Des chaînes d'approvisionnement des logiciels fiables dans l'administration publique

« ...quiconque crée une application (ou un artéfact logiciel) consomme des dizaines, voire des centaines de paquets Open Source téléchargés sur Internet... »

OMDIA[1]

Contenu et provenance des logiciels

Les équipes de développement logiciel du gouvernement fédéral des États-Unis s'efforcent de respecter le décret exécutif (EO) 14028, qui contient une section intitulée « Enhancing Software Supply Chain Security[2] » (Renforcer la sécurité de la chaîne d'approvisionnement des logiciels). L'Office of Management and Budget (OMB) et le National Institute of Standards and Technology (NIST) ont formulé des conseils en ce sens[3, 4].

La chaîne d'approvisionnement des logiciels englobe tous les éléments associés à du code et toutes les personnes qui interagissent avec à n'importe quelle étape du cycle de vie de développement logiciel. Elle inclut les composants, les bibliothèques, les outils, les processus, les systèmes et les individus qui codent, créent, déploient et exploitent les logiciels. L'omniprésence de l'Open Source a renforcé le besoin de disposer de chaînes d'approvisionnement des logiciels éprouvées. Dans une étude menée auprès d'entreprises du monde entier en 2024, 96 % des codes bases analysés contenaient des éléments Open Source, et 77 % du code dans sa globalité ont des origines Open Source[5]. En cas d'attaque par logiciel malveillant, porte dérobée ou tout autre code malveillant, un composant Open Source vulnérable met en péril tous les autres composants qui en dépendent.

Certaines équipes dans l'administration publique ont adopté des outils et processus individuels pour renforcer la sécurité de la chaîne d'approvisionnement des logiciels, par exemple en créant des nomenclatures logicielles (SBOM) et en effectuant des analyses de vulnérabilité. L'inconvénient de la plupart des processus actuels est qu'ils sont manuels, chronophages et sujets aux erreurs. La plupart des agences gouvernementales se basent sur des processus décousus que les pirates informatiques peuvent exploiter pour perturber les services publics ou dérober des informations sensibles ou confidentielles.

Pour se conformer à l'EO 14028, les équipes chargées des logiciels doivent adopter une approche holistique pour détecter et corriger les vulnérabilités tout au long du cycle de vie de développement logiciel (codage, création, déploiement et surveillance). Les processus et outils qui renforcent la confiance dans la chaîne d'approvisionnement des logiciels ne doivent pas ralentir la distribution des logiciels ni alourdir la charge de travail des équipes d'exploitation. Au contraire, les meilleures solutions fournissent la base d'une usine logicielle moderne qui accélère le rythme et la qualité de la distribution des logiciels.

L'approche holistique de Red Hat en faveur d'une chaîne d'approvisionnement des logiciels éprouvée

Red Hat® Trusted Software Supply Chain (TSSC) est un ensemble de fonctionnalités qui contribuent à sécuriser le cycle de vie de développement logiciel, et aident ainsi les équipes chargées des logiciels dans l'administration publique à se conformer à l'EO 14028 (Figure 1). Partie intégrante de la solution TSSC, Red Hat Trusted Application Pipeline regroupe trois outils modulaires : Red Hat Developer Hub, Red Hat Trusted Artifact Signer et Red Hat Trusted Profile Analyzer. Ces outils accélèrent le passage entre les différents niveaux du framework SLSA (Supply-chain Levels for Software Artifacts), un cadre qui permet de renforcer progressivement la sécurité de la chaîne d'approvisionnement des logiciels. Ce framework fournit une liste de contrôles et de normes visant à empêcher la falsification,

1 *« Building resiliency for a supply chain that users can trust », OMDIA, 28 novembre 2023*

2 *« Executive Order on Improving the Nation's Cybersecurity », La Maison-Blanche, 12 mai 2021*

3 *« Enhancing the Security of the Software Supply Chain through Secure Software Development Practices », Office of Management and Budget, M-22-18, 14 septembre 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, février 2024*

5 *« 2024 Open Source Security and Risk Analysis Report », synopsis. 2024*

Framework SLSA

Dirigé par un groupe indépendant de tout fournisseur, le SLSA (Supply-chain Levels for Software Artifacts) est un framework complet visant à assurer l'intégrité de la chaîne d'approvisionnement des logiciels. Les agences publiques peuvent utiliser les technologies Red Hat pour suivre ce framework, un niveau après l'autre.

