Red Hat
Product Security

General Distribution

Red Hat Security Declaration

Secure Software Development Life Cycle

May 6, 2024

Table of Contents

Disclaimer

This document is provided for informational purposes only. It is intended to describe Red Hat's approach to security and its security ecosystem as of the publication date and is subject to change at Red Hat's sole discretion. The information is provided "as is" with no guarantee or warranty of accuracy, completeness, or fitness for a particular purpose. Red Hat is not responsible for any errors or omissions in the document. If further detail or clarification is required, please contact your Red Hat representative and they will forward the request to the Red Hat Product Security team for further consideration.

Document purpose

This document describes the implementation of a secure software development life cycle for all Red Hat software.

Red Hat Secure Development Life cycle

How Red Hat aligns with secure development industry practices

Throughout Red Hat software development, we strive to reduce the number of vulnerabilities in released software, reduce supply chain risks, mitigate the potential impact of undetected or unaddressed vulnerabilities, and address the root causes of vulnerabilities to prevent future recurrences. Red Hat maintains a software development life cycle (SDL) process that addresses risk assessment, vulnerability assessment, and security testing protocols of Red Hat software. Red Hat's SDL process follows the NIST SP 800-218 Secure Software Development Framework, conducting security reviews related to secure architecture, secure pipeline, threat modeling, Static and Dynamic Application Security Testing, antimalware scanning, penetration testing, and incident response throughout the supported life cycle of Red Hat Software.

Additionally, Red Hat has an internal process designed to ensure that our software supply chain consistently upholds security standards on the development, build, test, and production environments for all software. This is an essential checkpoint to confirm that every Red Hat system that processes, handles, or modifies code is approved before being integrated into our production pipeline.

By following the structure of NIST SSDF SP-800-218, Red Hat produces code adhering to industry best practices (when applicable), including but not limited to the standards and practices as outlined in the following:

- NIST Secure Software Development Framework (NIST SSDF SP-800-218)
- NIST Security and Privacy Controls for Information Systems and Organizations (NIST SP 800-53 r5)
- NIST Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (NIST 800-161 r1)
- NIST Assessing Security Requirements for Controlled Unclassified Information (NIST SP 800-171A)
- U.S. Improving the Nation's Cybersecurity (U.S. Executive Order 14028)
- UK Telecommunications (Security) Act 2021
- Digital Operational Resilience Act (DORA) (EU Regulation 2022/2554)
- Road vehicles Cybersecurity engineering (ISO/SAE 21434) / Road vehicles Functional Safety (ISO 26262)
- Federal Risk and Authorization Management Program (FedRAMP r5)

- Payment Card Industry Data Security Standard (PCI DSS v4)
- OWASP Top 10 (2021)
- Systems and software engineering software life cycle processes (ISO/IEC/IjuEEE 12207:2017) (where feasible)

Compliance & security certifications

Red Hat focuses on accelerating security requirement implementation and compliance framework achievement. Product Security coordinates the planning of security certification efforts across Red Hat software portfolios. We also coordinate the attainment of security certifications to support Red Hat's market success in restricted sales markets. Product Security develops tools and solutions that automate security and compliance functions and conducts critical analysis functions to inform security and risk decisions across Red Hat.

In addition to aligning with the secure development requirements listed above, Red Hat software also has certifications and attestations in alignment with other industry standards. Red Hat has obtained certifications and attestation reports for FedRAMP, ISO 27001, SOC2, and other assurances to meet customer requirements. Visit the Red Hat compliance activities and government standards page for the complete list of certifications.

Security culture under Product Security management

Red Hat's open and transparent software development approach builds on well-known upstream open source community software projects that reflect the contributions of developers around the world and uses widely used and recognized open source licenses. In contrast to many software vendors and publishers, Red Hat curates upstream community source code for review and inclusion into our software products, which undergo extensive composition, security screening, and quality assurance testing prior to release. We also have a continuous, dedicated process to support our customers through tracking product components, assessing implications of identified vulnerabilities for their impact, and continuously providing security updates using the approach outlined in an open approach to vulnerability management.

