Trusted software supply chains in government

"...anyone crafting a new application (or software artifact) is consuming dozens, if not hundreds, of open source packages downloaded from the internet.."

OMDIA[1]

What is in your software, and where has it been?

U.S. federal government software development teams are working to comply with Executive Order (EO) 14028, which contains a section titled "Enhancing Software Supply Chain Security."[2] The Office of Management and Budget (OMB) and National Institute of Standards and Technology (NIST) have issued guidance.[3,4]

The software supply chain encompasses everything and everyone that touches code at any time in the software development lifecycle (SDLC). This includes components, libraries, tools, processes, systems, and the people that code, build, deploy, and operate software. The ubiquity of open source has increased the urgency of trusted software supply chains. In a 2024 study of global organizations, 96% of codebases examined contained open source, and 77% of all code originated in open source.[5] A vulnerability in any open source component puts every other component that depends on it at risk for malware, backdoors, or other malicious code.

Some government teams have adopted individual tools and processes to enhance software supply chain security–for example, by creating software bills of material (SBOMs) and performing vulnerability scans. The shortcoming of most current processes is that they are manual, time consuming, and error prone. In most agencies the processes are also disjointed, leaving gaps that hackers can exploit to disrupt government services or exfiltrate sensitive or private information.

To comply with EO 14028, government software teams need a holistic approach to detecting and remediating vulnerabilities across the entire SDLC—code, build, deploy, and monitor. Processes and tools that enhance trust in the software supply chain do not have to slow down software delivery or create more work for operations teams. On the contrary, the right solutions provide the foundation for a modern software factory that speeds up the pace and quality of software delivery.

Red Hat's holistic approach to a trusted software supply chain

Red Hat® Trusted Software Supply Chain (TSSC) is a collection of capabilities that build security guardrails throughout the SDLC, helping government software teams comply with EO 14028 (Figure 1). Part of TSSC, Red Hat Trusted Application Pipeline is a set of 3 modular tools: Red Hat Developer Hub, Red Trusted Artifact Signer, and Red Hat Trusted Profile Analyzer. Government software teams can use these tools to move up the maturity levels in Supply-chain Levels for Software Artifacts (SLSA), a framework for incrementally enhancing software supply chain security. SLSA provides a checklist of standards and controls to prevent tampering, improve integrity, and make software

1 *"Building resiliency for a supply chain that users can trust."* OMDIA. 28 November 2023.

2 *"Executive Order on Improving the Nation's Cybersecurity."* The White House. 12 May 2021.

3 *"Enhancing the Security of the Software Supply Chain through Secure Software Development Practices,"* Office of Management and Budget. M-22-18. 14 September 2022.

4 *"Strategies for the Integration of Software Supply Chain Security in DevSecOps CI/CD Pipelines."* National Institute of Standards and Technology, NIST SP 800-204D. February 2024.

5 *"2024 Open Source Security and Risk Analysis Report."* Synopsis. 2024.

Supply-chain Levels for Software Artifacts (SLSA)

Led by a vendor-neutral steering group, SLSA is an end-to-end framework for software supply chain integrity. Agencies can use Red Hat technologies to advance through SLSA build levels.

- Level 1: Provenance
- Level 2: Hosted build platform
- Level 3: Hardened builds

Red Hat Trusted Software Supply Chain solutions

Red Hat Trusted Application Pipeline, including:

- Red Hat Trusted Profile Analyzer
- Red Hat Developer Hub
- Red Hat Trusted Artifact Signer

Red Hat OpenShift®

Red Hat Advanced Cluster Security for Kubernetes

Red Hat Quay

packages and infrastructure more secure. Red Hat Trusted Application Pipeline also helps software teams work more efficiently by identifying vulnerabilities earlier in the SDLC than they would otherwise. This practice, sometimes called shifting left, reduces time-consuming rework by limiting the propagation of vulnerable components to other code.

