root Labs per Section 6 and Root Labs has exhausted the thirty (30) day extended research period without a remediation or providing a reasonable alternative (VEX enforcement, workaround, alternative image);
- Customer provides written notice specifying the SLA failure; and
- Root fails to cure within forty-five (45) days of such notice.

9.2 Refund Upon Termination

Upon termination pursuant to Section 9.1, Customer is entitled to a pro-rata refund of prepaid fees for the unused portion of the subscription term, less fees attributable to the sixty (60) days following the effective termination date to facilitate Transition Services.

9.3 Limitations

Termination under this Section does not apply to:

- CVEs where a CVE Surge Condition existed.
- CVEs excluded under Section 7.
- Situations where Customer has failed to reasonably cooperate with Root's remediation efforts.

10. MODIFICATIONS

Root may modify this SLA by posting an updated version to www.root.io/sla. Material changes will be communicated with at least thirty (30) days notice. If changes are not acceptable to Customer, Customer may elect to terminate the Agreement and receive a pro-rata refund of prepaid fees for the unused portion of the subscription term, less fees attributable to the sixty (60) days following the effective termination date to facilitate Transition Services.