Red Hat Insights 2022

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

セキュリティー脅威に晒されている可能性のある環境についての理解

Last Updated: 2022-06-20

Red Hat Insights 2022 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

セキュリティー脅威に晒されている可能性のある環境についての理解

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 システムでのセキュリティー脆弱性の状況を評価して監視するだけでなく、インフラストラクチャーの脆弱性のレベルを理解して、一連のアクションを計画します。

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 INSIGHTS FOR RHEL VULNERABILITY サービスの概要

Vulnerability サービスを使用すると、RHEL インフラストラクチャーの Common Vulnerabilities and Exposures (CVE) に対するリスクを素早く評価して、全体的に監視し、最も重要な問題とシステムをこれまで以上に理解し、修復を効率的に管理できるようになります。

データが Vulnerability サービスにアップロードされると、システムおよび CVE のグループをフィルタリングしてソートし、ビューを絞り込み、最適化することができます。また、個別の CVE がシステムに深刻なリスクを及ぼす場合は、個別の CVE にコンテキストを追加することもできます。リスクの影響度を理解したら、CVE のステータスを適切なステークホルダーに報告してから、Ansible Playbook を作成して問題を修復し、組織のセキュリティーを保護します。

本書では、Vulnerability サービスの主な機能と、その使用方法を説明します。レポートおよび修復の詳細は、以下のドキュメントを参照してください。

- Vulnerability Service と Ansible Playbook を使用したセキュリティーエクスポージャーの修正
- 脆弱性サービスレポートの生成

1.1. INSIGHTS FOR RHEL VULNERABILITY サービスの要件および前提条件

Vulnerability サービスは、RHEL 6、7、および 8 のすべてのサポート対象バージョンで利用できます。Vulnerability サービスを使用する前に、以下の条件を満たしている必要があります。

- **各システムに Insights クライアントがインストールされ、Insights for RHEL アプリケーションに登録されている。** Insights for Red Hat Enterprise Linux スタートガイドの手順 に従ってクライアントをインストールしてシステムを登録します。
- **Vulnerability サービスが、Red Hat Subscription Manager (RHSM) および Satellite 6 以降が管理する RHEL システムで完全にサポートされている。** RHSM と Satellite 6、または subscription.redhat.com (カスタマーポータル) に登録されている RHSM 以外の、パッケージ更新の取得方法を使用すると、想定外の結果に陥る可能性があります。
- **Satellite 5 および Spacewalk がホストする RHEL システムでは、Vulnerability サービスの修正は完全にサポートされておらず、適切に機能しない場合があります。**
- **機能によっては、組織の管理者が提供する特別な権限が必要です。** 具体的には、特定の CVE およびシステムに関連付けられた Red Hat セキュリティーアドバイザリー (RHSA) を表示し、Insights for Red Hat Enterprise Linux Patch サービスで脆弱性を表示およびパッチするには、ユーザーアクセスで付与されるパーミッションが必要です。

1.2. 脆弱性サービスユーザーのユーザーアクセス

Insights for Red Hat Enterprise Linux アプリケーションの特定の機能にアクセスするには、Red Hat Hybrid Cloud Console > User Access > Groups で付与されている正しい権限が必要です。組織管理者または **ユーザーアクセス管理者** は、必要なロールを持つユーザーアクセスグループのメンバーとしてあなたを追加する必要があります。

デフォルトでは、Red Hat Hybrid Cloud Console のユーザーアクセスには、**Vulnerability administrator** (すべてのアクセス) および **Vulnerability viewer** (読み取り専用アクセス) のロールが事前設定されています。組織がデフォルトのロールでは不十分なアクセスを提供していると判断した場合、**User Access administrator** は、一連のユーザーが必要とする特定のアクセス許可を提供するようにカスタムロールを設定できます。

本章の以下のセクションでは、Vulnerability サービスユーザーのデフォルトロールを説明します。

重要

ユーザーアクセスの変更は、Red Hat アカウントの組織管理者、または **User Access administrator** ロールを持つ User Access グループのメンバーであるアカウントユーザーで実行する必要があります。

関連情報

- **ロールベースアクセス制御(RBAC)のユーザーアクセス設定ガイド**

1.2.1. Vulnerability administrator ロール

Vulnerability administrator ロールは、**Default access グループ** のデフォルトロールです。アカウント上の Red Hat Enterprise Linux ユーザー向けのすべての Insights は、デフォルトで **Default アクセスグループ** のメンバーです。デフォルト設定では、**Vulnerability 管理者**ロールを持つグループのメンバーは、すべての Vulnerability サービスリソースにアクセスできます。

組織は、デフォルトロールの制限が多すぎるか、または許容度を超えるかを決定する場合があります。一部の機能へのアクセスを制限したり、**User Access 管理者** はロールをカスタマイズし、必要なアクセス許可を使用してロールを設定できます。事前設定されたロールをカスタマイズすると、**Default アクセスグループ** が置き換えられます。

1.2.2. Vulnerability ビューアーロール

デフォルト設定では、**Vulnerability ビューアー** ロールは Vulnerability サービスリソースを読み取ることができます。これは事前設定されたロールですが、**Default アクセスグループ** には含まれません。**Vulnerability ビューアー** ロールには以下のパーミッションが含まれます。

- Vulnerability サービスの結果、ページ、および一覧を表示してトリアします。
- Red Hat Enterprise Linux の Insights に結果の報告をオプトアウトしているシステムを表示します。
- .JSON および .CSV 出力のフィルターおよびエクスポートデータを設定します。
- Red Hat Enterprise Linux > Vulnerability > Reports で高度なレポートを表示して作成します。

組織が Vulnerability ビューアーのロールのデフォルト設定が不十分であると判断した場合、User Access 管理者は、必要な特定のアクセス許可を使用してカスタムロールを作成できます。

第2章 COMMON VULNERABILITIES AND EXPOSURES (CVE)

Common Vulnerabilities and Exposures (CVE) は、公開されているソフトウェアパッケージで識別されているセキュリティーの脆弱性です。CVE は、Mitre Corporation が運用する連邦政府の調査および開発センターの「National CyberSecurity FFRDC (NCF)」で識別および一覧表示され、National Cyber Security Division of the United States Department of Homeland Security から資金を得ています。CVE の全リストは、https://cve.mitre.org にあります。

Vulnerability サービスは、RHEL システムに影響のある CVE を特定し、潜在的なリスクと解決方法の把握に必要な情報を提供します。

一般的に知られている不正使用の CVE や CVE に関連のあるセキュリティールールを強調表示することで、Vulnerability サービスは脅威インテリジェンスを強化し、RHEL 環境に最も影響を与える可能性のあるリスクをもたらす CVE を判断できるようにします。

