BigFix Insights for Vulnerability Remediation
実装ガイド

Special notice

Before using this information and the product it supports, read the information in Notices.

Edition notice

This edition applies to BigFix version 11 and to all subsequent releases and modifications until otherwise indicated in new editions.

目次

第 1 章. BigFix Insights for Vulnerability Remediation..... 6

第 2 章. System requirements..... 8

Tenable.io の API 要件..... 12

Tenable.sc の API 要件..... 18

Qualys の API 要件..... 19

第 3 章. デプロイメントと構成..... 24

Tenable.io 向けのデプロイメントと構成..... 24

Tenable.sc 向けのデプロイメントと構成..... 31

Qualys 向けのデプロイメントと構成..... 37

第 4 章. IVR アプリケーションのセットアップ..... 44

第 5 章. IVR ETL のスケジュール..... 47

第 6 章. IVR Fixlet とタスク..... 49

第 7 章. IVR 構成ファイルの更新と検証..... 58

第 8 章. IVR の資格情報の更新..... 59

第 9 章. ビジネス・インテリジェンス・レポート..... 60

Power BI レポート..... 60

Qualys 用 Power BI レポート..... 62

Tenable.io 用 Power BI レポート..... 72

Tenable.sc 用 Power BI レポート..... 82

Tableau レポート..... 88

Qualys 用 Tableau レポート..... 90

Tenable.io 用 Tableau レポート..... 97

Tenable.sc 用 Tableau レポート..... 110

第 10 章. 参照..... 119

構成ファイル..... 119

IVR ソリューションの構成設定..... 127

コマンド行インターフェース..... 132

ログ....133
IVR のトラブルシューティング....134
cURL コマンドを使用した Qualys による IVR のトラブルシューティング....136
既知の制限....138
第 11 章. リリース・ノート....140
付録 A. 用語集....144
Notices....clvi
索引....

第 1 章. BigFix Insights for Vulnerability Remediation

このセクションでは、本製品がどのように機能するのかを理解するために必要な BigFix Insights for Vulnerability Remediation インフラストラクチャーおよび主要な概念について詳述します。

BigFix Insights for Vulnerability Remediation は、BigFix を脆弱性データのソースと統合します。この目的は、検出された脆弱性を修復し、リスクを減らして、セキュリティーを改善するための、最良のパッチと構成設定を適用する方法を BigFix ユーザーにガイドすることです。

BigFix Insights for Vulnerability Remediation は、高度な相関アルゴリズムを使用して、BigFix の情報と脆弱性データを集約して処理し、分析レポートを行います。分析が出力されることにより、検出された脆弱性に対して使用可能な最新のパッチが推奨されるため、ベースライン作成ウィザードによる修復が容易になります。

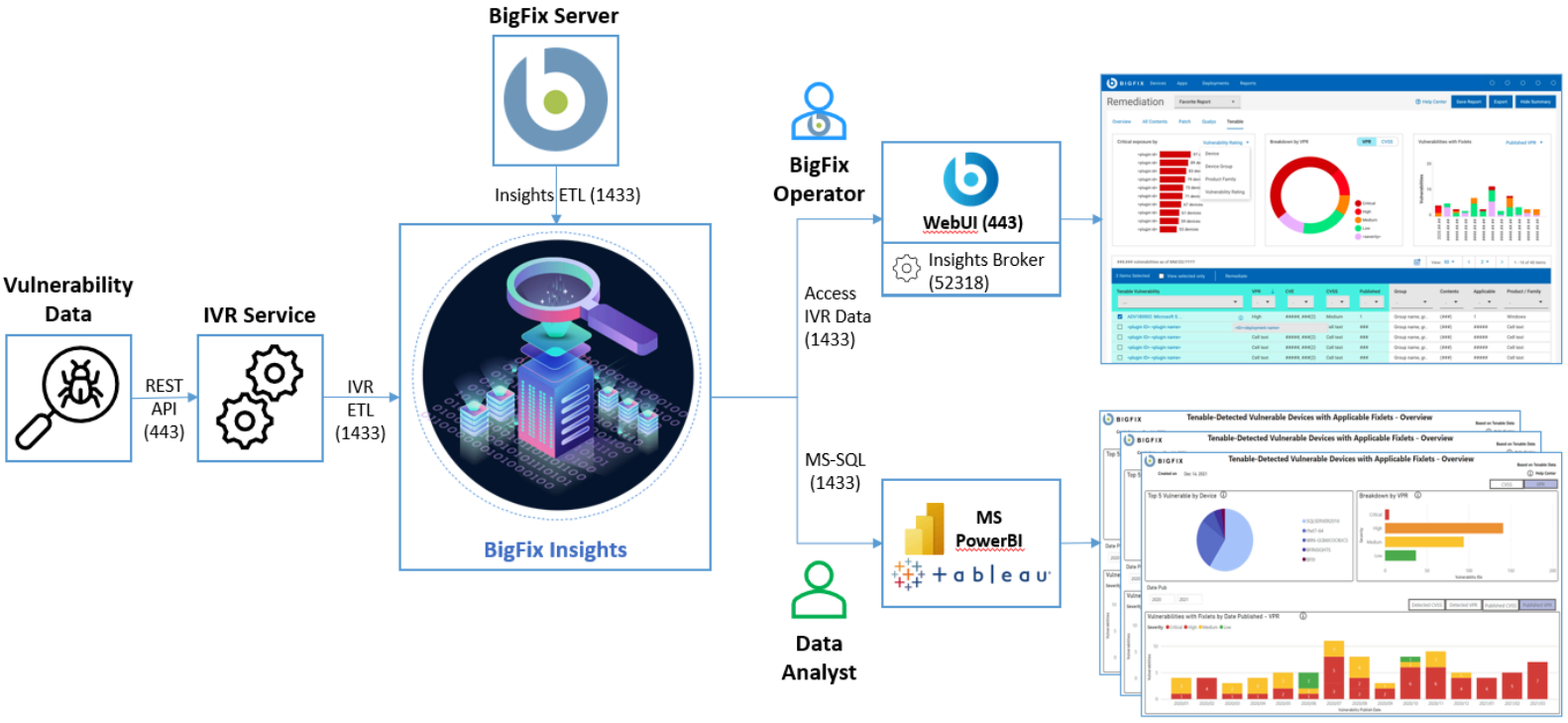
IVR データは、次で利用できます。

- WebUI IVR アプリケーション - WebUI が Insights を介して IVR データにアクセスできるようにする必要があります。IVR アプリケーションのインストールの詳細については、「IVR アプリケーションのセットアップ」を参照してください。
- データ分析向け BI ツール - PowerBI および Tableau の既存の IVR レポート。IVR レポートの詳細については、リンクを参照してください。

IVR の制限事項:

- 特定の BigFix Insights インスタンスでは、自動取得の脆弱性データのソースは 1 つだけサポートされます
- 1 つの BigFix WebUI インスタンスで管理できる BigFix Insights データベースは 1 つだけです。この制限は、1 つの WebUI インスタンスを介して BigFix Insights の複数のインスタンスに同時に接続したり管理したりすることはできないことを意味します。

図 1. BigFix Insights for Vulnerability Remediation のアーキテクチャーの概要



第 2 章. System requirements

Learn more about the prerequisites and system requirements for BigFix Insights for Vulnerability Remediation (IVR) service.

表 1. Prerequisites and system requirements for IVR service

Hardware requirements	
CPU	minimum 2 cores (recommended 4)
RAM	On top of host OS requirements: • < 1M Findings from Vulnerability Management Product = 16GB • < 2M Findings from Vulnerability Management Product = 32GB • < 3M Findings from Vulnerability Management Product = 48GB • < 4M Findings from Vulnerability Management Product = 64GB
Disc space	• < 1M Findings from Vulnerability Management Product = 4GB - 8GB preferred • < 2M Findings from Vulnerability Management Product = 8GB - 12GB preferred • < 3M Findings from Vulnerability Management Product = 12GB - 16GB preferred • < 4M Findings from Vulnerability Management Product = 16GB - 20GB preferred
Execution Time	The overall run time of data synchronization and processing depends on: • CPU Speed • Number of findings • Number of assets in insights

表 1. Prerequisites and system requirements for IVR service (続く)

	• Number of patch sites loaded within the BFE environment • API latency • Conflicting workloads on IVR machine
Software requirements	
BigFix Component Requirements	• BigFix Insights WebUI App (v6) (minimum)
Prerequisites	• Microsoft VC++ Redistributable package 2012 https://www.microsoft.com/en-in/download/details.aspx?id=30679 • Microsoft® ODBC Driver 17 for SQL Server® https://www.microsoft.com/en-us/download/details.aspx?id=56567 注: The Fixlet will attempt to deploy the pre-requisites automatically.
Operating system	• Microsoft Windows 2016 • Microsoft Windows 2019

表 1. Prerequisites and system requirements for IVR service (続く)

Supported BigFix versions	• Windows - based BigFix Server, Version 10 注: BigFix Insights for Vulnerability Remediation does not currently support non-Windows-based BigFix Server environments.
BigFix License Requirements	• BigFix Lifecycle • BigFix Compliance • BigFix Remediate
Supported Vulnerability Management Platforms	• Qualys VMDR v2 REST API: https://www.qualys.com/docs/qualys-api-vmpc-user-guide.pdf • Tenable.SC versions from 5.17 up to 6.4 • Tenable.IO 注: It is required to use **Administrator** user role within Tenable to enable the generation of API keys that are used by IVR to maintain the interface with Tenable.

表 1. Prerequisites and system requirements for IVR service (続く)

BI tool	• Power BI Desktop/Server, 2021 + (Rec. May 2021) 注: Microsoft offers two distinct products called Power BI desktop. Use the one that is optimized for Power BI Report Server: https://www.microsoft.com/en-us/download/details.aspx?id=56723 • Tableau Desktop/Server, 2020.4 +
Network requirements	• Connectivity to Vulnerability Management API Server URL (port 443 by default) • Connectivity to BigFix Insights SQL database (port 1433 by default) 注: IVR now supports proxy-based connectivity. Refer to the link for more information. • By default WebUI IVR app listens on port 52318. It can be changed in the WebUI application configuration file with `_WebUIAppEnv_INSIGHT_BROKER_PORT` setting.

表 1. Prerequisites and system requirements for IVR service (続く)

System limitations	• Only one source of vulnerability data for automatic ingestion is supported for a given BigFix Insights instance • A single BigFix WebUI instance can manage only one BigFix Insights database.

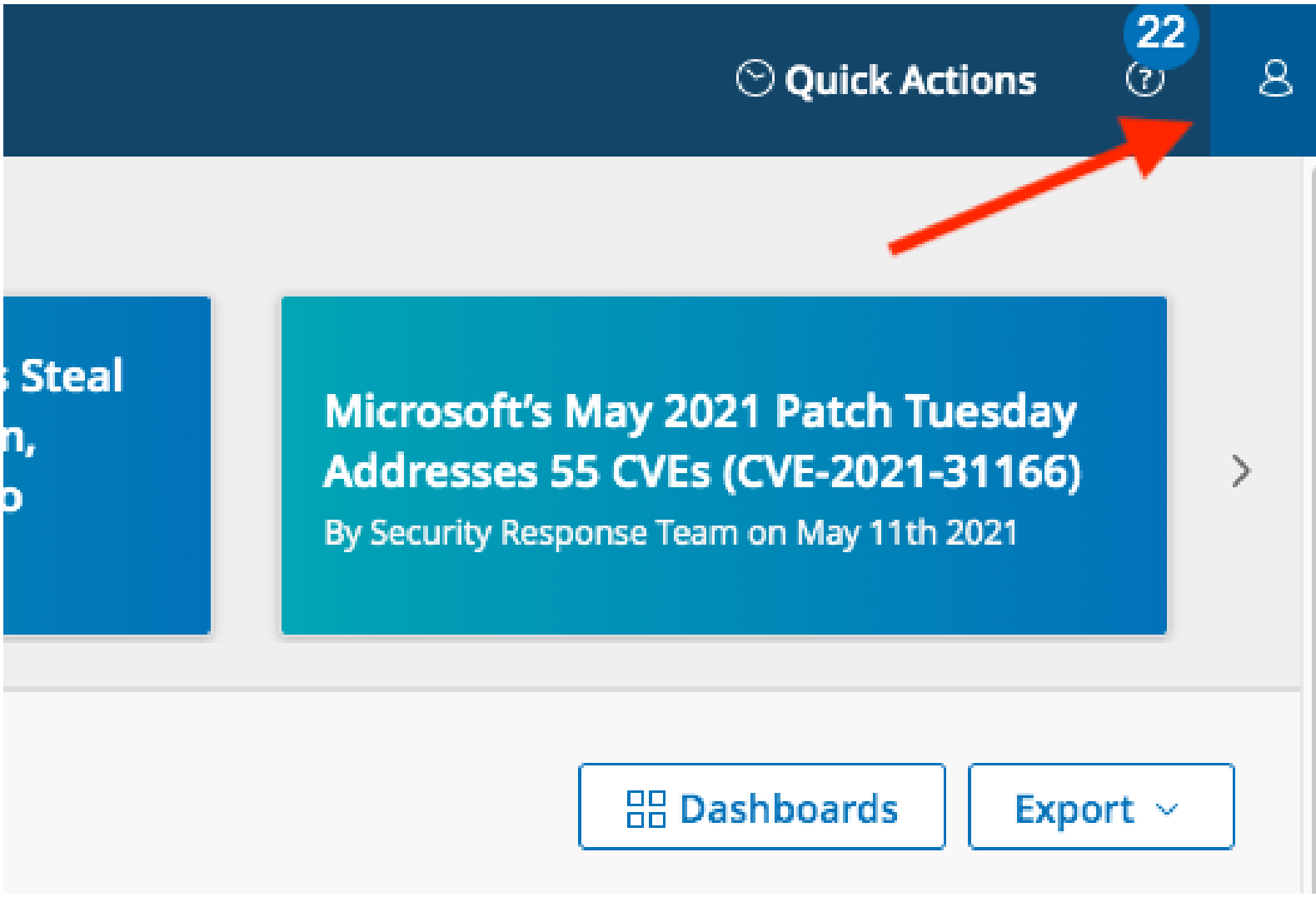
Tenable.io の API 要件

IVR が Tenable から重要な脆弱性データを取得できるようにするには、以下の要件を満たす必要があります。

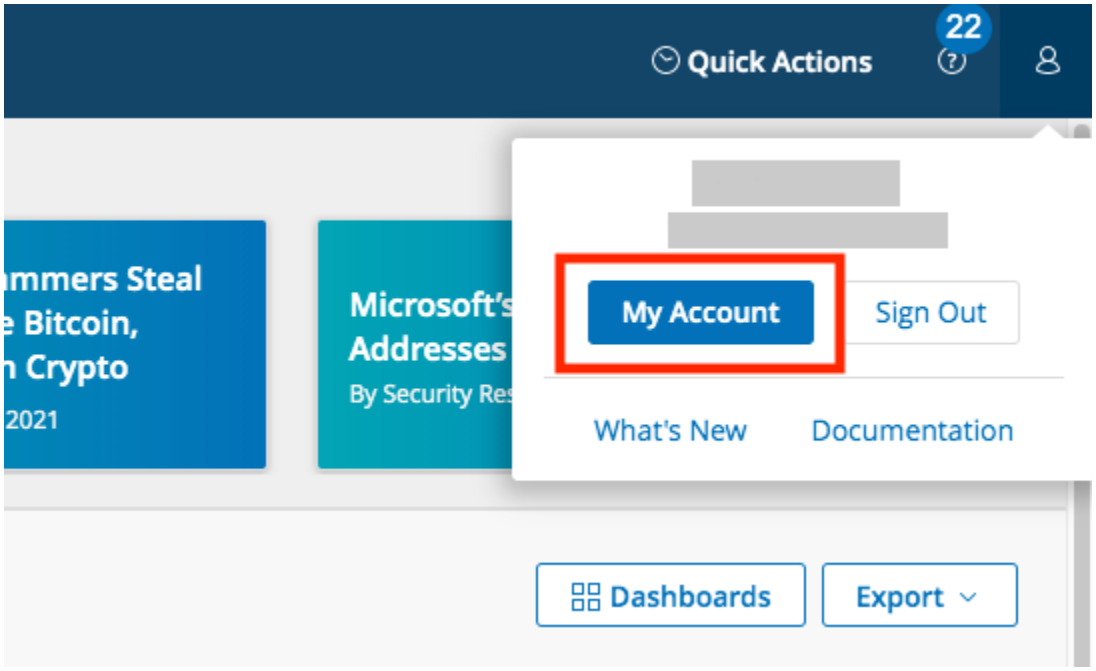
- Tenable 内の管理者ユーザー・ロールを持つユーザー
- 「すべてのアセット」を「表示可能」に設定します。詳しくは、Tenable の権限を参照してください。

ユーザーの API キーを生成するには、以下の手順を実行します。

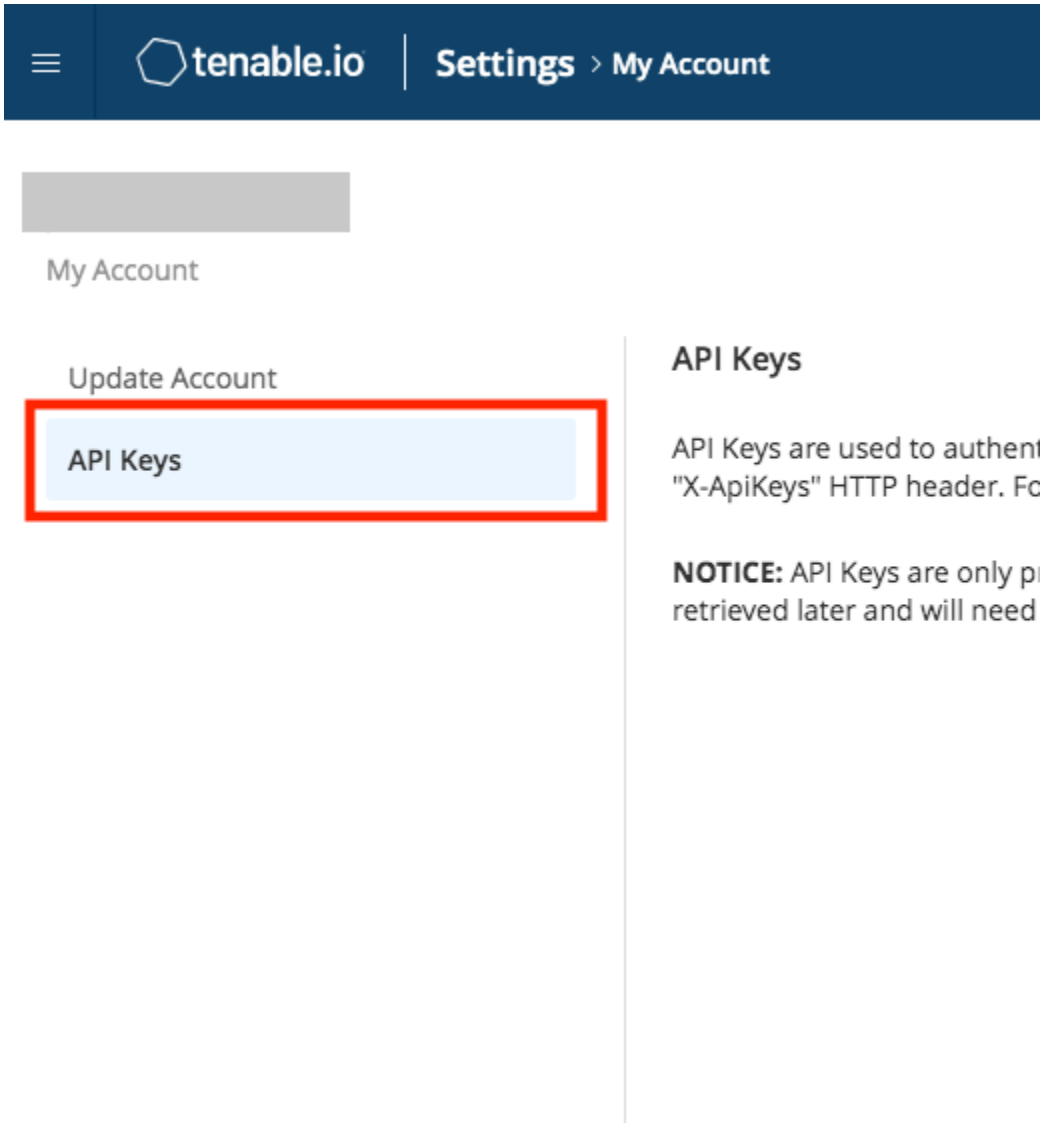
1. Tenable.io Web ユーザー・インターフェースで、ヘッダーの右上隅にあるボタンをクリックします。



