VMDR

操作ガイド

2020 年 7 月 1 日

無断複写・転載を禁じます。2020 年クォリスジャパン株式会社

Qualys および Qualys ロゴは Qualys, Inc. の登録商標です。その他すべての商標は、各所有者に帰属します。

クォリスジャパン株式会社
〒 100-6208
東京都千代田区丸の内 1-11-1
パシフィックセンチュリープレイス 8 階
03-6860-8296

目次

本書について 4
Qualys について 4
Qualys サポート 4

VMDR について 5
動作方法 6

アセットの特定 7
Cloud Agent による開始 7
その他のアセット検索方法 10

脆弱性の検出 11

VMDR 優先順位付けレポート 12
優先順位付けレポートの生成 12
VMDR 優先順位付けレポートの読み取り 14

パッチ管理 19
VMDR レポートから脆弱性にパッチを適用 19

本書について

Qualys VMDR（Vulnerability Management, Detection, and Response）に関心をお寄せいただきありがとうございます。Qualys VMDR では、Qualys クラウドプラットフォームの機能を拡張することにより、グローバルなハイブリッド IT 環境内において重大な脆弱性をリアルタイムに検出、評価、優先順位付け、およびパッチ処理します。これらはすべて 1 つのソリューションで行われます。

Qualys について

Qualys, Inc. (NASDAQ: QLYS）は、セキュリティとコンプライアンスを目的とするクラウドソリューションのパイオニアであり、リーディングカンパニーです。Qualys のクラウドプラットフォームおよび統合されたアプリケーションは、重要なセキュリティインテリジェンスをオンデマンドで提供し、IT システムと Web アプリケーションの監査、コンプライアンス、および保護の全範囲を自動化することにより、ビジネスにおけるセキュリティ業務の簡略化とコンプライアンスのコスト削減を支援します。

1999 年の創立以来、Qualys は、Accenture、BT、Cognizant Technology Solutions、Deutsche Telekom、富士通、HCL、HP Enterprise、IBM、Infosys、NTT、Optiv、SecureWorks、Tata Communications、Verizon、Wipro などのマネージドサービスプロバイダやコンサルティング企業との戦略的パートナーシップを構築してきました。Qualys は、CSA（Cloud Security Alliance）の創立メンバーでもあります。詳細については、www.qualys.com をご覧ください。

Qualys サポート

Qualys は綿密なサポートを提供します。不明な点には、オンラインドキュメント、電話サポート、および E メールによる直接サポートを通じて、可能な限り迅速にお答えします。弊社は 24 時間年中無休でサポートを提供します。サポート情報については、www.qualys.com/support/ をご覧ください。

VMDR について

VMDR（Vulnerability Management, Detection, and Response）を使用すると、グローバルなハイブリッド IT 環境内において重大な脆弱性および誤設定をリアルタイムに検出、評価、優先順位付け、およびパッチ処理します。これらはすべて 1 つのソリューションで行われます。これにより、環境の改善および安全確保にかかる時間を短縮できます。

Cloud Agent を使用した継続的な脆弱性評価、ネットワークスキャナおよび複数タイプのセンサを使用したネットワークレベルの表示が可能で、人工知能を活用して、該当するコンテキストに基づいて脅威を即座に評価し優先順位付けできます。

VMDR は、まずアセットの検出とインベントリから開始され、環境内にすべてのデバイスの正確なアカウントがあることが確認されます。

それでは、操作を始めてみましょう。

サブスクリプションタイプの確認

VM ユーザの場合、アップグレードすることで VMDR 機能を体験できます。その後、さらに機能を使用したい場合は、VMDR を購入できます。

アップグレードによって取得できる機能

- 次の環境内でのアセットインベントリ：証明書、クラウド、コンテナ、モバイルデバイス

- 次のアセットの特定に役立つ無制限のセンサ ：仮想パッシブセンサ、Cloud Agent、モバイルエージェント、コンテナセンサ

- 200 以上の検索可能な属性を使用して瞬時にアセットを検索

- トレンド情報を表示するカスタマイズ可能なダッシュボードとウィジェット

VMDR にアップグレードした場合の追加機能

- CIS ベンチマークに基づいて、アセットにおける設定評価を行い、セキュリティ上の誤設定を特定できる Security Configuration Assessment

- 常時更新される Real-Time Threat Indicator に基づく脅威ベースの優先順位付け

- 外部ペリミターなどに対する重大な脆弱性および変更のリアルタイムの E メール警告

- 検出された脆弱性のコンテキスト内で未適用のパッチの検出

- 優先順位付けレポートから直接、未適用のパッチの配置を開始

注記 : パッチの配置を利用できるのは、Patch Management アドオンのあるユーザのみです。

動作方法

VMDR を使用すると、リアルタイムのアセット検出および脆弱性情報の取得、脅威インテリジェンスに従った脆弱性の優先順位付けまたはショートリスト化、適切な改善パッチの検出および配置をワンクリックで行うことができます。

