Red Hat ツールで CMS ソフトウェア・サプライチェーンのセキュリティを強化

「ソフトウェア・サプライチェーンを理解し、SBOM を取得し、それを使用して既知の脆弱性を分析することは、リスクを管理するうえで非常に重要です」[1]

大統領令 (EO 14028)
Improving the Nation's Cybersecurity
(国家のサイバーセキュリティ向上)

課題：手動のプロセスがリスクを生む

大統領令 (EO) 14028「Improving the Nation's Cybersecurity (国家のサイバーセキュリティ向上)」には、「Enhancing Software Supply Chain Security (ソフトウェア・サプライチェーンのセキュリティ強化)」というタイトルのセクションが含まれています。[1]これは、医療機関に対するランサムウェア攻撃の激化[2]により、メディケアおよびメディケイド・サービス・センター (CMS) のソフトウェア・サプライチェーンを保護することの重要性が浮き彫りになっていることを意味します。重要性を示す一例として、2024 年、UnitedHealthcare は攻撃を受け、ロックされた暗号化システムのロック解除のために身代金 2,200 万米ドルを支払ったにもかかわらず、患者データがダークウェブに公開されてしまいました。[3]

CMS ソフトウェア・サプライチェーンは、ソフトウェア開発ライフサイクル (SDLC) のあらゆる時点でコードに触れるすべてのものと人で構成されています。これには、コンポーネント、ライブラリ、ツール、プロセス、システムが含まれているだけでなく、ソフトウェアのコーディング、構築、導入、運用を行う CMS スタッフと請負業者が含まれます。オープンソースまたは独自のコンポーネントのいずれかに脆弱性があると、それに依存する他のすべてのコンポーネントがマルウェア、バックドア、または任務を妨害する可能性のあるその他の悪意のあるコードの危険にさらされます。

現在の課題は、SDLC の中で使用される CMS プロセスの多くが手動なために、時間がかかり、人的ミスが発生しやすいことです。さらにリスクが高まる要因として、さまざまな CMS チームや部門がそれぞれ異なるプロセスに従っていることが挙げられます。このため、攻撃者が任務を妨害し、個人を特定できる情報 (PII) や個人の健康情報 (PHI) の窃取に利用できるギャップが生じます。EO 14028 に準拠し、信頼できるソフトウェアを構築するには、SDLC のすべての段階 (コーディング、構築、デプロイ、監視) において、セキュリティに重点を置いた CMS プロセスが必要です。

実際のところ、セキュリティを強化すれば、CMS ソフトウェアの提供が遅れるのではなく高速化できます。特に、SDLC で脆弱性を早期に特定 (「シフトレフト」) すると、他のコードへの脆弱なコンポーネントの伝播が制限されるため、再作業の必要性が減ります。

Red Hat が提供できるサポート

CMS は、Red Hat Trusted Software Supply Chain の一部である Red Hat® Trusted Application Pipeline を使用することで、EO 14028 への準拠を単純化できます。Trusted Application Pipeline は、次の 3 つのモジュール式ツールのセットです。

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

これらのツールは、CMS が Supply-chain Levels for Software Artifacts (SLSA) フレームワーク[4]の成熟度レベル (サイドバーに説明があります) を上げるのに役立ちます。

CMS のソフトウェア・サプライチェーンのセキュリティ強化は、次の 3 つの部分からなるプロセスとして考えられます。

Red Hat Trusted Software Supply Chain ソリューション

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

1 「Fact sheet: 2024 report on the cybersecurity posture of the United States」、ホワイトハウス、2024 年 5 月 7 日。
2 「Ransomware on the rise: Healthcare industry attack trends 2024」、Security Intelligence、2024 年 9 月 26日。
3 「UnitedHealth's cyberattack response costs to surpass $2.3B this year」、Healthcare Dive、2024 年 7 月 16 日。
4 「Safeguarding artifact integrity across any software supply chain」、SLSA、2024 年 12 月 12 日にアクセス。

1. 悪意のあるコードの防止と特定

「**ソースの完全性：**ソースコードに対するすべての変更がソフトウェア製作者の意図を反映しているようにする」[4]

ソフトウェア・コンポーネントを信頼するには、それを誰が、どこで、なぜ構築したのかを CMS が知る必要があります。Trusted Application Pipeline ツールを使用して、ソフトウェア・サプライチェーンの早い段階で脆弱性を発見します。たとえば、次を実行します。

- 各ビルドのソフトウェア部品表 (SBOM) を生成、保存、管理します。これには、SLSA レベル 1 に必要な来歴メタデータと、米国サイバーセキュリティ・社会基盤安全保障庁 (CISA) からの保留中のセキュア・ソフトウェア開発証明書フォームが含まれます。
- ソフトウェアチームのメンバーに、ソフトウェア提供チェーン全体で成果物 (コンテナイメージ、バイナリー、ドキュメントなど) に署名、検証、および証明することを要求します。Trusted Artifact Signer は、オープンソースの sigstore プロジェクトに基づく暗号化署名ツールです。
- CMS セキュリティポリシーを適用します。これには、特定の共通脆弱性識別子 (CVE) アドバイザリーのチェック、CVE と他のセキュリティ・アドバイザリーの相互参照、ランタイム時に悪意のあるコードを実行するために悪用される可能性のあるパッケージマネージャーを含むコンテナイメージのチェックなどが含まれます。

