Red Hat Insights 1-latest

FedRAMP に準拠した Vulnerability サービスレポートの生成

CVE セキュリティーの脆弱性に晒された RHEL システムの通知

Last Updated: 2024-03-27

Red Hat Insights 1-latest FedRAMP に準拠した Vulnerability サービスレポートの生成

CVE セキュリティーの脆弱性に晒された RHEL システムの通知

法律上の通知

概要

FedRAMP® に準拠して脆弱性サービスレポートを生成し、CVE セキュリティーの脆弱性にさらされている RHEL システムを通知します。 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。

目次

第1章 INSIGHTS FOR RED HAT ENTERPRISE LINUX 脆弱性サービスレポートの概要

DevOps チーム、セキュリティーチーム、エグゼクティブチームなどのさまざまなステークホルダーに、インフラストラクチャーのセキュリティー脆弱性を伝達する機能は極めて重要です。Vulnerability サービスを使用すると、以下のレポートをダウンロードしてオフラインで分析したり、他のユーザーと共有することができます。

- **Executive Reports**: エグゼクティブに向けたインフラストラクチャーのセキュリティー脆弱性に関する PDF 形式のサマリーおよび概要
- **CVE reports**: インフラストラクチャーが晒されている CVE を選択したり、フィルタリングした PDF 形式のレポート。脆弱性データのハイライトおよび共有が目的。
- **Vulnerability data export** エクスポートの実行時に設定したフィルターをもとに選択した CVE データの JSON または CSV ファイルへのエクスポート。

第2章 エグゼクティブレポート

インフラストラクチャーでのセキュリティー脆弱性をまとめた概要エグゼクティブレポートをダウンロードできます。エグゼクティブレポートは、エグゼクティブを対象として設計された 2 - 3 ページの PDF ファイルで、以下の情報が含まれます。

ページ 1

- 分析する RHEL システムの数
- システムが現在影響を受ける個別の CVE 数
- インフラストラクチャー内のセキュリティールールの数
- アドバイザリーがある CVE のリスト

ページ 2

- 重大度別の CVE の割合 (CVSS ベーススコア範囲)
- 7、30、および 90 日間に公開された CVE の数
- セキュリティールールや既知の不正使用など、インフラストラクチャー内で上位 3 つの CVE

ページ 3

- 重大度別のセキュリティールールの内訳
- 上位 3 つのセキュリティールール (重大度やセキュリティーリスクに晒されているシステムの数を含む)

2.1. エグゼクティブレポートのダウンロード

以下の手順に従い、レポートをダウンロードします。

手順

1. Security > Vulnerability > Reports タブに移動し、必要に応じてログインします。
2. **Executive report** カードで、**Download PDF** をクリックします。
3. **Save File**、**OK** の順にクリックします。

検証

1. PDF ファイルが **Downloads** フォルダーまたは指定した場所にあることを確認します。

2.2. VULNERABILITY サービス API を使用したエグゼクティブレポートのダウンロード

Vulnerability サービス API を使用してレポートをダウンロードできます。

- リクエスト URL: https://console.openshiftusgov.com/api/vulnerability/v1/report/executive

- Curl:

```
curl -X GET "{CONSOLE_URL}/api/vulnerability/v1/report/executive" -H  "accept:
application/vnd.api+json"
```