アセットの特定

VMDR 用に Cloud Agent をインストールするか、既存のエージェントをアップグレードして、アセットの特定を開始します。アセットを分類し編成するためのタグを割り当てます。スキャナ、パッシブセンサ、クラウドインベントリ、コンテナインベントリ、モバイルデバイスインベントリなどの方法を使用して、インベントリを作成することもできます。詳細については、「アセットの特定」を参照してください。

脆弱性および誤設定の検出

常に最新を維持するシグニチャデータベースにより、継続的に、ソフトウェアの脆弱性を検出し、セキュリティの誤設定を特定します。「Vulnerabilities」タブに、アセットと脆弱性の視点から脆弱性の状態が完全に表示されます。詳細については、「脆弱性の検出」を参照してください。

脅威の優先順位付け

VMDR 優先順位付けレポートを実行することで、Real-Time Threat Indicator に基づいてアセットの脆弱性のリスク重大度を優先順位付けし、最初に改善すべき脆弱性を特定します。詳細については、「VMDR 優先順位付けレポート」を参照してください。

未適用のパッチの検出および配置

Patch Management アプリケーションの優先順位付けレポートに基づいて、最優先の該当パッチを配置します。詳細については、「パッチ管理」を参照してください。

アセットの特定

Cloud Agent、スキャナ、およびセンサを設定して、オンプレミス、クラウド、モバイル、コンテナ、アプリケーションにある IT アセットを継続的に検出してインベントリを作成し、すべてをリアルタイムに表示します。

Cloud Agent による開始

VMDR 用に Cloud Agent を新規にインストールするか、既存の Cloud Agent をアップグレードして、インベントリの作成を開始します。

VMDR では、Cloud Agent の未適用パッチを検出するために専用のエンジンのアクティブ化が必要です。このエンジンは非常に軽量で効率的ですが、VMDR 用に Cloud Agent をアクティブ化するには、コンポーネントの各ホストに 20MB のダウンロード容量および 100MB の空き容量が必要です。

新しいエージェントのインストール

既存のエージェントのアップグレード

要件の確認

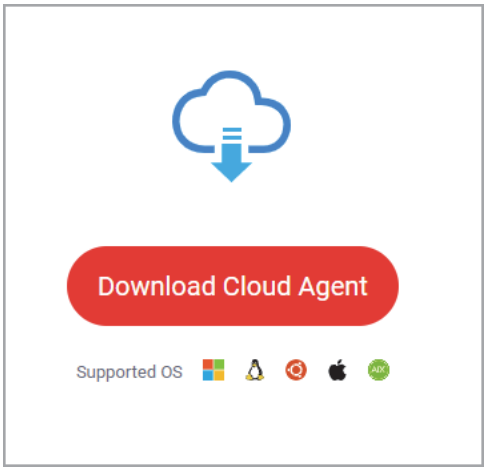
Cloud Agent のインストールおよび実行のシステム要件は次のとおりです。

- ホストから HTTPS ポート 443 経由で、Qualys クラウドプラットフォーム（または Qualys プライベートクラウドプラットフォーム）にアクセスする必要があります。

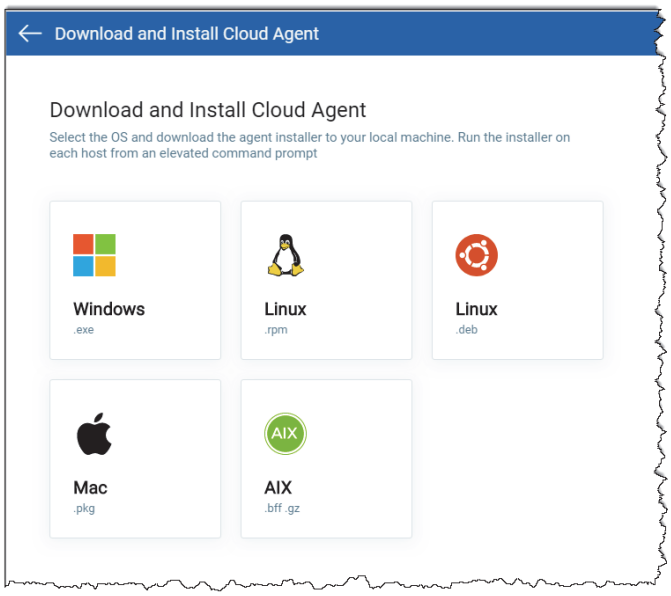
- （Windows の場合）ホストに対するローカル管理者権限が必要です。プロキシ設定がサポートされています。

- （Linux、Mac、AIX の場合）ルート権限、Sudo によってルート権限を委譲された非ルート権限、または十分な特権のある非ルート権限が必要です。プロキシ設定がサポートされています。