We take a deliberate approach to adding upstream code to our stable downstream releases. This approach allows for a more thorough review of potentially inappropriate code or vulnerabilities to deliver a platform that is stable but not static when it comes to upstream innovation. Our product security process is continuous and builds on the NIST Secure Software Development Framework (SSDF) outlined in NIST Special Publication 800-218. Combining these practices and workflows helps deliver a comprehensive look at upstream code integrity, ultimately providing a software foundation with a stronger security posture.

Red Hat has a dedicated Product Security organization that is responsible for overseeing the complete software product portfolio. Product Security is a separate organization from the software developers in the Red Hat Product and Global Engineering organization. Product

Security guides Red Hat with clear, open, and efficient secure development and vulnerability management practices.

Red Hat Product Security provides the guidance, stability, and security needed to confidently deploy enterprise solutions. Red Hat also provides a defined productization pipeline for software. Red Hat operates and maintains the infrastructure that stores, configures, and packages software to provide confidentiality, availability, and integrity of Red Hat's software through a secured infrastructure.

For more information about Product Security, read the Product Security Overview.

Continual security training

Secure Development training is an effective way to improve the quality of Red Hat software by providing the opportunity for associates to improve their security skills and knowledge. This training is required for all associates involved with the development of code and must be completed on an annual basis. The training includes a mandatory secure development introduction module and a selection of classes from an identified catalog of additional security courses to fulfill the requirement.

Software supply chain

Red Hat's software is built from open source projects. Red Hat pulls third-party software from upstream communities and makes them enterprise-ready. Red Hat reviews all software components for known unfixed CVEs for remediation upstream and continuously performs vulnerability checks throughout the life cycle. Red Hat also conducts malware and anti-virus checking and other security activities and testing as part of our SDL.

Maintain the integrity and security of application source code

Red Hat maintains policies and procedures for maintaining appropriate cryptographic key management for proper encryption to protect its secure development infrastructure. Red Hat maintains policies and procedures requiring software review and patches before distribution to maintain software integrity and prevent unintended modification of Red Hat software.

All Red Hat software comes from upstream and publicly available upstream projects. These projects use various methods and tools, for example, GitLab, to track changes and version control. As projects are productized, the software is pulled into dedicated Red Hat build servers and is reviewed, tested, and packaged by authorized Red Hat employees. Red Hat software build environments also follow change management practices. All code within the Red Hat software build environment is managed by an assortment of teams, with separation of duties, that involves change tracking using trusted sources and signed by authorized personnel with Red Hat keys. All software packages are signed by Red Hat signing servers prior to release to Red Hat subscribers so that the authenticity of the packages can be verified.

Access controls grant specific access to specific individuals to different parts of the code development stack. Ownership of the configuration and access is controlled by primarily responsible business units of release engineering, product security, system operations, and information technology so that no one team has full control of the end-to-end development and release toolchain.

Red Hat distributes software in the form of RPM packages, container images, and OS images. All software is signed. If the signature is not verified, then the binary content cannot be installed and hence cannot be executed, except for OS images that require an end user to validate the signed hashes or signatures prior to installation.

Software packages are signed with the Red Hat GPG key. GPG stands for GNU Privacy Guard, or GnuPG, a free software package used for ensuring the authenticity of distributed files. If the verification of a package signature fails, the package may be altered and therefore cannot be trusted.

- RPM packages: All Red Hat Enterprise Linux packages are signed with the Red Hat GPG key.
- Container Images: Red Hat supported open source software is available as container images, distributed from the Red Hat-certified registry and signed with GPG. Verifying image signing for Red Hat container registry images is done automatically every time a container image is pulled to a host system.

Red Hat's Product Security team guides and reviews quality engineering and release environments. To learn more about Red Hat's software supply chain visit Understanding open source software supply chain risks and Understanding software supply chain threats.

Software security activities

Red Hat designs software to meet appropriate security and risk mitigation requirements. Following secure development activities throughout the software development life cycle enables security to be built into the design, architecture, and code of the product. Adherence to SDL enables security to be built into the design and architecture of a software product. Red Hat rigorously tests the security of software prior to release.

Threat modeling

The purpose of the threat modeling process is to aid Engineering in documenting identified security threats to an application and making well-informed decisions about security requirements to mitigate them.