- Niveau 1 : provenance
- Niveau 2 : plateforme de build hébergée
- Niveau 3 : renforcement des builds

Solutions Red Hat Trusted Software Supply Chain

Red Hat Trusted Application Pipeline inclut les produits suivants :

- 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

améliorer l'intégrité et sécuriser les paquets logiciels ainsi que l'infrastructure. La solution Red Hat Trusted Application Pipeline permet également aux équipes responsables des logiciels de travailler plus efficacement en identifiant les vulnérabilités plus rapidement dans le cycle de vie de développement. Parfois appelée « shift left », cette pratique réduit les remaniements chronophages en limitant la propagation de composants vulnérables dans d'autres parties du code.

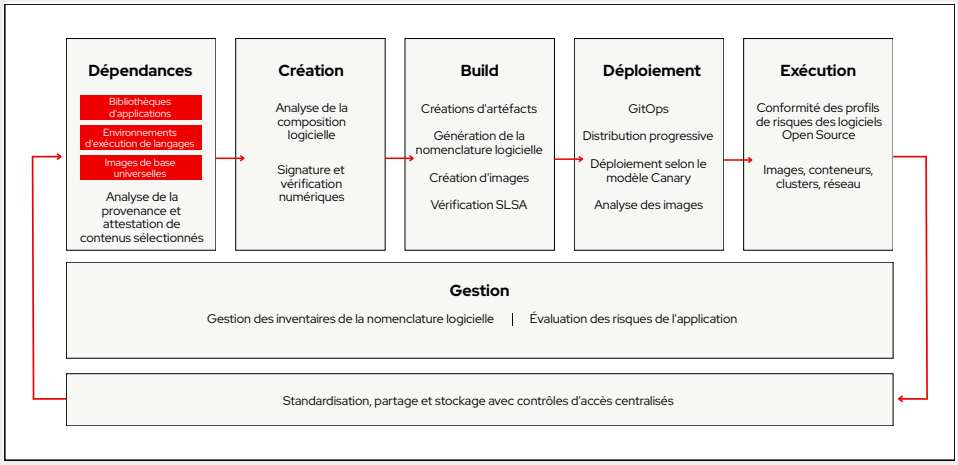

Figure 1. Création d'un parcours vers une chaîne d'approvisionnement des logiciels fiable à l'aide des technologies Red Hat tout au long du cycle de vie de développement logiciel

Lors de la phase de codage

Les outils de Red Hat Trusted Application Pipeline offrent les bénéfices suivants :

- Les équipes de développement sont obligées d'extraire du contenu uniquement à partir de référentiels de confiance. Les référentiels Git font office de source de vérité unique et permettent de suivre toutes les modifications apportées au code.
- Toutes les dépendances au sein du pipeline sont visibles dans Red Hat Developer Hub, y compris le code, les fichiers binaires et les bibliothèques. Il est facile d'identifier les vulnérabilités dans le cycle de vie de développement logiciel grâce à des contrôles automatisés. Developer Hub fournit une plateforme de développement interne (IDP), des modèles de développement logiciel, de la documentation technique, un catalogue de logiciels centralisé ainsi qu'un écosystème de plug-ins.
- La gestion des vulnérabilités est simplifiée au moment du codage avec Red Hat Trusted Profile Analyzer.
- Il est possible de suivre la provenance et les attestations du code source. Trusted Application Pipeline fournit des informations exploitables grâce à l'identification et l'analyse des dépendances afin de déterminer le rayon d'impact de chaque vulnérabilité.

Lors de la phase de création

Sécurisez les systèmes de création en vérifiant l'authenticité et l'origine des logiciels tiers et du code Open Source. Les outils de Red Hat Trusted Application Pipeline offrent les bénéfices suivants :

- Il est possible de générer, stocker et gérer des nomenclatures logicielles avec des attestations SLSA pour chaque build. Trusted Profile Analyzer ajoute aux nomenclatures logicielles des métadonnées sur la provenance au format CycloneDX ou SPDX (Software Package Data Exchange). Ces métadonnées permettent aux équipes responsables des logiciels de répondre aux exigences du niveau SLSA 1 et du formulaire d'attestation de développement de logiciels sécurisés (Secure Software Development Attestation Form) de la Cybersecurity and Infrastructure Security Agency (CISA).

