# 脆弱性ダッシュボードの表示

この章では、Cisco Secure Workload の脆弱性ダッシュボードの機能について詳しく説明します。これは、修復取り組みに優先順位を付けるために、ワークロード全体の Common Vulnerabilities and Exposures（CVE）を識別して表示します。

脆弱性ダッシュボードには、Common Vulnerability Scoring System（CVSS）や Cisco Security Risk Score などのスコアリングシステムを使用して、シビラティ（重大度）別に既知の CVE が一覧表示されます。これらのスコアは、すぐに対応が必要な脆弱性に優先順位を付けるのに役立ちます。ユーザーは、エクスプロイトの複雑さやアクセス要件などのさまざまな属性に基づいて CVE をフィルタリングできます。ダッシュボードは、NIST や Microsoft などの信頼できるソースから 24 時間ごとに CVE データを更新します。ユーザーはインベントリフィルタを作成し、マイクロセグメンテーションポリシーを設定し、仮想パッチ適用ルールを生成して、特定された脆弱性に関連するリスクを軽減できます。

脆弱性ダッシュボードは、ワークロード内の脆弱性を特定するための重要なリソースとして機能し、プロアクティブなセキュリティ管理を可能にします。ダッシュボードの機能を活用することで、組織はリスク評価に基づいて修復戦略に効果的に優先順位を付けることができます。

**注目** 最近の GUI の更新により、ユーザーガイドで使用されているイメージやスクリーンショットの一部に、製品の現在の設計が完全に反映されていない可能性があります。最も正確に視覚的に参照するには、このガイドを最新バージョンのソフトウェアと組み合わせて使用することを推奨します。

表 *1:* 機能情報

| 機能名 | リリース | 機能説明 | どこにあるか |
|---|---|---|---|
| Cisco Vulnerability Management for Deep CVE Insights と Cisco Risk Score for Prioritization の統合 | 3.9 パッチ 2 | CVE の Cisco Security Risk Score を使用して、インベントリフィルタ、影響を受けるワークロードからの通信をブロックするマイクロセグメンテーション ポリシー、および CVE を Cisco Secure Firewall に公開する仮想パッチ適用ルールを作成できます。 | 脆弱性ダッシュボード（2 ページ）<br>Cisco Security Risk Score ベースのフィルタ |


- 脆弱性ダッシュボード （2 ページ）
- [CVE] タブ （5 ページ）
- [パッケージ（Packages）] タブ （5 ページ）
- [ワークロード（Workloads）] タブ （6 ページ）
- [ポッド（Pods）] タブ （7 ページ）


# 脆弱性ダッシュボード

スコアリングシステムと範囲を選択して、重大度およびその他の属性に関する詳細に従って CVE を表示します。

Cisco Secure Workload で使用されるさまざまなスコアリングシステムは、次のとおりです。

- 共通脆弱性評価システム（CVSS）：CVSS は、CVE の重大度（低からクリティカル）を定性的に評価します。スコアは、最も重大な重大度の応答に優先順位を付けるために役立ちます。CVSS V3 は、CVSS スコアリングメカニズムの最新バージョンです。
- Cisco Security Risk Score：Cisco Security Risk Score は、ワークロードに含まれる CVE の正確なリスク評価を提供します。リスクスコアは、組織のリスクプロファイルを把握し、セキュリティチームが修復戦略に優先順位を付けるために役立ちます。

表 *2:* スコアリングシステムと対応する属性

| スコアリングシステム | 属性 |
|---|---|
| Cisco Security Risk Score | • Cisco Security Risk Score と重大度<br>• アクティブなインターネット侵害<br>• エクスプロイトされやすい脆弱性<br>• 修正可能<br>• エスプロイトされやすいマルウェア<br>• 狙われやすいターゲット<br>• エクスプロイト可能と予測 |
| CVSS V3 | • CVE スコアと重大度<br>• Attack Complexity<br>• 攻撃元区分<br>• 可用性への影響<br>• ベース重大度<br>• 機密性への影響<br>• 完全性への影響<br>• 必要な権限<br>• スコープ<br>• ユーザ対話 |
| CVSS V2 | • CVE スコアと重大度<br>• アクセスの複雑さ<br>• Access Vector<br>• 認証<br>• 可用性への影響<br>• 機密性への影響<br>• 完全性への影響<br>• 重大度 |

ダッシュボードには、選択した範囲の脆弱性の分布や、さまざまな属性ごとの脆弱性がハイライト表示されます。たとえば、エクスプロイトの複雑さによって、脆弱性がネットワークを介してエクスプロイトされる場合や、攻撃者がワークロードへのローカルアクセスを必要とする場合があります。さらに、統計情報では、リモートでエクスプロイト可能で、複雑さが最も低い脆弱性を除外できます。