重要

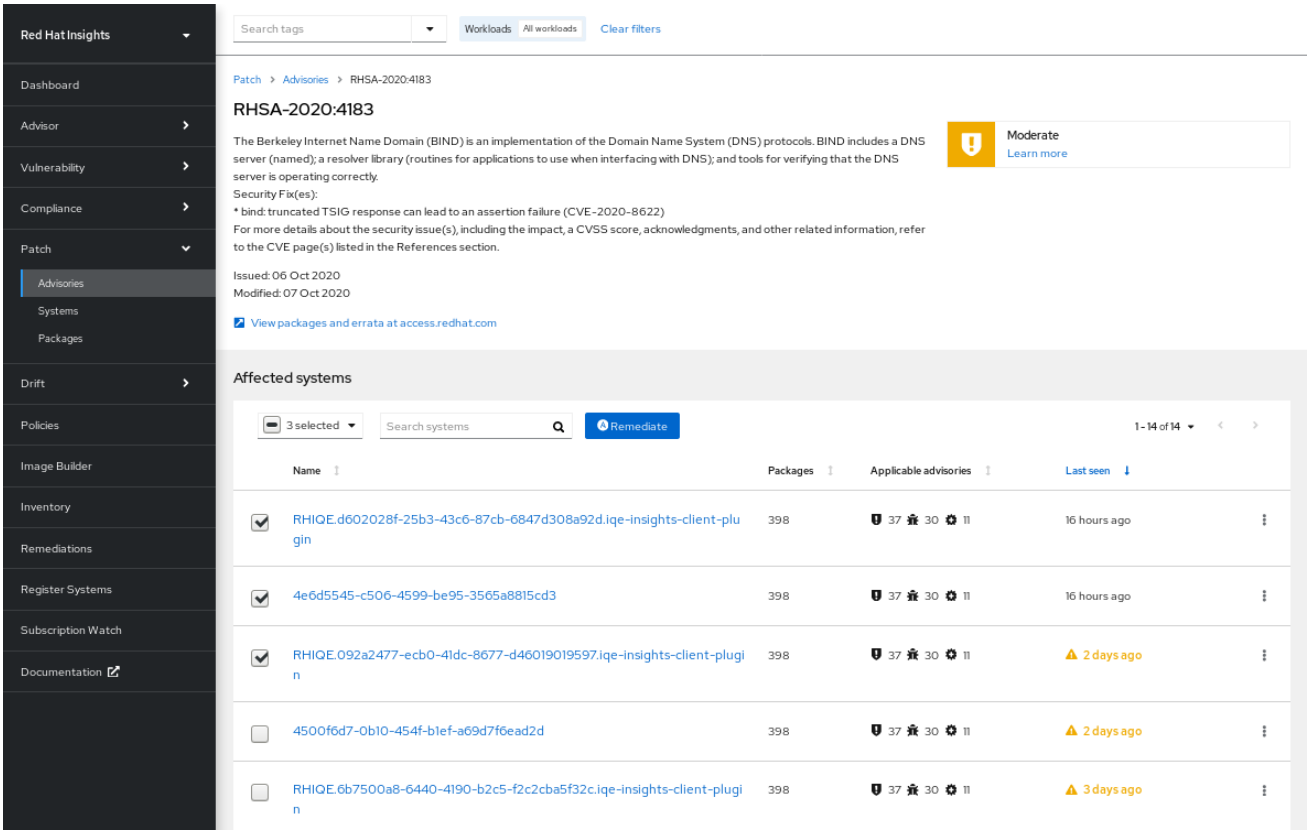
Vulnerability サービスには、https://cve.mitre.org のエントリーリストに含まれる CVE がすべて含まれるわけではありません。Red Hat CVE (Red Hat が 発行する セキュリティーアドバイザリー (RHSA)) のみが Vulnerability サービスに含まれています。

2.1. RED HAT SECURITY ADVISORIES (RHSA)

Red Hat セキュリティーアドバイザリー (RHSA) のエラータでは、修正または軽減策が利用可能な Red Hat 製品のセキュリティー脆弱性が文書にまとめられています。Red Hat Insights の Vulnerability サービスでは、CVE のリスクに晒される各システムに紐付けられているアドバイザリー ID が表示されます。

CVE を選び、セキュリティールールカードの **Filter by affected systems** のリンクを選択してこの情報を表示します。システムにアドバイザリーが存在する場合には、RHSA ID が **Exposed systems** リストの **Advisory** コラムで、システムの横にリンクとして表示されます。アドバイザリーがない場合は、Advisory 列が表示されなかったり、「Not available」と表示されます。

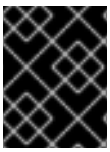
システムにアドバイザリーが存在する場合は、影響を受けるシステムの一覧など、RHSA に関する詳細情報を表示できます。Patch サービスでは、システムを選択し、Ansible Playbook を作成して修復を適用できます。



2.2. セキュリティールール

セキュリティールールは、リスクの割合が高いことや、CVE に関連するセキュリティーリスクが理由で、CVE が目立たせます。これらは、重大なメディア報道を受ける可能性のあるセキュリティー上の欠陥であり、Red Hat Product Security チームによって精査され、Product Security Incident Response Plan ワークフローを使用して RHEL 環境の露出を判断するのに役立ちます。これらのセキュリティールールにより、組織を保護するための適切なアクションを実行できます。

セキュリティールールは、システムで実行している RHEL のバージョンを分析するだけにとどまらず、詳細にわたる脅威インテリジェンスを提供します。また、セキュリティールールは、Insights クライアントが収集するシステムメタデータを分析して、手動でキュレートされ、セキュリティーの脅威にさらされるかどうかを判断します。Vulnerability サービスにより、セキュリティールールのリスクに晒されるシステムが特定された場合には、セキュリティーリスクが高まる可能性があり、早急に問題を対処する必要があります。



重要

リスクに晒されているシステムでセキュリティールールに対応することが最優先事項です。

最後に、CVE に晒されているシステムすべてが、その CVE に関連するセキュリティールールのリスクに晒されているわけではありません。脆弱なバージョンのソフトウェアを実行している場合でも、他の環境条件により、特定のポートが閉じられたり、SELinux を実行している場合など、その他の環境状態により脅威が緩和される可能性があります。

2.2.1. Insights for RHEL ダッシュボードでのセキュリティールールの特定

以下の手順に従って、インフラストラクチャーがセキュリティールールのリスクに晒されていることを確認します。

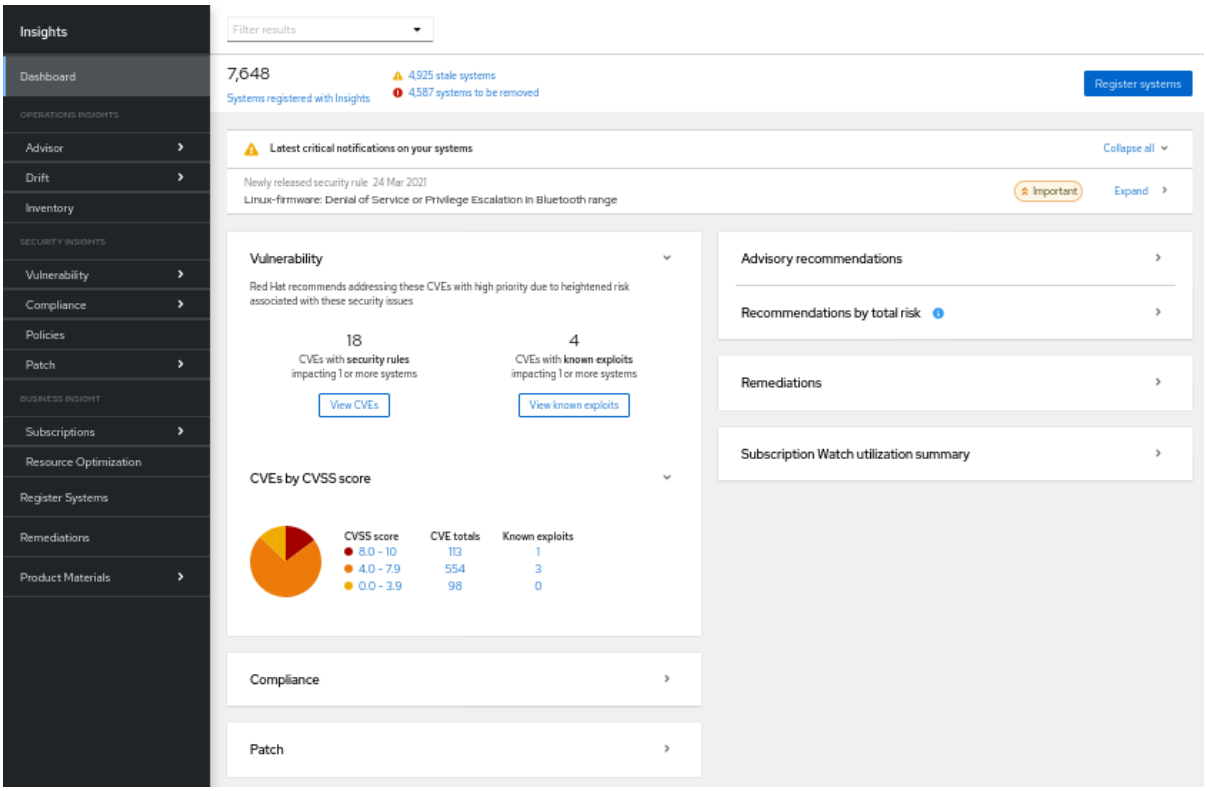
手順

1. Insights for Red Hat Enterprise Linux ダッシュボード に移動します。

注記

以下のスクリーンショットでは、セキュリティー脆弱性評価に関係のないサービスのパネルは最小化して簡潔にまとめています。

:



