OpenShift Cluster Manager 2023

Red Hat Insights を使用した OpenShift クラスターでのセキュリティー脆弱性の評価

Insights Vulnerability ダッシュボードを使用して CVE 脆弱性へのクラスターの露出を評価する

Last Updated: 2023-12-05

OpenShift Cluster Manager 2023 Red Hat Insights を使用した OpenShift クラスターでのセキュリティー脆弱性の評価

Insights Vulnerability ダッシュボードを使用して CVE 脆弱性へのクラスターの露出を評価する

法律上の通知

概要

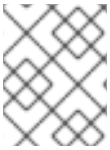
目次

第1章 RED HAT INSIGHTS FOR OPENSHIFT 脆弱性ダッシュボードサービスの概要

Red Hat Insights for OpenShift Vulnerability ダッシュボードサービスは、OpenShift クラスターインフラストラクチャーの CVE (Common Vulnerabilities and Exposures) への露出に関する情報を提供します。

CVE とは、公開されているソフトウェアパッケージで特定されたセキュリティーの脆弱性または不具合です。Vulnerability ダッシュボードサービスを使用すると、クラスターが CVE にさらされているかどうかを評価し、包括的な監視を実行できるため、組織にもたらされる最も高いリスクをよりよく理解し、優先順位を付けることができます。脆弱性ダッシュボードは、次の CVE データを提供します。

- OpenShift クラスターインフラストラクチャー
- Red Hat マーケットプレイスでホストされる一部の Red Hat 製品



注記

脆弱性ダッシュボードサービスは、クラスター上で実行しているワークロードに関する CVE データを提供しません。

次の方法で、クラスターに影響を与える可能性のある CVE の操作、トリアージ、および評価ができます。

- CVE リストビュー (CVE の詳細ビューを表示します。表示、並べ替え、フィルター処理を行って、影響を受けるクラスターの CVE に関する詳細を取得できます)
- クラスターリストビュー (脆弱なクラスターの詳細ビューを表示します。影響を受けるクラスターの詳細を表示、並べ替え、フィルター処理できます)

重要

Red Hat は、接続されている OpenShift クラスターが悪用されているかどうかを判断しません。Vulnerability ダッシュボードサービスは、OpenShift Container Platform 環境内のクラスターおよびイメージにリスクを及ぼす可能性のある CVE を特定します。

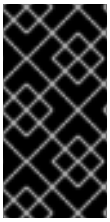
関連情報

- OpenShift 向けの Red Hat Insights を使い始める
- mitre.org の CVE に関する情報

1.1. VULNERABILITY ダッシュボードの CVE (COMMON VULNERABILITIES AND EXPOSURES) について

Vulnerability ダッシュボードを使用して、OpenShift クラスターに影響する CVE (Common Vulnerabilities and Exposures) を特定し、クラスターに存在する可能性のあるリスクを理解するのに役立ちます。

OpenShift クラスターに影響を与える CVE の可視性を使用して、最も重大な問題に優先順位を付けることができます。



重要

Vulnerability ダッシュボードには、https://cve.mitre.org のエントリーリストに含まれるすべての CVE が含まれているわけではありません。Red Hat が発行したセキュリティーアドバイザリー (RHSA) が含まれる CVE のみが Vulnerability ダッシュボードに含まれています。

関連情報

- CVE とは
- mitre.org での CVE に関する情報
- Red Hat エラータの説明

1.2. データ収集とセキュリティー

Red Hat Insights は、ユーザー名、パスワード、または証明書などの識別情報を収集しません。Red Hat Insights のデータ収集とコントロールの詳細は、Red Hat Insights のデータおよびアプリケーションセキュリティー を参照してください。

関連情報

- リモートヘルスモニタリングについて
- リモートヘルスモニタリングによって収集されるデータの表示
- リモートヘルスレポートのオプトアウト

第2章 OPENSHIFT インフラストラクチャーが CVE にさらされる可能性の判断

Red Hat Hybrid Cloud Console で OpenShift インフラストラクチャーが CVE にさらされるかどうかを判断するには、主に次の 2 つの点から始めます。

- Red Hat Hybrid Cloud Console > OpenShift > Vulnerability > CVEs（CVE リストビューとも呼ばれます)。このビューは、CVE に関する情報を取得するための開始点となります。
- Red Hat Hybrid Cloud Console > OpenShift > Vulnerability > Clusters（クラスターリストビューとも呼ばれます)。これは、クラスターに関する情報を取得するための開始点です。

