VULNERABILITY MANAGEMENT POLICY

Version Number:	2.1
Version Date:	10/09/2025
Owned by:	Security, GRC
Approved by:	Nate Fitch, Sr. V.P., Chief of Staff
Confidentiality Level:	Internal

Table of Contents

1. Purpose

This policy defines Docker's standardized process for managing vulnerabilities across its technology landscape—identifying, evaluating, prioritizing, remediating, and monitoring security weaknesses that could compromise system confidentiality, integrity, or availability.

The policy establishes:

- A structured lifecycle based on CVSS v3.1 scoring with automated scanning, manual assessments, and penetration testing
- Vulnerability evaluation criteria (exploitability, business impact, exposure context) with severity-based prioritization
- Defined remediation SLAs for each severity level
- Formal change management procedures for all remediation actions
- Risk management process with stakeholder review for SLA exceptions
- Configuration hardening and continuous monitoring requirements
- Regular performance metrics review by security and executive leadership

This framework reduces attack surface, maintains customer trust, ensures service continuity, and supports compliance with ISO/IEC 27001:2022 and SOC 2 requirements.

2. Scope

This policy applies to all components of Docker’s operational, development, and infrastructure environments. It governs vulnerability management across all production and extends to all asset classes, including application code, container images, endpoint devices, cloud infrastructure, and internal tools.

All individuals involved in the management, maintenance, deployment, or oversight of these systems fall under the scope of this policy. This includes Docker employees, contractors, third-party vendors, and service providers who are responsible for technology operations, development pipelines, system configuration, or security monitoring.

3. Roles and Responsibilities

Role	**Responsibilities**
Security Team	Leads vulnerability management across Docker systems. Defines severity classification, tracks remediation timelines, verifies patch completeness, and coordinates risk management process. Provides security oversight, escalates risks, and ensures auditability of processes.

Engineering Teams	Responsible for remediating vulnerabilities in application code, infrastructure, and services. Executes patching, code changes, or configuration updates within SLA windows. Collaborates with security to assess risk and validate fixes.
Infrastructure Teams	Monitors and scans cloud infrastructure and container environments. Applies updates to runtime environments, base images, and supporting systems. Maintains posture tools and integrates security checks into CI/CD pipelines.
Product Owners and Risk Stakeholders	Provide business context for vulnerability prioritization. Participate in risk acceptance decisions for findings that cannot be remediated within defined SLAs. Help assess impact of vulnerabilities on product or service functionality.
Compliance and Governance Teams	Ensure documentation and audit readiness for internal and external reviews. Collaborate with security and engineering on policy enforcement and audit remediation efforts.
All Docker Personnel	Responsible for promptly reporting any observed vulnerabilities or security issues. Must not ignore known security weaknesses and are expected to support remediation efforts as appropriate to their role.

4. Definitions

Vulnerability - A weakness in system design, implementation, configuration, or operation that could be exploited to compromise the confidentiality, integrity, or availability of Docker's information systems or data.

Common Vulnerability Scoring System (CVSS) - An industry-standard framework for rating the severity of security vulnerabilities on a scale from 0.0 to 10.0, providing consistent criteria for prioritizing remediation based on technical severity and exploitability characteristics.

Remediation SLA (Service Level Agreement) - The maximum time allowed to fix a vulnerability from the point of confirmation, determined by severity level.

Compensating Controls - Alternative security measures implemented when a vulnerability cannot be directly remediated within the required SLA, designed to reduce risk exposure until full remediation is possible.

System Hardening - The process of securing systems by reducing their attack surface through configuration changes, removing unnecessary services, applying security patches, and implementing security best practices to minimize vulnerabilities.

5. Vulnerability Management Lifecycle

5.1 Identification

Activity	Expectations
Vulnerability Scanning	Docker will monitor critical assets through frequent, recurring vulnerability scans. Scanning methods include Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), cloud infrastructure scanning, and endpoint scanning, ensuring timely detection of security weaknesses across the environment.
Vulnerability Disclosure Program	Docker encourages responsible reporting of security issues across its products and services. Researchers can submit findings to **security@docker.com**, and valid reports will be acknowledged within a timely manner.
Penetration Testing	Docker will use independent (external) assessors to perform penetration tests against Docker's external networks.
Security Reviews	Docker will use independent assessors to perform security-centric reviews of the code that makes up critical Docker assets.
Monitoring Advisories	Docker will use strategies to subscribe to relevant security feeds to stay updated on various vendor and customer advisories and vulnerability disclosures.

5.2 Evaluation

Each vulnerability is assessed using the Common Vulnerability Scoring System (CVSS) version 4.0 to determine its base severity. Additional contextual factors such as exploit availability, data sensitivity, exposure in production environments, and business impact are used to refine prioritization.

Severity	CVSS Score	Remediation SLA
Critical	9.0–10.0	15 days
High	7.0–8.9	45 days
Medium	4.0–6.9	90 days
Low	0.1–3.9	No specific remediation guideline (remediate at discretion)

SLAs begin upon confirmation of the vulnerability in Docker's systems or its software. Remediation deadlines are strictly enforced unless a formal exception is granted through risk acceptance. Final discretion for severity is dependent on known vulnerability exploitability.

5.3 Remediation

Vulnerabilities must be remediated within the SLA period assigned to their severity. Remediation may include code fixes, patch application, system configuration updates, permission restrictions, or compensating controls.

All patch deployments and infrastructure changes must follow Docker's Change Management Policy.

If full remediation cannot be completed on time, compensating measures must be documented, approved, and tracked until the vulnerability is resolved.

5.4 Risk Management

When remediation of a vulnerability is not feasible within defined SLA windows, the issue must be escalated into Docker's Risk Management process by submitting a risk ticket via Docker's Risk Submission Portal. This initiates a formal workflow including risk assessment, assignment of ownership, and a treatment decision.

6. Reporting and Notification

Vulnerabilities may be reported internally or externally. Internal teams should report potential security flaws via the Slack channel #help-security-grc or by emailing security@docker.com. External security researchers or partners may report vulnerabilities to security@docker.com, in accordance with Docker's responsible disclosure policy.

7. System Hardening

System Hardening - Docker's critical infrastructure, software and services, and employee laptops will be hardened for security.

8. Enforcement and Exceptions

All Docker personnel are expected to comply with this policy in full. Failure to adhere may result in disciplinary action, up to and including termination of employment or contract. In cases involving willful misconduct, malicious activity, or violations of law, Docker may initiate legal proceedings. The organization reserves the right to monitor, audit, and inspect user activity on its systems to ensure compliance.

Any exceptions to this policy must be formally requested, documented, and approved by Docker's GRC or Legal team. Exception requests must clearly outline the business justification and associated risks, and should be submitted to Docker's Risk Submission Portal.

9. Change History

Date	Version	Responsible Party	Description of Change
10/09/2025	2.1	Nate Fitch, Sr. V.P., Chief of Staff	Revised policy approved
09/29/2025	2.0	Chad Fryer Sr. Security Engineer, GRC Emre Ugurlu, Sr. Security Engineer, GRC	Policy annual review and update
10/21/2024	1.4	Salima Allarakhia, Senior Engineering Manager, Security	Policy annual review and update Draft document approved
10/21/2024	1.3	Karen Hajioannou, Senior Security & Compliance Engineer	Policy annual review and update
2/24/2023	1.2	Todd Smith, Vice President of IT	Draft document approved
2/3/2023	1.1	Rachel Taylor, Senior Manager, Security, Risk & Trust	Draft Submitted for review
12/19/2022	1.0	Rachel Taylor, Senior Manager, Security, Risk & Trust	Basic document outline