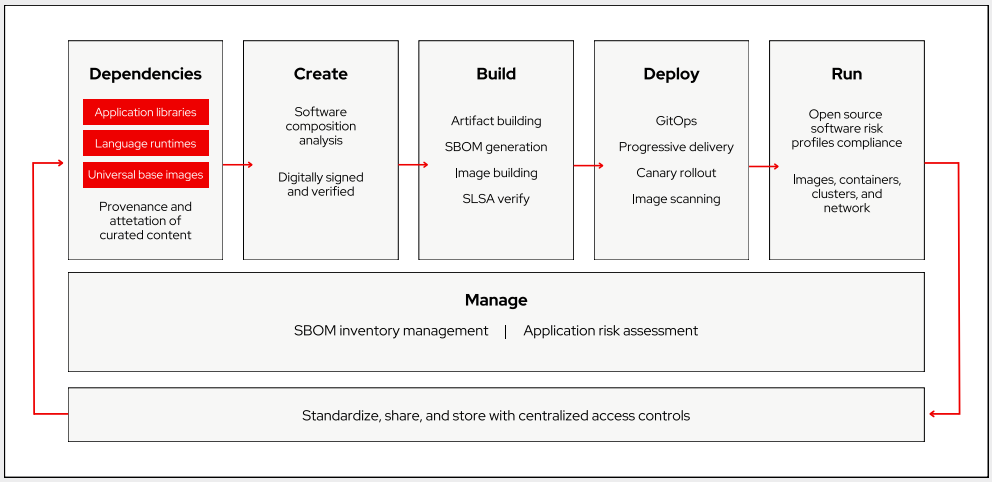

Figure 1. Build a golden path to a trusted software supply chain using Red Hat technologies throughout the SDLC.

During the code phase

Use Red Hat Trusted Application Pipeline tools to:

- Require developers to pull content only from trusted repositories. Git repositories serve as a single source of truth and track all code changes.
- View all dependencies within the pipeline, including code, binaries, and libraries, from within Red Hat Developer Hub. Identify vulnerabilities early in the SLDC with automated checks. Developer Hub provides an internal developer platform (IDP), software development templates, technical documentation, a centralized software catalog, and a plug-ins ecosystem.
- Simplify vulnerability management at code time using Red Hat Trusted Profile Analyzer.
- Track source code provenance and attestations. Trusted Application Pipeline provides actionable insights by identifying and analyzing dependencies to map each vulnerability's impact radius.

During the build phase

Safeguard build systems by verifying the authenticity and origin of third-party software and open source code. Use Red Hat Trusted Application Pipeline tools to:

- Generate, store, and manage SBOMs with SLSA attestations for each build. Trusted Profile Analyzer adds provenance metadata to SBOMs in either the CycloneDX or Software Package Data Exchange (SPDX) format. Including provenance in SBOMs helps software teams meet the requirements for SLSA build level 1 and the pending Secure Software Development Attestation Form from Cybersecurity and Infrastructure Security Agency (CISA).

The importance of provenance in SBOMs

Some agency teams already generate basic SBOMs, but most of these do not record the artifact's provenance—who created it, when, and with which dependencies. Simply knowing that an application contains component A is of limited value if component A (or any of its dependencies) was developed by an untrustworthy source or modified during its lifecycle to contain a vulnerability. Red Hat Trusted Profile Analyzer adds provenance to SBOM components, including libraries, binaries, runtimes, and codebases.

"Supply chain security is one of the most important priorities facing enterprise IT organizations today, especially as more and more business-critical systems and applications incorporate or leverage open source artifacts."

Al Gillen
Group Vice President, Development and Open Source, IDC

- Enforce agency security policies—for example, by checking for a specific common vulnerability and exposure (CVE) advisory, cross-referencing CVEs and other security advisories, and checking for container images that include a package manager (Figure 2). Package managers can be exploited to run malicious code at runtime.
- Manage risk during the build process by using Red Hat Trusted Profile Analyzer to analyze the impact of CVE and Vulnerability Exploitability eXchange (VEX) advisories. View remediation instructions from within Trusted Profile Analyzer.
- Require team members to sign and verify built artifacts throughout the software delivery chain. Trusted Artifact Signer reduces management overhead by using keyless signing and verification instead of long-lived key pairs that need to be managed, distributed, and revoked or renewed.

