Red Hat Insights 2022

Vulnerability サービスおよび Ansible Playbook を使用したセキュリティー公開の修復

RHEL 環境における CVE セキュリティー脆弱性の修復の自動化

Last Updated: 2022-06-19

Red Hat Insights 2022 Vulnerability サービスおよび Ansible Playbook を使用したセキュリティー公開の修復

RHEL 環境における CVE セキュリティー脆弱性の修復の自動化

Enter your first name here. Enter your surname here.
Enter your organisation's name here. Enter your organisational division here.
Enter your email address here.

法律上の通知

概要

Vulnerability サービスを使用して、RHEL 環境で CVE セキュリティー脆弱性を修復します。

目次

多様性を受け入れるオープンソースの強化

Red Hat では、コード、ドキュメント、Web プロパティーにおける配慮に欠ける用語の置き換えに取り組んでいます。まずは、マスター (master)、スレーブ (slave)、ブラックリスト (blacklist)、ホワイトリスト (whitelist) の 4 つの用語の置き換えから始めます。この取り組みは膨大な作業を要するため、今後の複数のリリースで段階的に用語の置き換えを実施して参ります。詳細は、Red Hat CTO である Chris Wright のメッセージをご覧ください。

RED HAT ドキュメントへのフィードバック

弊社のドキュメントに関するご意見やご感想をお寄せください。フィードバックを提供するには、ドキュメントのテキストを強調表示し、コメントを追加します。

前提条件

- Red Hat カスタマーポータルにログインしている。
- Red Hat カスタマーポータルでは、このドキュメントは **Multi-page HTML** 表示形式です。

手順

フィードバックを提供するには、以下の手順を実施します。

1. ドキュメントの右上隅にある **フィードバック** ボタンをクリックして、既存のフィードバックを確認します。

注記

フィードバック機能は、**マルチページ HTML** 形式でのみ有効です。

2. フィードバックを提供するドキュメントのセクションを強調表示します。
3. ハイライトされたテキスト近くに表示される **Add Feedback** ポップアップをクリックします。ページの右側のフィードバックセクションにテキストボックスが表示されます。
4. テキストボックスにフィードバックを入力し、**Submit** をクリックします。ドキュメントに関する問題が作成されます。
5. 問題を表示するには、フィードバックビューで問題リンクをクリックします。

第1章 RHEL システムで CVE 脆弱性を修復するための ANSIBLE PLAYBOOK の作成

以下のドキュメントでは、Vulnerability サービスユーザーが Ansible Playbook を作成し、RHEL システムで CVE の修復を自動化する方法を説明します。

Vulnerability サービスを使用する場合には、修復する問題の選択時に、利用可能なアプローチが 2 つあります。

- 単一システムに影響する複数の CVE を修復します。
- 単一の CVE の影響を受ける複数のシステムを修復します。

第2章 1台のシステムに影響する複数の CVE の修復

単一のシステムで CVE の脆弱性を修復するには、以下の手順を行います。

手順

1. 必要に応じて Red Hat Enterprise Linux > Vulnerability > Systems タブに移動し、ログインします。
2. 名前でシステムを検索するか、リストをスクロールして修正するシステムを見つけます。
3. システム名をクリックして、システムの詳細と CVE 公開の一覧を表示します。
4. CVE 名の左側にあるチェックボックスを使用して、このシステムで修復する CVE を選択し、**Remediate** をクリックします。
5. **Add to existing playbook** または **Create new Playbook** を選択し、任意の名前を指定します。**Next** をクリックします。
6. Remediation の確認の情報が正しいことを確認します。デフォルトでは、**autoreboot** が有効になっています。必要に応じて、**Turn off autoreboot** をクリックし、**Submit** をクリックします。
7. Remediations で Playbook を見つけ、yaml ファイルをダウンロードします。
8. Yaml ファイルを Ansible ワークフローに追加します。

第3章 単一の CVE の影響を受ける複数のシステムの修復

単一の CVE の脆弱性のシステムを修復するには、以下の手順を行います。

手順

1. 必要に応じて Red Hat Enterprise Linux > Vulnerability > CVE タブに移動し、ログインします。
2. CVE をクリックし、個別の CVE に関する詳細情報を表示します。また、スクロールダウンして公開される全システムを表示します。
3. **Remediate** するシステムを選択し、修復をクリックします。
4. **Add to existing playbook** または **Create new Playbook** を選択し、任意の名前を指定します。**Next** をクリックします。
5. Remediation の確認の情報が正しいことを確認します。デフォルトでは、**autoreboot** が有効になっています。必要に応じて、**Turn off autoreboot** をクリックし、**Submit** をクリックします。
6. Remediations で Playbook を見つけ、yaml ファイルをダウンロードします。
7. Yaml ファイルを Ansible ワークフローに追加します。

第4章 参考資料

Vulnerability サービスや他の Insights for Red Hat Enterprise Linux サービスに関する詳細は、以下の資料をご利用いただけます。

- **RHEL システムでのセキュリティー脆弱性の評価および監視**
- **Vulnerability サービスレポートの生成**
- Insights for Red Hat Enterprise Linux ドキュメント
- Insights for Red Hat Enterprise Linux 製品サポートページ