2. 「My account」ボタンをクリックします。ユーザー・アカウント・メニューが表示されます。

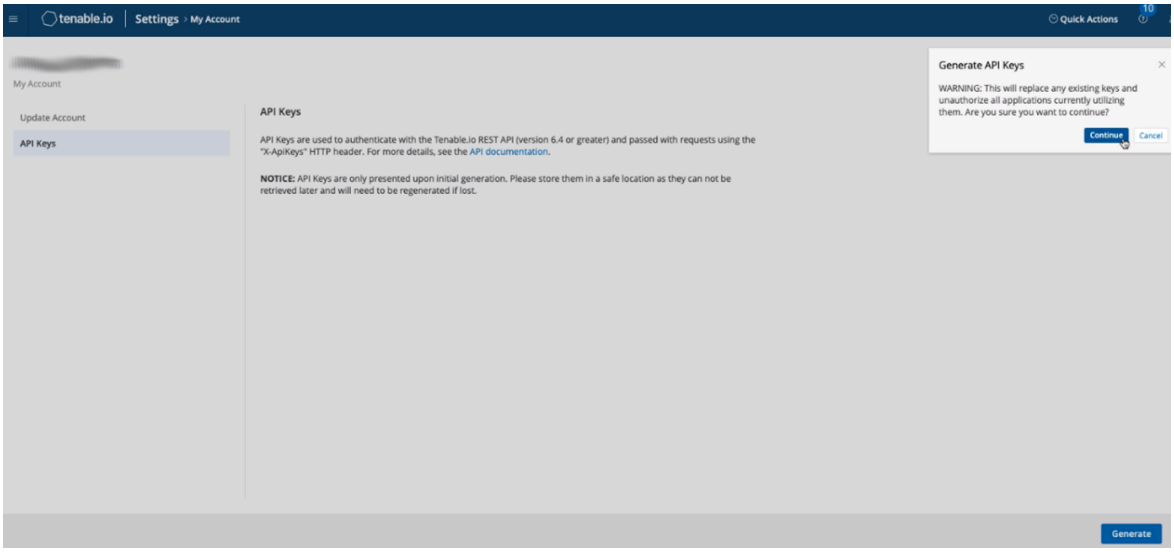


3. 左側のナビゲーションから「API Keys」を選択します。

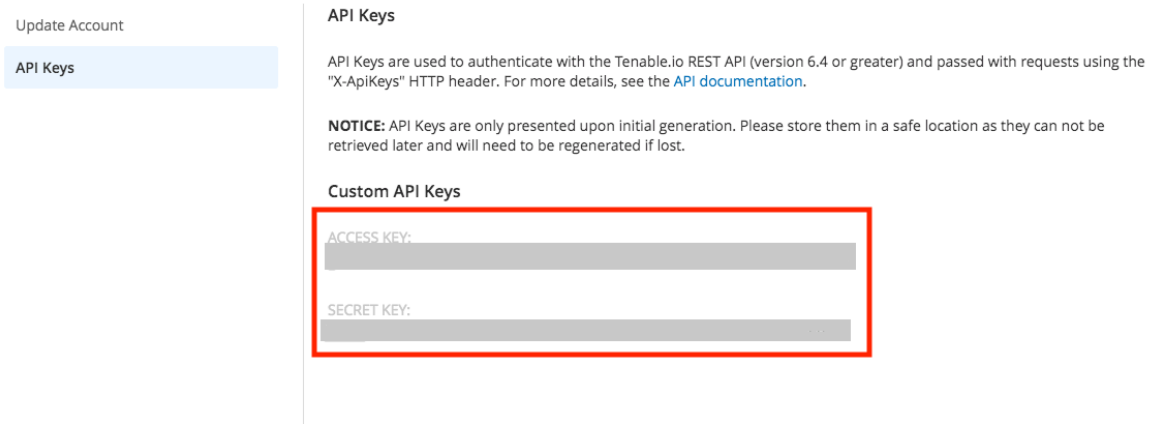


4. ブラウザーの右下にある「Generate」ボタンをクリックします。

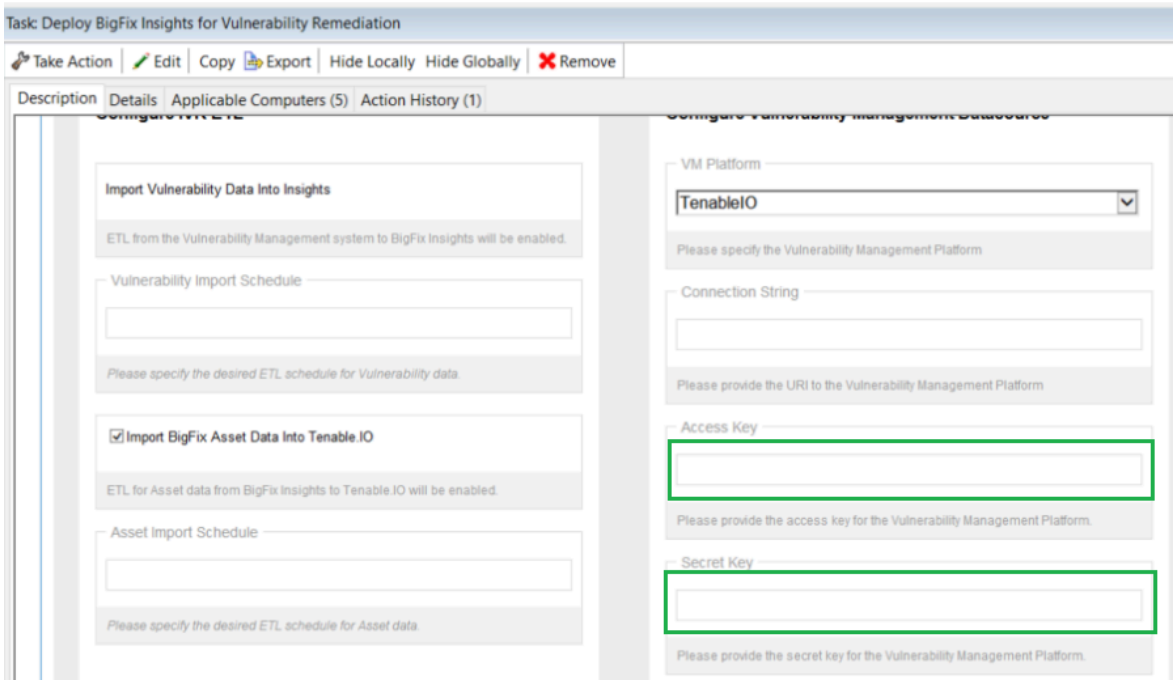
5. ポップアップ・ボックスで「Continue」をクリックして、警告を確認します。



6. Tenable.io によって、新しいアクセス・キーとシークレット・キーが生成されます。生成された 2 つのキーをコピーし、IVR 構成ページに貼り付け、インターフェースを有効にします。キーは **1** 回しか表示されないため、アクセス・キーとシークレット・キーは安全な場所にコピーしておいてください。タブを閉じた後に、API キーを Tenable.io から取得することはできません。



API キー が生成されたら、デプロイメント・プロセスに進むことができます。Deployment Fixlet で、アクセス・キーと秘密鍵を指定する必要があります。



ユーザー・ロールと権限について詳しくは、次のページを参照してください。https://docs.tenable.com/tenableio/Content/Settings/UserRoles.htm

API キーが生成されると、次の curl コマンドを使用して API 資格情報を検証できます。

a. Vuln エクスポート UUID を取得します。

```
curl --request POST --url https://cloud.tenable.com/vulns/export --header "Accept: application/json" --header "Content-Type: application/json" --header "X-ApiKeys: accessKey=redactedaccesskey; secretKey=redactedsecretkey"
```

b. 指定された UUID の Vuln エクスポートの状況を取得します。

```
curl --request GET --url https://cloud.tenable.com/vulns/export/21a70c98-8e8d-4b64-b7e0-4c57a245126f/status --header "Accept: application/json" --header "Content-Type: application/json" --header "X-ApiKeys: accessKey=redactedaccesskey; secretKey=redactedsecretkey"
```

c. 指定された UUID の vuln データのチャンク 1 を取得します。

```
curl --request GET --url https://cloud.tenable.com/vulns/export/21a70c98-8e8d-4b64-b7e0-4c57a245126f/chunks/1 --header "Accept: application/octet-stream" --header "X-ApiKeys: accessKey=redactedaccesskey; secretKey=redactedsecretkey"
```

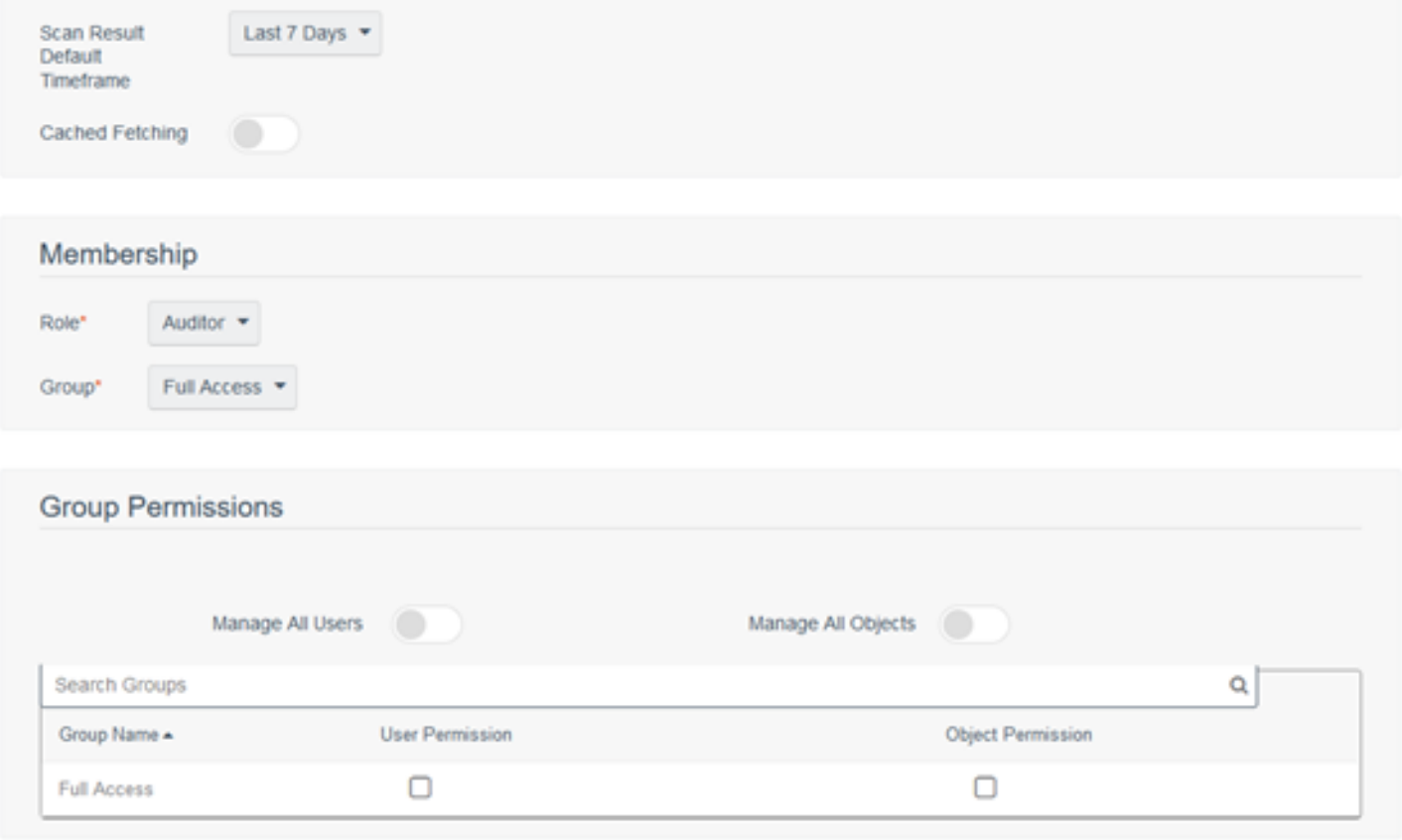
上のそれぞれの例では、「redactedaccesskey」と「redactedsecretkey」を、統合に使用されるものと同じ API キー/資格情報に置き換えます。また、API 呼び出し 2 と 3 については、要求 URL のサンプル UUID (21a70c98-8e8d-4b64-b7e0-4c57a245126f) を API 呼び出し 1 から返された UUID 値に置き換えます。

Tenable.sc の API 要件

IVR サーバーには Tenable ユーザー· アカウントが必要です。Tenable.sc IVR アダプターに使用されるユーザーには、環境内の互換性のあるマシンが必要です。

Tenable に使用される IVR アカウントには、デフォルトのフル· アクセス· グループと監査員のロール権限が割り当てられている必要があります。これにより、データ· フローを完了するために必要なアカウントアクセスが提供されます。さらに、カスタム· アクセス許可を使用してユーザーを定義すると、IVR によって取得されるアセットのスコープを制限できます。Tenable 内のグループは、表示可能なホストとリポジトリーの両方で制限できます。一般に、監査員のロールも利用して、最小権限の原則に従う必要があります。IVR データ· フローでは、アカウントに受信するための表示設定が付与されている場合にのみ、情報が取得されます。

次は、新規ユーザーが作成されたときの、「ユーザーの作成」ページの「メンバーシップ」セクションの様子を示しています。



Tenable の影響に関するステートメント

IVR は、pytenable ライブラリー (Tenable によって開発) を使用します。IVR は、デフォルトのバッチ・サイズ 1000 を利用します。これは、これまでのやり方にならったものであり、Tenable によって規定されています。デフォルト設定を使用する場合は、Tenable.sc アダプターの実行時に IVR サーバーに顕著な影響が出ないようにする必要があります。

Qualys の API 要件

Qualys API の要件

Qualys API は、サブスクリプション設定に基づいて、顧客が行うことができる API 呼び出しに制限を適用します。制限は、「セッション」V2 API (セッション・ログイン/ログアウト) を除くすべての Qualys API の使用に適用されます。デフォルトの API 制御設定は、サービスによって提供されます。これらの設定は、Qualys サポートによってサブスクリプションごとにカスタマイズされる場合があります。

詳細については、 次のリンクを参照してください。https://www.qualys.com/docs/qualys-api-limits.pdf。

API 呼び出しの数を見積もるには、次の式を使用します。

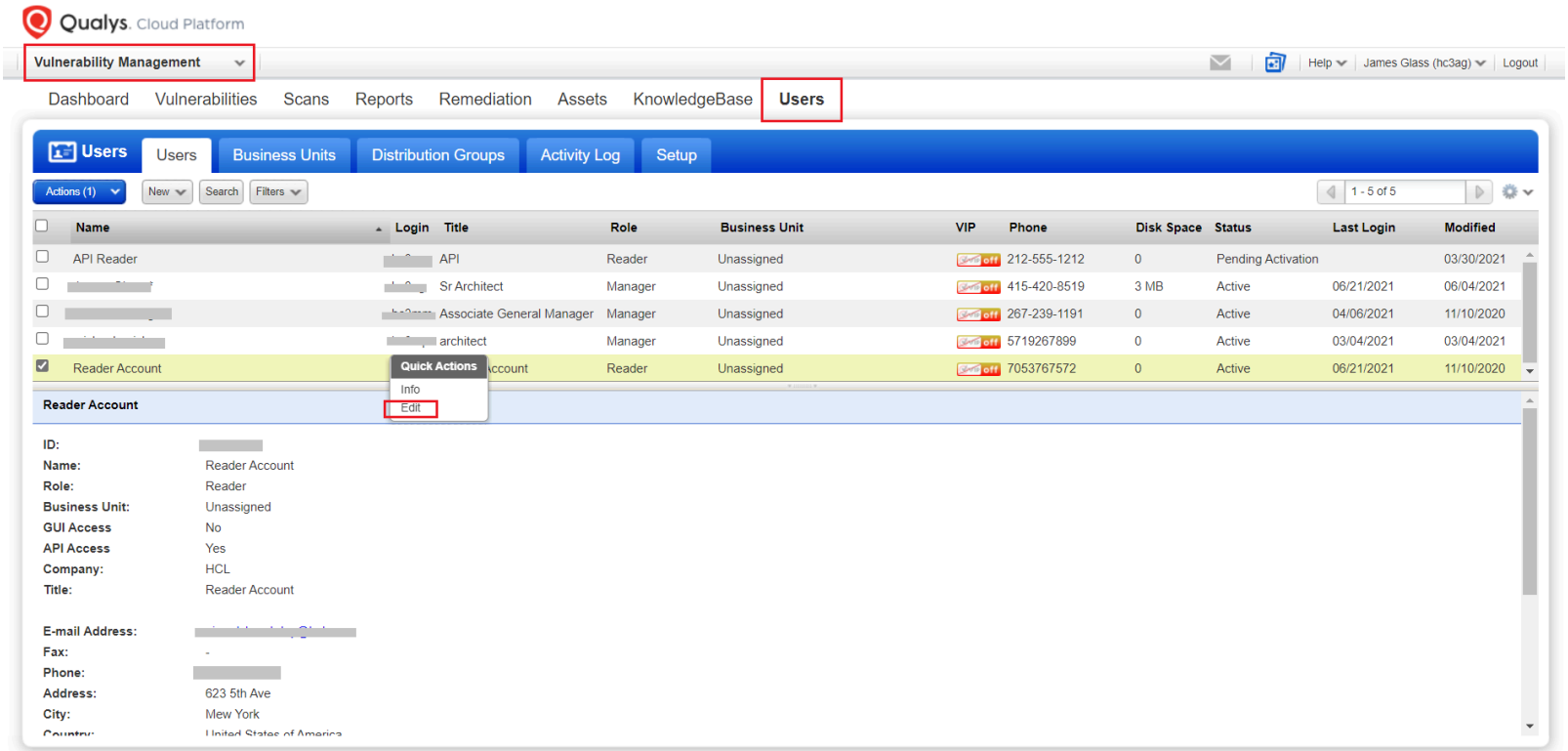
```
Total number of API calls = (number of devices / batch size ) + (number of unique vulnerabilities / 350)
```