CVE およびクラスターリストビューから次の 2 つの追加ビューに移動できます。

- CVE 詳細ビュー
- クラスター詳細ビュー

より詳細な情報を提供します。

注記

これらのビューの名前は記述されておらず、Insights の脆弱性情報をナビゲーションする場合に役立つフレームワークを提供するために使用されます。

これらのビューでできること

4 つのビューでは、

- CVE リストビュー
- CVE 詳細ビュー
- クラスターリストビュー
- クラスター詳細ビュー

情報を表示、フィルタリング、および並べ替えることができます。結果の表示方法を変更すると、クラスターへの公開と優先順位付けに役立ちます。結果をより適切に分析するために使用できる情報の概要を次に示します。

- **CVE リストビュー**: CVE ID、公開日、重大度、CVSS スコア、公開されたクラスター
- **CVE 詳細ビュー**: 名前、ステータス、バージョン、プロバイダー
- **クラスターリストビュー**: 名前、ステータス、バージョン、CVE の重大度、プロバイダー
- **クラスター詳細ビュー**: CVE ID、公開日、重大度、CVSS スコア

このドキュメントの後半のセクションでは、これらのビューでの情報の表示、フィルタリング、および並べ替えについて詳しく説明します。

第3章 CVE リストビューを使用したクラスターに影響する脆弱性の特定

CVE リストビューでは、クラスターに影響を与える CVE をトリアージして、組織を保護するための適切な措置を講じることができます。また、CVE ID をクリックして 1 つの CVE に注目し、その CVE によって公開されているクラスターを正確に理解するのに役立つ詳細を表示することもできます。

CVE 一覧ビューのデフォルトビューで、以下が表示されます。

- **CVE ID**: CVE、CVE ID 番号の詳細を表示します。
- **Publish date (公開日)**: CVE が公開された日付を表示します。
- **Severity (重大度)**: CVE の重大度評価 (Critical、Important、Moderate、Low、または Unknown) を表示します。
- **CVSS base score**: Common Vulnerability Scoring System (CVSS) のベーススコア 0-10 を表示します。
- **Exposed clusters**: 現在影響を受けるクラスターの数を表示します。

こちらのビューから、この基準を使用してフィルター処理および並べ替えを行うと、クラスターに影響を与える最も重大な CVE に焦点を当てることができます。

注記

CVE リストページのデフォルトのビューには、デフォルトのフィルター選択 (**Exposed clusters** および **1 or More clusters**) が表示され、組織内の 1 つ以上のクラスターに影響を与える CVE が表示されます。Vulnerability ダッシュボードによって報告されたクラスターに影響を与えないものを含め、すべての CVE を表示するには、フィルターの横にある **X** をクリックしてフィルターを削除します。

3.1. CVE リストビューの取得

Vulnerability ダッシュボードを使用して、組織に影響を与える CVE を表示し、目的のセキュリティー体制を実現するのに役立つ情報を確認できます。

前提条件

- Red Hat アカウントとクラスターが同じ組織に登録されている。
- アカウントに、接続された OpenShift クラスターが含まれている。
- Red Hat Hybrid Cloud Console にログインしている。

手順

1. **Red Hat Hybrid Cloud Console** に移動します。
2. **OpenShift** をクリックします。
3. **Vulnerability** をクリックします。
4. **CVE** をクリックします。

No CVEs found というメッセージが表示された場合、Red Hat Insights は OpenShift インフラストラクチャーに影響する CVE を検出していません。

3.2. CVE リストビューの結果を調整することによる組織の保護

Vulnerability ダッシュボードを最大限に活用するには、以下の方法で CVE リストビューの結果を絞り込みます。

- 特定の CVE の検索
- 特定の CVE に関する情報の検索
- CVE リストビューでの結果のフィルタリング
- 重大度別の CVE のフィルター
- CVE リストビューでの結果のソート