L'importance de la provenance pour les nomenclatures logicielles

Si certaines équipes dans l'administration publique génèrent déjà des nomenclatures logicielles de base, la plupart d'entre elles n'enregistrent pas la provenance de l'artéfact, c'est-à-dire son créateur, sa date de création et ses dépendances. Il ne suffit pas de savoir qu'une application contient le composant A, surtout si ce composant A (ou l'une de ses dépendances) a été développé par une source non fiable ou modifié au cours de son cycle de vie de sorte qu'il contient désormais une vulnérabilité. La solution Red Hat Trusted Profile Analyzer ajoute la provenance au niveau des composants de la nomenclature logicielle, notamment les bibliothèques, les fichiers binaires, les environnements d'exécution et les codes bases.

« La sécurité de la chaîne d'approvisionnement est l'une des priorités majeures pour les entreprises informatiques d'aujourd'hui, d'autant plus que de plus en plus de systèmes et d'applications essentiels à leur activité intègrent ou exploitent des artéfacts Open Source. »

Al Gillen
Vice-président du Groupe, Développement et Open Source, IDC

- Les agences peuvent appliquer des politiques de sécurité en vérifiant l'existence d'un avis sur des CVE (Common Vulnerabilities and Exposures) spécifiques, en procédant à une référence croisée des CVE et d'autres avis de sécurité, ainsi qu'en vérifiant les images de conteneurs qui incluent un gestionnaire de paquets (Figure 2). Il est possible d'exploiter les gestionnaires de paquets pour exécuter du code malveillant pendant leur exécution.
- Red Hat Trusted Profile Analyzer permet de gérer les risques au cours du processus de création en analysant l'impact des CVE et des VEX (Vulnerability Exploitability eXchange). Les instructions pour corriger les vulnérabilités sont visibles directement dans Trusted Profile Analyzer.
- Les membres des équipes sont obligés de signer et vérifier les artéfacts de builds tout au long de la chaîne de distribution logicielle. Trusted Artifact Signer réduit les coûts de gestion en utilisant la signature et la vérification sans clé plutôt que des paires de clés durables qui doivent être gérées, distribuées et révoquées ou renouvelées.

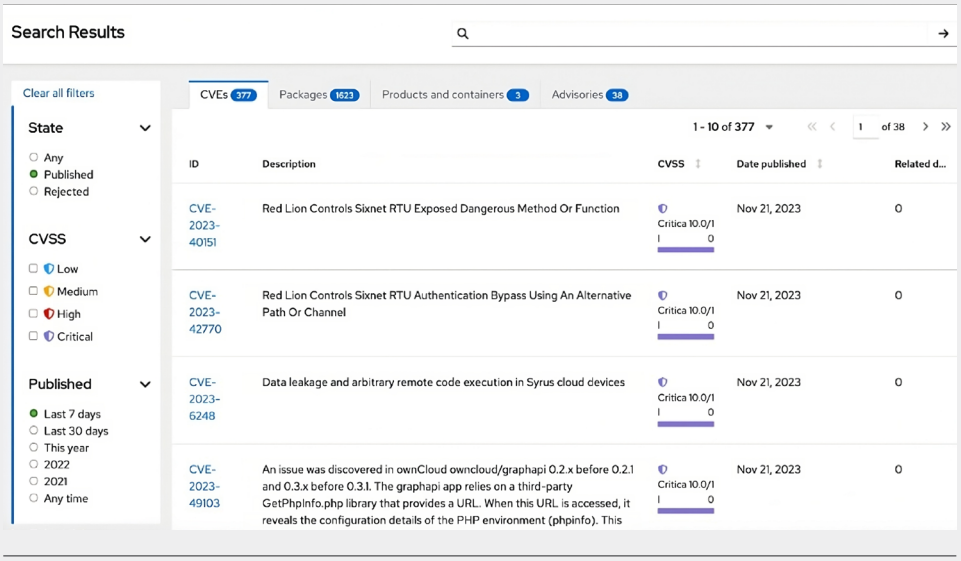

Figure 2. Recherche de CVE et visualisation de leur impact dans l'outil Trusted Profile Analyzer