2. システムパネルで **最新の重要な通知** を確認します。これらは,、セキュリティーリスクが高い「Important」または「Critical」と評価したセキュリティールールです。 これらは最も重大な問題となる可能性があるため、修復を優先する必要があります。

   a. 各通知の右側にある **展開** ボタンをクリックして、関連する CVE およびインフラストラクチャーでセキュリティー上の問題点が含まれるシステムの数を表示します。

注記

重要な通知にセキュリティールールが表示されているにも拘らず、セキュリティーリスクのあるシステムが 0 の場合があります。この場合、CVE がインフラストラクチャーに存在しても、セキュリティールールの条件が存在しない場合もあります。

   b. セキュリティールールの名前と関連する CVE の下にある CVE ID リンクをクリックします。

   c. セキュリティールール CVE の影響を受けるシステムを表示し、任意でセキュリティーリスクに晒されたシステムを選択して Playbook を作成します。

3. 次に、**Vulnerability** カードに情報を表示します。

   a. システムに影響のある **セキュリティールール** が割り当てられた CVE の数を書き留めま

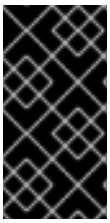
す。 この数字には、重大度に関係なく、システム 1 台以上に影響のあるセキュリティールールが含まれます。

i. **View CVEs** をクリックします。重大度の低いセキュリティールールの修復の優先順位は、重大度の高いセキュリティールールの次にするように検討します。

2.3. 既知の不正使用

Red Hat は Metasploit データを分析して、CVE を悪用するコードが公開されているか、また CVE が一般的に悪用されていないかを判断します。Vulnerability サービスは、対象基準を満たす CVE に「既知の不正使用」ラベルを適用します。

脅威評価がこのように強化されることで、極めてリスクの高い CVE を特定して先に対処できるようになります。Red Hat は、「既知の不正使用」ラベルの CVE を最優先ですべて確認し、これらの問題の修正に向けて取り組むことを推奨します。



重要

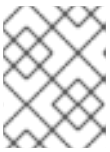
Vulnerability サービスで、悪用されていることが分かっている CVE がお使いのインフラストラクチャーのシステムに存在することが分かります。「既知の不正使用」のラベルは、RHEL システムで脆弱性の悪用が行われていることを示すわけではありません。Vulnerability サービスでは、そのような判断はされません。

2.3.1. Insights for Red Hat Enterprise Linux ダッシュボードでの不正使用が分かっている CVE の特定

以下の手順に従って、Insights for RHEL ダッシュボードの Vulnerability カードで、不正使用されていることが分かっている CVE を特定します。

手順

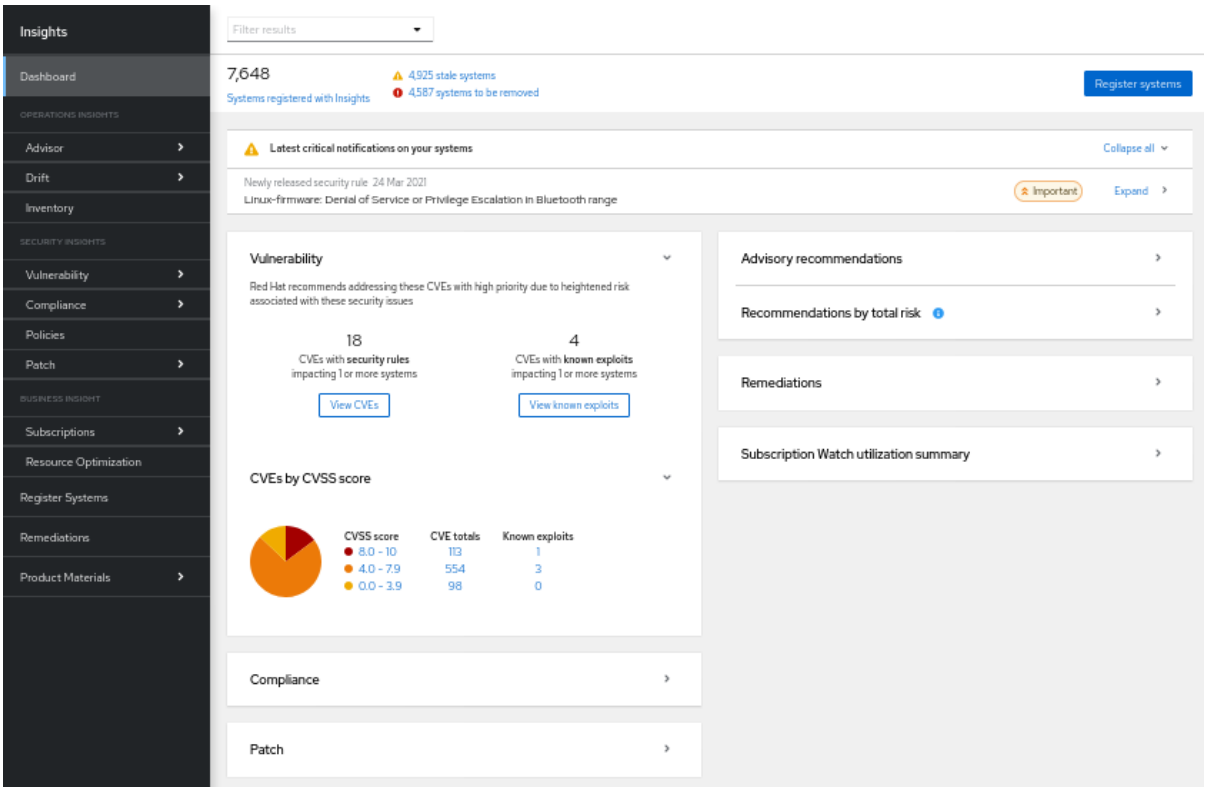
1. Insights for Red Hat Enterprise Linux ダッシュボード に移動します。



注記

以下のスクリーンショットでは、セキュリティー脆弱性評価に関係のないサービスのパネルは最小化して簡潔にまとめています。

:



2. **Vulnerability** カードで、**1台以上のシステムに影響を与える不正使用されている CVE と表示されている数** を書き留めます。

3. **View known exploits** をクリックします。

4. CVE 一覧で、不正使用されていることが分かっている CVE がフィルタリングされたリストを確認します。

第3章 VULNERABILITY サービスの結果調整

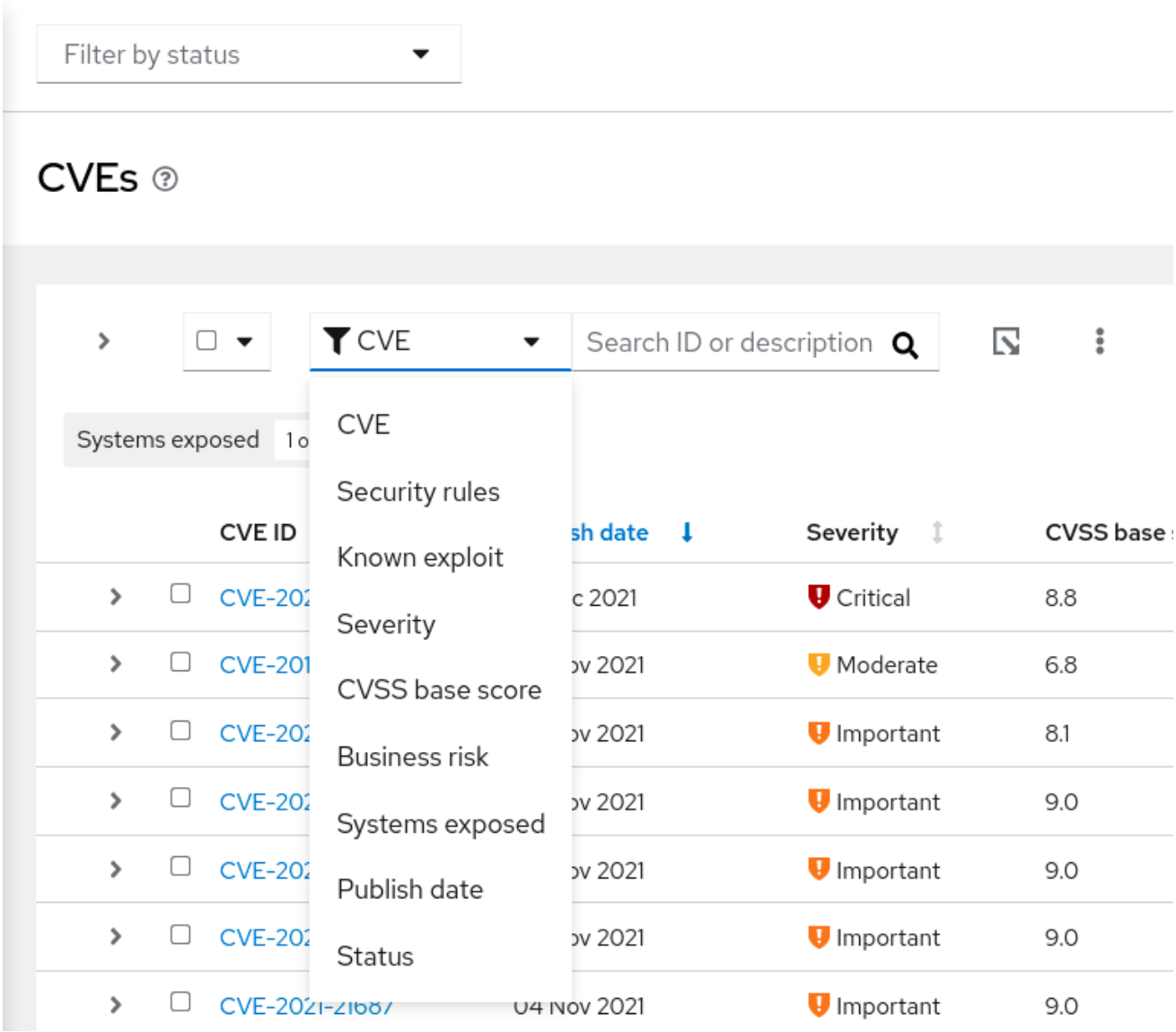
結果をステークホルダーに報告する場合も、システム修復の優先順位を決定する場合でも、Vulnerability サービスでは、データのビューを細かく調整し、最も重要なシステム、ワークロードまたは問題にフォーカスできるようにする方法が多数あります。以下のセクションでは、データの編成、および結果を絞り込むために使用できるソート、フィルタリング、およびコンテキスト機能について説明します。

3.1. CVE-LIST フィルターおよび SYSTEM-LIST フィルター

フィルタリングにより、CVE および関連システムの表示一覧が絞り込まれるため、特定の問題にフォーカスしやすくなります。CVE 一覧にフィルターを適用して、重大度やビジネスリスクに応じて CVE にフォーカスします。以下に例を示します。個々の CVE を選択した後、影響を受けるシステムの結果リストにフィルターを適用して、たとえば、特定の RHEL メジャーバージョンまたはマイナーバージョンのシステムに焦点を合わせます。

フィルターは、左側のフィルターのドロップダウンリストからプライマリーフィルターを選択し、右側のフィルターオプションのドロップダウンリストからセカンダリーサブフィルターを選択してアクティベートされます。選択したフィルターはフィルターメニューに表示され、各フィルターの横にある X をクリックしてフィルタリングを解除できます。

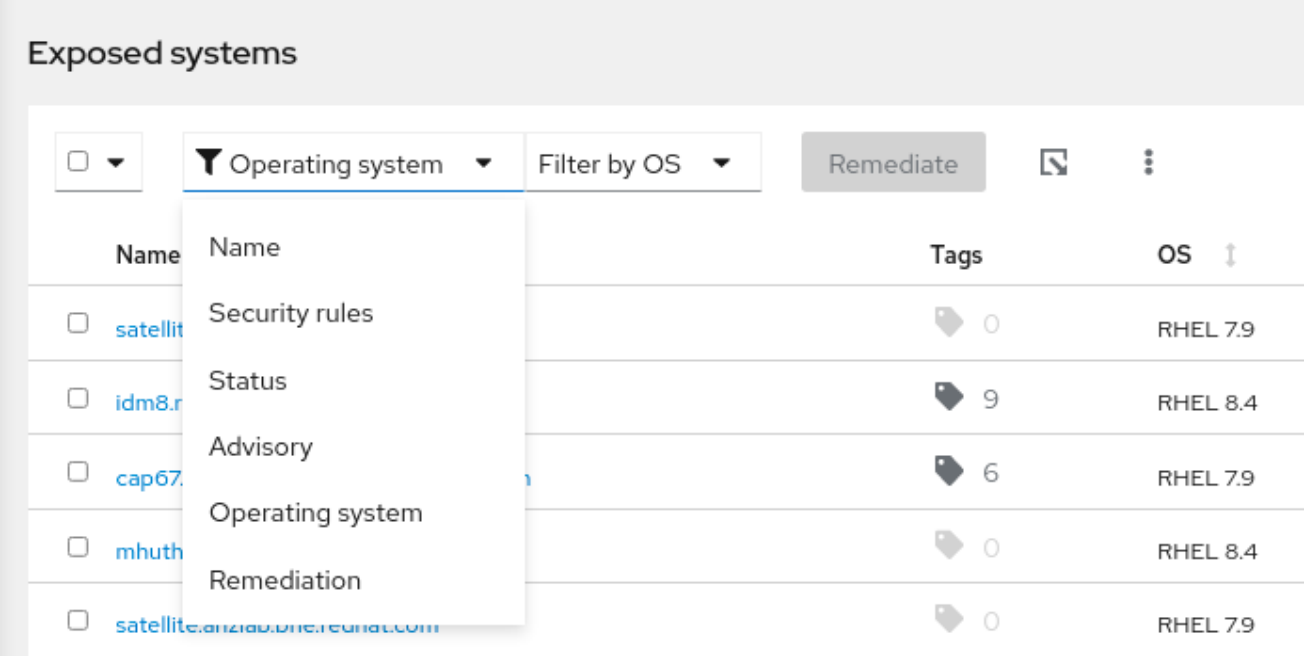
CVE 一覧のフィルター



以下の主要フィルターは、CVEs ページからアクセスできます。プライマリーフィルターを選択し、サブフィルターにパラメーターを定義します。

- **CVE.**ID または説明を検索します。
- **Security rules.**Security rule ラベルの付いた CVE のみを表示します。
- **既知の不正使用**Known exploit 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 base score.**1 つ以上の範囲を選択します。All、0.0-3.9、4.0-7.9、8.0-10.0、N/A (該当なし)
- **Business risk.**1 つ以上の値を選択します (High、Medium、Low、Not defined)。
- **Systems exposed .**現在影響を受けるシステムがある CVE だけを表示するか、影響を受けるシステムがない CVE のみを表示するよう選択します。
- **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)。
- **Status.**1 つ以上の値を選択します。Not reviewed、In review、On-hold、Scheduled for patch、Resolved、No action - risk accepted, Resolved via mitigation