新しいエージェントのインストール



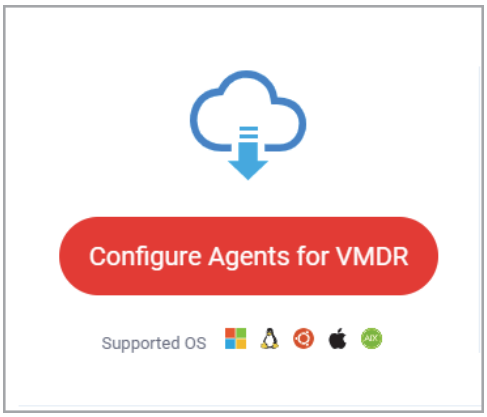
「Help」メニューの「Welcome」オプションを選択して、「Welcome」ページを表示します。「Identify Assets」項で、「Download Cloud Agent」ボタンをクリックします。



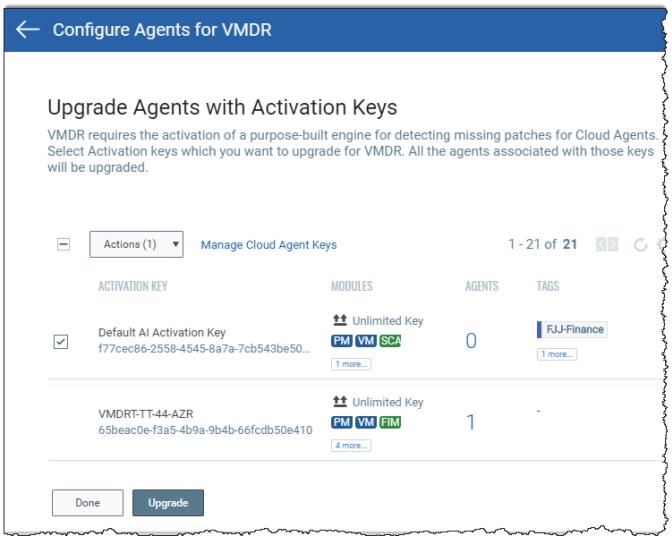
OS を選択し、ローカルマシンにエージェントインストーラをダウンロードします。昇格した権限のコマンドプロンプトで各ホストのインストーラを実行します。

例えば、「Windows」をクリックして、ページ上に表示されるエージェントインストール手順に従います。エージェントインストールに使用できるデフォルトの AI アクティブ化キーが用意されています。キーを追加または管理するには、「Cloud Agent」→「Agent Management」を選択します。

既存のエージェントのアップグレード



「Help」メニューの「Welcome」オプションを選択して、「Welcome」ページを表示します。「Identify Assets」項で、「Configure Agents for VMDR」ボタンをクリックします。



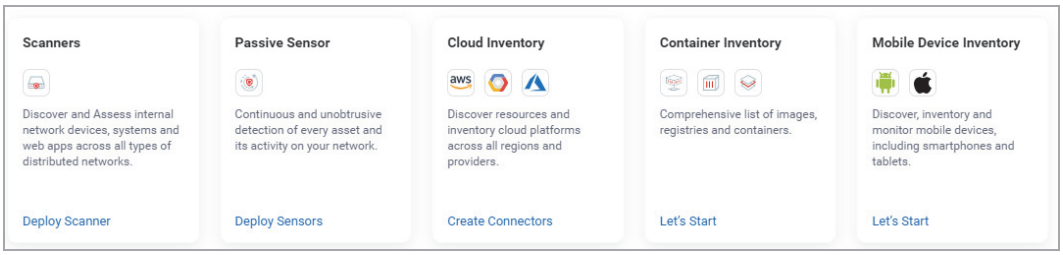
必要なアクティブ化キーを選択し、「Upgrade」をクリックします。選択したアクティブ化キーが VMDR 用にアップグレードされます。

詳細については、『Cloud Agent 操作ガイド』をダウンロードしてください。

その他のアセット検索方法

スキャナ、センサ、またはコネクタを使用して、オンプレミス（デバイスおよびアプリケーション）、モバイル、エンドポイント、クラウド、コンテナ、OT および IoT アセットのインベントリを作成することもできます。

「Help」メニューの「Welcome」オプションを選択して、「Welcome」ページを表示します。「Identify Assets」項で、インベントリの設定を開始する方法を選択します。