3.2.1. 特定の CVE の検索

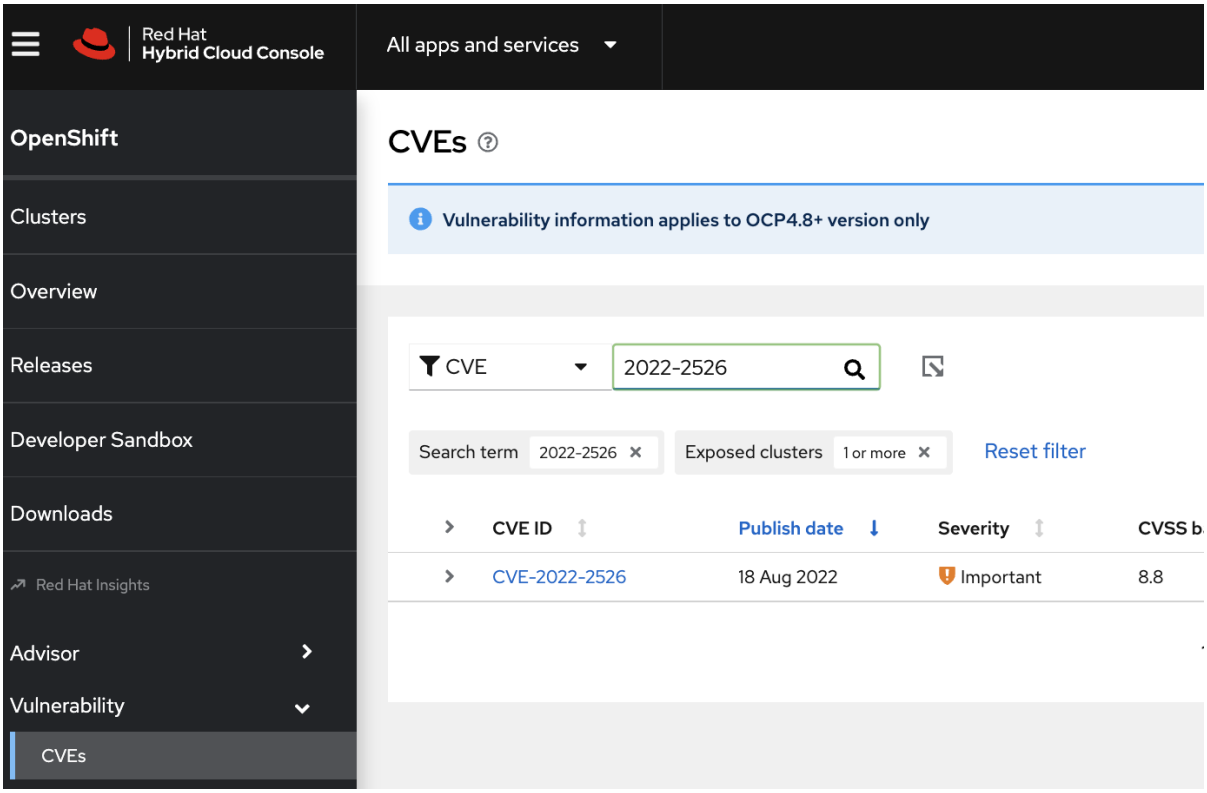
CVE ID がわかっている場合は、CVE リストビューのフィルターを使用して、その CVE に関する詳細を検索できます。

前提条件

- Red Hat アカウントとクラスターが同じ組織内で登録されている。
- アカウントに、接続された Red Hat-administered OpenShift クラスターが含まれている。
- Red Hat Hybrid Cloud Console にログインしている。

手順

1. Red Hat Hybrid Cloud Console > OpenShift > Vulnerability > CVEs に移動します。
2. フィルタードロップダウンリストで **CVE** を選択します。
3. CVE ID (この例では **CVE-2022-2526**) を検索ボックスに入力するか貼り付けます。
4. 検索結果が表示されるまで待ちます (または、Return キーまたは Enter キーを押します)。検索結果には、**CVE ID**、**Publish date**、**Severity**、**CVSS base score**、および **Exposed clusters** が表示されます。