ここで、

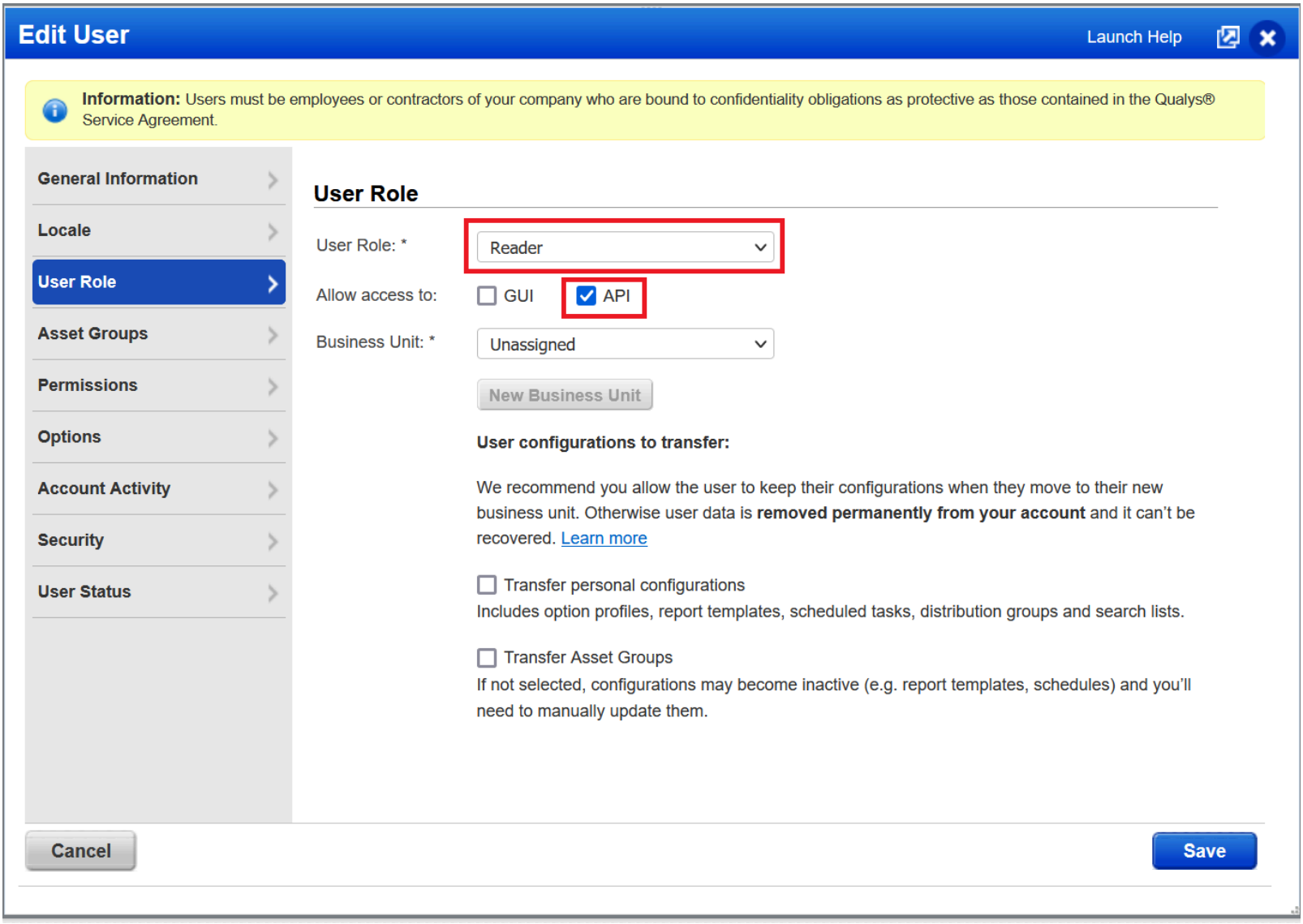
- `batch size` - 単一の API 呼び出しで取得できるデバイスの最大数を記述する構成可能パラメーター
- `number of devices` - スキャンされたネットワークで使用可能なデバイスの数
- `number of unique vulnerabilities` - スキャンされたネットワークで検出された固有の脆弱性の数
- `350` - 単一 API 呼び出しで Qualys 知識ベース API に取得できる脆弱性の最大数

Qualys API ユーザー要件

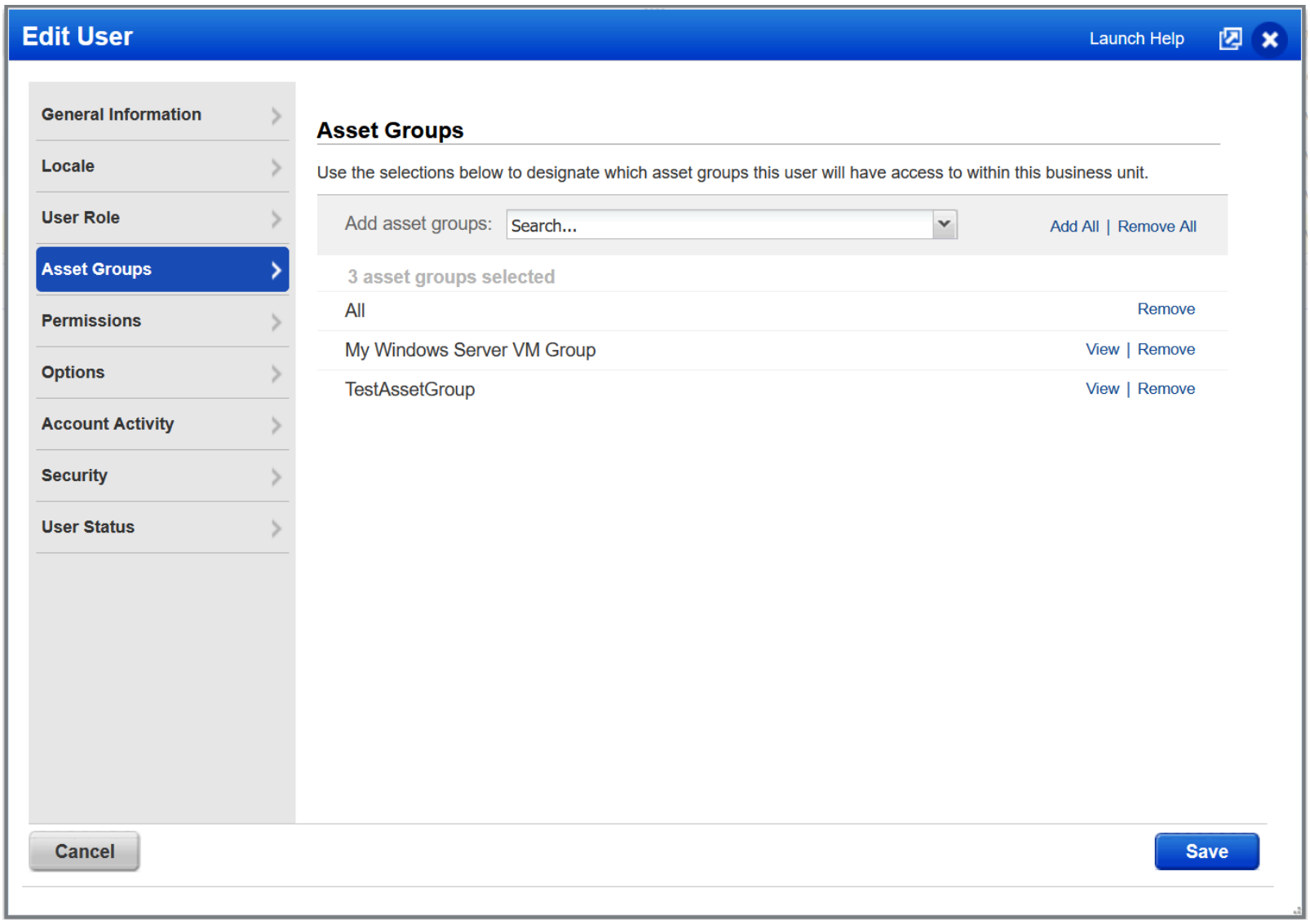
「読者」のユーザー・ロールを使用することをお勧めします。ユーザー・アカウントを編集するには、「脆弱性管理」ダッシュボードの「ユーザー」タブを選択します。「ログイン」にカーソルを置き、「編集」をクリックします。



「ユーザー・ロール」タブで、ユーザー・ロールに「読者」を選択し、「API へのアクセスを許可」を選択します。

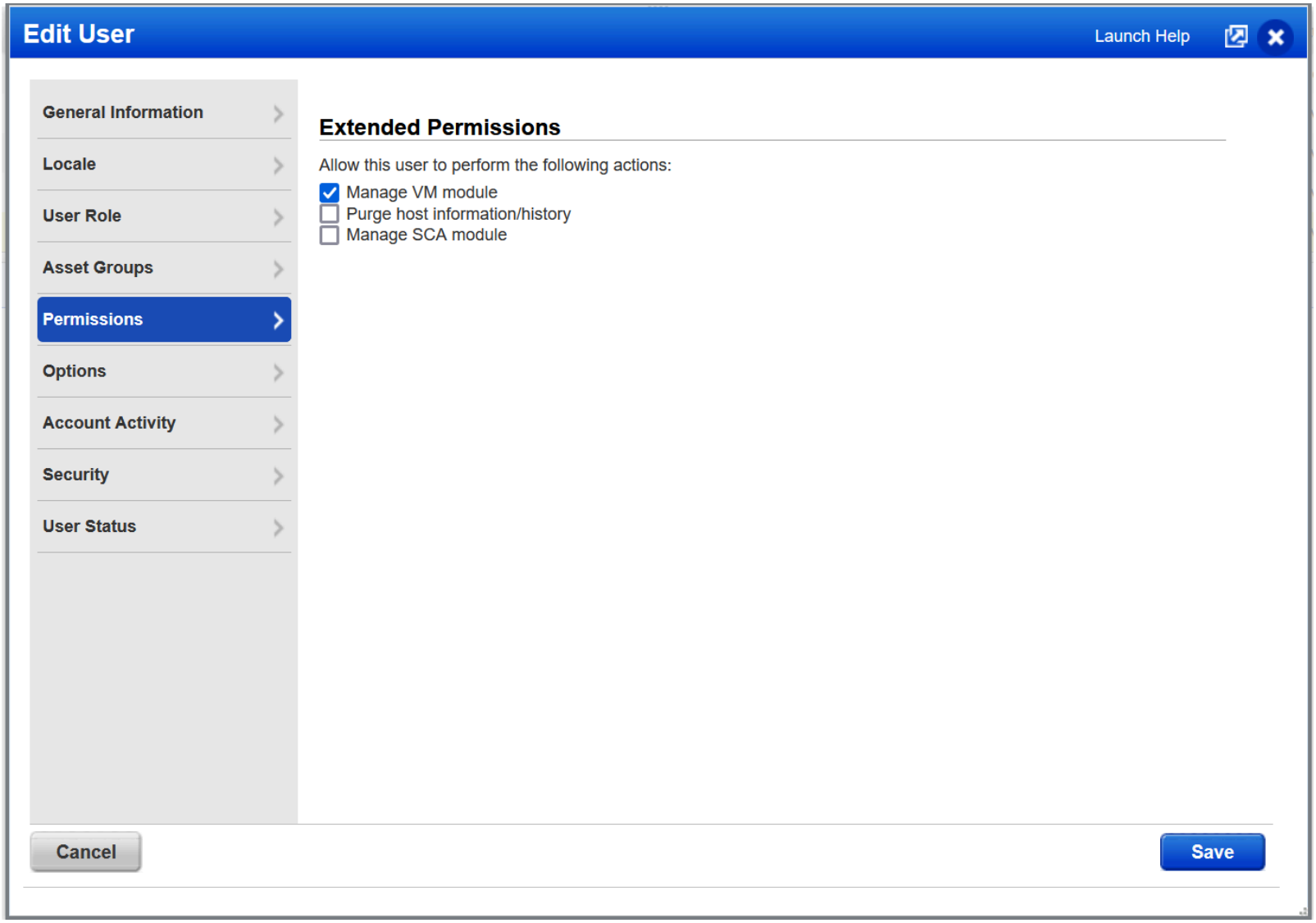


「アセット・グループ」タブでは、アクセス権を追加するアセット・グループを選択できます。



アセット・グループをユーザーに割り当てる方法について詳しくは、リンクを参照してください。

「権限」タブで、「VM モジュールの管理」を選択します。



ユーザー・ロールと権限の詳細については、リンクを参照してください。

第 3 章. デプロイメントと構成

このモジュールは、BigFix Insights for Vulnerability Remediation ソリューションを以下にデプロイして構成するためのステップを説明します。

Tenable.io

Tenable.sc

Qualys

BigFix Insights for Vulnerability Remediation ソリューションで使用可能な他の Fixlet とタスクについての詳細は、リンクを参照してください。

Tenable.io 向けのデプロイメントと構成

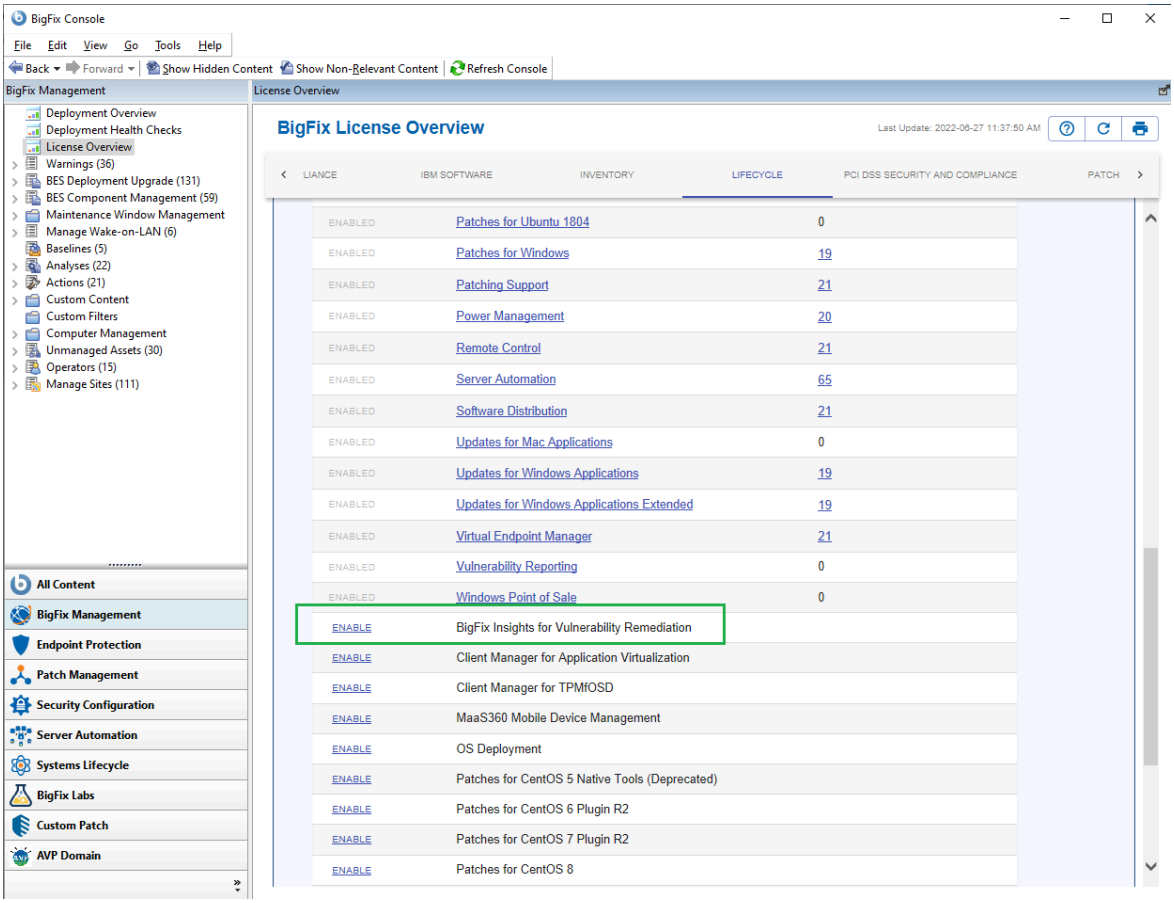
このモジュールでは、BigFix Insights for Vulnerability Remediation ソリューションをデプロイおよび構成するためのステップを示します。

BigFix Insights for Vulnerability Remediation サービスをインストールして構成するには、以下のステップを実行します。

注:
最新のリリース・ビルドを使用するには、旧バージョンをアンインストールします。

1. コンテンツ・サイトを有効にします。

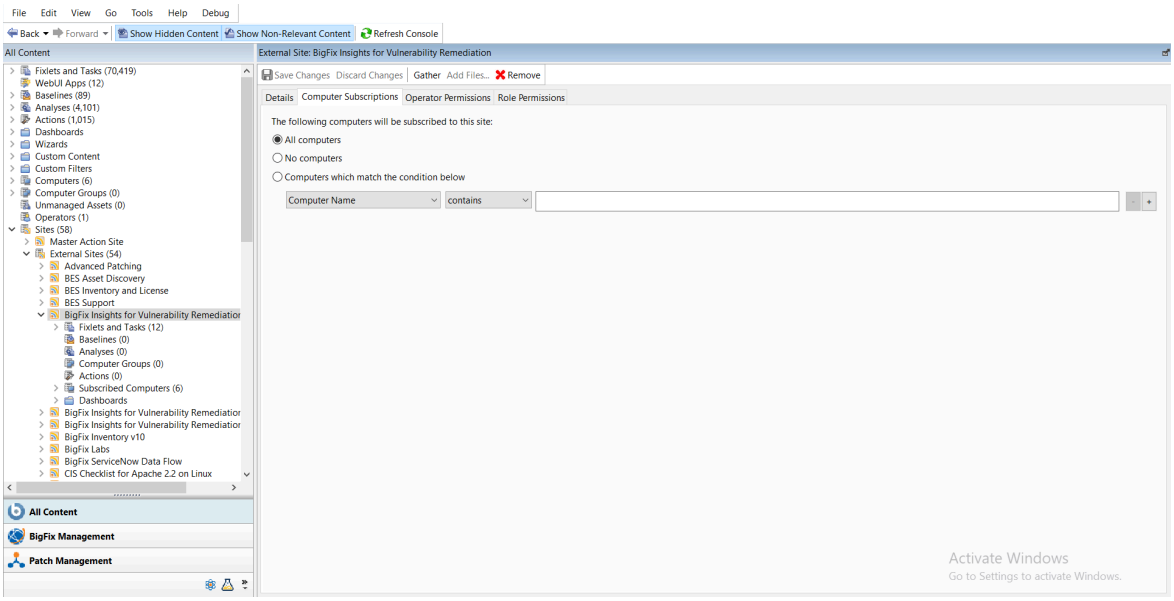
   「BigFix ライセンスの概要」ダッシュボードに移動します。「コンプライアンス/ライフサイクル」パネルで、「BigFix **Insights for Vulnerability Remediation** を有効にする」Fixlet を「クリック」して、必要なコンテンツを収集します。



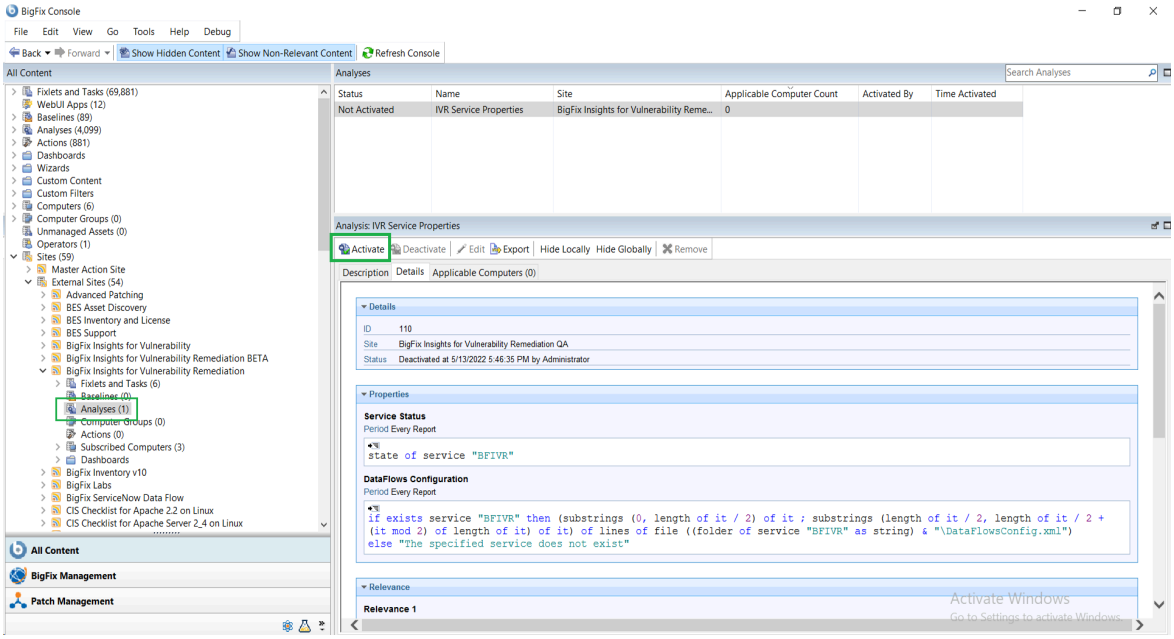
注:

「ライセンスの概要」ダッシュボードについて詳しくは、リンクを参照してください。

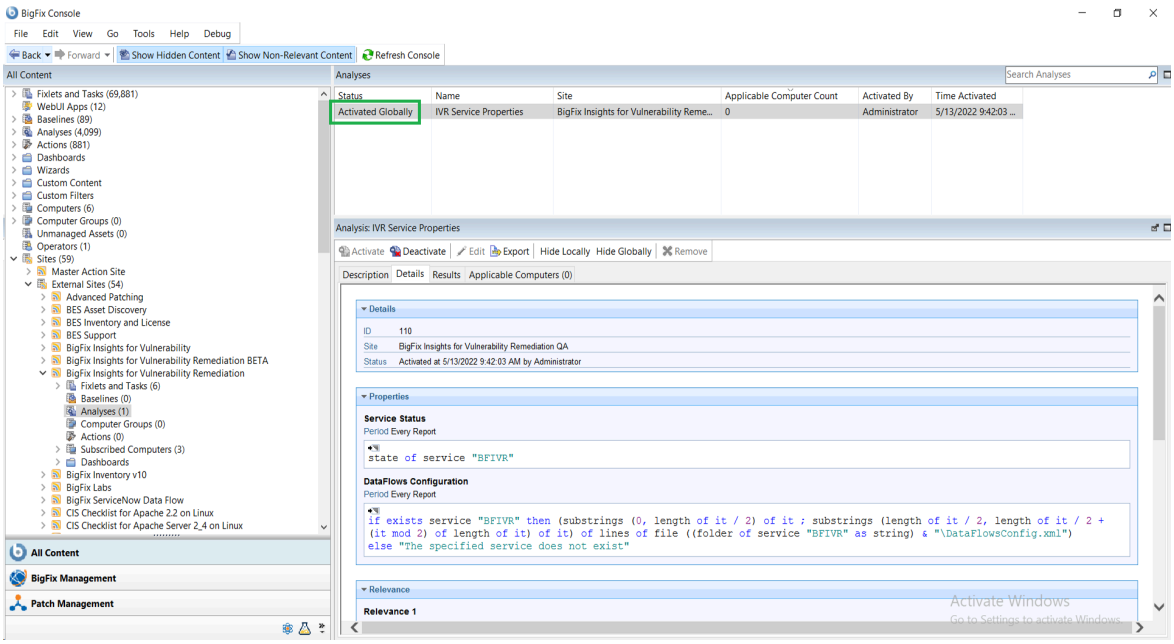
2. コンピューターをサイトにサブスクライブします。すべてのコンピューターにサブスクライブすることをお勧めします。「コンピューターのサブスクリプション」タブの詳細については、リンクを参照してください。



3. 分析をアクティブにします。



分析の状況は、「全体でアクティブ化済み」になる必要があります。



> 注:
> 「コンピューターのサブスクリプション」タブの詳細については、リンクを参照してください。

4. ソリューションをターゲット・サーバーにデプロイします。
    a. 「BigFix **Insights for Vulnerability** Remediation」外部サイトの「Insights **for Vulnerability Remediation** をデプロイ」Fixlet を「クリック」します。

    b. 説明パネルの空欄に必要な情報を入力し、「アクションの実行」で IVR サービスをデプロイします。

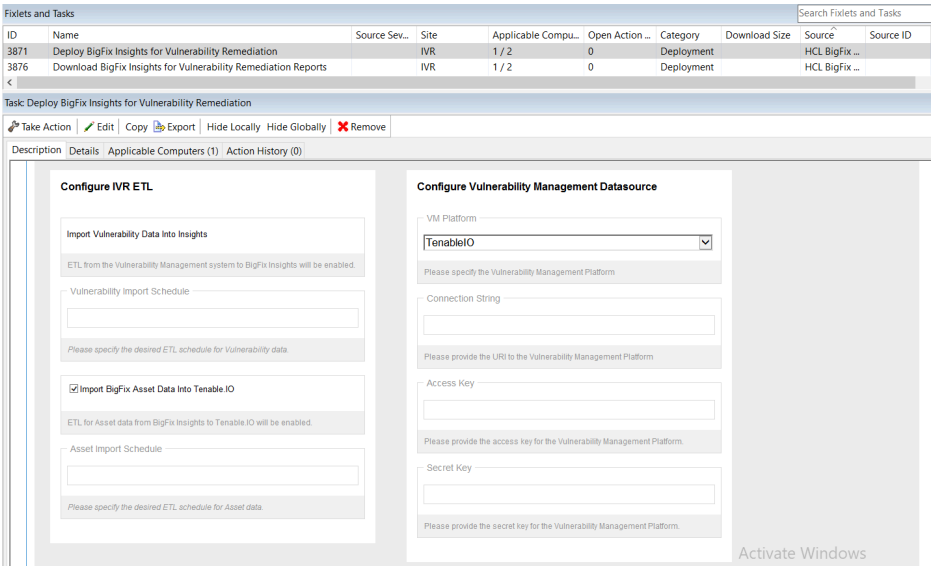
    以下を指定してください。
    - デプロイメントのオプション
        - インストール・パス
    - Insights データソースの構成
        - データベースのホスト名 - Insights データベースのホスト名、DNS 名、IP アドレス
        - データベース - データベース名
        - アカウント - BigFix Insights データベースのユーザー名
        - パスワード - 上で指定したユーザー名のパスワード
    - IVR ETL を構成

- 脆弱性データを Insights にインポート - 脆弱性データに必要な ETL スケジュールを指定します
- BigFix アセット・データを Tenable.IO にインポート - アセット・データに必要な ETL スケジュールを指定します*

  脆弱性データの ETL スケジュールでは、cron 時刻ストリング形式が使用されます。スケジューラーの詳細については、リンクを参照してください。

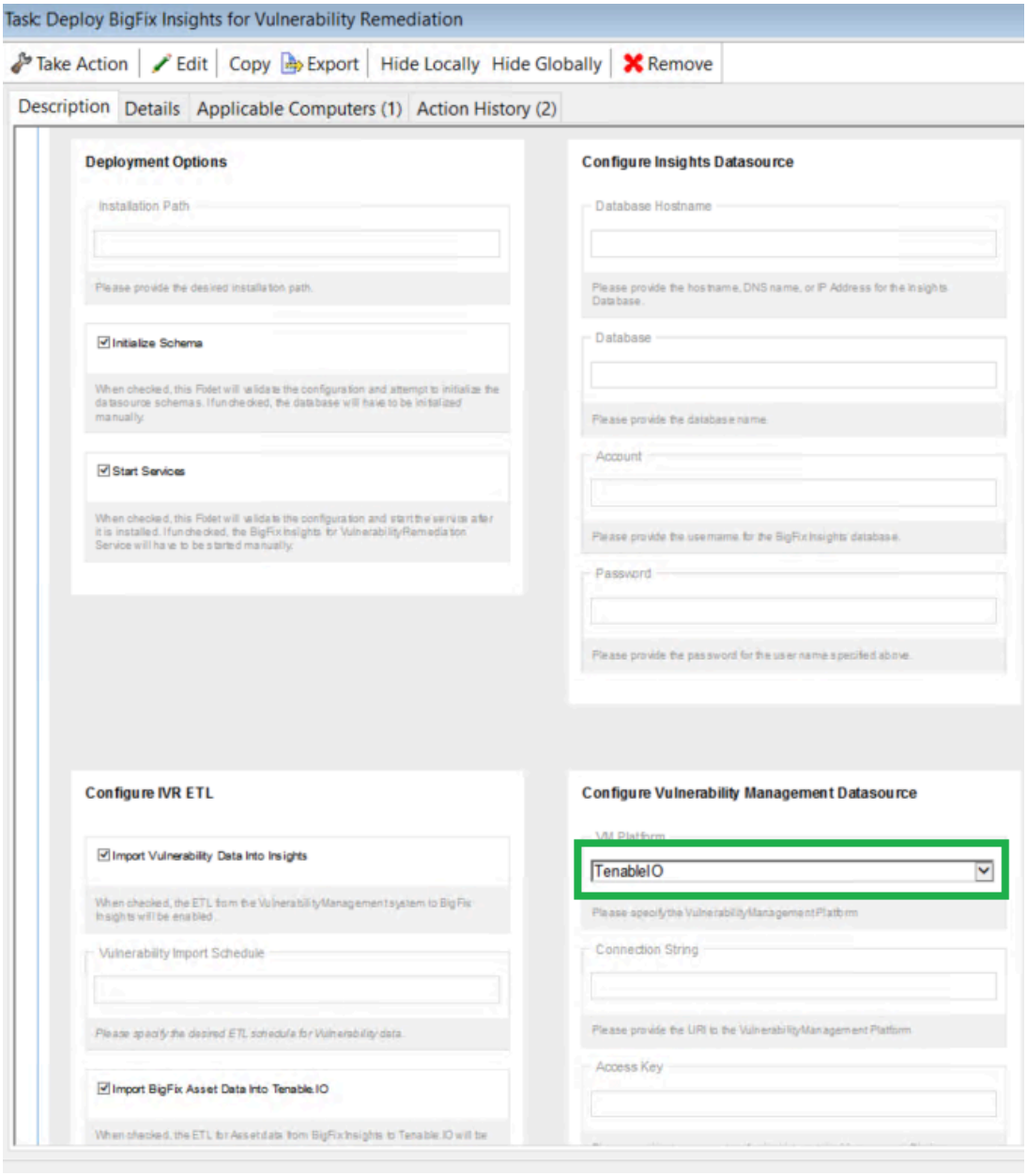
  BigFix Insight の dataource_device_id という名前の列は、IVR 目的のデバイス識別子の役割を果たします。この識別子は bigfix_asset_id とラベル付けされ、Tenable.IO に転送されます。

  *Tenable.IO は、BigFix IVR がエンドポイント資産データを Tenable.IO に送信できるオプション機能を提供します。これは潜在的に Tenable ユーザーが以前は知られていなかった資産に関する情報にアクセスできるようにします。資産のより包括的で最新のビューを提供することにより、Tenable.IO と BigFix は、潜在的なセキュリティー上のリスクの特定と軽減、十分に活用されていないリソースの特定、コンプライアンスの取り組みの促進に役立ちます。Tenable.IO の資産について詳しくは、以下のページhttps://docs.tenable.com/tenableio/Content/Platform/Explore/ExploreAssets.htmをご覧ください。

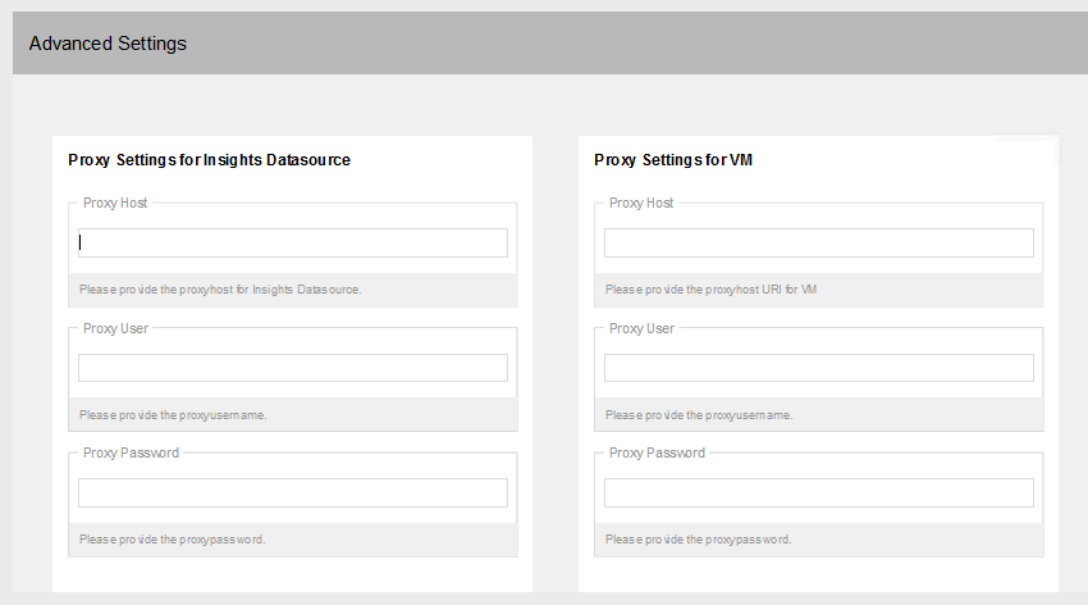


- 脆弱性管理データ・ソースを構成
  - VM プラットフォーム - VM プラットフォームを指定します
  - 接続ストリング - 脆弱性管理プラットフォームの URL

- アクセス・キー - 脆弱性管理プラットフォームのアクセス・キー
- 秘密鍵 - 上記で指定したユーザー名の秘密鍵



プロキシーの詳細を指定するには、「詳細設定」を「クリック」します。このオプションは必須ではありません。



注:
以下の前提条件に注意してください。

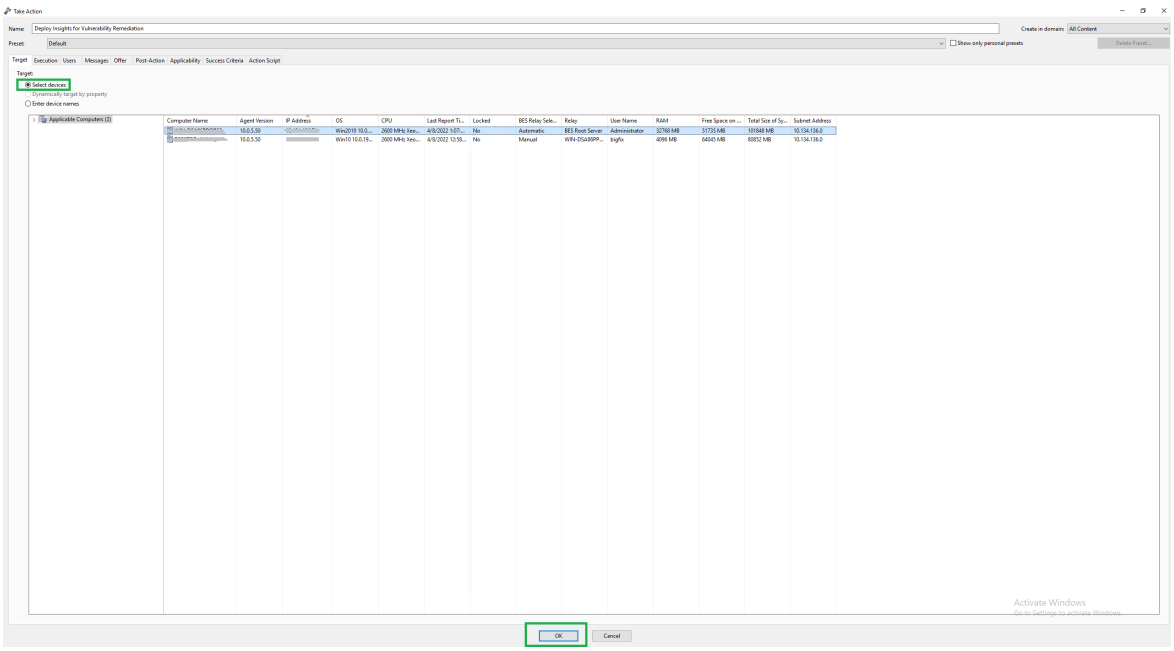
- Microsoft Visual Studio C++ 2012 再頒布可能パッケージ:https://www.microsoft.com/en-in/download/details.aspx?id=30679
- Microsoft ODBC Driver 17 for SQL Server: https://www.microsoft.com/en-us/download/details.aspx?id=56567
  - https://www.microsoft.com/en-us/download/details.aspx?id=56567

  Fixlet は前提条件のデプロイを自動的に試みます。

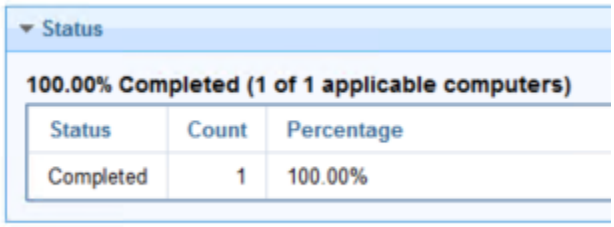
警告:
BigFix Insights for Vulnerability サービスは 1 台を超えるマシンにデプロイしないでください。

警告:
IVR サービスごとに 2 つを超えるデータフローを使用しないでください。

5. 「ターゲット」タブでターゲット・デバイスを選択し、「OK」をクリックします。



デプロイメントが完了するまで待機してください。状況には 100% 完了と表示されます。



6. 「説明」パネルで「サービスの開始」オプションが選択されている場合、 **BigFix Insights for Vulnerability Remediation** サービスが「サービス」に表示され、状態は「実行中」となります。選択していない場合は、**BigFix Insights for Vulnerability Remediation** サービスを手動で開始する必要があります。これは、デプロイメントが完了済みであることを示します。デプロイメントは、ログ・ファイル install.log でチェックできます。

   他の IVR タスクの詳細については、次のリンクを参照してください。

Tenable.sc 向けのデプロイメントと構成

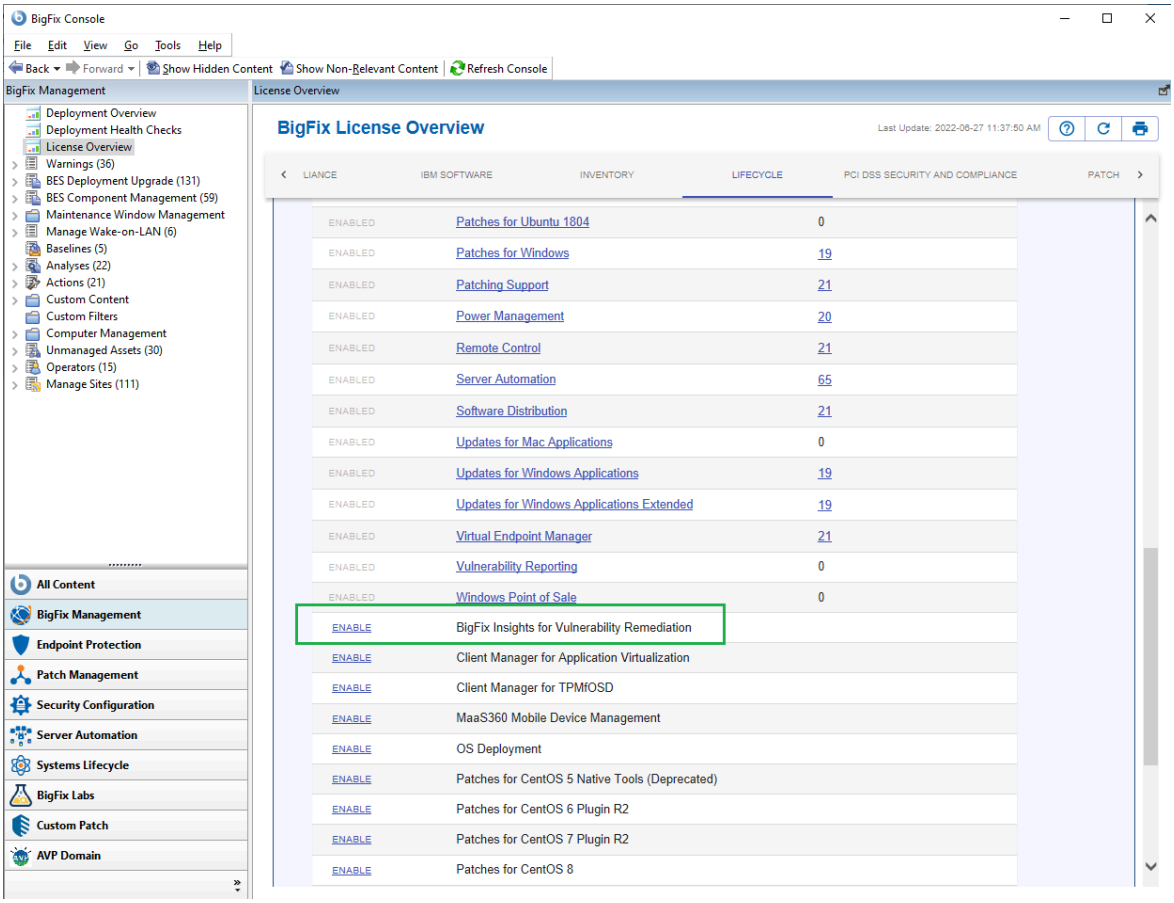
このモジュールでは、BigFix Insights for Vulnerability Remediation ソリューションをデプロイおよび構成するためのステップを示します。