第3章 CVE による報告

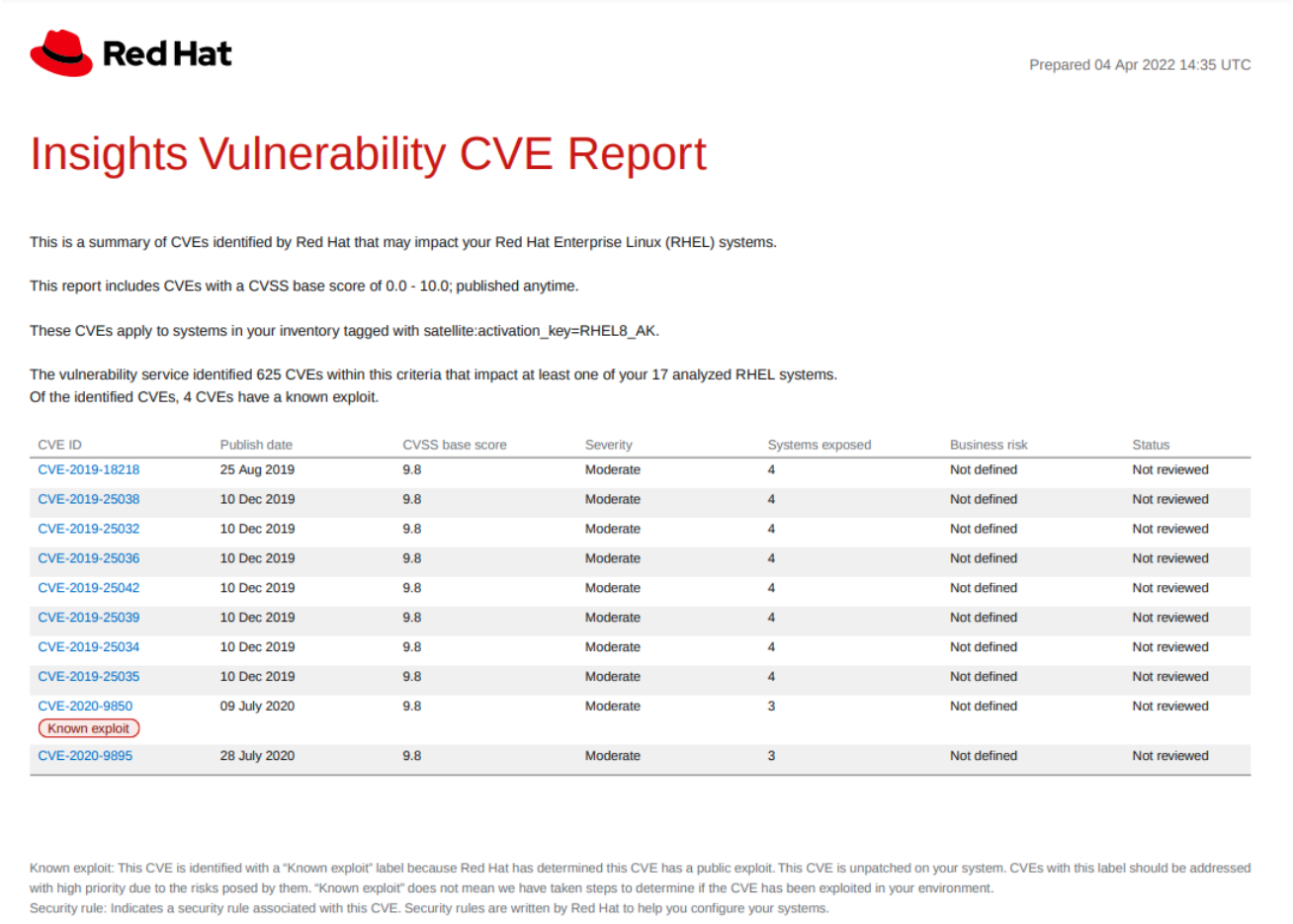
システムが影響を受ける CVE のフィルターされたリストを示す PDF レポートを作成できます。各レポートに、関連する名前を付け、フィルターを適用し、ユーザーノートを追加して、集中データを特定のステークホルダーに表示します。

PDF レポートを設定する際に、以下のフィルターを適用できます。

- **Security rules:** セキュリティールールラベルの付いた CVE のみを表示します。
- **Known exploit:** 既知の不正使用ラベルの付いた CVE のみを表示します。
- **Severity:** 1 つ以上の値 (Critical、Important、Moderate、Low、または Unknown) を選択します。
- **CVSS ベーススコア。** All、0.0-3.9、4.0-7.9、8.0-10.0、N/A (該当なし) から、1 つまたは複数の範囲を選択します。
- **ビジネスリスク。** High、Medium、Low、Not defined から、1 つまたは複数の値を選択します。
- **Status:** Not reviewed、In review、On-hold、Scheduled for patch、Resolved、No action - risk accepted, Resolved via mitigation から、1 つまたは複数の値を選択します。
- **Publish date:** 以下から選択します (All、Last 7 days、Last 30 days、Last 90 days、Last year、More than 1 year)。
- **Applies to OS:** フィルターして表示するシステムの RHEL マイナーバージョンを選択します。
- **Tags:** タグ付けされたシステムのグループを選択します。タグおよびシステムグループの詳細は、システムタグとグループ を参照してください。
- **Advisory:** 関連するアドバイザリー (エラータ) のある CVE のみを表示するか、アドバイザリーのない CVE のみを表示するか、またはすべての CVE を表示するかを選択します。