5. CVE および影響を受けるクラスターの一覧の詳細は、ハイパーリンク CVE ID をクリックします。

3.2.2. 特定の CVE に関する情報の検索

特定の CVE を見つけたら、CVE 詳細ビューを開くことができます。ここでは確認できる追加情報は、以下のようになります。

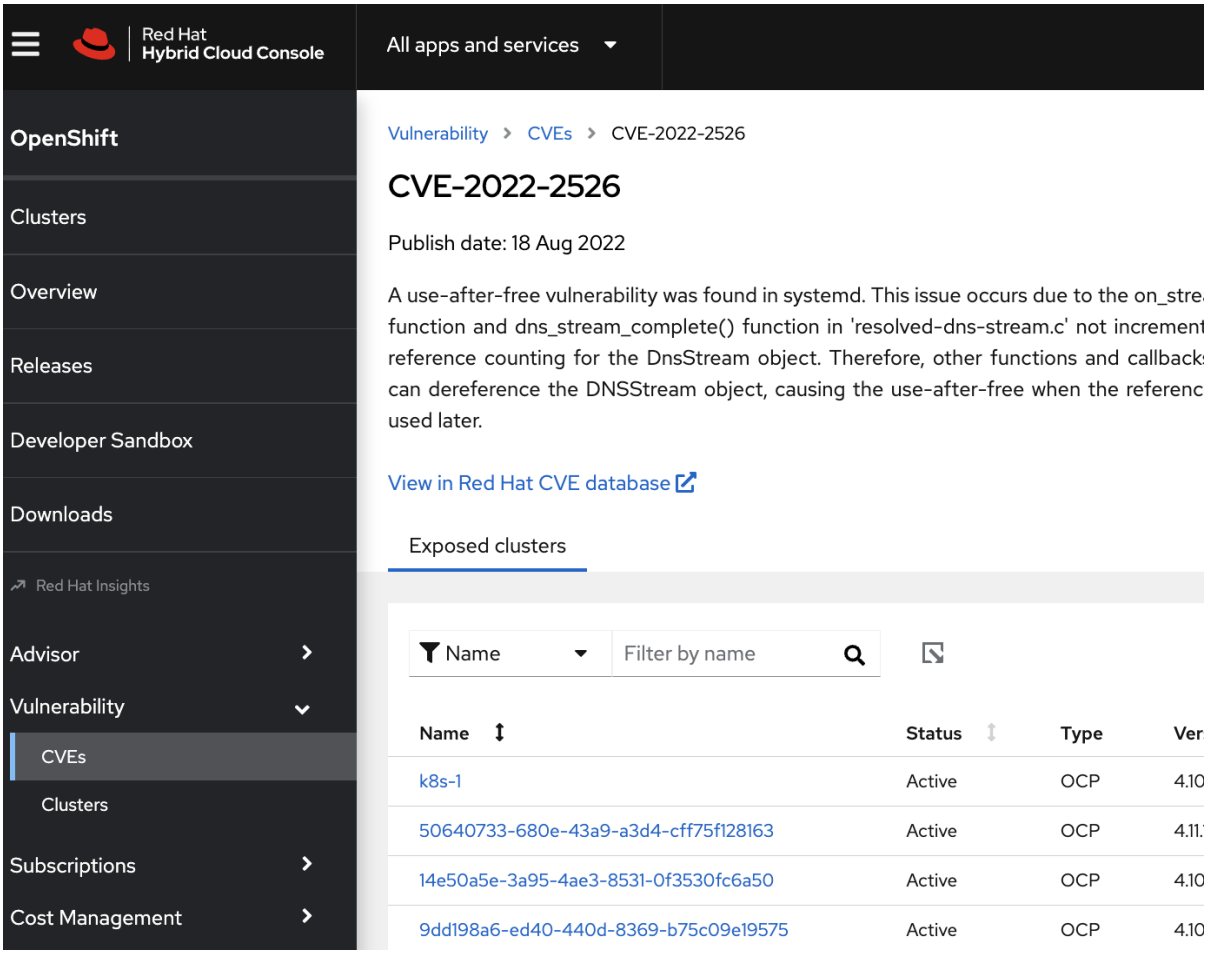
- CVE ID
- 公開日
- CVE に関する簡単な説明
- 重大度
- CVSS ベーススコア
- 次の並べ替え可能な列を持つ公開されたクラスターのリスト:
  - Name (クラスターの名前)
  - ステータス
  - Type
  - バージョン
  - Provider
  - Last seen

前提条件

- Red Hat アカウントとクラスターが同じ組織内で登録されている。
- アカウントに、接続された Red Hat-administered OpenShift クラスターが含まれている。
- Red Hat Hybrid Cloud Console にログインしている。

手順

1. **Red Hat Hybrid Cloud Console > OpenShift > Vulnerability > CVEs** に移動します。
2. 結果のリストを確認し、関連する CVE ID (例：2022-2526) を見つけます。
3. CVE ID 列の **CVE ID** をクリックします。CVE に関する追加情報が表示されます。



注記

クラスターが CVE の影響を受けない場合は、No matching clusters found というメッセージが表示されます。

3.2.3. CVE リストビューでの結果のフィルタリング

CVE リストビューでは、CVE のリストにフィルターを適用して、CVE の重大度レベルや OpenShift の特定のバージョンのクラスターなどの特定の情報に焦点を当てることができます。個々の CVE を選択した後、プライマリーフィルターとセカンダリーフィルターを結果のクラスターリストに適用できます。適用することのできるフィルターおよびオプションは以下のとおりです。