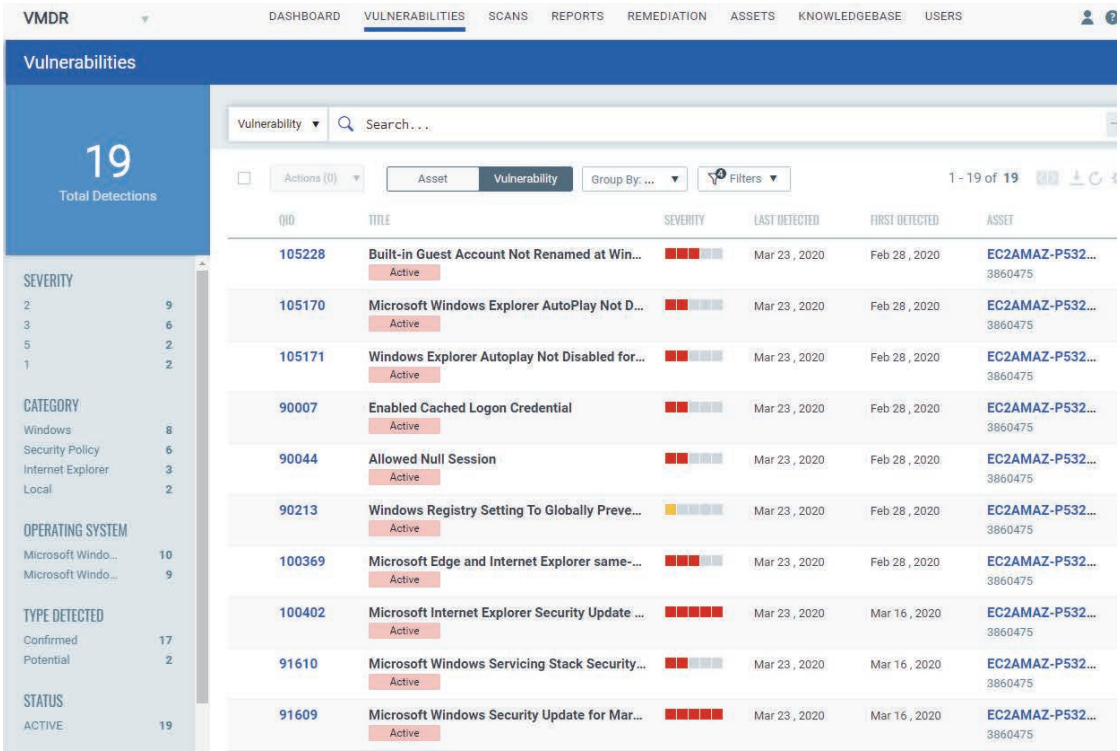


次のステップ

VMDR の「Vulnerability」タブにすべてのアセットと脆弱性の詳細が表示されます。

脆弱性の検出

インベントリが作成されると、「Vulnerability」タブにアセットの脆弱性状態が表示されます。脆弱性別およびアセット別に脆弱性を検索できます。Cloud Agent、スキャナ、センサで特定されたすべてのアセットとそれらに関連する脆弱性の詳細が「Vulnerability」タブに一覧表示されます。



「Asset」と「Vulnerabiliy」で表示を切り替えて、特定のアセットまたは脆弱性にドリルダウンします。「Quick Action」メニューから「View Details」をクリックして、詳細を表示します。

脆弱性が Qualys でパッチ対応可能で、Patch Management アドオンがサブスクリプションで有効になっている場合、詳細表示に「Patch Now」オプションが表示されます。これにより、Patch Management で配置ワークフローを開始できます。Patch Management が無償バージョンの場合は、未適用のパッチのリストが表示されるだけです。

Security Configuration Assessment アドオンがある場合、CIS ベンチマークに基づいてアセットの設定評価を実行し、セキュリティ上の誤設定を特定できます。

VMDR 優先順位付けレポート

VMDR 優先順位付けレポートを使用すると、最も重要なアセットの最もリスクの高い脆弱性を自動的に優先順位付けできます。これにより、検出される可能性のある数千もの脆弱性を重大度の高いものに絞り込むことができます。

優先順位付けレポートの機能：

- リスクが最も高い脆弱性に最初にパッチを適用するために、適切な箇所にリソースを集中させる。

- 攻撃者が悪用する可能性のある脆弱性を特定し改善することで、組織のセキュリティ状態を向上させる。

- 適切な脅威インジケータを選択できるようセキュリティアナリストに権限を与える。例えば、組織がユーザの財務データを所有している場合、「High Data Loss」インジケータに基づいて脆弱性を優先順位付けすることで、悪用された場合にデータ取得につながる可能性のある脆弱性を最初に特定し改善できます。

- 特定の脆弱性を修正する固有パッチの特定を容易にする。

- ボタンをクリックして、統合ワークフロー内の同じプラットフォームから配置されるパッチを検出することで、改善にかかる時間を短縮する（Patch Management アプリケーションがサブスクリプションで有効になっている場合）。

優先順位付けレポートの生成

リアルタイムの脅威インテリジェンスを使用して、環境に応じて最初に改善すべき脆弱性を特定し優先順位付けします。このレポートには、最も重大な脅威も表示され、パッチの優先順位付けも表示されます。