システムリストフィルター



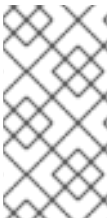
CVE の詳細ページのシステム一覧から、以下のプライマリーフィルターにアクセスできます。

- **Name.**CVE ID を入力して、特定の CVE を検索します。
- **Security rules.**CVE にそれに関連するセキュリティールールがある場合は、同じセキュリティールールに対して脆弱な他のシステムでフィルターするか、セキュリティールールの影響を受けるシステムを表示します。
- **Status.**特定のステータスまたはワークフローカテゴリーのシステムを表示します。

- **アドバイザリー。**この CVE に Red Hat アドバイザリーが適用されるシステムを表示します。
- **Operating system.**特定の RHEL (マイナー) バージョンを実行しているシステムを表示します。
- **修正**Ansible Playbook に含まれるシステム、手動による修復、または現在の修復計画に含まれていないシステムを表示します。

3.1.1. セキュリティールールの CVE のフィルター

セキュリティールール (特に重大度の高いセキュリティールールなど) は、お使いのインフラストラクチャーに非常に大きな脅威となる可能性があり、リスクの特定および修復の優先順位を 1 番として考える必要があります。以下の手順に従い、CVE リストで重大度の高いセキュリティールール CVE だけを表示して影響を受けるシステムを特定します。



注記

CVE に晒されているシステムすべてが、その CVE に関連するセキュリティールールのリスクに晒されているわけではありません。脆弱なバージョンのソフトウェアを実行している場合でも、他の環境条件により、特定のポートが閉じられたり、SELinux が有効な場合など、その他の環境状態により脅威が緩和される可能性があります。

手順

1. Insights for Red Hat Enterprise Linux で Red Hat Enterprise Linux > Vulnerability > CVEs に移動します。
2. ツールバーでフィルタードロップダウンリストをクリックします。
   a. **Security rules** フィルターを適用します。
   b. **Has security rule** のサブフィルターを適用します。
3. 下方向にスクロールしてセキュリティールールの CVE を表示します。セキュリティールールのある CVE では、CVE ID のすぐ下にあるセキュリティールールラベルを表示します。

3.1.2. 既知の不正使用 CVE のフィルタリング

「既知の不正使用」のラベルが付いた CVE で、Red Hat は、CVE を悪用するコードが公開されているか、不正使用が行われたと一般的に知られているかなど、不正使用が行われているかどうかを判断します。このような理由から、不正使用されていることが分かっている CVE は、優先的に特定と修復を図る必要があります。

重要

Red Hat では、登録されているシステムが悪用されているかどうかの判断は行いません。重大なリスクを伴う可能性がある CVE を特定するだけです。

以下の手順に従って、CVE 一覧から不正使用されていることが分かっている CVE をフィルタリングします。

手順

1. Insights for Red Hat Enterprise Linux で Red Hat Enterprise Linux > Vulnerability > CVEs に移動します。
2. ツールバーでフィルタードロップダウンリストをクリックします。
   a. **Known exploit** フィルターを適用します。
   b. **Has a known exploit** サブフィルターを適用します。
3. スクロールダウンして、既知の不正使用 CVE の一覧を表示します。

3.1.3. セキュリティールールのリスクに晒されているシステム一覧のフィルタリング

CVE 一覧をフィルタリングし、最も重大な脅威だけを表示した後に、個別の CVE を選択して、セキュリティーリスクに晒されたシステム一覧を表示して、その一覧にフィルターを適用します。

手順

1. Security-rule CVE を選択したら、**Exposed systems** 一覧まで下方向にスクロールします。一覧に含まれるシステムすべてに、CVE がセキュリティールールに追加される、セキュリティールールの条件が含まれるわけではありません。以下のフィルターを適用して、セキュリティールール条件のあるシステムのみを表示します。
2. プライマリーフィルターのドロップダウンリストから **Security rules** フィルターを選択します。
3. セカンダリードロップダウンリストの **Has security rule** ボックスにチェックを入れます。
4. セキュリティールールにも条件が存在する CVE に晒されているシステムを表示します。

3.2. INSIGHTS FOR RHEL グループフィルター

システムやワークロードのグループ別に Vulnerability サービスの結果をフィルタリングする機能を使用すると、特定のグループに所属するとのタグが付いたシステムだけを表示できます。これらは、Satellite ホストグループ、または Insights クライアント設定ファイルに追加されたカスタムタにより SAP ワークロード (または SAP ID) を実行しているシステムが考えられます。

グループのフィルタリングは、ページの上部にある **Filter results** ボックスを使用して、Insights for RHEL アプリケーション全体にわたってグローバルに設定できます。サービスやページが変わっても、グループの選択項目は維持されます。ただし、機能は Insights for RHEL のサービスによって異なります。

グループのフィルタリングは、Vulnerability ダッシュボードと Vulnerability サービスの CVE およびシステムリストで機能します。

本書の ***タグおよびシステムグループ*** のセクションでは、グループタグや、カスタムタグの設定について説明します。

3.2.1. グループ別のダッシュボード、CVE、およびシステム一覧のフィルタリング

以下の手順に従って、グループ別に Vulnerability サービスの CVE およびシステムの一覧を絞り込みます。

手順

1. Red Hat Hybrid Cloud Console に移動し、ログインします。
2. Insights for Red Hat Enterprise Linux アプリケーションを開きます。
3. Insights アプリケーションのページの上部にある **Filter results** ボックスの下矢印をクリックします。
4. システムのフィルタリングに使用するグループを選択します。
   検索またはスクロールして、利用可能なタグを表示します。利用可能なタグの全一覧を確認するには、リストの下部までスクロールし、**View more** をクリックします。

   任意:

   a. SAP ワークロードを選択します。

   b. 特定の SAP ID でシステムを選択します。

   c. Satellite ホストコレクションを選択します。

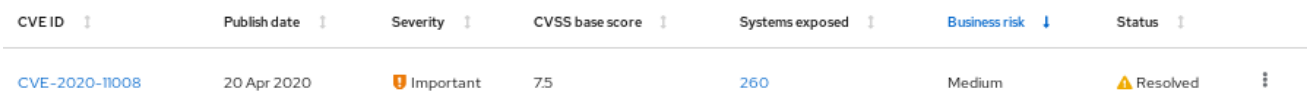
   d. カスタムグループタグで識別されるシステムを選択します。
   カスタムタグの作成方法は、本書の「**カスタムのシステムタグ付け**」を参照してください。
5. サービスに移動し、選択したグループに所属するシステムまたは CVE のみを表示します。

3.3. CVE のビジネスリスクの定義

Vulnerability サービスでは、CVE のビジネスリスクを、High、Medium、Low、または Not Defined (デフォルト) などのオプションで定義できます。

CVE の一覧では各 CVE の重大度を示していますが、ビジネスリスクを割り当てることで、組織に与える可能性のある影響に基づいて CVE をランク付けできます。これにより、大規模な環境でリスクを効率的に管理し、運用上の意思決定を改善できます。