- **CVE ID**: ID または説明でフィルタリングします。

- **Publish date**: All、Last 7 days、Last 30 days、Last 90 days、Last year、または More than 1 year ago から選択します。
- **Severity**: 1 つ以上の値 (Critical、Important、Moderate、Low、または Unknown) を選択します。
- **CVSS base score**: 0 ~ 10 の範囲で入力します。
- **Exposed clusters**: 現在影響を受けるクラスターの CVE のみを表示するか、影響を受けるクラスターがない CVE だけを表示するように選択します。

前提条件

- Red Hat アカウントとクラスターが同じ組織内で登録されている。
- アカウントに、接続された OpenShift クラスターが含まれている。
- Red Hat Hybrid Cloud Console にログインしている。

手順

1. Red Hat Hybrid Cloud Console > OpenShift > Vulnerability > CVEs に移動します。CVE リストビューのデフォルトのビューには、**Exposed clusters**、および **1 or More clusters** のデフォルトのフィルター選択が表示されます。
2. 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 (**公開日** など) を選択します。
3. フィルターのドロップダウンリストからセカンダリーフィルターを選択します。この例では、**Filter by publish date** ドロップダウン矢印から **Last 30 days** を選択します。

注記

選択したフィルターはフィルター選択メニューの下に表示されます。

4. フィルターの選択を確認してから、生成される情報を確認します。この例は、過去 30 日間の CVE を示しています (存在する場合)。
5. フィルターを無効にします。必要に応じて、選択した各フィルター (またはデフォルトのフィルター) の横にある **X** をクリックします。

最後のアクションで一致する CVE が見つかりません (No matching CVEs found) というメッセージが表示された場合、これはクラスターが CVE の影響を受けていないことを意味します。

注記

フィルターは、選択を解除するか、Vulnerability ダッシュボードセッションを離れるまでアクティブなままになります。意図しない結果を回避するために、不要なフィルターをリセットまたは選択解除します。

3.2.4. 重大度別の CVE のフィルター

Vulnerability ダッシュボードでは、CVE リストをフィルタリングして、最も重要な CVE を表示できます。

前提条件

- Red Hat アカウントとクラスターが同じ組織内で登録されている。
- アカウントに、接続された OpenShift クラスターが含まれている。
- Red Hat Hybrid Cloud Console にログインしている。

手順

1. Red Hat Hybrid Cloud Console > OpenShift > Vulnerability > CVEs に移動します。
2. ドロップダウンリストをクリックします。
3. **Severity** を選択します。
4. **Filter by Severity** フィールドのドロップダウン矢印をクリックします。
5. フィルター (たとえば、**Critical**) を選択して、Critical と指定されたすべての CVE を表示します。
6. CVE ID をクリックして、追加情報を取得します。

3.2.5. CVE リストビューでの結果のソート

このビューで CVE のリストを並べ替えて、最も関連性の高い情報を優先することもできます。たとえば、クラスターに影響する重要な CVE をすべて表示するには、重大度または CVSS ベーススコアで並べ替えます。CVE ページの結果は、以下の列で並べ替えることができます。

- CVE ID
- Publish date
- Severity
- CVSS base score
- Exposed clusters

前提条件

- Red Hat アカウントとクラスターが同じ組織内で登録されている。
- アカウントに、接続された OpenShift クラスターが含まれている。
- Red Hat Hybrid Cloud Console にログインしている。

手順

1. Red Hat Hybrid Cloud Console > OpenShift > Vulnerability > CVEs に移動します。
2. ソートする列の横にあるソート矢印をクリックします。

3.3. 関連情報

- 重大度評価

- 公式の CVSS ドキュメント

第4章 CLUSTERS 一覧ビューを使用して、CVE に対して脆弱であるクラスターを判別するのに役立てる

クラスターのリストビューでは、組織内の脆弱なクラスター (CVE にさらされたクラスターとも呼ばれます) のリストを確認できます。このビューには、脆弱なクラスターに関する情報を検索したり、クラスターに影響を与えるすべての CVE を表示したり、結果としてクラスターに影響を与えた CVE のいずれかにさらされているすべてのクラスターを表示するために選択できるオプションが含まれています。

以下の情報がクラスターの一覧ビューの上部に表示されます。

- **名前**: CVE の影響を受ける脆弱なクラスターの名前を表示します。
- **ステータス**: 接続の状態を表示します (Connected、Stale、Not applicable、またはクラスターの N/A)。
- **バージョン**: クラスターの OpenShift Container Platform バージョン (4.8 以降) を表示します。
- **CVE の重大度**: クラスターに影響する CVE の重大度レベル (Critical、Important、Moderate、Low) を表示します。
- **プロバイダー**: クラスターのクラウドプロバイダーの名前を表示します。
- **最終確認日時**: 情報が最後にクラスターから Vulnerability ダッシュボードサービスに最後にアップロードされた時間 (形式は分、時間、または日) を表示します。