CVE レポートでは、CVE と、Red Hat CVE データベースで該当する CVE ページへのリンクが記載されるため、各 CVE の詳細を確認できます。このリストは、主に CVE の公開日によって順序付けられ、リストの上部に最新の CVE が公開されます。

Insights 脆弱性 CVE レポートの例



Red Hat

Prepared 04 Apr 2022 14:35 UTC

Insights Vulnerability CVE Report

This is a summary of CVEs identified by Red Hat that may impact your Red Hat Enterprise Linux (RHEL) systems.

This report includes CVEs with a CVSS base score of 0.0 - 10.0; published anytime.

These CVEs apply to systems in your inventory tagged with satellite:activation_key=RHEL8_AK.

The vulnerability service identified 625 CVEs within this criteria that impact at least one of your 17 analyzed RHEL systems.
Of the identified CVEs, 4 CVEs have a known exploit.

CVE ID	Publish date	CVSS base score	Severity	Systems exposed	Business risk	Status
CVE-2019-18218	25 Aug 2019	9.8	Moderate	4	Not defined	Not reviewed
CVE-2019-25038	10 Dec 2019	9.8	Moderate	4	Not defined	Not reviewed
CVE-2019-25032	10 Dec 2019	9.8	Moderate	4	Not defined	Not reviewed
CVE-2019-25036	10 Dec 2019	9.8	Moderate	4	Not defined	Not reviewed
CVE-2019-25042	10 Dec 2019	9.8	Moderate	4	Not defined	Not reviewed
CVE-2019-25039	10 Dec 2019	9.8	Moderate	4	Not defined	Not reviewed
CVE-2019-25034	10 Dec 2019	9.8	Moderate	4	Not defined	Not reviewed
CVE-2019-25035	10 Dec 2019	9.8	Moderate	4	Not defined	Not reviewed
CVE-2020-9850 Known exploit	09 July 2020	9.8	Moderate	3	Not defined	Not reviewed
CVE-2020-9895	28 July 2020	9.8	Moderate	3	Not defined	Not reviewed

Known exploit: This CVE is identified with a "Known exploit" label because Red Hat has determined this CVE has a public exploit. This CVE is unpatched on your system. CVEs with this label should be addressed with high priority due to the risks posed by them. "Known exploit" does not mean we have taken steps to determine if the CVE has been exploited in your environment.
Security rule: Indicates a security rule associated with this CVE. Security rules are written by Red Hat to help you configure your systems.