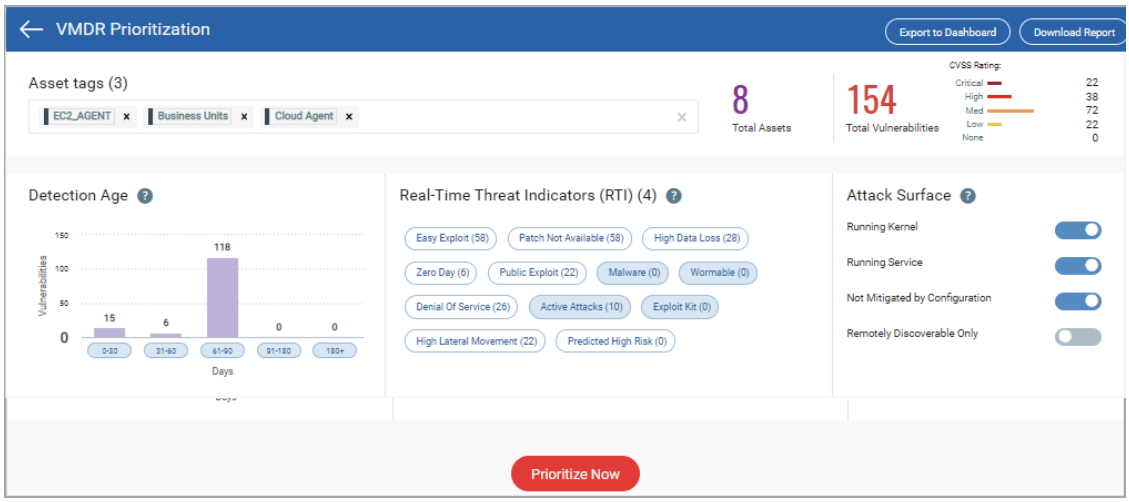
優先順位付けレポートの生成を開始する前に、アセットの脆弱性状態が収集されていることを確認します。Cloud Agent を使用するか、またはスキャナ、パッシブセンサ、クラウドインベントリ、コンテナインベントリ、モバイルデバイスインベントリなどの方法を使用して、アセットインベントリを作成することができます。Cloud Agent およびセンサで特定されたすべてのアセットとそれらに関連する脆弱性の詳細が「Vulnerability」タブに一覧表示されます。「アセットの特定」を参照してください。

1.「Prioritization」→「Reports」を選択し、「Create Report」をクリックします。初めてレポートを生成する場合は、「Prioritization」タブの をクリックします。

2.「Asset tags」を選択して、優先順位付けされたリストを選択されたアセットに関連付けられた脆弱性に絞り込み、矢印ボタンをクリックして、VMDR 優先順位付けレポートを実行します。

続行するには、少なくとも 1 つのアセットタグを選択する必要があります。

3. VMDR 優先順位付けレポートのフィルタを選択します。



Age:「Detection Age」タブまたは「Vulnerability Age」タブを選択し、時間フィルタを選択します。デフォルトでは、検出からの経過時間フィルタが選択されています。レポートには、選択した期間範囲に一致する脆弱性が表示されます。

Real-Time Threat Indicators: 目的の Real-Time Threat Indicator（RTI）を選択します。レポートには、選択した RTI の " いずれか " に一致する脆弱性が表示されます。

Attack Surface: これらのフィルタを選択して、優先順位が最高ではない脆弱性をレポートから削除することで、組織にとって最も重大な脆弱性に集中することができます。

4.「Prioritize Now」をクリックして脅威インテリジェンスを有効にし、選択したアセットのネットワーク上の最もリスクが高い脆弱性を優先順位付けします。

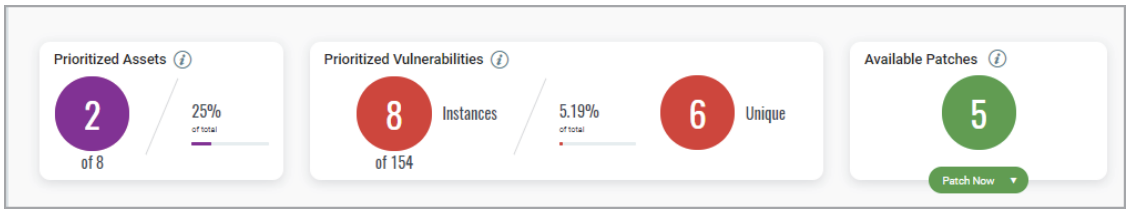
レポートを生成したら、脆弱性のパッチ適用を実行し（Patch Management アプリケーションがサブスクリプションで有効になっている場合）、ウィジェットの形式でレポートをダッシュボードにエクスポートするか、CSV 形式でレポートをダウンロードできます。