2. 構築プロセス中のリスクの管理

「**ビルドの整合性：**パッケージには開発者が意図したソースと依存関係があり、アーティファクトは改ざんされていない」[4]

Trusted Application Pipeline を使用して次のことを実行します。

- CMS 開発者と請負業者に、信頼できるリポジトリからのみコンテンツを取得するよう要求します。Git リポジトリが信頼できる単一の情報源として機能し、すべてのコードの変更を追跡します。
- コード、バイナリー、ライブラリなど、パイプライン内のすべての依存関係を確認します。自動チェックにより、SDLC の初期段階で脆弱性を特定できます。
- ソースコードの出所と証明を追跡し、依存関係を特定および分析して、脆弱なコンポーネントの影響範囲を確認します。
- サードパーティのソフトウェアおよびオープンソースのコードの信頼性と出所を検証し、ビルドシステムを保護します。
- ビルド中のユニットテスト、統合テスト、ユーザーテストを自動化します。
- アーティファクトが変更されるたびに、開発者のデジタル署名を自動的に添付します。デジタル署名は証拠保全となります。
- バージョン管理を提供するために、すべてのコード送信をイミュータブルな台帳に記録します。そうすることで、署名および検証されたビルドアーティファクトのみが他のコードに伝播またはデプロイされます。
- コンテナイメージをターゲットのホスト・プラットフォームにデプロイするための、セキュリティ重視の自動化されたリリースワークフローを強制することで、構成のドリフトを防ぎます。
- ポリシーをコードとして実装し、不審なビルドアクティビティをブロックします。
- Red Hat Quay を使用してプロダクション環境にイメージをデプロイする前に、セキュリティリスクを特定して軽減します。

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

ベンダーに依存しない運営グループが主導する SLSA は、ソフトウェア・サプライチェーンの整合性のためのエンドツーエンドのフレームワークです。

レベル 1：パッケージがどのように構築されたかを示す来歴

レベル 2：ビルド後の改ざんを防ぐのに役立つ署名済み来歴

レベル 3：ビルド中の改ざんを防ぐのに役立つ署名済み来歴

3. 実行時におけるアプリケーションの継続的監視

「**可用性：**パッケージを長期にわたって維持し、変更履歴を将来の調査やインシデント対応のために保存する」[4]

CMS が環境内のマルウェアをより早く検出できれば、より早い段階で拡散を阻止してミッションへの影響を抑えることができます。Red Hat には、Red Hat テクノロジーでの動作が認定済みの監視ソフトウェアを提供している多数のベンダーからなるエコシステムがあります。こうしたソフトウェアと Trusted Application Pipeline ツールを併用して次のことを実行します。

- 複数のクラウドホスト型プラットフォームまたはオンプレミスのプラットフォームにデプロイされたコンテナ化されたアプリケーションの健全性とセキュリティを継続的に監視します。
- サードパーティからの SBOM および脆弱性悪用可能性交換 (VEX) アドバイザリーと、CMS ビルドプロセスを取り込んで管理します。
- CVE の影響を分析して、ライブラリ、サードパーティのコード、アプリケーションが使用されている場所を把握します。
- Trusted Profile Analyzer が提供する厳選された推奨事項を使用して、脆弱性を短時間で修復します。
- Red Hat Advanced Cluster Security を使用してセキュリティ問題を検出し、修復します。アラートは重大度別にグループ化されているため、アラート疲れを回避することができます。
- 新たな脅威に関して既存のビルドイメージを継続的にスキャンします。CMS は、Red Hat OpenShift® AI を使用して機械学習 (ML) モデルをトレーニングし、ソフトウェアの異常な動作を認識してリスクをスコアリングすることもできます。

まとめ：EO 14028 に準拠し、信頼を育む

Trusted Application Pipeline の使用によって CMS のミッションにもたらされるメリットは、EO 14028 への準拠から始まりますが、そこで終わるわけではありません。最も重要なメリットは、CMS ソフトウェア、ツール、プロセスに対する、患者、従業員、その他の機関からの信頼が深まることです。セキュリティの視点から SDLC 全体を見ることにより、CMS は、イノベーションを遅らせることなく、回復力と信頼性が高くセキュリティに重点を置いたソフトウェアを作成し、任務を達成することができます。

詳細はこちら

Red Hat の CMS の取り組みについて詳しくは、red.ht/cms をご覧ください。

政府の信頼できるソフトウェア・サプライチェーンの詳細についてお読みください。

Red Hat について

Red Hat は、受賞歴のあるサポート、トレーニング、コンサルティング・サービスをお客様に提供し、複数の環境にわたる標準化、クラウドネイティブ・アプリケーションの開発、複雑な環境の統合、自動化、セキュリティ保護、運用管理を支援します。

アジア太平洋
+65 6490 4200
apac@redhat.com

オーストラリア
1 800 733 428

インド
+91 22 3987 8888

インドネシア
001 803 440 224

日本
03 4590 7472

韓国
080 708 0880

マレーシア
1 800 812 678

ニュージーランド
0800 450 503

シンガポール
800 448 1430

中国
800 810 2100

香港
800 901 222

台湾
0800 666 052

fb.com/RedHatJapan
twitter.com/RedHatJapan
linkedin.com/company/red-hat

jp.redhat.com
#1567557_1224