デフォルトでは、特定の CVE のビジネスリスクフィールドは **Not Defined** に設定されます。ビジネスリスクを設定したら、CVE 行の横にある Red Hat Enterprise Linux > Vulnerability > CVEs 一覧に表示されます。



また、各 CVE の詳細カードにビジネスリスクが表示されます。これには、より多くの情報が表示され、影響を受けるシステムが一覧表示されます。

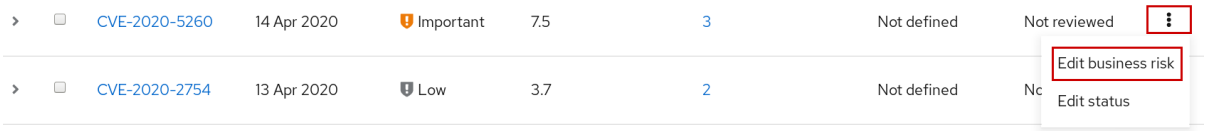
3.3.1. 単一の CVE のビジネスリスクの設定

単一の CVE にビジネスリスクを設定するには、以下の手順を実施します。

注記

CVE のビジネスリスクは、影響を受ける**すべて**のシステムで同じになります。

1. 必要に応じて Red Hat Enterprise Linux > Vulnerability > CVEs ページに移動し、ログインします。
2. ビジネスリスクを設定する CVE を特定します。
3. CVE 行の右側にある **more-actions** アイコン (垂直ドット) をクリックし、**Edit business risk** をクリックします。



4. ビジネスリスクの値を適切なレベルに設定し、必要に応じてリスク評価の証明を追加します。
5. **Save** をクリックします。

3.3.2. 複数の CVE のビジネスリスクの設定

以下の手順に従い、選択する複数の CVE に同じビジネスリスクを設定します。

1. 必要に応じて Red Hat Enterprise Linux > Vulnerability > CVEs に移動し、ログインします。
2. ビジネスリスクを設定する CVE のボックスにチェックを入れます。
3. ビジネスリスクを設定するには、以下の手順を実行します。
   a. ツールバーで Filter ドロップダウンメニューの右側にある **more-actions** (3 つの垂直ドット) をクリックし、**Edit business risk** をクリックします。
   b. 適切なビジネスリスク値を設定し、必要に応じてリスク評価の理由を追加します。
   c. **Save** をクリックします。

3.4. VULNERABILITY サービス分析からのシステムの除外

Vulnerability サービスを使用すると、特定のシステムを脆弱性分析から除外することができます。除外することで、組織の目標と関連せのないシステムで問題を確認、再確認する時間と労力を軽減できます。

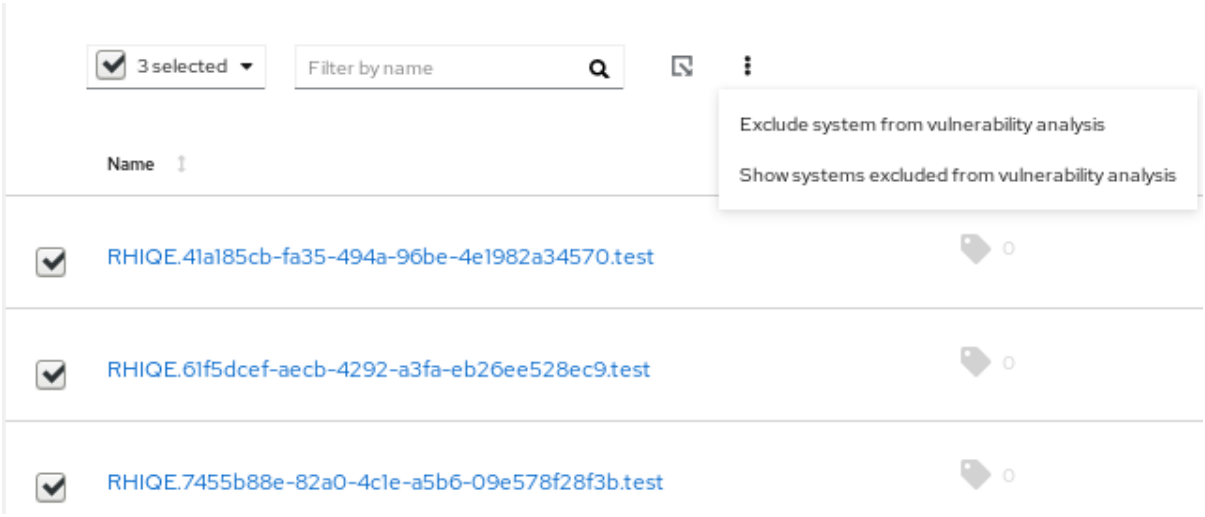
たとえば、QA、Dev、および Production というサーバーのカテゴリーがあり、QA サーバーの脆弱性を確認する必要がない場合には、Vulnerability サービスの分析対象からこれらのシステムを除外できます。

脆弱性分析からシステムを除外すると、Insights クライアントはシステム上のスケジュールに従ってそのまま実行されますが、システムの結果は Vulnerability サービスには表示されません。クライアントがそのまま稼働されるので、他の Insights for Red Hat Enterprise Linux サービスで必要なデータをアップロードできます。また、フィルターを使用してこれらのシステムの結果を確認することもできます。

選択した RHEL システムをVulnerability サービスの分析から除外するには、以下の手順を実行します。

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. 脆弱性分析から除外する各システムのボックスにチェックを入れます。
3. システムのリストの上部のツールバーにある more-actions アイコンをクリックし、**脆弱性分析からシステムの除外**を選択します。



4. 任意で、**システムの行**の more-actions アイコンをクリックし、**脆弱性分析からシステムの除外**を選択して、**単一**のシステムを除外できます。

3.5. 以前に除外したシステムの表示

以前に除外したシステムを表示するには、以下の手順を実行します。

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. システムのリストの上部にあるツールバーにある more-actions アイコンをクリックし、**Show systems excluded from analysis** を選択します。
3. 脆弱性分析から除外されたシステムを参照してください。これは、**Applicable CVEs** コラムの **Excluded** の値で検証できます。

3.6. システムの脆弱性分析の再開

システムの脆弱性分析を再開するには、以下の手順を実行します。

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. システムのリストの上部にあるツールバーにある **more-actions** アイコンをクリックし、**Show systems excluded from analysis** を選択します。
3. 結果の一覧で、脆弱性分析を再開する各システムのボックスにチェックを入れます。
4. **その他のアクション**アイコンを再度クリックし、**Resume analysis for system**を選択します。

3.7. CVE ステータス

システムに影響を与える CVE を管理する方法として他に、CVE のステータスを設定することが挙げられます。Vulnerability サービスを使用すると、以下の方法で CVE のステータスを設定できます。

- **全** システムに CVE のステータスを設定します。
- **特定の CVE + システムペア**のステータスを設定します。

ステータス値は事前設定されており、以下のオプションが含まれます。

- 未確認 (デフォルト)
- In-review
- On-hold
- Scheduled for patch
- Resolved
- No action - risk accepted
- Resolved via mitigation

CVE のステータスを設定すると、ライフサイクルによる順序づけが、順序の認識から変更までにわたり容易になります。ステータスを定義すると、組織は、ライフサイクル内のどの部分で重大度の最も高い CVE が存在するのか、またビジネスのニーズに合わせて最も重要な問題への対処に焦点を合わせる必要がある状況について、より効果的に監視できます。CVE のステータスは、Vulnerability サービスおよび個別の CVE ビューの全 CVE テーブルに表示されます。