BigFix Insights for Vulnerability Remediation サービスをインストールして構成するには、以下のステップを実行します。

注:
最新のリリース・ビルドを使用するには、古いバージョンをアンインストールする必要があります。

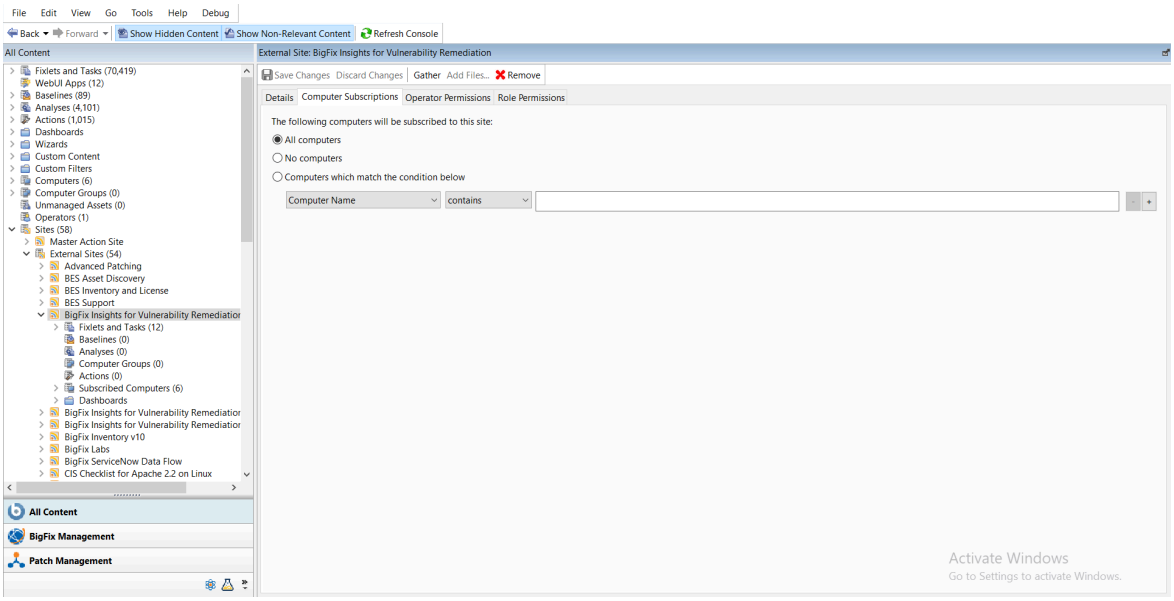
1. コンテンツ・サイトを有効にします。

   「BigFix ライセンスの概要」ダッシュボードに移動します。「コンプライアンス/ライフサイクル」パネルで、「BigFix **Insights for Vulnerability Remediation** を有効にする」Fixlet を「クリック」して、必要なコンテンツを収集します。

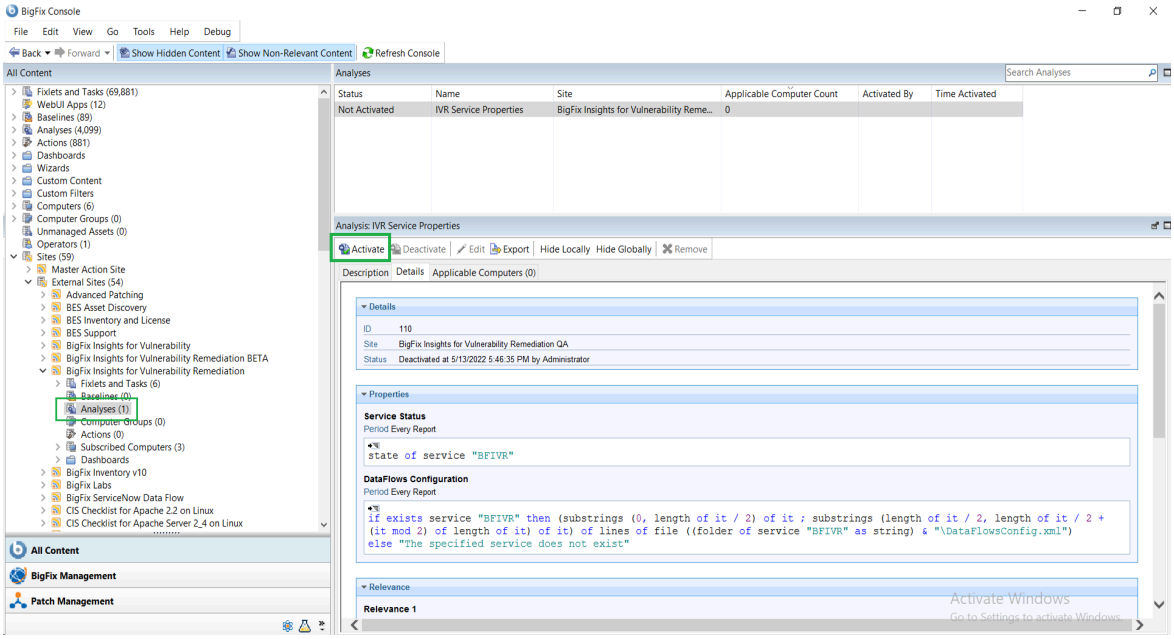


注:
「ライセンスの概要」ダッシュボードについて詳しくは、リンクを参照してください。

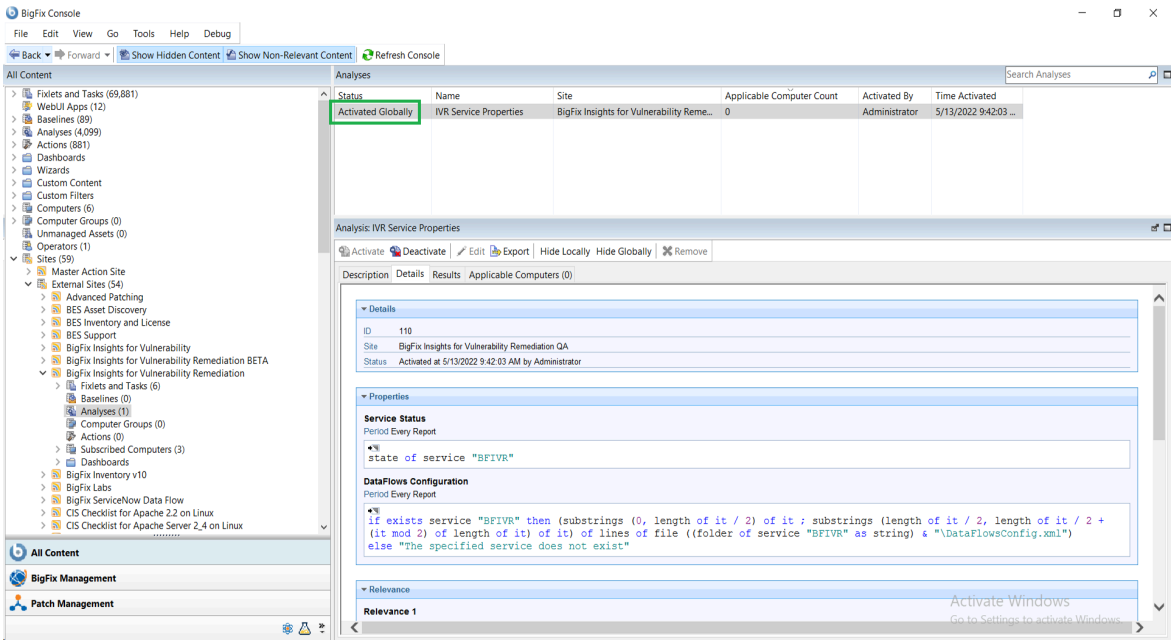
2. コンピューターをサイトにサブスクライブします。すべてのコンピューターにサブスクライブすることをお勧めします。「コンピューターのサブスクリプション」タブの詳細については、リンクを参照してください。



3. 分析をアクティブにします。



分析の状況は、「全体でアクティブ化済み」になる必要があります。



> 注:
> 「コンピューターのサブスクリプション」タブの詳細については、リンクを参照してください。

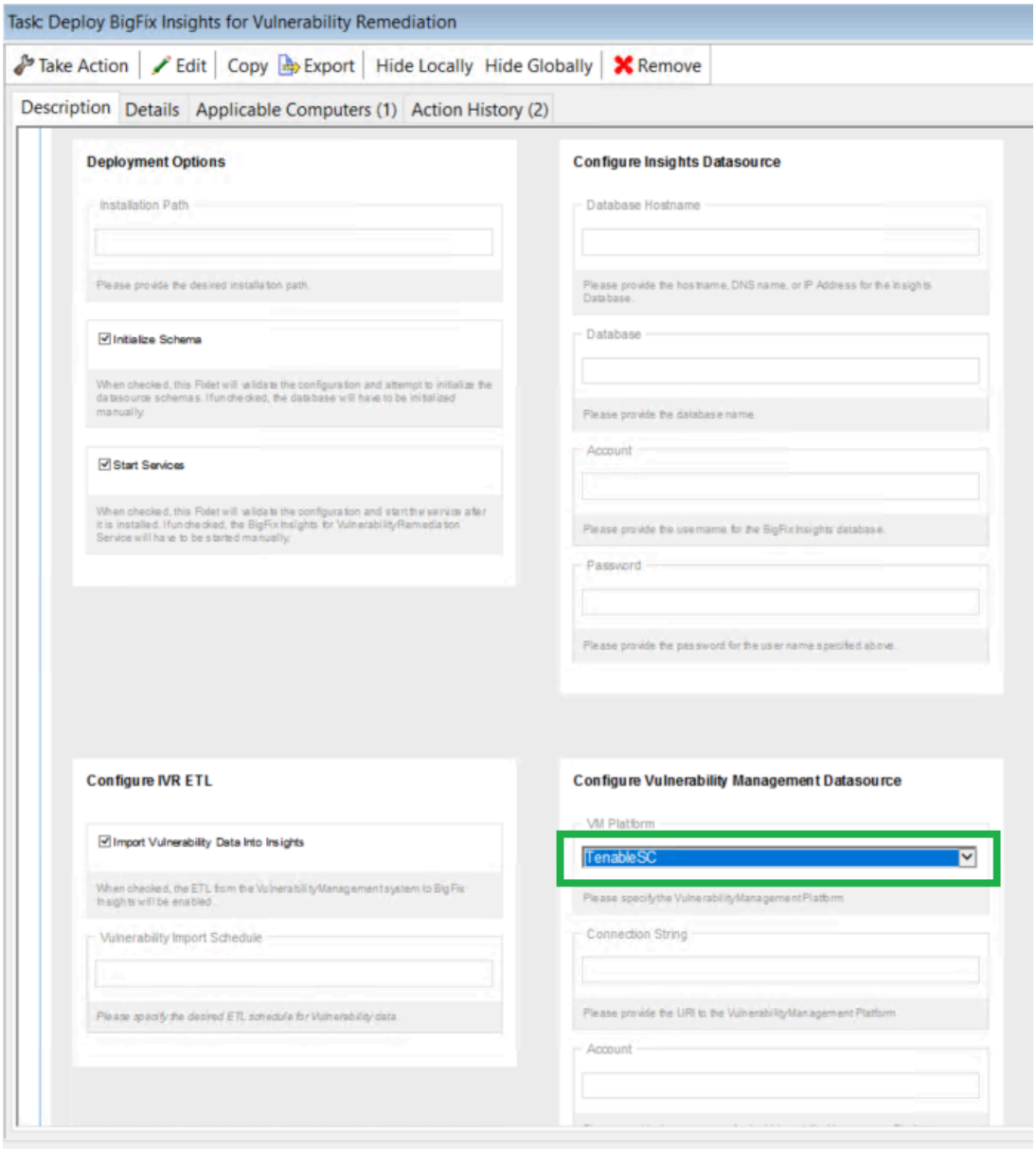
4. ソリューションをターゲット・サーバーにデプロイします。
    a. 「BigFix **Insights for Vulnerability** Remediation」外部サイトの「Insights **for Vulnerability Remediation** をデプロイ」Fixlet を「クリック」します。

    b. 説明パネルの空欄に必要な情報を入力し、「アクションの実行」で IVR サービスをデプロイします。

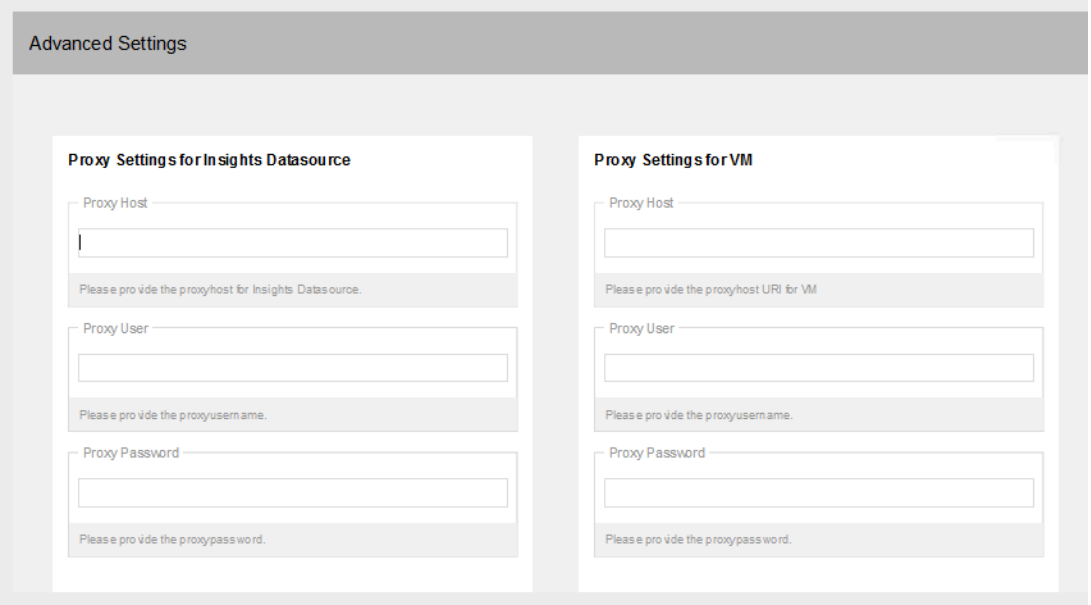
    以下を指定してください。
    - デプロイメントのオプション
        - インストール・パス
    - Insights データベースを構成
        - データベースのホスト名 - Insights データベースのホスト名、DNS 名、IP アドレス
        - データベース - データベース名
        - アカウント - BigFix Insights データベースのユーザー名
        - パスワード - 上で指定したユーザー名のパスワード
    - IVR ETL を構成

- 脆弱性インポート・スケジュール - 脆弱性データに必要な ETL スケジュールを指定します。脆弱性データの ETL スケジュールでは、cron 時刻ストリング形式が使用されます。スケジューラーの詳細については、リンクを参照してください。

- 脆弱性管理データ・ソースを構成
  - VM プラットフォームを指定
  - 接続ストリング - 脆弱性管理プラットフォームの URL
  - アカウント - 脆弱性管理プラットフォームのユーザー名
  - パスワード - 上で指定したユーザー名のパスワード



プロキシーの詳細を指定するには、「詳細設定」を「クリック」します。このオプションは必須ではありません。



注:
以下の前提条件に注意してください。

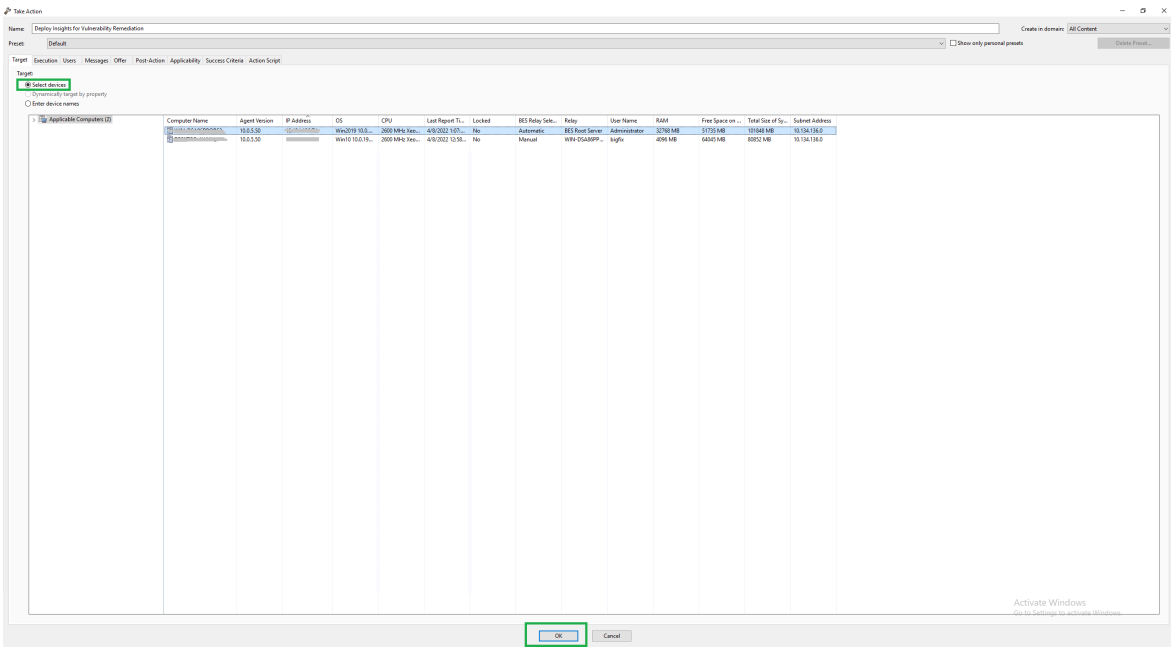
- Microsoft Visual Studio C++ 2012 再頒布可能パッケージ:https://www.microsoft.com/en-in/download/details.aspx?id=30679
- Microsoft ODBC Driver 17 for SQL Server: https://www.microsoft.com/en-us/download/details.aspx?id=56567
  - https://www.microsoft.com/en-us/download/details.aspx?id=56567

Fixlet は前提条件のデプロイを自動的に試みます。

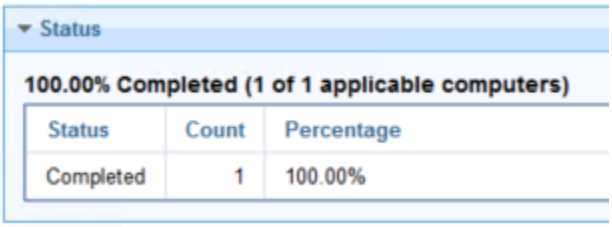
警告:
BigFix Insights for Vulnerability Remediation サービスは 1 台を超えるマシンにデプロイしないでください。

警告:
IVR サービスごとに 1 つを超えるデータ・フローを使用しないでください。

5. ターゲット・デバイスを選択し、「OK」をクリックします。



デプロイメントが完了するまで待機してください。状況には 100% 完了と表示されます。



6. 「説明」パネルで「サービスの開始」オプションが選択されている場合、 **BigFix Insights for Vulnerability Remediation** サービスが「サービス」に表示され、状態は「実行中」となります。選択していない場合は、**BigFix Insights for Vulnerability Remediation** サービスを手動で開始する必要があります。これは、デプロイメントが完了済みであることを示します。デプロイメントは、ログ・ファイル install.log でチェックできます。

   他の IVR タスクの詳細については、次のリンクを参照してください。

Qualys 向けのデプロイメントと構成

このモジュールでは、BigFix Insights for Vulnerability Remediation ソリューションをデプロイおよび構成するためのステップを示します。