VMDR 優先順位付けレポートの読み取り

VMDR　優先順位付けレポートを使用して、最初に改善すべき脆弱性を検出できます。レポートは「Summary」と「Details」の 2 つの項で構成されています。

Summary

VMDR 優先順位付けレポートの「Summary」項には、次の 3 つの項の検出結果が表示されます。



Prioritized Assets

選択したアセットタグに応じて、このレポートのアセットが特定されます。「Prioritized Assets」は、全部のアセットのうち、選択した検出からの経過時間、RTI、攻撃ベクトルの組み合わせに一致する脆弱性を持つアセットの数です。

上記の例では、8 つのアセットが選択したアセットタグに一致しています。8 つのアセットのうち、2 つのアセットには、選択された検出からの経過時間、RTI、アタックサーフェスの組み合わせに一致した脆弱性があります。

Prioritized Vulnerabilities

「Prioritized Vulnerabilities」項には、アセットで検出されて優先順位付けされた脆弱性のサマリが表示されます。

Instances: この数は、選択した検出からの経過時間、RTI、アタックサーフェスの組み合わせに一致する脆弱性の総数を示します。

この数には、複数のアセットで検出された 1 つの脆弱性（すなわち、1 つの QID）の複数の発生回数が含まれる場合があります。

上記の例では、8 つのアセットで 154 の脆弱性が検出されています。154 の脆弱性のうち、8 つの脆弱性が、2 つのアセットで選択された検出からの経過時間、RTI、アタックサーフェスの組み合わせに一致しています。

Unique: 特定 / 検出された脆弱性インスタンスのうちの一意の脆弱性の数です（重複する QID インスタンスは除く）。

上記の例では、8 つのインスタンスのうち 6 つが一意の脆弱性です。

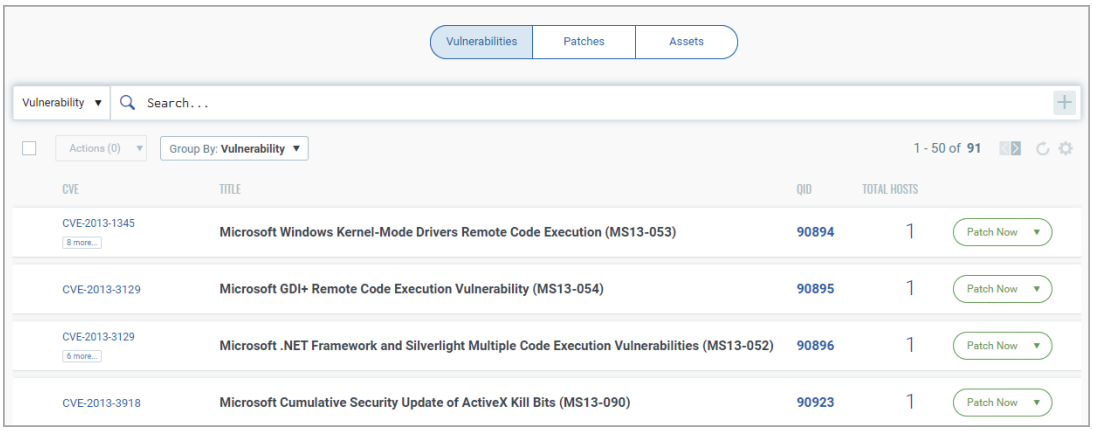
Available Patches

Qualys で入手できるパッチの数です。「Patch Now」をクリックして、脆弱性へのパッチ適用プロセスを開始します。詳細については、「パッチ管理」を参照してください。

> 注記 ：「Patch Now」ボタンが有効になるのは、Qualys が自動的にパッチを適用でき、Patch Management アプリケーションがサブスクリプションで有効になっている場合のみです。

Details

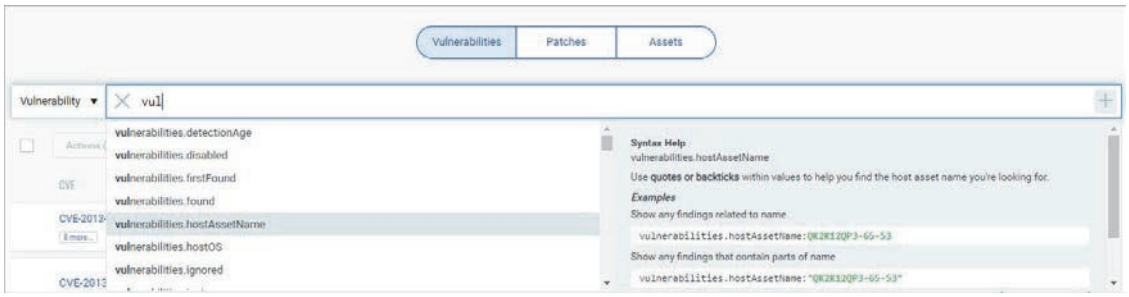
「Details」項には、優先順位付けされた脆弱性、パッチ、優先順位付けされたアセットに関する詳細情報が表示されます。タブを使用して、3 つのビューを切り替えます。「Vulnerabilities」タブ、「Patches」タブ、「Assets」タブには、トークンを使用する詳細検索機能があります。