4.1. クラスター一覧ビューの取得

クラスター一覧ビューで、脆弱なクラスターに関する情報をソートおよびフィルタリングできます。このビューのデータは、組織にとって重要な情報に集中するのに役立ちます。Clusters 一覧ビューでデータを表示するには、以下を実行します。

前提条件

- Red Hat アカウントとクラスターが同じ組織に登録されている。
- アカウントに、接続された OpenShift クラスターが含まれている。
- Red Hat Hybrid Cloud Console にログインしている。

手順

1. **Red Hat Hybrid Cloud Console**に移動します。
2. **OpenShift** をクリックします。
3. **Vulnerability** をクリックします。
4. **Clusters** をクリックします。

4.2. CLUSTERS リストビューの結果の調整による組織の保護

Vulnerability ダッシュボードを最大限に活用するには、Clustersリストビューの結果を次のように調整できます。

- クラスター一覧ビューでの結果のフィルタリング

- CVE の重大度によるクラスターのフィルタリング
- クラスターデータのソート

4.2.1. クラスター一覧ビューでの結果のフィルタリング

Vulnerability ダッシュボードのクラスターのリストにフィルターを適用して、特定の情報 (CVE の重大度評価など) または OpenShift Container Platform の特定のバージョンのクラスターに焦点を当てることができます。CVE を選択した後、影響を受けるクラスターの結果リストにフィルターを適用できます。

クラスター一覧ビューでフィルタリングに選択できるオプションは次のとおりです。

- **名前**: CVE の影響を受ける脆弱なクラスターの名前でフィルター処理します。
- **ステータス**: クラスターの接続ステータス (Connected、Disconnected、Stale、Not applicable または N/A) でフィルター処理します。
- **バージョン**: クラスターのバージョン (OpenShift Container Platform 4.8 以降) でフィルター処理します。
- **CVE の重大度**: セキュリティー関連の問題およびクラスターで影響を受けるイメージの数の重大度 (All clusters、Critical、Important、Moderate、Low) でフィルター処理します。
- **プロバイダー**: クラスターのクラウドプロバイダーの名前でフィルター処理します。

前提条件

- Red Hat アカウントとクラスターが同じ組織内で登録されている。
- アカウントに、接続された OpenShift クラスターが含まれている。
- Red Hat Hybrid Cloud Console にログインしている。

手順

1. **Red Hat Hybrid Cloud Console > OpenShift > Vulnerability > Clusters** に移動します。
2. 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 (**CVEs severity** など) を選択します。
3. セカンダリーフィルター (例: **Filter by CVEs severity**) を選択します。
4. 重大度評価を選択します (例: **Critical**)。選択したフィルターはフィルター選択メニューの下に表示されます。
5. 結果の情報を確認します。重大度レベルが Critical の CVE に対して脆弱であるクラスターは、一覧で最初に表示されます。

注記

デフォルトのビューは **All clusters** で、CVE からの影響を受けないクラスターであっても、すべてのクラスターを表示します。Vulnerability ダッシュボードによって報告された少なくとも 1 つの CVE の影響を受けるクラスターのみを表示する場合は、このフィルターを削除します。

フィルターは、選択を解除するか、Vulnerability ダッシュボードセッションを離れるまでアクティブなままになります。意図しない結果を回避するために、不要なフィルターをリセットまたは選択解除します。フィルターを無効にするには、選択した各フィルター (またはデフォルトのフィルター) の横にある **X** をクリックします。

4.2.2. CVE の重大度評価によるクラスターのフィルタリング

フィルターを Vulnerability ダッシュボードのクラスターの一覧に適用し、CVE の重大度レベルなどの情報に集中できるようにします。Red Hat は、重大度評価を Critical、Important、Moderate、および Low の 4 段階評価を使用して CVE に適用します。評価を使用すると、組織を保護するためのアクションを実行できます。手順モジュールには、ユーザーが行う手順と、ユーザーの動機を記載した手順を含める必要があります。

前提条件

- Red Hat アカウントとクラスターが同じ組織内で登録されている。
- アカウントに、接続された OpenShift クラスターが含まれている。
- Red Hat Hybrid Cloud Console にログインしている。