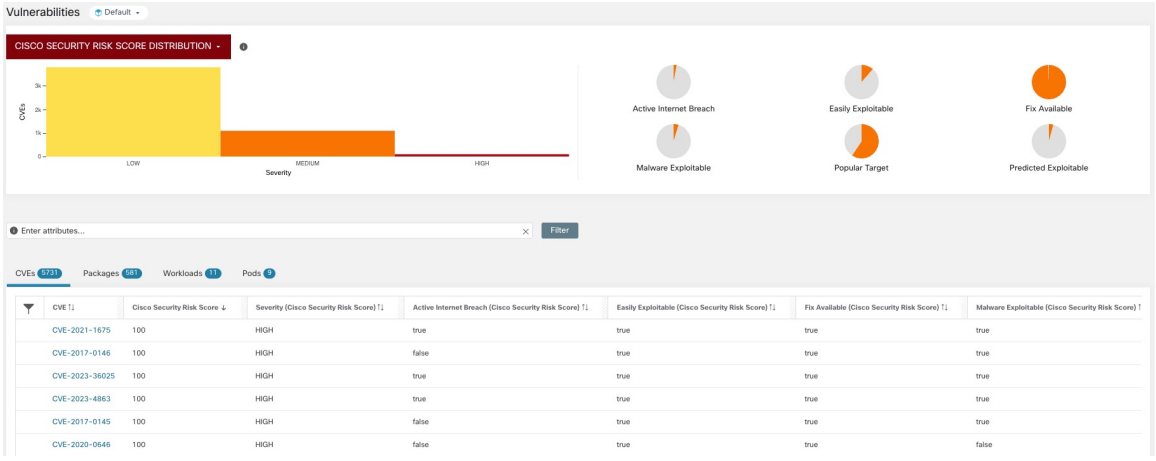
Cisco Secure Workload の CVE 脅威データベースは、NIST、Microsoft、Oracle、Cisco Vulnerability Management などの一般的なソースから最新の CVE の詳細を取得することで、24 時間ごとに更新されます。Cisco Secure Workload クラスタがエアギャップ環境にある場合は、https://updates.tetrationcloud.com から CVE 脅威データパックをダウンロードし、Cisco Secure Workload にアップロードする必要があります。

ワークロードに含まれる既知の CVE のスコアと必要な属性を使用することで、次のことが可能です。

- インベントリフィルタを作成します。「インベントリフィルタ」を参照してください。
- マイクロセグメンテーションポリシーを設定して、影響を受けるワークロードからの外部通信をブロックし、仮想パッチ適用ルールを Cisco Secure Firewall Management Center に公開します。

[脆弱性（Vulnerabilities）] ページを表示するには、ナビゲーションウィンドウから、**[調査（Investigate）] > [脆弱性（Vulnerabilities）]**の順に選択します。さまざまな評価システムを使用して特定された脆弱性が表示されます。すぐに対処する必要があるワークロードと、リスクを軽減するためにすぐにパッチを適用する必要があるパッケージを特定するために、評価システムに応じて、グラフとウィジェットに脆弱性の数が、関連するリスクレベルおよび属性とともに表示されます。

**図 *1 : [*脆弱性（***Vulnerabilities***）*]* ページ**




次のタブは、グラフまたはウィジェットの選択した部分に基づいてフィルタ処理されます。

- [CVE（CVEs）] タブには、選択した範囲内の注意が必要な脆弱性が強調表示されます。
- [パッケージ（Packages）] タブには、パッチを適用する必要があるパッケージが一覧表示されます。

- [ワークロード（Workloads）] タブには、選択した範囲内の影響を受けるワークロードが一覧表示されます。
- [ポッド（Pods）] タブには、選択した範囲内の影響を受ける Kubernetes ポッドが一覧表示されます。

詳細を確認するには、タブで必要な行をクリックします。たとえば、[パッケージ（Packages）] タブの行をクリックすると、そのパッケージまたはバージョンがインストールされているワークロードと、そのパッケージに関連する脆弱性が表示されます。表示されたリストは、ダウンロードリンクを使用して、JSON ファイルまたは CSV ファイルとしてダウンロードできます。