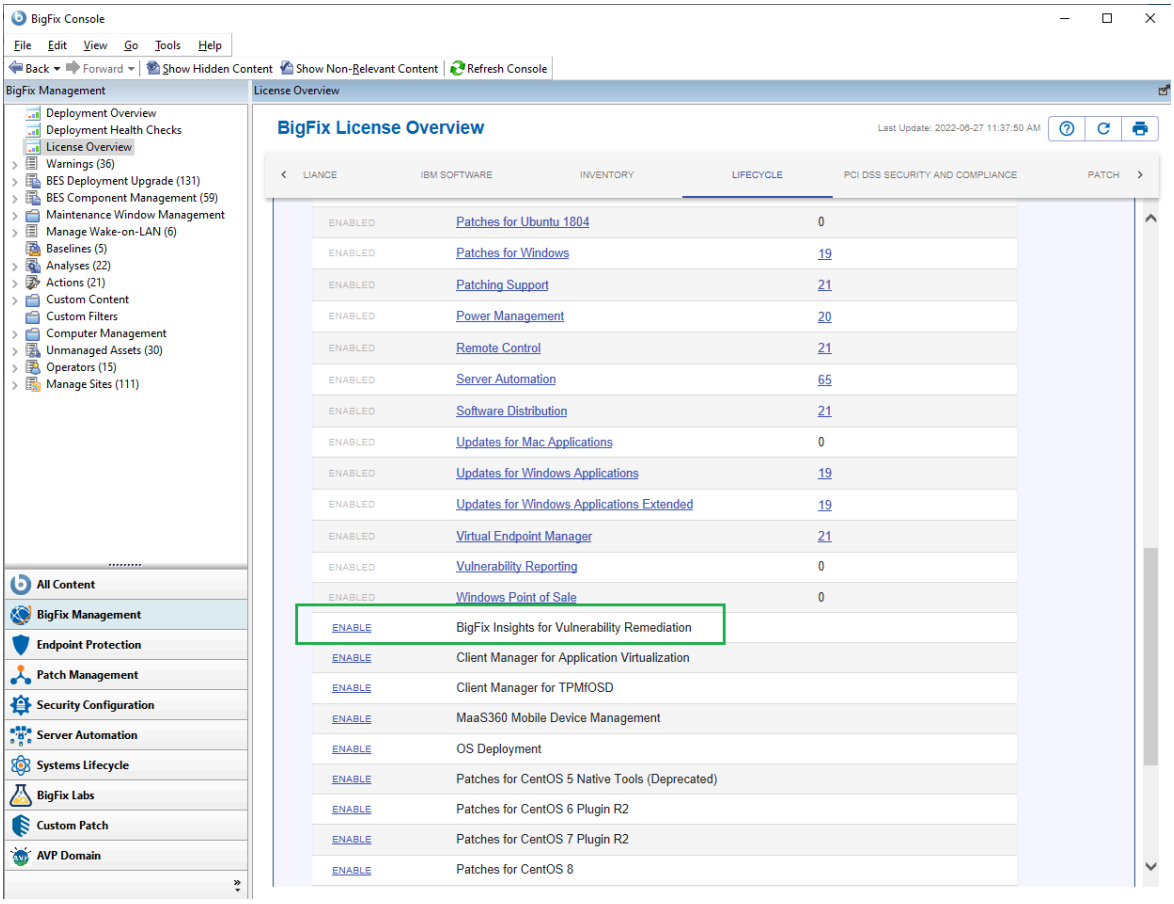
BigFix Insights for Vulnerability Remediation サービスをインストールして構成するには、以下のステップを実行します。

注:
最新のリリース・ビルドを使用するには、古いバージョンをアンインストールする必要があります。

注:
IVR を導入する前に、Qualys アカウントで API アクセスが許可されていることを確認します。詳しくは、「Qualys API のトラブルシューティング」を参照してください。

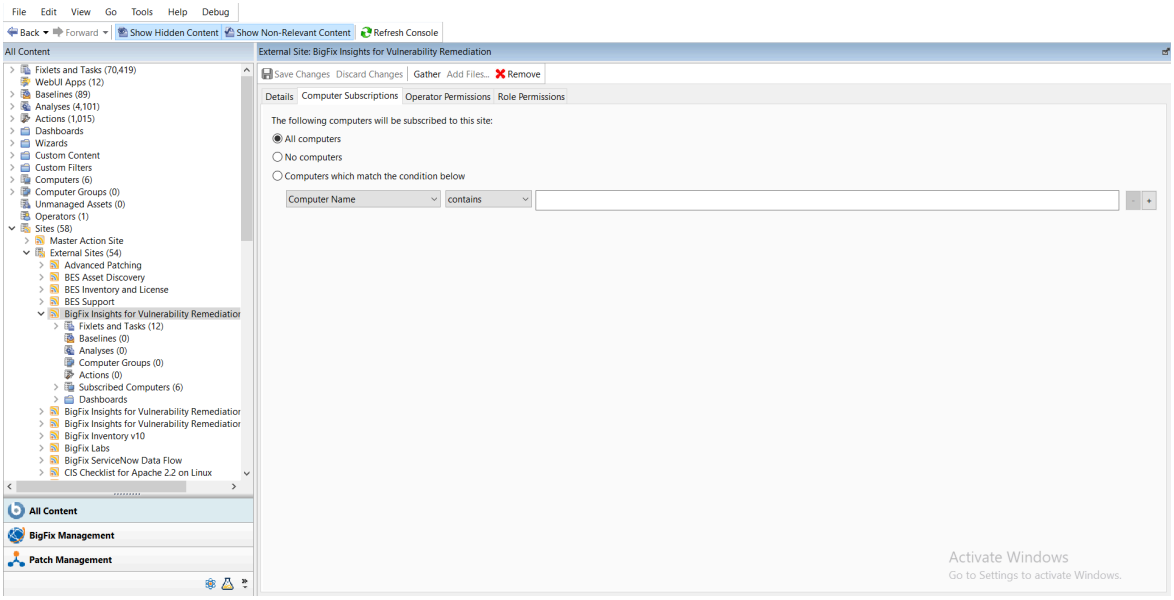
1. コンテンツ・サイトを有効にします。

「BigFix ライセンスの概要」ダッシュボードに移動します。「コンプライアンス/ライフサイクル」パネルで、「BigFix **Insights for Vulnerability Remediation** を有効にする」Fixlet を「クリック」して、必要なコンテンツを収集します。

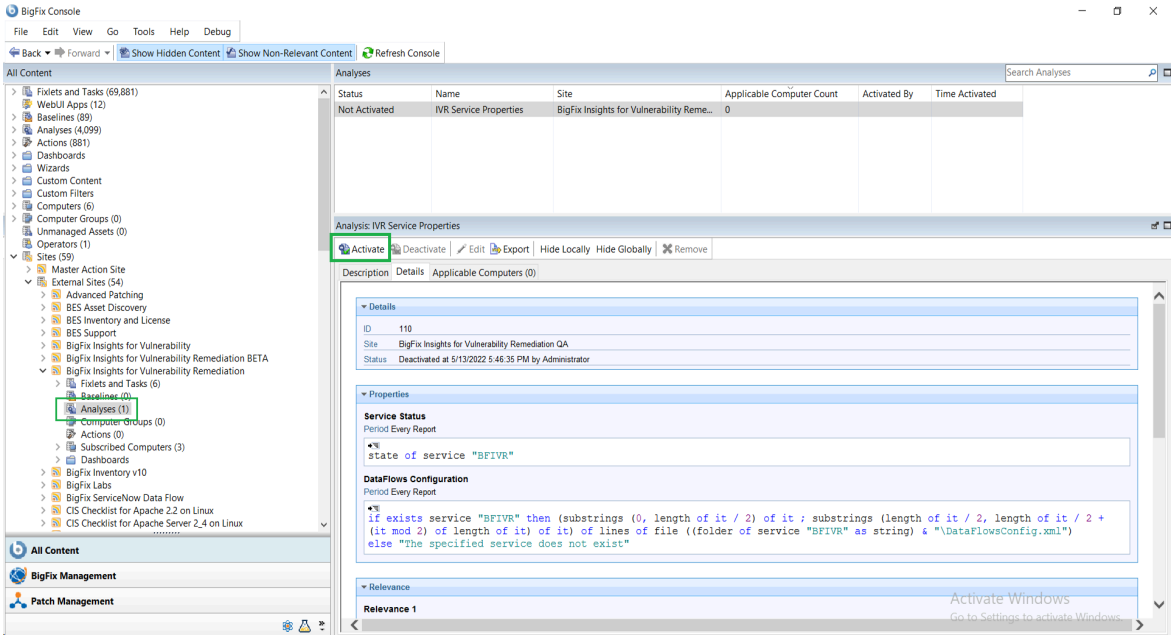


注:
「ライセンスの概要」ダッシュボードについて詳しくは、リンクを参照してください。

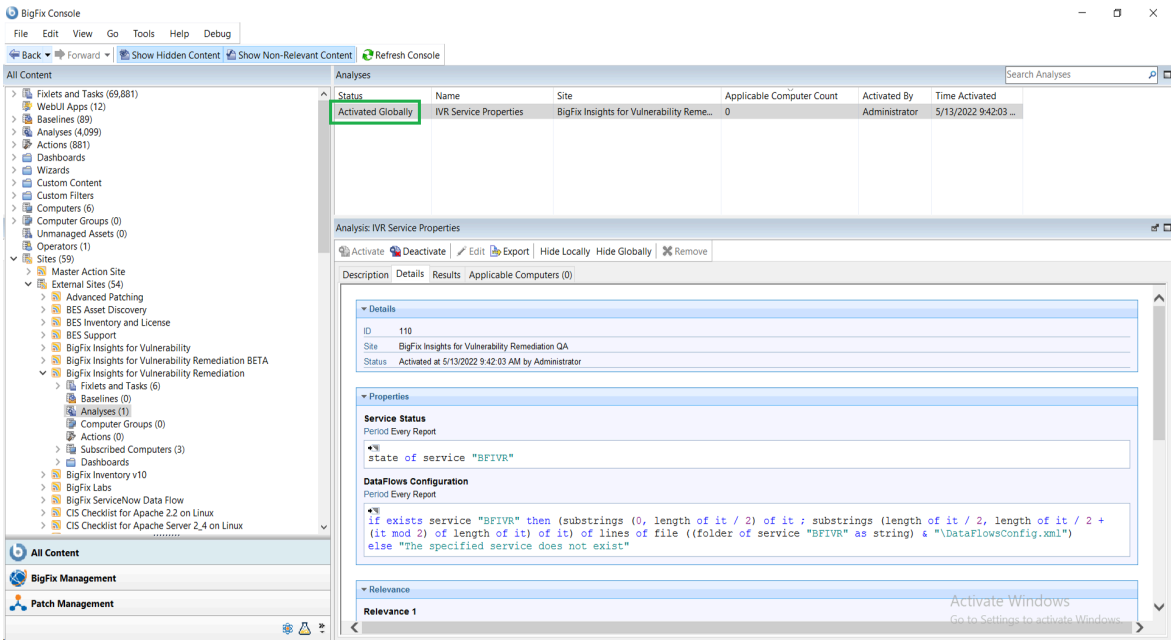
2. コンピューターをサイトにサブスクライブします。すべてのコンピューターにサブスクライブすることをお勧めします。「コンピューターのサブスクリプション」タブの詳細については、リンクを参照してください。



3. 分析をアクティブにします。



分析の状況は、「全体でアクティブ化済み」になる必要があります。



> 注:
> 「コンピューターのサブスクリプション」タブの詳細については、リンクを参照してください。

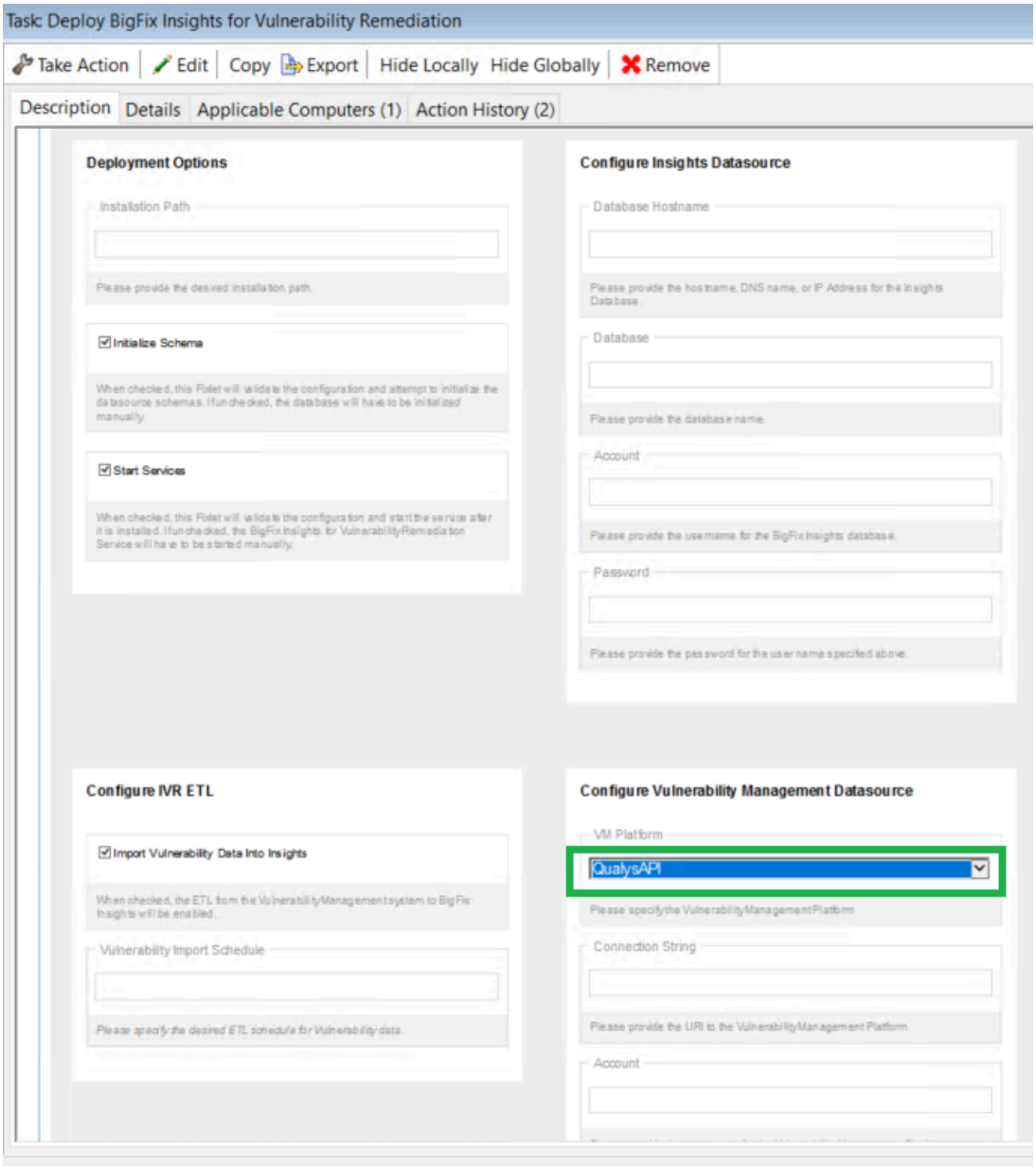
4. ソリューションをターゲット・サーバーにデプロイします。
    a. 「BigFix **Insights for Vulnerability** Remediation」外部サイトの「Insights **for Vulnerability Remediation** をデプロイ」Fixlet を「クリック」します。

    b. 説明パネルの空欄に必要な情報を入力し、「アクションの実行」で IVR サービスをデプロイします。

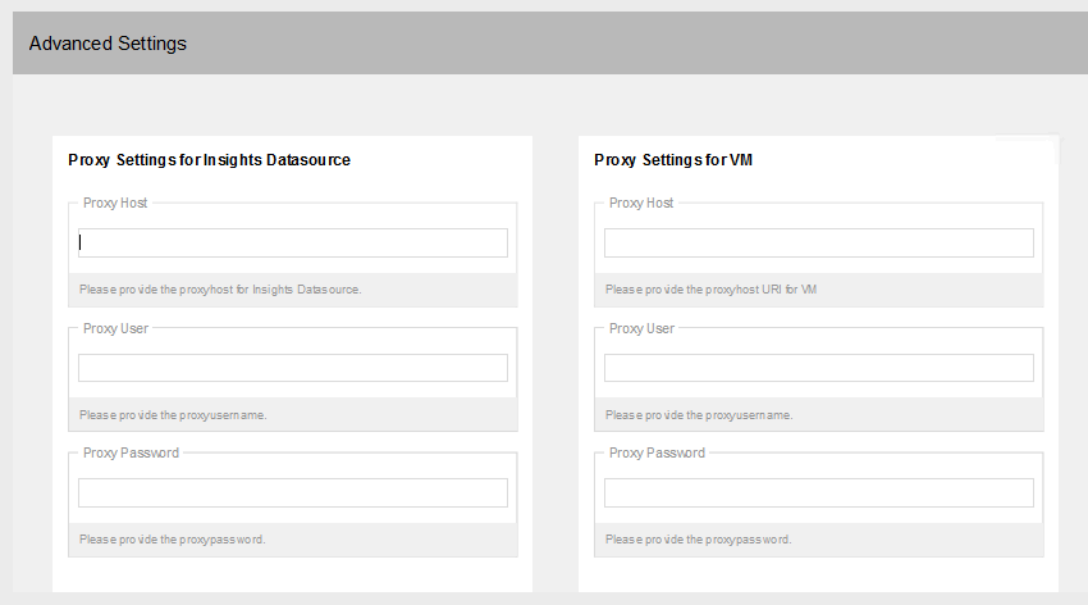
    以下を指定してください。
    - デプロイメントのオプション:
        - インストール・パス
    - Insights データベースを構成
        - データベースのホスト名 - Insights データベースのホスト名、DNS 名、IP アドレス
        - データベース - データベース名
        - アカウント - BigFix Insights データベースのユーザー名
        - パスワード - 上で指定したユーザー名のパスワード
    - IVR ETL を構成

- 脆弱性のインポート・スケジュール - 脆弱性データの ETL スケジュールでは、cron 時刻ストリング形式が使用されます。スケジューラーの詳細については、リンクを参照してください。

- 脆弱性管理データ・ソースを構成:
  - VM プラットフォームを指定
  - 接続ストリング - 脆弱性管理プラットフォームの URL
  - アカウント - 脆弱性管理プラットフォームのユーザー名
  - パスワード - 上で指定したユーザー名のパスワード



プロキシーの詳細を指定するには、「詳細設定」を「クリック」します。このオプションは必須ではありません。



注:

以下の前提条件に注意してください。

- Microsoft Visual Studio C++ 2012 再頒布可能パッケージ:https://www.microsoft.com/en-in/download/details.aspx?id=30679
- Microsoft ODBC Driver 17 for SQL Server: https://www.microsoft.com/en-us/download/details.aspx?id=56567
  - https://www.microsoft.com/en-us/download/details.aspx?id=56567

Fixlet は前提条件のデプロイを自動的に試みます。

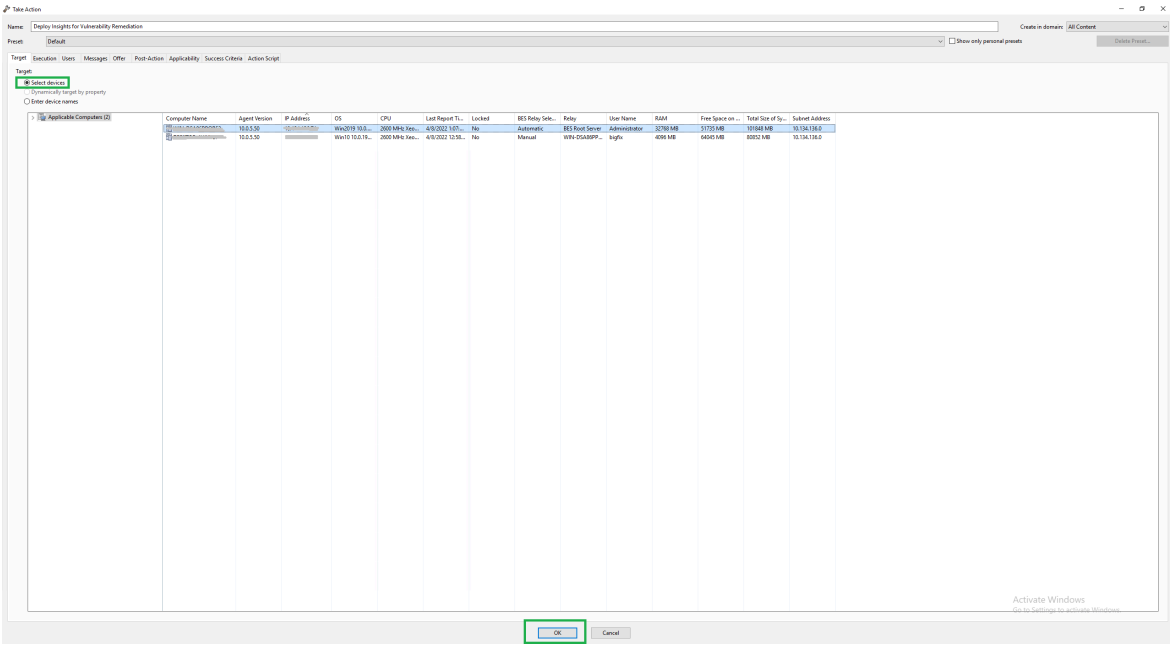
警告:

BigFix Insights for Vulnerability Remediation サービスは 1 台を超えるマシンにデプロイしないでください。

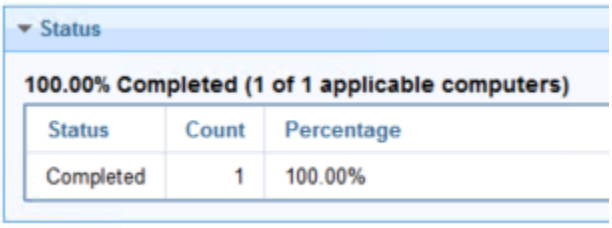
警告:

IVR サービスごとに 1 つを超えるデータ・フローを使用しないでください。

5. ターゲット・デバイスを選択し、「OK」を「クリック」します。デプロイメントが完了するまで待機してください。



状況には 100% 完了と表示されます。



6. 「説明」パネルで「サービスの開始」オプションが選択されている場合、 **BigFix Insights for Vulnerability Remediation** サービスが「サービス」に表示され、状態は「実行中」となります。選択していない場合は、**BigFix Insights for Vulnerability Remediation** サービスを手動で開始する必要があります。これは、デプロイメントが完了済みであることを示します。デプロイメントは、ログ・ファイル install.log でチェックできます。

他の IVR タスクの詳細については、次のリンクを参照してください。

第 4 章. IVR アプリケーションのセットアップ

このモジュールを使用し、WebUI IVR アプリケーションをインストールしてセットアップします。

WebUI IVR アプリケーションを完全に機能させるには、次のすべてのアクションが実行されていることを確認します。

1. **WebUI** をデプロイします。

   BigFixWebUI の資料を参照してください。この資料には、*BigFix WebUI* のインストール、保守、使用の方法が記載されています。

2. **Insights** をデプロイします。

   BigFix Insights の資料を参照してください。この資料には、BigFix Insights のセットアップ方法が記載されています。

3. **IVR** サービスをデプロイして構成します。

   さまざまな脆弱性管理製品の BigFix Insights for Vulnerability Remediation ソリューションをデプロイおよび構成するには、IVR の資料を参照してください。

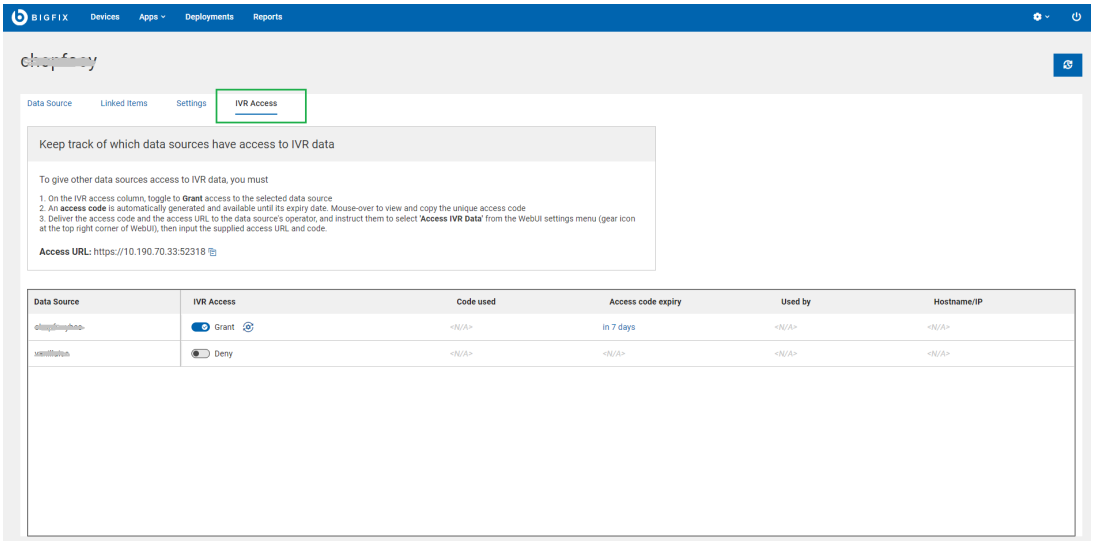
4. **ETL** を実行します。

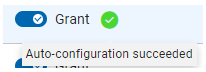
   a. Insights ETL の実行 - Insights ETL の実行方法については、Insights ETL の資料を参照してください。
   b. IVR データ・フローの実行 - IVR ETL の実行方法については、IVR データ・フローの資料を参照してください。

5. WebUI IVR アクセスを構成します。

   WebUI IVR の構成には、次の 2 つの方法があります。
   - プライマリー・データ・ソースとして

     BigFix Insights の初期セットアップが実行され次第。WebUI ナビゲーション・バーの 歯車アイコン をクリックし、「Insights」を選択してデータベースに接続し、「IVR データにアクセス」タブをクリックします。



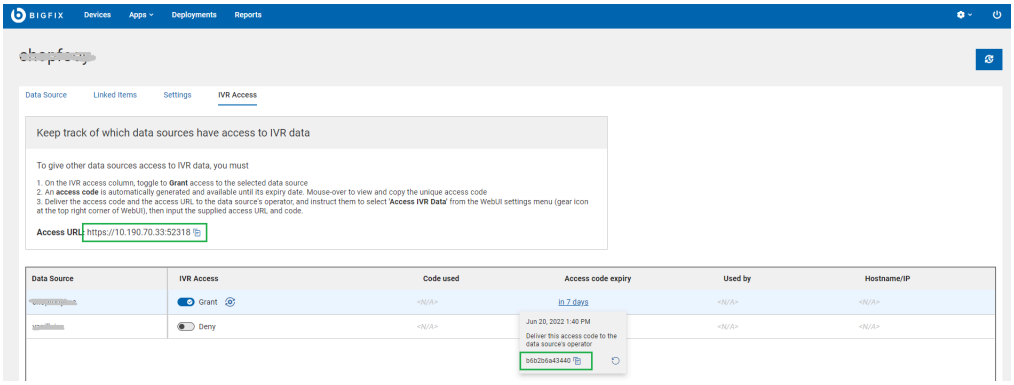
- 選択したデータ・ソースへのアクセスの「認可」に切り替えます。
-  をクリックすると、IVR が自動的に構成されます。完了すると、シンボルが 

に変更されます。

◦ セカンダリー・データ・ソースとして

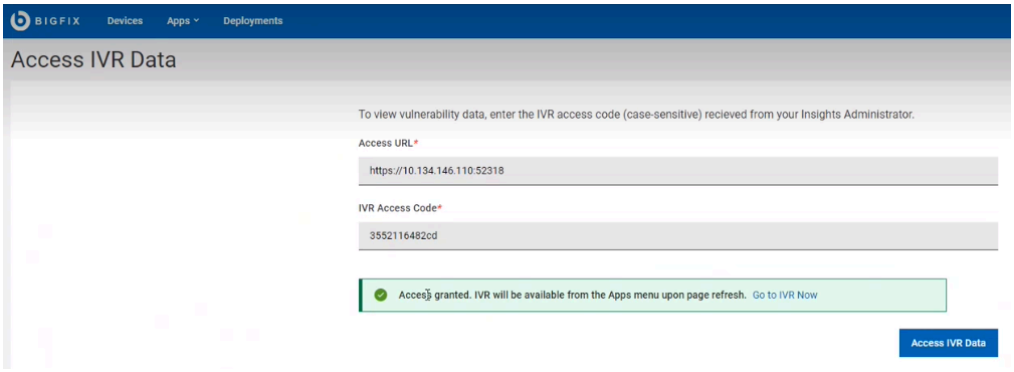
セカンダリー・データ・ソースとしてアクセスを構成するには、「IVR アクセス」タブで次のステップを実行します。

- 「IVR アクセス」列で、選択したデータソースへのアクセスの「認可」に切り替えます。
- アクセス・コードは自動的に生成され、有効期限が切れるまで使用可能になります。マウス・カーソルを置くと、固有のアクセス・コードを表示およびコピーできます。

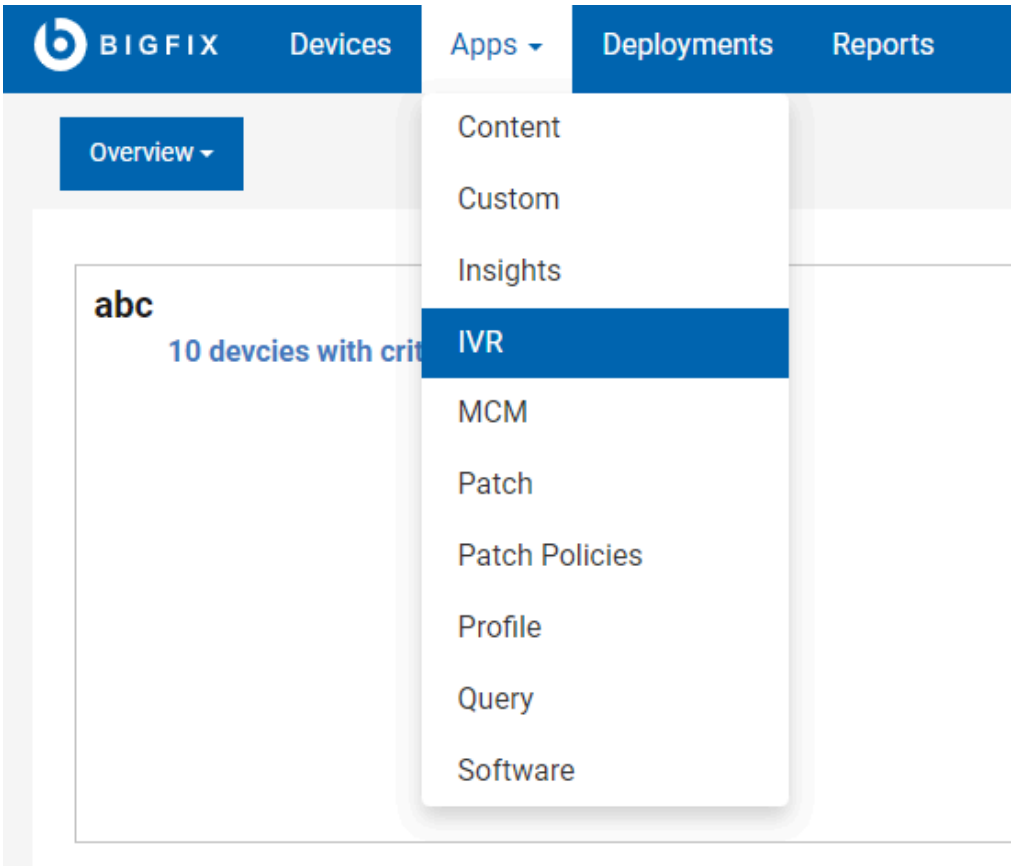


- アクセス・コードとアクセス URL をデータ・ソースのオペレーターに送信し、WebUI 設定メニュー (WebUI の右上隅歯車アイコン) から「IVR データにアク

セス」を選択し、提供されたアクセス URL およびコードを入力するように指示します。



- アクセスが認可されると、IVR アプリケーションが「WebUI アプリケーション」ドロップダウン・メニューに表示されます。



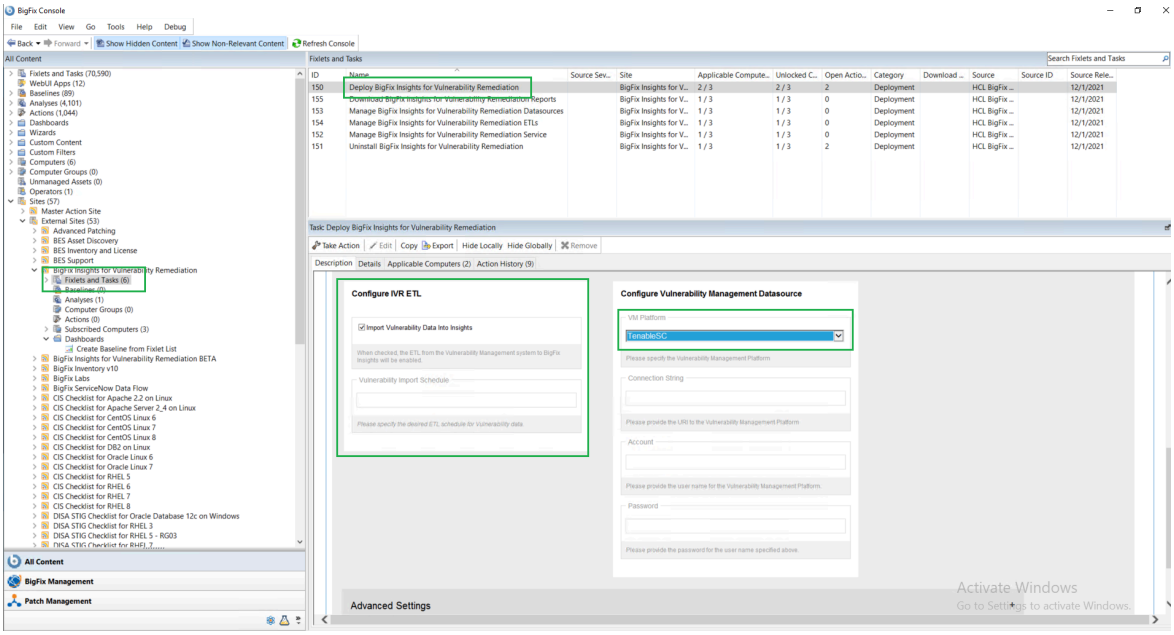
6. IVR アプリケーション・ユーザーズ・ガイド

第 5 章. IVR ETL のスケジュール

抽出、変換、読み込み (ETL) プロセスでは、データ・ソースからデータを抽出して、IVR のデータベースに保存します。ETL プロセスは時間とリソースを大幅に消費するため、カスタマイズしたスケジュールで実行して障害を最小限に抑える必要があります。IVR では、ETL の毎日、毎週、毎月のスケジュールを設定できます。

IVR で ETL をスケジュールするには、次のステップを実行します。

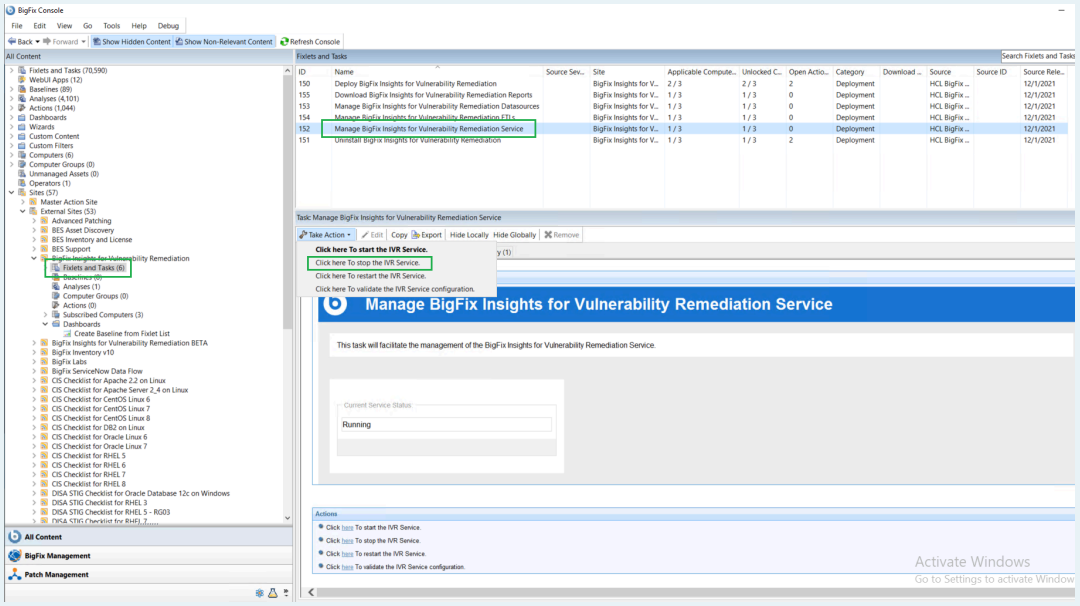
1. 最初の IVR ETL のスケジューリングは、デプロイメント中に行われます。IVR サービスのデプロイ方法と ETL の構成方法については、リンクを参照してください。



2. IVR サービスの初期構成が完了したら、「BigFix Insights for Vulnerability Remediation ETL の管理」Fixlet を使用して IVR ETL を構成できます。

注:

このタスクを実行するには、IVR サービスを停止する必要があります。サービスを停止するには、「BigFix Insights for Vulnerability Remediation Service の管理」Fixlet と、IVR サービスの停止の「アクションの実行」を使用します。



データ・フローが正常に完了したことを確認するには、 logs フォルダーに移動し、それぞれの dataflow_*.log ファイルを開きます。ファイルに次のメッセージがあるかどうかを確認します。

```
execute LogLevels.INFO DataFlow Execution Completed
```

```
2022-06-10 13:40:32.188547      22552   perform_aggregations    LogLevels.INFO  Executing Stored Procedure: ivr.PerformAggregates_VulnerabilityDiscrepan
2022-06-10 13:40:33.266659      22552   perform_aggregations    LogLevels.INFO  Aggregations Performed In: 0:00:04.421870
2022-06-10 13:40:33.266659      22552   execute_LogLevels.INFO  DataFlow Execution Completed In: 0:00:57.671877
2022-06-10 13:40:33.297909      22552   execute_ivrmetrics_sql_command  LogLevels.INFO  IVR_Metrics table inserted with execution details
```

第 6 章. IVR Fixlet とタスク

BigFix Insights for Vulnerability Remediation で使用可能な Fixlet とタスクについての詳細をご確認ください。

Insights for Vulnerability Remediation のデプロイ

BigFix Insights for Vulnerability Remediation レポートのダウンロード

BigFix Insights for Vulnerability Remediation データ・ソースの管理

BigFix Insights for Vulnerability Remediation ETL の管理

BigFix Insights for Vulnerability Remediation サービスの管理

BigFix Insights for Vulnerability Remediation のアンインストール

BigFix Insights for Vulnerability Remediation のアップグレード

BigFix Insights for Vulnerability Remediation のホワイトリスト・レポートのダウンロード URL

Insights for Vulnerability Remediation のデプロイ

Tenable.io

Tenable.sc

Qualys

BigFix Insights for Vulnerability Remediation レポートのダウンロード

このタスクを使用して、PowerBI または Tableau プラットフォームのレポートをデプロイします。

BigFix Insights for Vulnerability Remediation では、次の 3 つの主なユース・ケースに対処するためのビジネス・インテリジェンス・レポートを利用できます。

- 脆弱性 (使用可能な **Fixlet** あり) - 修復に使用できる、一致する BigFix Fixlet を持つ脆弱性のリスト。レポートには、各脆弱性に関連する最新の Fixlet と、脆弱性に関連付けられた CVE エントリーがリストされます。
- 脆弱性 (使用可能な **Fixlet** なし) - 修復に使用可能な Fixlet がない脆弱性のリスト
- 脆弱性の不一致 - スキャン・システムが問題を特定したが、BigFix では適用可能な修復が見つかっていない脆弱性のリスト。

レポート作成 Fixlet は動的ダウンロードを使用します。レポートをダウンロードするには、特定の URL が DownloadWhitelist.txt に追加されていることを確認します。

- Tenable.io
  - http://software.bigfix.com/download/ivr/1.4/Dashboards_PowerBI_Tenableio.tmp
  - http://software.bigfix.com/download/ivr/1.4/Dashboards_Tableau_Tenableio.tmp
- Tenable.sc
  - http://software.bigfix.com/download/ivr/1.4/Dashboards_PowerBI_Tenable.tmp
  - http://software.bigfix.com/download/ivr/1.4/Dashboards_Tableau_Tenable.tmp
- Qualys
  - http://software.bigfix.com/download/ivr/1.4/Dashboards_PowerBI_Qualys.tmp
  - http://software.bigfix.com/download/ivr/1.4/Dashboards_Tableau_Qualys.tmp

BigFix サーバー上のファイルの場所は、次のようになります。

```
C:\Program Files (x86)\BigFix Enterprise\BES Server\Mirror Server\Config
```