手順

1. **Red Hat Hybrid Cloud Console > OpenShift > Vulnerability > Clusters** に移動します。
2. ドロップダウンリストをクリックします。
3. プライマリーフィルター (**CVEs severity**) を選択します。
4. セカンダリーフィルター (**Filter by CVEs severity**) をクリックします。
5. **All clusters** の選択を解除します。
6. 重大度レベルを選択します (この例では **Critical** を選択します)。選択したオプションの重大度レベルで評価された CVE が含まれるクラスターのリストが表示されます。
7. **(オプション) Name** 列に表示されているクラスターのいずれかをクリックして、クラスターに関する詳細情報を取得します。

4.2.3. 重大度別のクラスターのフィルターに関する詳細情報

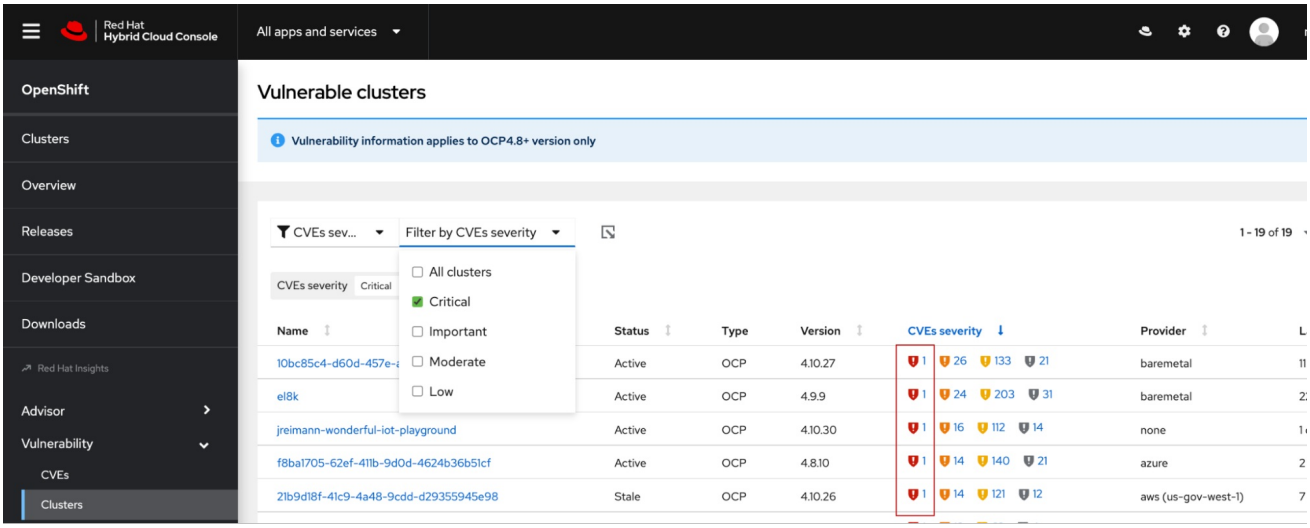
Vulnerability ダッシュボードでは、CVE Severity フィルターを使用して、Critical、Important、Moderate、または Low の CVE の影響を受けるクラスターを表示できます。デフォルトのフィルターである **All clusters** は、脆弱なクラスターと CVE の重大度評価の両方を表示し、CVE に対して脆弱でないクラスターも表示します。