# [CVE] タブ

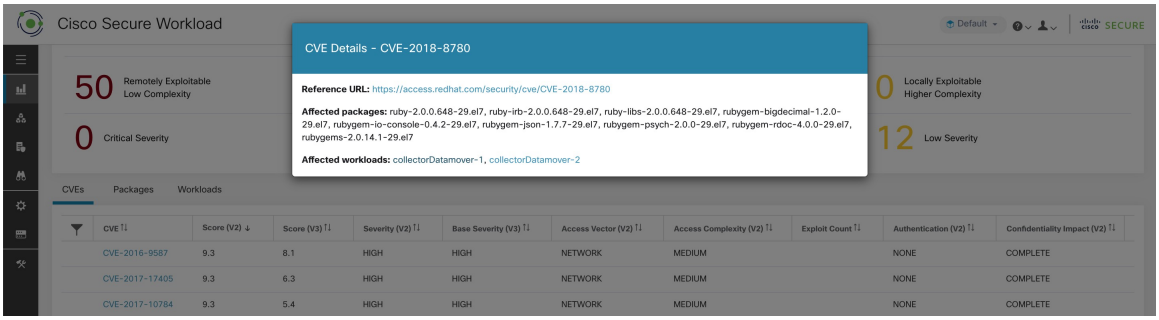
スコアリングシステムと選択した範囲に基づいて、[CVE] タブにワークロードで特定された脆弱性が一覧表示されます。CVE ごとに、基本的な影響指標に加えて、Cisco Secure Workload の脅威インテリジェンスに基づくエクスプロイト情報が表示されます。

- エクスプロイト数：前年に組織で CVE のエクスプロイトが確認された回数。
- 最終エクスプロイト：Cisco Secure Workload の脅威インテリジェンスによって、組織で CVE のエクスプロイトが最後に確認された時間。

グラフと円グラフを使用して、スコアリングシステムの重大度または必須属性に基づいて CVE をフィルタ処理できます。たとえば、いずれかのスコアリングシステムで [重大（Critical）] の重大度バーをクリックすると、テーブルには重大な CVE を含むワークロード、パッケージ、およびポッドのみが表示されます。

[CVE] タブで必要な行をクリックして、その脆弱性と影響を受けるワークロードの詳細を取得します。

**図 *2 : CVE* の詳細**




# [パッケージ（Packages）] タブ

[パッケージ（Packages）] タブには、攻撃対象領域を減らすためにアップグレードする必要がある、影響を受けるソフトウェアパッケージが一覧表示されます。

影響を受けるパッケージ、パッケージをともなうワークロード、およびパッケージ内の特定された CVE の詳細を取得するには、[パッケージ（Packages）] タブで必要な行をクリックします。

**図 *3:* パッケージの脆弱性と影響を受けるワークロードの詳細**

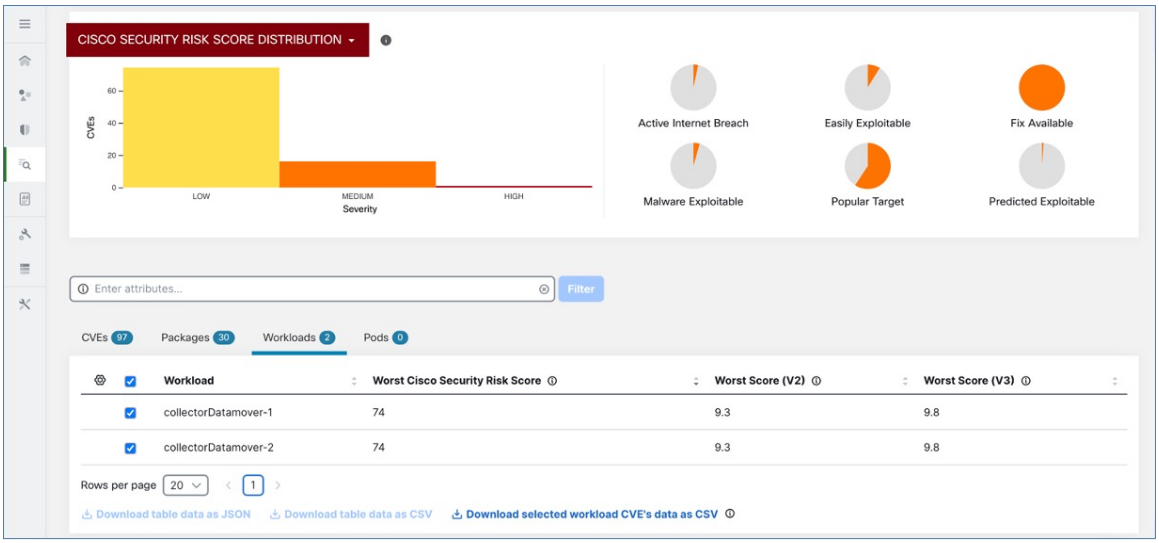
# [ワークロード（Workloads）] タブ

[ワークロード（Workloads）] タブには、ソフトウェアの更新またはパッチに関してすぐに注意が必要なワークロードが一覧表示されます。

[ワークロード（Workloads）] タブで目的の行をクリックして、選択したワークロードに存在する脆弱なパッケージの詳細を取得します。ワークロードプロファイルを表示するには、ダイアログボックスのタイトルの横にあるワークロード名をクリックします。

