Enhancing CMS software supply chain security with Red Hat tools

"Understanding the supply chain of software, obtaining an SBOM, and using it to analyze known vulnerabilities are crucial in managing risk."[1]

Executive Order 14028
Improving the Nation's Cybersecurity

Challenge: Manual processes create risk

Executive Order (EO) 14028, "Improving the Nation's Cybersecurity," contains a section titled, "Enhancing Software Supply Chain Security."[1] Escalating ransomware attacks on healthcare organizations[2] have highlighted the importance of protecting the Center for Medicare and Medicaid Services (CMS) software supply chain. A cautionary tale: United Healthcare paid US$22 million in ransom to unlock encrypted systems locked after a 2024 attack, but nevertheless saw its patient data exposed on the dark web.[3]

The CMS software supply chain comprises everything and everyone that touches code at any time in the software development lifecycle (SDLC). This includes components, libraries, tools, processes, systems, and the CMS staff and contractors who code, build, deploy, and operate software. *A vulnerability in any open source or proprietary component puts every other component that depends on it at risk for malware, backdoors, or other malicious code that can disrupt the mission.*

The challenge today is that many CMS processes used during the SDLC are manual, making them slow, time-consuming, and susceptible to human error. Compounding the risk, different CMS teams and departments follow different processes, leaving gaps that attackers exploit to disrupt the mission and exfiltrate personally identifiable information (PII) and personal health information (PHI). To comply with EO 14028 and build trusted software, CMS needs security-focused processes at every stage of the SDLC: code, build, deploy, and monitor.

The good news is that stronger security practices can actually speed up CMS software delivery rather than slowing them down. In particular, identifying vulnerabilities earlier in the SDLC ("shifting left") reduces the need for rework by limiting the propagation of vulnerable components to other code.

Red Hat can help

CMS can simplify compliance with EO 14028 by using Red Hat® Trusted Application Pipeline, part of Red Hat Trusted Software Supply Chain. Trusted Application Pipeline is a set of 3 modular tools:

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

These tools can help the CMS move up the maturity levels in the Supply-chain Levels for Software Artifacts (SLSA) framework[4] described in the sidebar.

Think of enhancing software supply chain security at CMS as a 3-part process.

Red Hat Trusted Software Supply Chain solutions

Red Hat Trusted Application Pipeline:

- 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

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

1 *"Fact sheet: 2024 report on the cybersecurity posture of the United States."* The White House, 7 May 2024.
2 *"Ransomware on the rise: Healthcare industry attack trends 2024."* Security Intelligence, 26 Sept. 2024.
3 *"UnitedHealth's cyberattack response costs to surpass $2.3B this year."* Healthcare Dive, 16 July 2024.
4 "Safeguarding artifact integrity across any software supply chain." SLSA, accessed 12 Dec. 2024.

1. Prevent and identify malicious code

"**Source integrity:** Ensure that all changes to the source code reflect the intent of the software producer."[4]

To trust a software component, CMS needs to know who built it, where, and why. Use Trusted Application Pipeline tools to catch vulnerabilities early in the software supply chain. For example, to:

- Generate, store, and manage a Software Bill of Materials (SBOMs) for each build, including the provenance metadata required for SLSA level 1 and the pending Secure Software Development Attestation Form from Cybersecurity and Infrastructure Security Agency (CISA).
- Require software team members to sign, verify, and attest to artifacts (container images, binaries, documents, etc.) throughout the software delivery chain. Trusted Artifact Signer is a cryptographic signature tool based on the open source sigstore project.
- Enforce CMS security policies such as 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, which can be exploited to run malicious code at runtime.

2. Manage risk during the build process

"**Build integrity:** The package has the sources and dependencies that the developer intended, and no artifact has been tampered with."[4]

Use Trusted Application Pipeline tools to:

- Require CMS developers and contractors 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. Automated checks can identify vulnerabilities early in the SDLC.
- Track source code provenance and attestations, and identify and analyze dependencies to see the impact radius of a vulnerable component.
- Safeguard build systems by verifying the authenticity and origin of 3rd-party software and open source code.
- Automate unit, integration, and user testing during build.
- Attach the developer's digital signature automatically 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 policy as code to block suspicious build activities.
- Identify and mitigate security risks before deploying the image to the production environment with Red Hat Quay.

Supply-chain Levels for Software Artifacts (SLSA)[4]

Led by a vendor-neutral steering group, SLSA is an end-to-end framework for software supply chain integrity:

Level 1—Provenance showing how the package was built

Level 2—Signed provenance to help prevent tampering *after* the build

Level 3—Signed provenance to help prevent tampering *during* the build

3. Monitor applications continuously at runtime

"**Availability:** The package can be maintained over time, and change histories are kept for future investigations or incident response."[4]

The earlier the CMS can detect malware in its environment, the sooner it can halt the spread to limit mission impact. Red Hat has a rich ecosystem of vendors with monitoring software certified to run with Red Hat technologies. Use this software in conjunction with Trusted Application Pipeline tools to:

- Continuously monitor the health and security of containerized applications deployed across multiple cloud-hosted or on-premise platforms.
- Ingest and manage SBOMs and vulnerability exploitability eXchange (VEX) advisories from 3rd parties and CMS build processes.
- Analyze CVE impact with visibility into where libraries, 3rd-party code, and applications are used.
- Remediate vulnerabilities in less time by using the curated recommendations provided by Trusted Profile Analyzer.
- Detect and remediate security issues using Red Hat Advanced Cluster Security. Alerts are grouped by severity, helping to avoid alert fatigue.
- Scan existing build images for emerging threats continuously. CMS can also use Red Hat OpenShift® AI to train machine learning (ML) models to recognize anomalous software behavior and score the risk.

Summary: comply with EO 14028, foster trust

Benefits to the CMS mission from using Trusted Application Pipeline start with EO 14028 compliance, but do not end there. The overarching benefit is deeper trust in CMS software, tools, and processes by patients, the workforce, and other agencies. Viewing the entire SDLC through a security lens will help the CMS create resilient, reliable, and security-focused software to achieve the mission—without slowing down innovation.

Learn more

Discover more about Red Hat's work with CMS at red.ht/cms.

Read more about Trusted software supply chains in government.

redhat.com
#1567557_1224