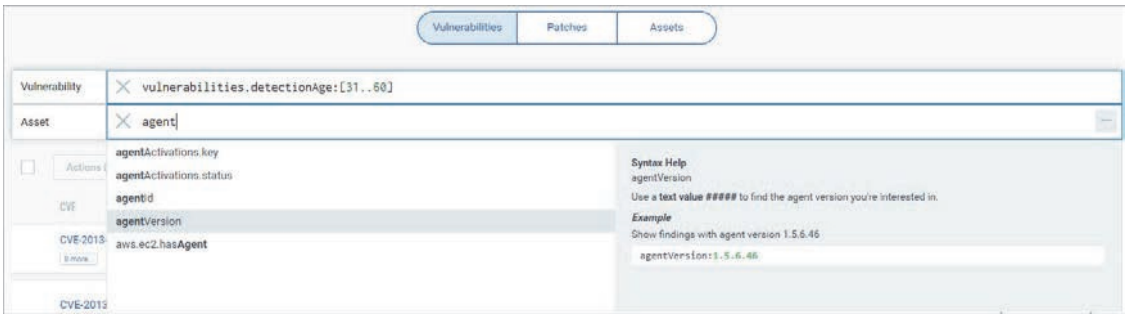
詳細検索

一度に複数の条件を指定して検索できます。

検索フィールドに入力を開始すると、脆弱性の重大度、検出からの経過時間など検索可能なプロパティが表示されます。目的のプロパティを選択します。



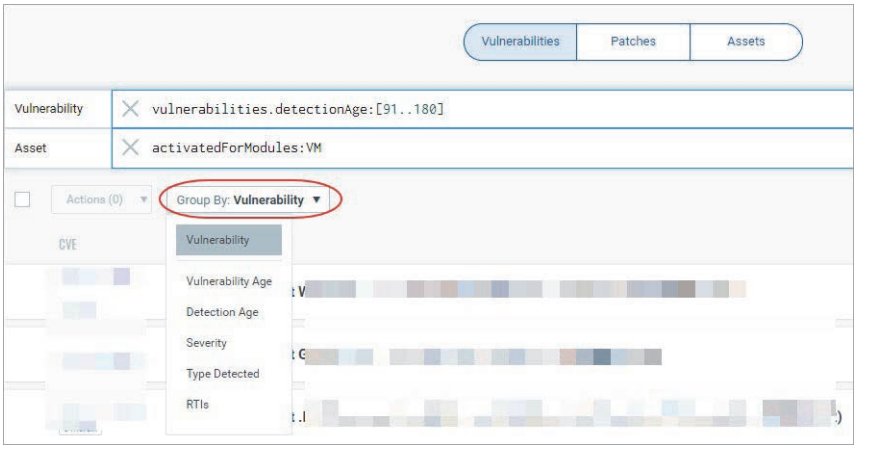
「Vulnerability」と「Asset」を組み合わせて検索するには、プラス記号（+）をクリックします。



入力を開始すると、エージェント ID、エージェントバージョンなど検索可能なアセットプロパティが表示されます。目的のアセットプロパティを選択します。

ここで、一致させたい値を入力し、「Enter」を押します。一致するものがそれぞれのタブに表示されます。

検索結果を取得したら、その結果を論理グループに分類することができます。検出からの経過時間、脆弱性の期間、重大度などのグループ化オプションがいくつか用意されています。



選択内容に応じた一意のグループの数とグループごとの脆弱性の数が表示されます。任意のグループをクリックすると、検索クエリが更新され、一致する脆弱性が表示されます。

ダッシュボードへのエクスポート

VMDR 優先順位付けレポートをウィジェットの形式でダッシュボードにエクスポートし、ウィジェットを継続的に監視することで、優先順位付けされたアセットの脆弱性を確認できます。

ダッシュボードにレポートをエクスポートする手順について説明します。

注記：「Export to Dashboard」ボタンが有効になるのは、レポートの生成後のみです。

1）VMDR 優先順位付けレポートで、「Export to Dashboard」をクリックします。

2）ウィジェット名を入力します。

3）ウィジェットを追加する「Dashboard」を選択し、「Export」をクリックします。

ウィジェットがダッシュボードに追加されます。

レポートのダウンロード（CSV 形式）

1 回のクリックで VMDR 優先順位付けレポートをローカルシステムに保存または保存およびダウンロードできます。レポートは、保存すると「Prioritization」タブのレポートリストに保存されます。