3.7.1. 影響を受ける全システムの CVE のステータス設定

以下の手順を使用して CVE のステータスを設定し、影響を受けるすべてのシステムでそのステータスが CVE に適用されるようにします。

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 行の右側にある **more-actions** アイコンをクリックし、**Edit status** を選択します。
3. 適切なステータスを選択し、必要に応じて、**Justification** テキストボックスに決定の絞り込みを入力します。
4. 個別のシステムにこの CVE に設定されたステータスがあり、これを保持する場合は、**個別のシステムステータスを上書きしない**にチェックを入れます。そうでない場合は、チェックボックスのチェックを外して、このステータスを影響を受けるすべてのシステムに適用します。

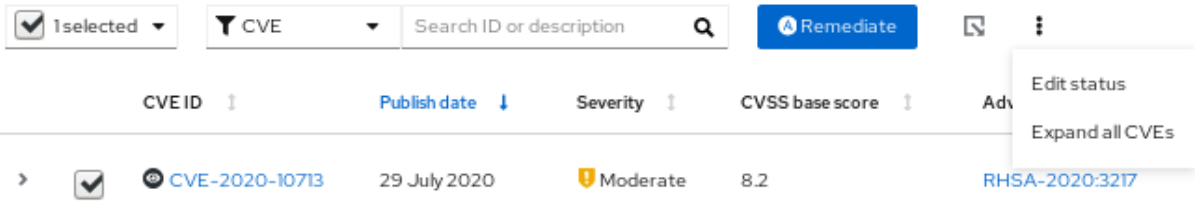
5. **Save** をクリックします。

3.7.2. CVE およびシステムペアのステータスの設定

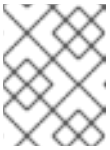
CVE とシステムのペアのステータスを設定するには、以下の手順を実行します。

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. システムを特定し、システム名をクリックして開きます。
3. リストから CVE を選択し、CVE ID の横にあるチェックボックスにチェックを付けます。
4. ツールバー内の **more-option** アイコンをクリックし、**編集ステータス**を選択します。



5. ポップアップカードで、以下のアクションを実行します。
   a. CVE およびシステムペアのステータスを設定します。



注記

Use overall CVE status ボックスにチェックマークを入れると、ペアのステータスを設定することはできません。

   b. 必要に応じて、ステータス決定の根拠を入力します。
   c. **Save** をクリックします。
6. 一覧で CVE を見つけ、ステータスが設定されていることを確認します。

3.8. 検索ボックスの使用

Vulnerability サービスの検索機能は、表示中のページのコンテキストで機能します。

- **CVE page**検索ボックスは、CVE リストの上部にあるツールバーにあります。CVE フィルターが設定されている場合は、CVE ID と説明を検索します。

- **システムページ。**検索ボックスは、リストの上部にあるツールバーにあります。システム名または UUID を検索します。

3.9. CVE リストデータのソート

Vulnerability サービスのソート機能は、表示ページのコンテキストにより異なります。

手順

1. **CVEs タブ**では、以下の列にソートを適用できます。
    - CVE ID
    - Publish date
    - 重大度
    - CVSS base score
    - Systems exposed
    - Business risk
    - Status
2. **システムタブ** では、以下のコラムをソートできます。
    - 名前
    - 該当する CVE
    - Last seen
3. Systems タブでシステムを選択すると、システム固有の CVE の一覧では、以下のソートオプションを使用できます。
    - CVE ID
    - Publish date
    - Impact
    - CVSS base score
    - Business risk
    - Status

第4章 システムタグとグループ

Insights for Red Hat Enterprise Linux を使用すると、管理者はグループタグを使用して、インベントリー内のシステムや個々のサービスでシステムをフィルターできます。グループは、Insights for RHEL へのシステムデータの偽装方法によって識別されます。Insights for RHEL では、実行中の SAP ワークロード、Satellite ホストグループ、および root アクセスを持つシステム管理者が定義したカスタムタグにより、システムのグループをフィルタリングして、システム上の Insights-client を設定できます。

注記

2020 年秋の時点では、インベントリー、advisor、vulnerability、patch、drift、および policies サービスは、グループおよびタグでフィルタリングできます。その他のサービスは後から続きます。

グローバルの **Filter results** ドロップダウンを使用して、SAP ワークロード、Satellite ホストグループ、または Insights-client 設定ファイルに追加されたカスタムタグ別に、フィルタリングします。

前提条件

Insights for Red Hat Enterprise Linux のタグ付け機能を使用するには、以下の前提条件および条件を満たしている必要があります。

- Insights クライアントが各システムにインストールされている。
- カスタムタグを作成するには、**/etc/insights-client/tags.yaml** ファイルに追加したりこのファイルに変更を加える root 権限相当のパーミッションが必要です。

4.1. SAP ワークロード

2025 年に Linux は SAP ERP ワークロードの必須オペレーティングシステムになるため、Red Hat Enterprise Linux および Insights for Red Hat Enterprise Linux を連携して、Insights for RHEL が SAP 管理者に選ばれる管理ツールとなるように取り組んでいます。

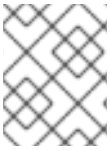
この継続的な取り組みの一環として、Insights for RHEL は SAP ワークロードおよび SAP ID (SID) を実行しているシステムを自動的にタグ付けしますが、管理者がカスタマイズする必要がありません。ユーザーは、グローバル **検索タグ** ドロップダウンメニューを使用して、Insights for RHEL アプリケーション全体でワークロードを簡単にフィルターできます。

4.2. SATELLITE ホストグループ

Satellite ホストグループは Satellite で設定され、Insights for Red Hat Enterprise Linux で自動的に認識されます。

4.3. システムタグ付けのカスタム

システムにカスタムグルーピングとタグ付けを適用して、個別のシステムにコンテキストマーカーを追加したり、Insights for Red Hat Enterprise Linux アプリケーションでこれらのタグ別にフィルタリングしたり、より簡単に関連システムに焦点を当てたりすることができます。この機能は、大規模な Insights for RHEL をデプロイする場合に特に有用です。これには、管理下で数百または数千ものシステムが含まれます。



注記

カスタムタグを作成するには、**/etc/insights-client/tags.yaml** ファイルに追加したりこのファイルに変更を加える root 権限相当のパーミッションが必要です。

4.3.1. タグ構造

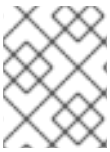
タグは、**namespace/key=value** のペアの構造を使用します。

- **Namespace.**名前空間は、インジェストポイントである **insights-client** の名前であり、変更することはできません。この **tags.yaml** ファイルは名前空間から抽象化され、アップロード前にクライアントによってインジェクトされます。
- **Key.**キーは、ユーザーが選択したキーまたはシステムの定義済みのキーにすることができます。大文字、文字、数字、記号、および空白文字の組み合わせを使用できます。
- **Value.**独自の記述文字列値を定義します。大文字、文字、数字、記号、および空白文字の組み合わせを使用できます。

4.3.2. tags.yaml ファイル

ユーザー定義のタグは **/etc/insights-client/tags.yaml** ファイルに追加されます。必要に応じて、任意の数の key=value ペアを **tags.yaml** に追加できます。YAML 構文を使用すると、コンテンツがわかりやすくなり、変更しやすくなります。

insights-client --group=eastern-sap を実行すると、タグ付け設定ファイル **/etc/insights-client/tags.yaml** が作成され、**group: eastern-sap** が追加されます。以下の **tags.yaml** ファイルの例は、グループ「eastern-sap」に追加されたタグを示しています。



注記

key=value のペアの作成時には、大文字、通常文字、数字、記号、および空白文字の組み合わせを使用できます。

例

```
# tags
---
group: eastern-sap
name: Jane Example
contact: jexample@corporate.com
Zone: eastern time zone
Location:
- gray_rack
- basement
Application: SAP
```

4.3.3. カスタムグループおよび tags.yaml ファイルの作成

insights-client --group=<name-you-choose> を使用してタグ作成し、**/etc/insights-client/tags.yaml** に追加します。これは、以下を実行します。