ワークロードを選択し、ワークロードに影響を与える脆弱性の概要を CSV ファイルとしてダウンロードします。

図 *4*: 影響を受けるワークロードの脆弱性の詳細

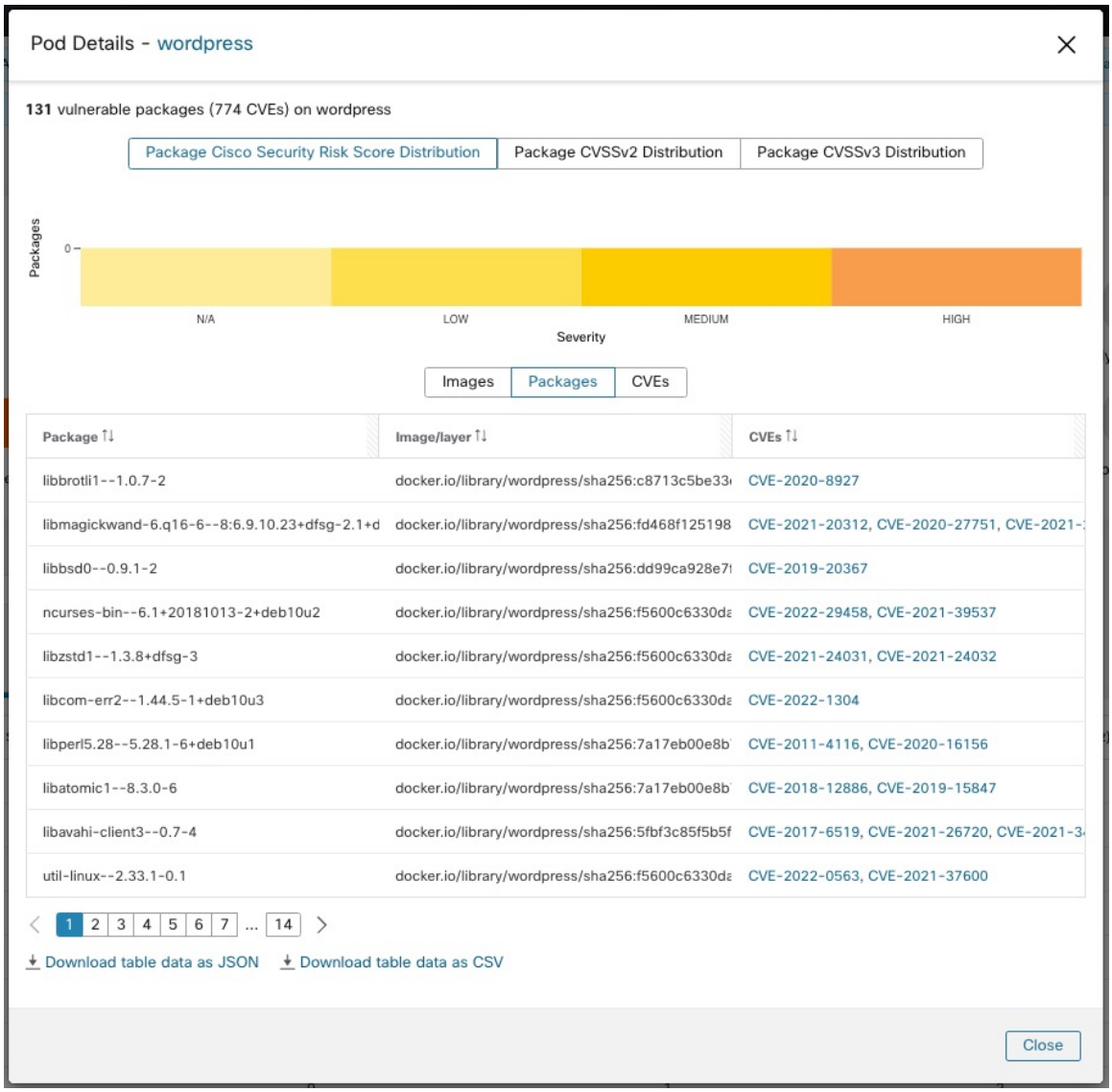



# [ポッド（Pods）] タブ

[ポッド（Pods）] タブには、ソフトウェアの更新またはパッチに関してすぐに注意が必要な Kubernetes ポッドが一覧表示されます。

影響を受ける Kubernetes ポッド、パッケージ、イメージ、および特定された CVE の詳細を取得するには、[ポッド（Pods）] タブで必要な行をクリックします。

図 *5 : Kubernetes* ポッドの *CVE* と影響を受けるパッケージ



翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。