3.1. CVE の PDF レポートの作成

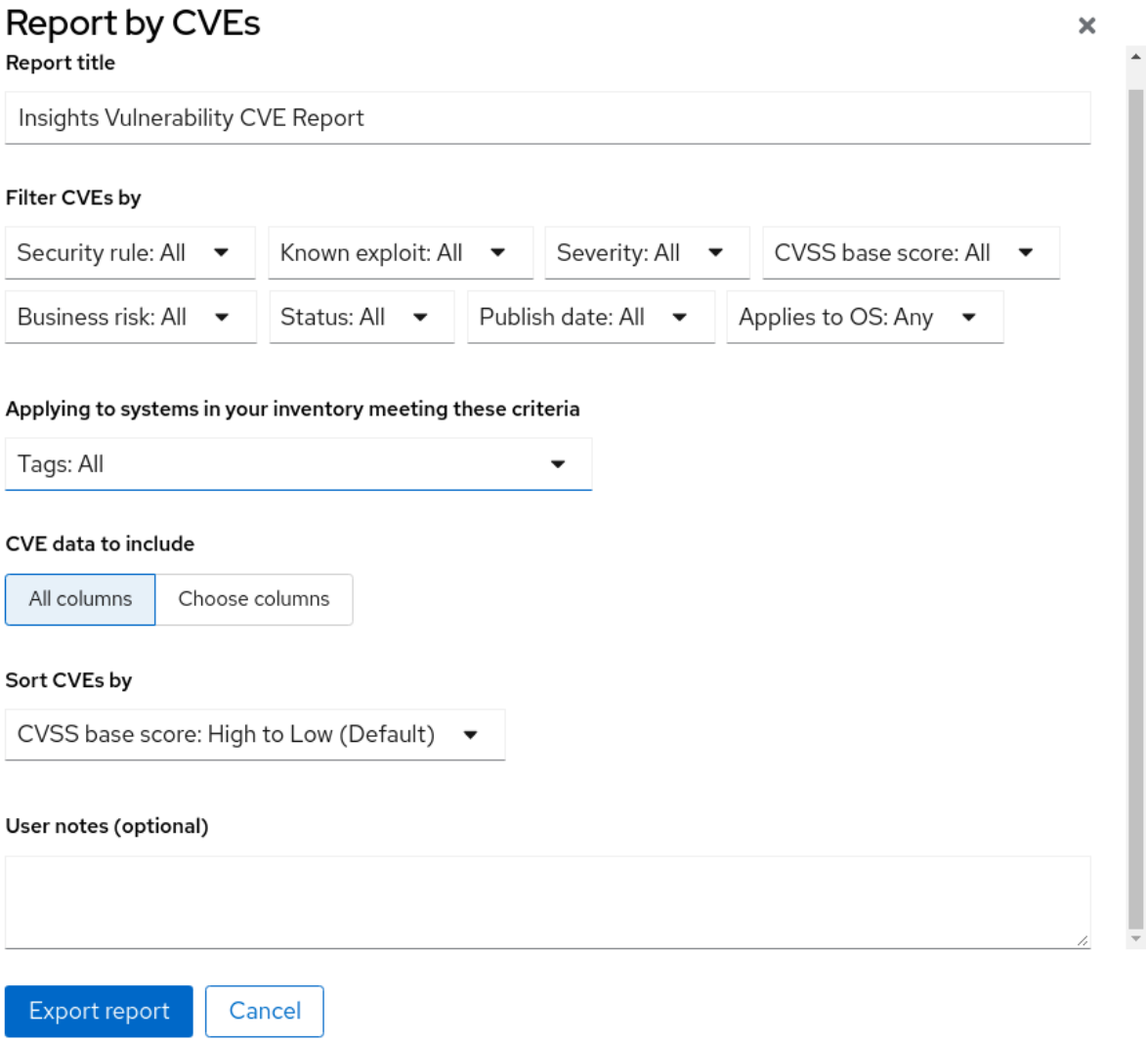
以下の手順に従って、お使いのシステムに影響する可能性がある CVE の特定の時点のスナップショットを作成します。

前提条件

- Red Hat Hybrid Cloud コンソール にログインしている。

手順

1. Insights for Red Hat Enterprise Linux アプリケーションの Security > Vulnerability > Reports ページに移動します。
2. **Report by CVEs** カードで、**Create report** をクリックします。
3. 必要に応じてポップアップカードで選択します。



a. 必要に応じて、レポートタイトルをカスタマイズします。

b. **Filter CVEs by** で、各フィルターのドロップダウンメニューをクリックして値を選択します。

c. **Tags** を選択して、タグ付けしたシステムグループのシステムのみ含めます。

d. 追加する CVE データでは、デフォルトで **Choose columns** がアクティブになっており、追加しない列の選択を解除できます。すべてのボックスにチェックマークを入れたままにするか、**All columns** をクリックしてすべてを表示します。

e. 必要に応じて、注記を追加して、対象オーディエンスのレポートコンテキストを指定します。

4. **Export report** をクリックし、アプリケーションがレポートを生成するのを確認します。

5. OS が要求されたら PDF ファイルを開くか、保存し、**OK** をクリックします。

第4章 JSON、CSV、または PDF ファイルとしての VULNERABILITY データのエクスポート

Vulnerability サービスを使用すると、RHEL インフラストラクチャーのシステムで CVE のデータをエクスポートできます。Vulnerability サービスでフィルターを適用して、特定の CVE またはシステムセットを表示すると、このフィルターの基準をもとにデータをエクスポートできます。