As this activity is conducted in the design phase of the software development life cycle (SDLC), it helps teams identify potential threats in their applications early on, allowing them to proactively address security concerns before they become major issues. Using the assessment

template in the SD Elements tool streamlines this process by providing a structured approach and a comprehensive catalog of security countermeasures to choose from.

By conducting threat modeling, Engineering, and Security Architects can work together to understand the potential attack vectors, prioritize risks, and select appropriate security countermeasures to mitigate those risks effectively. By collaborating from the outset, this effort ensures that security is integrated into the development process.

Security Architecture Review (SAR)

A Security Architecture Review (SAR) is an evaluation process to confirm that software development follows the Product Security secure design principles guidelines. The evaluation covers the following areas:

- Economy of mechanism
- Secure by Design by Default in Deployment
- Open Design
- Complete mediation through access control
- Least privilege
- Least common mechanism
- Psychological acceptability
- Compromise Recording
- Defense in depth

SAR activity is conducted by a Security Architect who assesses the design and implementation of software, with a focus on identifying and addressing potential weaknesses in the architecture.

A successful SAR not only verifies alignment with secure design principles but also provides valuable recommendations for improvements or mitigations to enhance the overall security posture of the software. The output of the SAR is crucial in building confidence in the security robustness of the software, aligning it with industry best practices and standards.

Software manifest / Software Bill of Materials (SBOM)

A Software Bill of Materials (SBOM) is a machine-readable, comprehensive inventory of software components and dependencies. This manifest contains license and provenance information for a specific version of the product software. SBOM files are considered static files associated with the specific software version and release date. SBOM files can contain different useful metadata, and not all SBOMs are the same. Red Hat follows the CISA guidelines regarding the six defined types of SBOM documents.

Red Hat will generate a build type SBOM that represents the components used to compose the release. This machine-readable SBOM will be in the Software Package Data eXchange (SPDX) format. The SBOM will contain the following data elements at a minimum: Supplier (including provenance data), Component Name, Unique Identifier, Version, Secure Hash Algorithm (SHA)

digest signature (used to validate the integrity of the SBOM), Relationship between components and their dependencies (for example, CONTAINS), and SBOM Author.

Currently, Red Hat SBOMs are published at Security Data - /sbom/beta/spdx/.

Static Application Security Testing (SAST)

Static Application Security Testing (SAST) is the process of scanning source code using automated tools for insecure coding techniques and potential security vulnerabilities in the software.

The precision of a SAST tool is determined by its scope of analysis and the specific techniques used to identify vulnerabilities.

Different levels of analysis include:

- Function level - The sequences of instruction.
- File or class-level - An extensible program-code-template for object creation.
- Application level - A program or group of programs that interact.

Red Hat uses all the above-mentioned levels to scan software offered under the Red Hat portfolio. Because the SAST tool is an automated tool, some false positives are generated, which are identified through manual analysis. We also discourage the non-conventional use of memory-unsafe languages to enhance performance. Scanning for hard-coded secrets is conducted during SAST.

We use multiple tools to conduct SAST. One tool is OpenScanHub, an internal Red Hat service that runs various static analyzers on RPM packages and tarballs on source code.

Dynamic Application Security Testing (DAST)

Dynamic Application Security Testing (DAST) is a procedure that actively conducts black box dynamic testing of applications to detect possible security vulnerabilities. DAST automates common attack patterns against running applications to identify potential vulnerabilities. While DAST can be used with any software, most DAST tools are primarily targeted to identify vulnerabilities in web applications.

Red Hat has implemented DAST into the software testing phase. Red Hat Product Security has a tool, RapiDAST, used for rapid, automated dynamic application security testing of software.

RapiDAST is an open source project created by Red Hat Product Security. RapiDAST is evolving. At this stage, its focus is scanning APIs as effectively and conveniently as possible through automation. Currently, the project uses OWASP ZAP – a popular open source web security testing tool as its core engine.

Penetration testing

Penetration testing is a method where a trusted party attempts to compromise a predetermined target. The goal is to identify weaknesses and vulnerabilities so they can be fixed before a hostile attacker finds the same results.