4.2.3.1. CVE の重大度指標

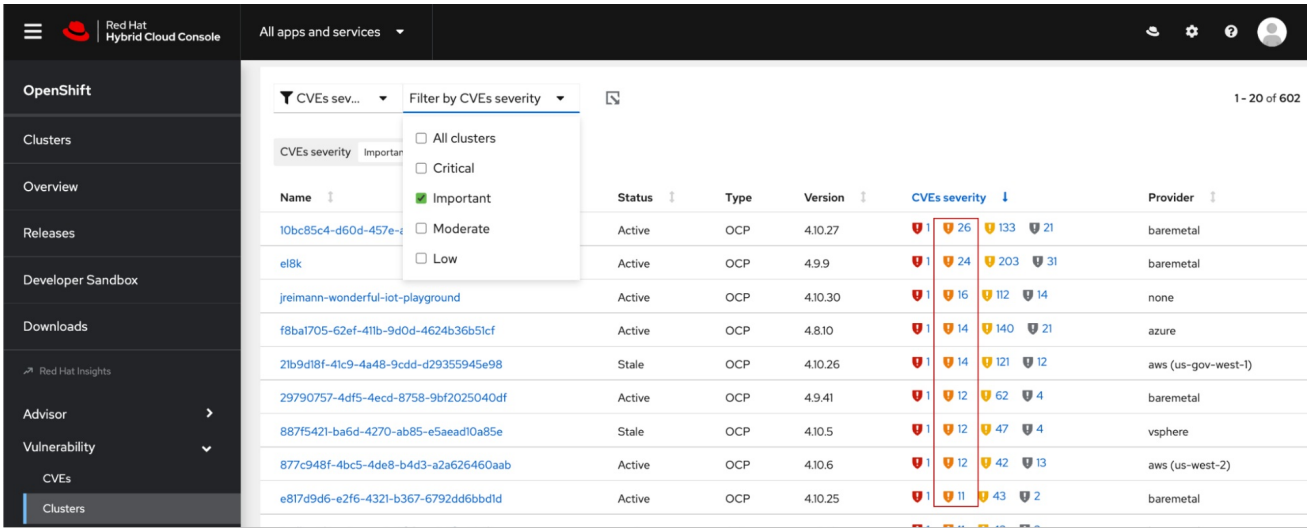
4 つのアイコンは、重大から低までの CVE の重大度の評価を表します。アイコンの横の数字は、そのクラスターに影響を与える重大度タイプの CVE のそれぞれの数を表します。この表現により、問題の重大度を迅速に評価できます。最も重大な問題は、中央に感嘆符が付いた色分けされた赤いアイコンで左側に表示されます。アイコンは、左から右に向かって、重大度の評価レベルが次第に低くなることを表しています。

4.2.3.2. コンテキストによる CVE 重大度のフィルタリング

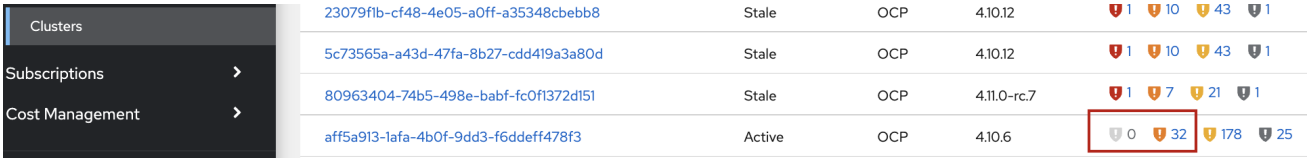
クラスター一覧ビューの CVE の重大度評価は、コンテキストでフィルタ処理ーされます。フィルターされた各結果は、常に最も重要な評価またはより高いレベルの評価のコンテキストで表示されます。CVEs 重大度オプションが Critical のものをフィルタリングすると、次の図に示すような結果が表示されます。この例では、重大な CVE からの影響を受けるクラスターが複数示されています。



フィルターを **Important** に変更すると、最上位クラスターに重大度が Important のCVE が 26 個あることを確認できます。また、クラスターに影響する別の CVE とその重大度レベルも表示されます。Critical な CVE が Important のフィルターでも表示されている点に注意してください。クラスターリストは CVE 重大度が Criticala でフィルタリングされていませんが、次の図に示すように、このフィルターでは、重大度が Critical の重要性が考慮されており、Important の CVE と Critical の CVE の数が表示されます。



この同じフィルターセッションでは、次の図に示すように、重大度が Critical の CVE が 0 個のクラスターと、重大度が Important の CVE が 32 個のクラスターが結果に表示されます。



このコンテキストでフィルタリングすると、最も重要な情報が最初に表示されます。

4.2.4. クラスターデータのソート

クラスター一覧ビューでは、以下のコラムを並べ替えることができます。

- **名前**: CVE の影響を受ける脆弱なクラスターの名前を表示します。
- **ステータス**: 接続の状態を表示します (Connected、Stale、Not applicable、またはクラスターの N/A)。
- **バージョン**: クラスターの OpenShift Container Platform バージョン (4.8 以降) を表示します。
- **CVEs severity**: セキュリティー関連の問題の重大度レベル (Critical、Low、Moderate、Important) と、クラスター内で影響を受けるイメージの数を示します。
- **プロバイダー**: クラスターのクラウドプロバイダー (AWS、Azure など) の名前を表示します。これは、より多くのクラウドプロバイダーが利用可能になるにつれて変化します。

関連情報

- Severity Ratings–Understanding Red Hat security ratings .

第5章 参考資料

Red Hat Insights for OpenShift の詳細は、以下の資料を参照してください。

- Red Hat Insights の概要ページ
- OpenShift の Red Hat Insights Advisor