- **etc/insights-client/tags.yaml** ファイルを作成します。

- **group=** キーおよび **<name-you-choose>** の値を **tags.yaml** に追加します。
- システムから Insights for Red Hat Enterprise Linux アプリケーションに新規アーカイブをアップロードすることで、最新の結果とともに新しいタグがすぐに表示されます。

初期 **グループ** タグを作成したら、必要に応じて **/etc/insights-client/tags.yaml** ファイルを編集し、タグを追加します。

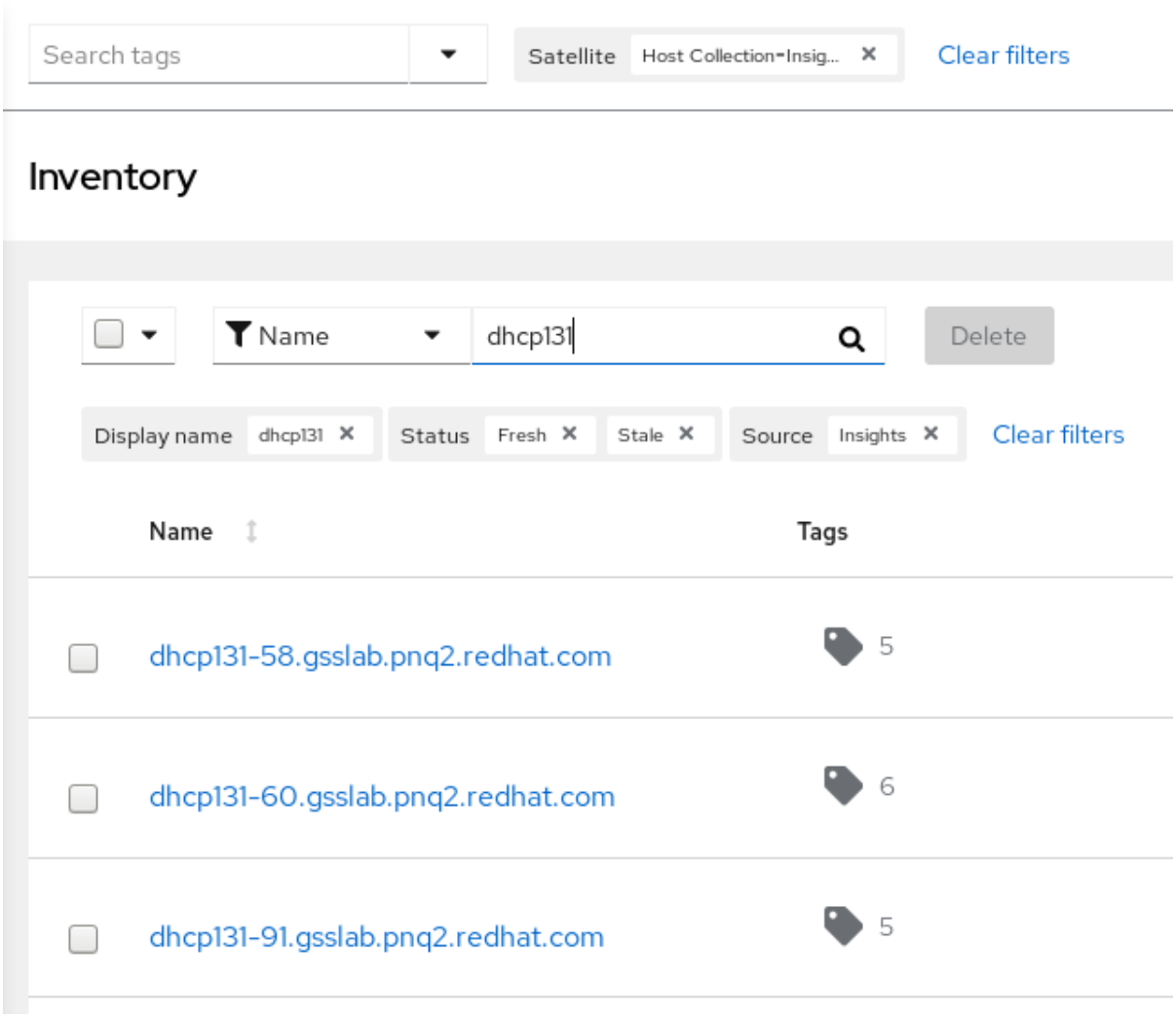
以下の手順では、初期グループおよび **/etc/insights-client/tags.yaml** ファイルを作成し、Insights for RHEL インベントリーにタグが存在することを検証する方法を説明します。

手順

1. **--group=** の後にカスタムグループ名を追加して、root で以下のコマンドを実行します。

```
[root@server ~]# insights-client --group=<name-you-choose>
```

2. 必要に応じて Red Hat Enterprise Linux > Inventory に移動し、ログインします。
3. ページ上部の **Filter results** ドロップダウンメニューをクリックします。
4. 一覧をスクロールするか、検索機能を使用して特定のタグを見つけます。
5. タグをクリックしてフィルター処理を行います。
6. お使いのシステムが脆弱性システム一覧の結果に含まれていることを確認します。
7. **Name** フィルターをアクティブにし、システムが表示されるまでシステム名を入力してから選択します。
8. システム名の横にタグシンボルがグレイになり、適用されるタグの正確な数を表す数字が表示されることを確認します。



4.3.4. タグの追加または変更を行うための tags.yaml の編集

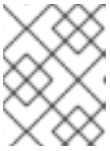
グループタグを作成したら、必要に応じて **/etc/insights-client/tags.yaml** の内容を編集して、タグの追加または変更を行います。システムに、複数のフィルター処理可能なタグを追加できます。

手順

1. コマンドラインで、編集するタグ設定ファイルを開きます。
   [root@server ~]# vi /etc/insights-client/tags.yaml

2. 必要に応じてコンテンツを編集するか、または追加値を追加します。以下の例は、システムに複数のタグを追加する際の **tags.yaml** の管理方法を示しています。

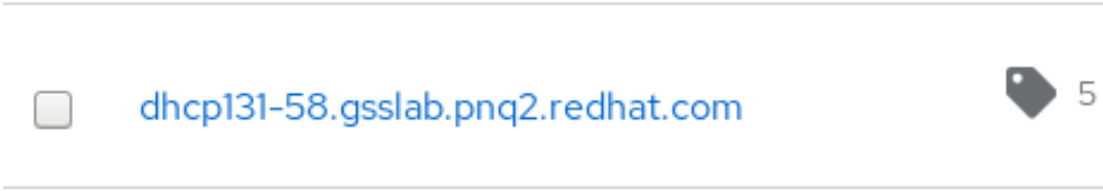
```
# tags
---
group: eastern-sap
location: Boston
description:
- RHEL8
- SAP
key 4: value
```



注記

必要な数の key=value ペアを追加します。大文字、文字、数字、記号、および空白文字の組み合わせを使用します。

3. 変更を保存してエディターを閉じます。
4. Insights for Red Hat Enterprise Linux へのアップロードを生成します。
[root@server ~]# insights-client
5. 必要に応じて Red Hat Enterprise Linux > Inventory に移動し、ログインします。
6. ページ上部の **Filter results** ドロップダウンメニューでタグを選択するか、タグの名前を入力して選択します。
7. 結果でシステムを検索します。
8. タグアイコンが禁止され、システムに適用されるタグの数を示す数字が表示されることを確認します。



9. タグをクリックすると、そのシステムに適用される各タグが表示されます。

第5章 参考資料

Vulnerability サービスの詳細は、以下の資料を参照してください。

- **Vulnerability Service と Ansible Playbook を使用したセキュリティーエクスポージャーの修正**
- **脆弱性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