手順について説明します。

注記 :「Save & Download」ボタンが有効になるのは、VMDR 優先順位付けレポートの生成後のみです。

1）VMDR 優先順位付けレポートで、「Save & Download」をクリックします。

2）レポートの名前と説明（オプション）を入力します。

3）レポートに含める脆弱性、パッチ、およびアセットの詳細を選択します。

Vulnerabilities: 脆弱性を含める場合、次の 2 つのオプションがあります。

Grouped (Unique): 一意の脆弱性と脆弱性が検出されたアセットの数のリストが含まれます。

All Instances: すべての脆弱性のリストが含まれます。脆弱性ごとに、その脆弱性が検出されたすべてのアセットが含まれます。

Patches: 使用できるパッチのリストが含まれます。

Assets: 脆弱性が検出されたアセットのリストが含まれます。

4）レポートの形式（CSV または PDF）を選択します。

注記 : すべてのインスタンスに関連する脆弱性データをレポートに含める場合は、CSV 形式のみがサポートされています。

5）必要に応じて、「Select Timezone」オプションを使用して、レポートに含める日付のタイムゾーンを変更できます。デフォルトでは、レポートの日付には、ブラウザのタイムゾーンが使用されます。

6）「Save」または「Save & Download」をクリックします。

「Save」をクリックすると、VMDR 優先順位付けレポートがレポートリストに保存されます。「Save & Download」をクリックすると、VMDR 優先順位付けレポートがレポートリストに保存され、ローカルシステムにダウンロードされます。

注記 ：ダウンロードしたレポートファイルには、カテゴリ（脆弱性、アセット、パッチ）ごとに最大 5000 レコードのオンラインレポートを格納できます。

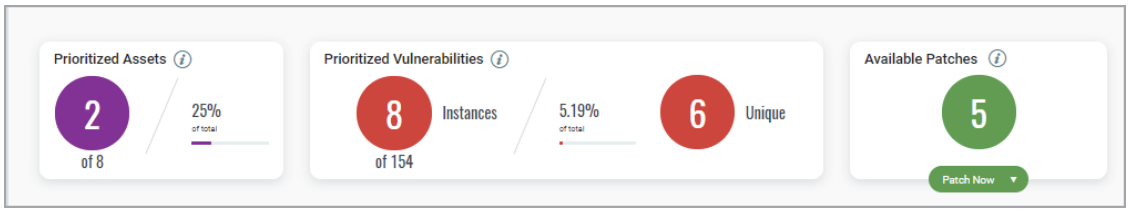
パッチ管理

VMDR 優先順位付レポートには、Qualys でパッチ対応可能なアセットと脆弱性を表示できます。パッチ適用プロセスをを開始し、レポートから直接脆弱性にパッチを適用できます。

注記：パッチの配置を VMDR 優先順位付レポートから直接利用できるのは、Patch Management アドオンのあるユーザのみです。

VMDR レポートから脆弱性にパッチを適用

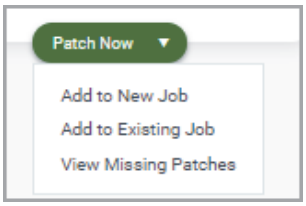
VMDR 優先順位付けレポートの「Summary」項には、次の 3 つの項の検出結果が表示されます。



「Available Patches」ウィジェットには、Qualys で使用できるパッチの数が表示されます。「Patch Now」をクリックして、脆弱性へのパッチ適用プロセスを開始します。

注記：「Patch Now」ボタンが有効になるのは、Qualys が自動的に脆弱性にパッチを適用でき、Patch Management アプリケーションがサブスクリプションで有効になっている場合のみです。

パッチ適用プロセスを開始するには、「Patch Now」ボタンをクリックし、次の 3 つの操作のいずれかを選択します。



Add to New Job - Patch Management アプリケーションでウィザードを開いて、ジョブを新規に作成します。ウィザードの手順に従い、ジョブを新規に作成してパッチ適用プロセスを開始します。

Add to Existing Job - Patch Management アプリケーションで既存のジョブのリストを表示します。既存のジョブ（無効状態）の 1 つを選択し、「Add」をクリックします。1 つのジョブに最大 200 のパッチを追加できます。有効にされたパッチは、オンデマンドおよび 1 回実行（繰り返しなし）のジョブに追加できません。

View Missing Patches - 優先順位付けされたアセットおよび脆弱性に対して未適用のパッチのリストを表示します。Patch Management が無償バージョンの場合は、未適用のパッチのリストが表示されるだけです。Patch Management アプリケーションの有償バージョンにアップグレードして、「Patch Now」オプションから配置ワークフローを開始する必要があります。

詳細については、『Patch Management ユーザガイド』を参照してください。