There are three types of penetration testing techniques:

- Black box testing is performed without prior internal knowledge of the target.
- Gray-box testing is performed with limited internal knowledge of the target.
- White-box testing is performed with complete knowledge of the target.

Red Hat Product Security Penetration Testers manually execute this testing by using a combination of automated and manual methods to identify and exploit security issues. Our Penetration Testers focus on the following areas, including but not limited to:

- Configuration and deploy management testing
- Authentication testing
- Authorization testing
- Session management testing
- Input validation testing
- Error handling
- Business logic testing
- API security testing
- Cryptography security testing
- Client-side testing
- Cloud security infrastructure testing
- Other channels testing

Malware scanning & testing

Software is scanned for the presence of malware during SDL. Malware scanning, or "antivirus", is scanning for known malicious software hiding inside other files. The details of our malware scanning tooling are confidential.

Results of software security activities

Results of secure development activities are stored as evidence in our central ticketing system. Any security issues found are analyzed, triaged, and remediated in accordance with Red Hat standards. All identified vulnerabilities are addressed following Vulnerability Management and Incident Response processes. Any results that do not meet Red Hat secure development standards are tracked with a remediation plan to completion until risk mitigation is implemented or risk is accepted.

Responding to vulnerabilities

Red Hat Product Security Incident Response Team

The Red Hat Product Security Incident Response Team handles the receipt, investigation, and public reporting of security vulnerability information relating to Red Hat software. Responding to Common Vulnerabilities and Exposures (CVEs) has been and continues to be a core function of Red Hat Product Security. This team identifies, assesses, and defines the severity level of CVEs, and tracks vulnerabilities within the Red Hat software provided to customers.

Response to attacks and security incidents

Red Hat's Product Security Incident Response Plan alerts key internal stakeholders, directing them to the required resources for the correction, testing, and distribution of the fixes to our subscribers to resolve the vulnerability.

The Red Hat Product Security Incident Response Plan provides the following:

- A roadmap for implementing incident response and incident handling.
- The structure and organization of the incident response capability.
- A high-level approach for how the incident response capability fits into the overall organization.
- Defines reportable incidents.
- Metrics for measuring the incident response capability within Red Hat.
- Defines the resources and management support needed to effectively maintain and mature incident response programs.
- Addresses the sharing of incident information.
- Reviewed and updated at least annually to address system and organizational changes or problems encountered during plan implementation, execution, or testing.
- Explicitly designates responsibility for incident response related to Red Hat software to Product Security.
- Is accessible to all Red Hat associates to consume as their role requires.
- Establishes a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components.
- Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implements the resulting changes accordingly.

How Red Hat works with Common Vulnerabilities and Exposures (CVEs)

Common Vulnerabilities and Exposures (CVEs) are a list of publicly disclosed computer security flaws. CVE is also shorthand for the CVE ID number assigned to a security flaw. CVEs help IT professionals coordinate their efforts to prioritize and address these vulnerabilities, making computer networks more secure.

Red Hat Product Security strives to provide the most actionable information about vulnerabilities, so specialized Security Bulletins are created to offer the best experience and information possible. These security bulletins aggregate information, diagnostic tools, and updates in one easy-to-understand interface. Additionally, whenever new software releases that contain security fixes become available, the Security Bulletins will highlight those fixes to help make informed decisions about upgrading to newer versions. A full list of all CVEs affecting Red Hat software can be found in our CVE Database.

Red Hat continuously engages in the security community as a major contributor to open source software. Red Hat is a CVE Numbering Authority (CNA) and Root CVE Numbering Authority (Root CNA) and uses CVE IDs to track security vulnerabilities. Red Hat Product Security maintains an open and frequently updated database of security updates, which you can view by CVE number. Visit the Product Security Center for customer guidance on security incidents. As a CNA, Red Hat also publishes data to the CVE project on affected software components for vulnerabilities assigned to a CVE by Red Hat.

All currently supported product releases, versions, and patches can be retrieved from the Red Hat Product Security Center. Customers can subscribe to advisories and notifications to receive information about releases and patches.

Vulnerability severity ratings

The Red Hat Product Security Incident Response Plan outlines the orchestration process that coordinates a response to all security vulnerabilities reported or discovered affecting Red Hat software. We use a four-phase approach ensuring that every flaw is analyzed and that we coordinate the remediation and disclosure of any affected software.