Lors de la phase de déploiement

Les niveaux 2 et 3 du framework SLSA visent à empêcher la falsification de provenance pendant et après la création. Trusted Artifact Signer permet de mettre en place des mesures de sécurité :

- La signature numérique du développeur est automatiquement apposée lors de la modification d'un artéfact. Les signatures numériques créent une chaîne de contrôle.
- Tous les codes ajoutés à un grand livre immuable sont journalisés pour permettre le contrôle des versions. De cette manière, seuls les artéfacts de builds signés et vérifiés peuvent être propagés dans d'autres parties du code ou déployés.
- Afin d'éliminer les écarts de configuration, le déploiement des images de conteneurs au sein des plateformes hôtes cible passe par un workflow de lancement automatisé et axé sur la sécurité.
- Des politiques de lancement en tant que code bloquent les activités suspectes au niveau des builds.

Lors de la phase de surveillance

Les outils de Red Hat Application Pipeline permettent de gérer les risques et d'améliorer la posture de sécurité des agences publiques :

- Surveillance en continu de l'état de santé et de la sécurité des applications conteneurisées déployées sur de nombreuses plateformes hôtes ou sur site
- Ingestion et gestion des nomenclatures logicielles et des avis de VEX provenant de tiers et de vos propres processus de build
- Analyse de l'impact des CVE avec une visibilité sur les environnements où les bibliothèques, le code tiers et les applications sont utilisés
- Correction plus précoce des vulnérabilités grâce à des recommandations formulées par Red Hat Trusted Profile Analyzer
- Détection et correction des problèmes de sécurité à l'aide de la solution Red Hat Advanced Cluster Security for Kubernetes ; les alertes sont regroupées par sévérité pour éviter tout déclenchement intempestif
- Analyse continue des images de build existantes à la recherche de menaces émergentes
- Identification et atténuation des risques de sécurité avant le déploiement d'une image dans l'environnement de production avec Red Hat Quay

Résumé des avantages : une chaîne d'approvisionnement des logiciels fiable pour soutenir votre mission

Conformité avec le décret exécutif EO 14028. Renforcez progressivement la sécurité de la chaîne d'approvisionnement des logiciels en suivant les niveaux du framework SLSA. Commencez par la création automatisée d'une nomenclature logicielle incluant la provenance (niveau 1). Empêchez la falsification de la nomenclature à l'aide de signatures numériques et d'attestations (niveau 2). Renforcez la confiance en ajoutant des contrôles de sécurité au workflow d'intégration et de distribution continues (CI/CD) (niveau 3).

Choix d'une approche « industrielle » de la distribution logicielle. Les fonctionnalités de Red Hat qui renforcent la sécurité de la chaîne d'approvisionnement des logiciels forment également la base d'une usine logicielle moderne permettant de publier des logiciels de haute qualité au rythme imposé par la mission de votre agence.

Hausse de la productivité des équipes de développement. L'application automatique de mesures de sécurité tout au long du cycle de vie de développement logiciel permet aux équipes de consacrer davantage de temps au codage plutôt qu'à la résolution des problèmes. Pour optimiser les gains de temps, les équipes peuvent utiliser Red Hat Ansible Automation Platform afin d'automatiser les tâches liées à la sécurité telles que la configuration et l'application de correctifs.

Pour aller plus loin

Parlez à un représentant Red Hat.

Découvrez comment nous pouvons aider votre agence à mener à bien sa mission.

À propos de Red Hat

Red Hat aide ses clients à standardiser leurs environnements, à développer des applications cloud-native et à intégrer, automatiser, sécuriser et gérer des environnements complexes en offrant des services d'assistance, de formation et de consulting primés.

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

EUROPE, MOYEN-ORIENT ET AFRIQUE (EMEA)
00800 7334 2835
europe@redhat.com

FRANCE
00 33 1 41 91 23 23
fr.redhat.com

fr.redhat.com
#1272825_0824