これらのレポートには Red Hat Insights for Red Hat Enterprise Linux アプリケーションからアクセスでき、.csv、.json、または PDF ファイルとしてエクスポートおよびダウンロードできます。

4.1. VULNERABILITY サービスからの CVE データのエクスポート

Vulnerability サービスから一部のデータをエクスポートするには、以下の手順を実行します。

手順

1. Security > Vulnerability > CVEs ページに移動し、必要に応じてログインします。
2. フィルターを適用し、各列の上部にあるソート機能を使用して、特定の CVE を見つけます。
3. CVE の一覧および Filters メニューの右側にある **Export** アイコン  をクリックし、ダウンロード設定に基づいて **Export to JSON**、**Export to CSV**、または **Export as PDF** を選択します。
4. ダウンロード先を選択し、**Save** をクリックします。

第5章 通知およびインテグレーションの有効化

Red Hat Hybrid Cloud Console の通知サービスを有効にして、脆弱性イベントがトリガーされるたびに通知を送信できます。たとえば、通知サービスを設定して、セキュリティー問題がインストール内のシステムに影響を与えるたびに電子メールメッセージを自動的に送信したり、毎日発生するすべての脆弱性イベントの電子メールダイジェストを送信したりできます。通知サービスを使用すると、イベントによりトリガーされる通知を把握するために Red Hat Insights for RHEL のダッシュボードを繰り返し確認する必要がなくなります。

メールメッセージの送信に加え、他の方法でイベントデータを送信するように通知サービスを設定できます。

- 認証済みクライアントを使用して Red Hat Insights API にイベントデータをクエリーする。
- Webhook を使用して受信要求を受け入れるサードパーティーのアプリケーションにイベントを送信する。
- 通知を Splunk などのアプリケーションと統合して、イベント通知をアプリケーションダッシュボードにルーティングする

通知管理者は通知サービス内のイベントの動作グループを設定します。動作グループは、各通知の配信方法と、通知をすべてのユーザーに送信するか、組織管理者のみに送信するかを指定します。

組織管理者は通知管理者ロールを持つユーザーアクセスグループを作成し、そのグループにアカウントメンバーを追加します。

イベントから電子メール通知を受信するユーザーは、イベントごとに個別の電子メールまたは毎日のイベントダイジェストを受信するように、ユーザー設定を設定できます。

関連情報

- 脆弱性イベントの通知とインテグレーションをセットアップする方法の詳細は、**Red Hat Hybrid Cloud Console での通知の設定** および **Red Hat Hybrid Cloud Console とサードパーティーアプリケーションのインテグレーション** を参照してください。

第6章 参考資料

Vulnerability サービスや他の Red Hat Insights for Red Hat Enterprise Linux サービスおよび機能に関する詳細は、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モニタリング**
- Automation Toolkit > Remediations
- Red Hat Insights for Red Hat Enterprise Linux ドキュメント
- Red Hat Insights for Red Hat Enterprise Linux 製品サポートページ

RED HAT ドキュメントへのフィードバック (英語のみ)

Red Hat ドキュメントに関するフィードバックをお寄せください。いただいたご要望に迅速に対応できるよう、できるだけ詳細にご記入ください。

前提条件

- Red Hat カスタマーポータルにログインしている。

手順

フィードバックを送信するには、以下の手順を実施します。

1. Create Issue にアクセスします。
2. **Summary** テキストボックスに、問題または機能拡張に関する説明を入力します。
3. **Description** テキストボックスに、問題または機能拡張のご要望に関する詳細を入力します。
4. **Reporter** テキストボックスに、お客様のお名前を入力します。
5. **Create** ボタンをクリックします。

これによりドキュメントに関するチケットが作成され、適切なドキュメントチームに転送されます。フィードバックの提供にご協力いただきありがとうございました。