Successful vulnerability management provides:

- A CVSS score based on flaw characteristics.
- Severity ratings based on offering characteristics.
- Tracking and coordination with all affected offerings.
- Transparency in security data (CVE pages, CSAF advisories, VEX, etc) and partnership with scanning vendors.

Red Hat Product Security rates the impact of security issues found in Red Hat software using a four-point scale: Low, Moderate, Important, and Critical and Common Vulnerability Scoring System (CVSS) base scores. These provide a prioritized risk assessment to help you understand

and schedule upgrades to your systems, enabling informed decisions on the risk each issue places in your unique environment.

Read about Severity ratings for more detailed information. Also, learn more about Red Hat's Open Approach to Vulnerability Management, which explains how and what factors are taken into consideration in setting the fix priorities.

Red Hat Security Data - Vulnerability Exploitability eXchange (VEX)

Red Hat security data is a central source of truth for Red Hat software regarding published, known vulnerabilities. The availability of accurate information in security data provides the correct risk assessment process that helps with vulnerability patching prioritization. Red Hat continuously improves our security data by adding more information to the existing data, introducing the best data formats, and cooperating with other vendors, including security scanner vendors, regarding our general approach to security data exchange.

In June 2022, Red Hat began publishing security advisories in the CSAF 2.0 format and shortly after started publishing VEX data using CSAF. These files are the official, authoritative source for Red Hat-released security patches. Since changing to the CSAF 2.0 data format, security advisories include detailed vulnerability affectedness and patching status at the software component level. VEX files include machine-readable data on unfixed vulnerabilities.

Red Hat VEX beta files are available at https://access.redhat.com/security/data/csaf/beta/vex/ and Red Hat security advisory files are available at https://access.redhat.com/security/data/csaf/v2/advisories/.

Visit The future of Red Hat security data Red Hat blog to learn more about Red Hat's security data publishing strategy.

Product life cycle process and software maintenance

See Product Life Cycle and Update Policies for more information regarding the life cycle of Red Hat's software offerings.

During the maintenance phase of support, Red Hat provides security patches for Critical and Important security vulnerabilities, along with urgent and selected high-priority bug fix advisories.

About Red Hat

Red Hat is the world's leading provider of enterprise open source software solutions, using a community-powered approach to deliver reliable and high-performing Linux, hybrid cloud, container, and Kubernetes technologies. Red Hat helps customers develop cloud-native applications, integrate existing and new IT applications, and automate and manage complex environments. A trusted adviser to the Fortune 500, Red Hat provides award-winning support, training, and consulting services that bring the benefits of open innovation to any industry. Red Hat is a connective hub in a global network of enterprises, partners, and communities, helping organizations grow, transform, and prepare for the digital future.

About Red Hat Product Security

Red Hat Product Security believes that everyone, everywhere, is entitled to the access and quality information needed to mitigate security and privacy risks. We strive to protect communities of customers, contributors, and partners from digital security threats. We believe open source principles are the best way to achieve this.

Our mission is to protect customers by empowering Red Hat to design, build, and operate trustworthy solutions while engaging in open ecosystems. We accomplish this through three major functional areas:

- Focusing on the requirements phase of the traditional SDL and enabling customers to attain critical certifications to support Red Hat's open hybrid cloud strategy and market success
- Driving the cycle of continuous security improvements in Red Hat's productization pipelines. Supporting the systems and teams that store, manipulate, and package software to ensure the confidentiality, availability, and integrity of Red Hat's software
- Supporting Red Hat Product and Global Engineering with clear, open, and efficient secure development and vulnerability management practices

Contacting Red Hat Product Security

Red Hat takes security very seriously, and we aim to take immediate action to address serious security-related problems that involve our software.

Please report any suspected security vulnerability in any Red Hat software to Red Hat Product Security at secalert@redhat.com. You can use our GPG key to communicate with us securely.

To report an issue in any Red Hat branded website or online service, please contact Red Hat Information Security at site-security@redhat.com.

For more contact details, visit Red Hat Product Security's contact page.