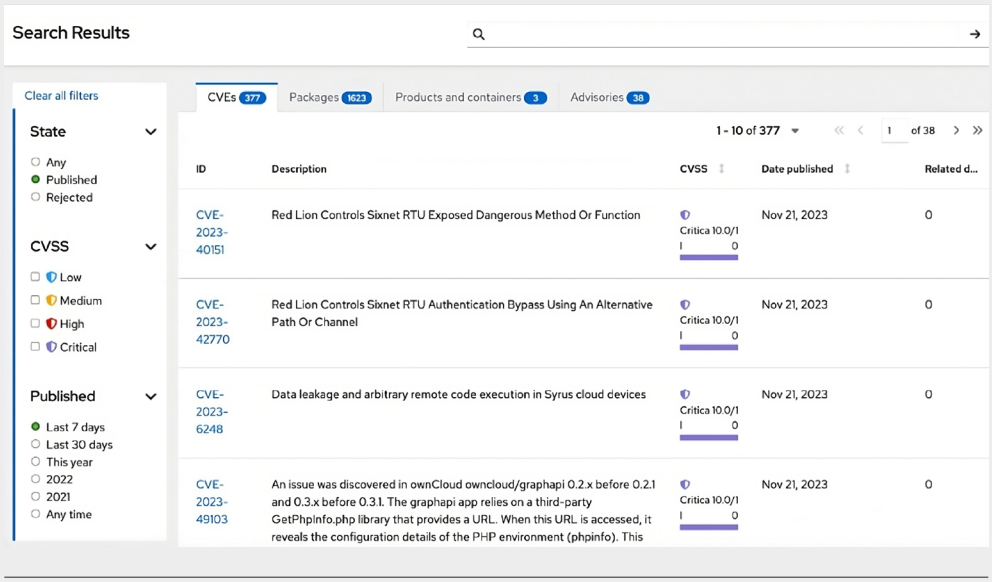

Figure 2. Search for CVEs and view their impact from within Trusted Profile Analyzer.

During the deploy phase

SLSA build levels 2 and 3 focus on preventing provenance tampering during and after the build. Create guardrails using Trusted Artifact Signer.

- Automatically attach the developer's digital signature whenever an artifact is changed. Digital signatures create a chain of custody.
- Log all code submissions in an immutable ledger to provide version control. In this way, only signed and verified build artifacts can propagate to other code or be deployed.
- Prevent configuration drift by enforcing an automated, security-focused release workflow for deploying container images to target host platforms.
- Implement release policies as code to block suspicious build activities.

During the monitor phase

Manage risk and improve your agency's security posture by using Red Hat Application Pipeline tools.

- Continuously monitor the health and security of containerized applications deployed across multiple hosted or on-premise platforms.
- Ingest and manage SBOMs and VEX advisories from third parties and your own build processes.
- Analyze CVE impact with visibility into where libraries, third-party code, and applications are used.
- Remediate vulnerabilities sooner with curated recommendations provided by Red Hat Trusted Profile Analyzer.
- Detect and remediate security issues using Red Hat Advanced Cluster Security for Kubernetes. Alerts are grouped by severity, helping to avoid alert fatigue.
- Continuously scan existing build images for emerging threats.
- Identify and mitigate security risks before deploying the image to the production environment, with Red Hat Quay.

Benefits summary: Trusted software supply chains support the mission

Comply with EO 14028. Enhance software supply chain security incrementally by advancing through the SLSA build levels. Start with automated creation of an SBOM that includes provenance (level 1). Add SBOM tampering prevention with digital signing and attestation (level 2). Further strengthen trust by integrating security checks into the continuous integration and continuous delivery (CI/CD) workflow (level 3).

Take a factory approach to software delivery. The same Red Hat capabilities that strengthen software supply chain security also form the foundation of a modern software factory that releases high-quality software at the speed the mission demands.

Increase developer productivity. Automatic enforcement of security guardrails throughout the SDLC helps developers spend less time fixing problems to gain more time for coding. For additional time savings, agency software teams can use Red Hat Ansible Automation Platform to automate security-related tasks such as configuration and patching.

Take the next steps

Talk to a Red Hatter.

Learn more about how Red Hat can help your agency achieve its mission.

About Red Hat

Red Hat helps customers standardize across environments, develop cloud-native applications, and integrate, automate, secure, and manage complex environments with award-winning support, training, and consulting services.

facebook.com/redhatinc
@RedHat
linkedin.com/company/red-hat

North America
1 888 REDHAT1
www.redhat.com

Europe, Middle East, and Africa
00800 7334 2835
europe@redhat.com

Asia Pacific
+65 6490 4200
apac@redhat.com

Latin America
+54 11 4329 7300
info-latam@redhat.com

redhat.com
#1272825_0824