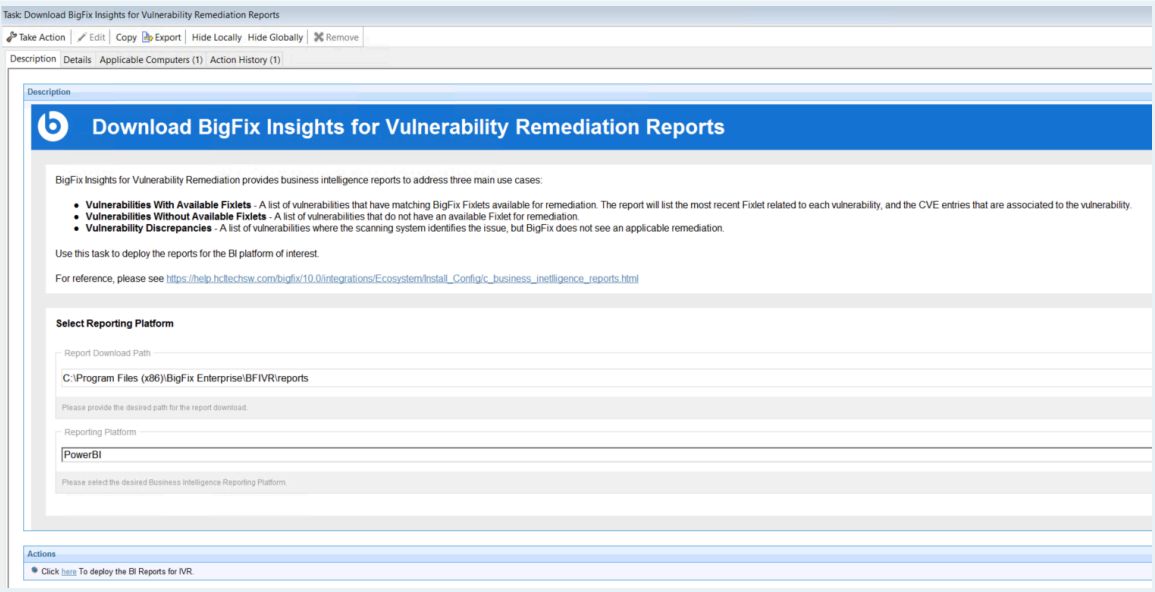
ファイルが存在しない場合は、同じ名前のファイルを新規に作成します。ファイルには、以下のようなファイル形式が含まれます。

http://127.0.0.1:52311/.*

http://software\.bigfix\.com/.*

動的ダウンロードのホワイトリストの詳細については、以下のリンクを参照してください。

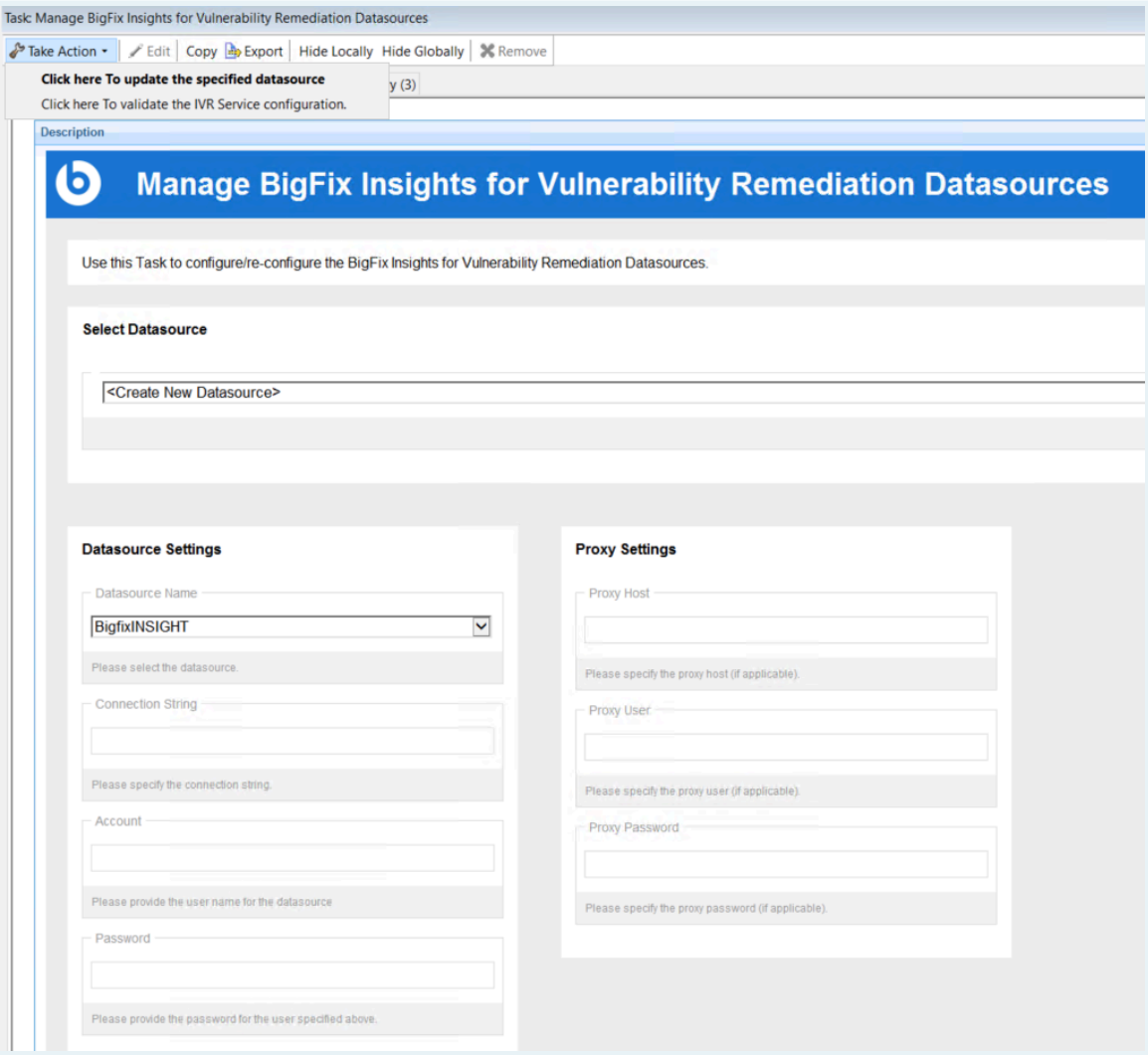
注:
このタスクを使用するには、この環境にデプロイされた IVR データ・フロー・サービスのインスタンスが 1 つだけ必要です。



BigFix Insights for Vulnerability Remediation データ・ソースの管理

このタスクを使用して、指定されたデータ・ソースを更新したり、IVR サービス構成を検証したりできます。このタスクには、各データ・ソースのプロキシー設定構成を指定するためのオプションも用意されています。

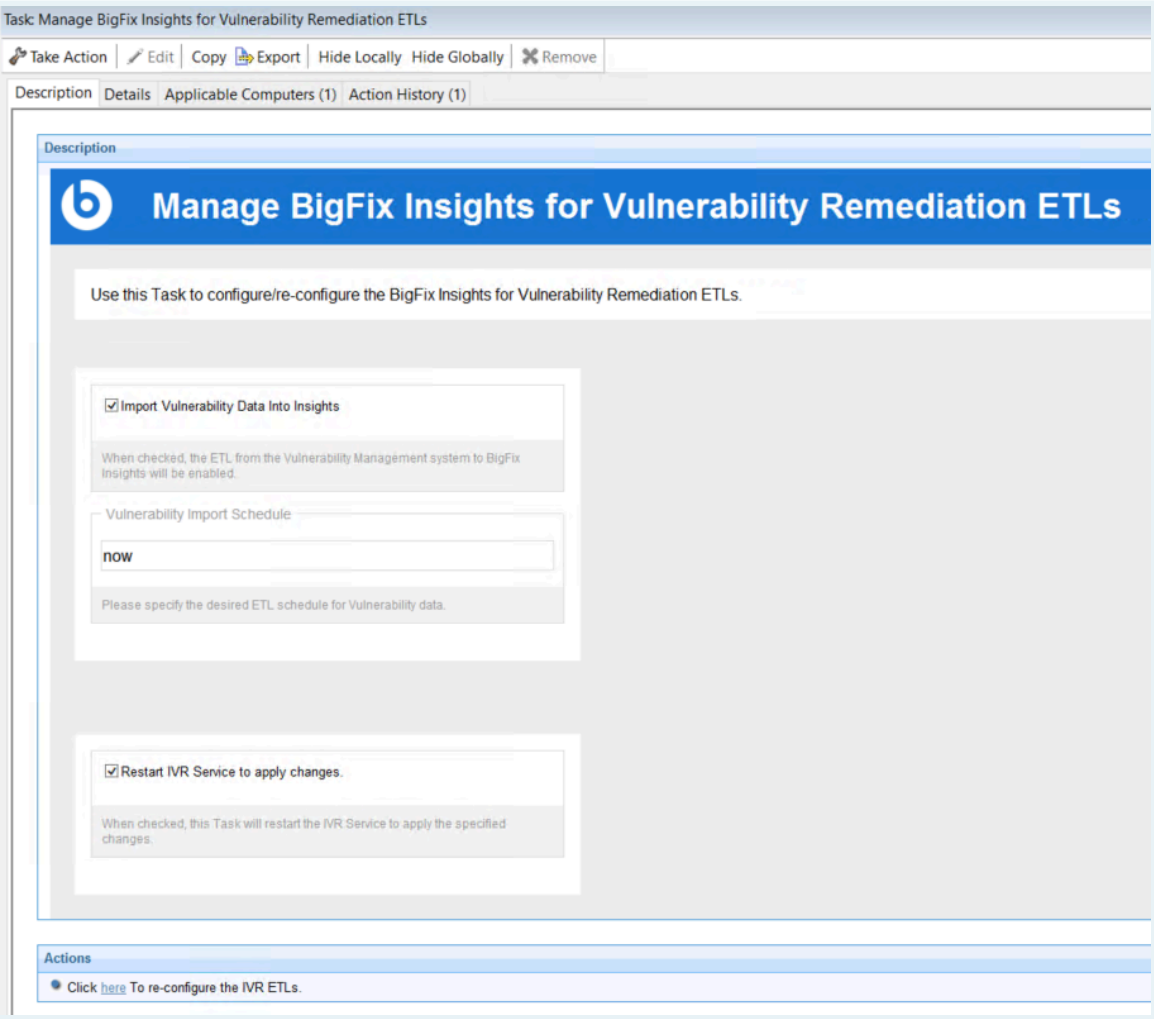
注:
このタスクを使用するには、この環境にデプロイされた IVR データ・フロー・サービスのインスタンスが 1 つだけ必要です。



BigFix Insights for Vulnerability Remediation ETL の管理

このタスクを使用して、BigFix Insights for Vulnerability Remediation ETL を構成/再構成します。この Fixlet を使用して IVR サービスを再起動することもできます。

注:
このタスクを使用するには、この環境にデプロイされた IVR データ・フロー・サービスのインスタンスが 1 つだけ必要です。

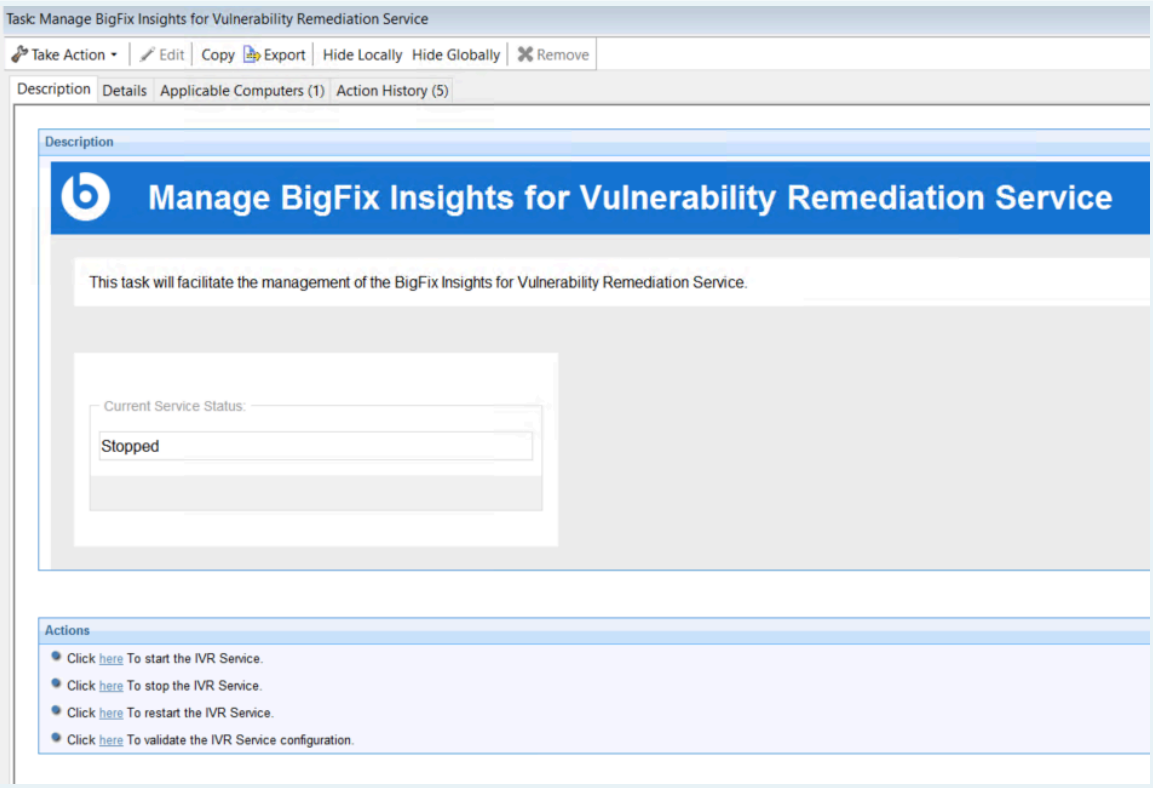


BigFix Insights for Vulnerability Remediation サービスの管理

このタスクにより、BigFix Insights for Vulnerability Remediation サービスの管理が簡単になります。このタスクを使用して、IVR サービスの構成を開始、停止、再起動、検証できます。

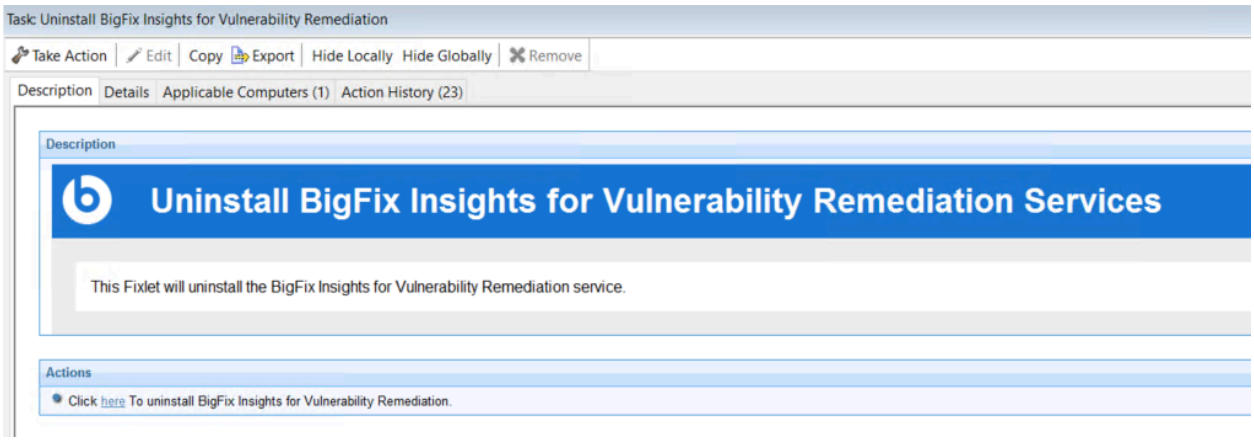
注:
データ・ソースまたは ETL Fixlet を既にデプロイ済みのサービスに更新する前にサービスを停止してから、サービスを再起動して最新の変更を適用することをお勧めします。

注:
このタスクを使用するには、この環境にデプロイされた IVR データ・フロー・サービスのインスタンスが 1 つだけ必要です。



BigFix Insights for Vulnerability Remediation のアンインストール

この Fixlet は、BigFix Insights for Vulnerability Remediation サービスをアンインストールします。



このプロセスにより、IVR サービスが削除されます。

注:
IVR フォルダーが開いているタブはすべて閉じてください。これにより、アンインストール・プロセス中にフォルダーが削除されなくります。

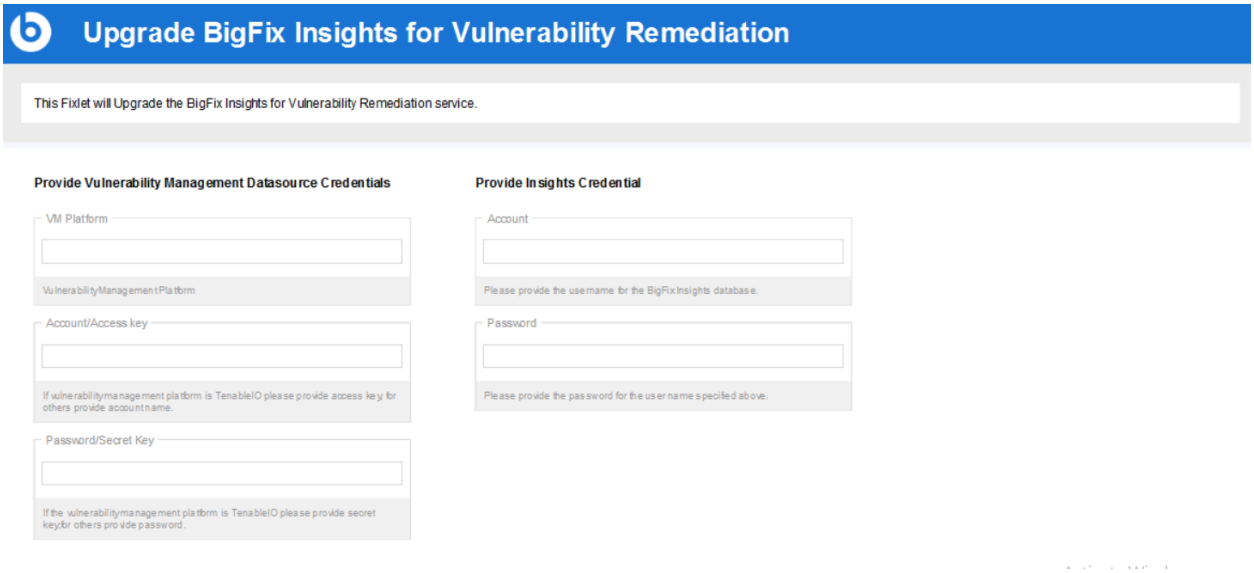
IVR サービスを削除したら、次のクエリーを実行して、SQL Server の IVR スキーマ (存在する場合) を削除します。

```
DECLARE @Sql VARCHAR(MAX), @Schema varchar(20)

SET @Schema = 'ivr' --put your schema name between these quotes

SELECT @Sql = COALESCE(@Sql,'') + 'DROP TABLE %SCHEMA%.' + QUOTENAME(TABLE_NAME) + ';'

+ CHAR(13)

FROM INFORMATION_SCHEMA.TABLES WHERE TABLE_SCHEMA = @Schema AND TABLE_TYPE = 'BASE

TABLE'

ORDER BY TABLE_NAME SELECT @Sql = COALESCE(@Sql,'') + 'DROP PROCEDURE %SCHEMA%.' +

QUOTENAME(ROUTINE_NAME) + ';' + CHAR(13)

FROM INFORMATION_SCHEMA.ROUTINES WHERE ROUTINE_SCHEMA = @Schema AND ROUTINE_TYPE =

'PROCEDURE'

ORDER BY ROUTINE_NAME SELECT @Sql = COALESCE(@Sql,'') + 'DROP FUNCTION %SCHEMA%.' +

QUOTENAME(ROUTINE_NAME) + ';' + CHAR(13)

FROM INFORMATION_SCHEMA.ROUTINES WHERE ROUTINE_SCHEMA = @Schema AND ROUTINE_TYPE =

'FUNCTION'

ORDER BY ROUTINE_NAME SELECT @Sql = COALESCE(REPLACE(@Sql,'%SCHEMA%',@Schema), '')

exec (@Sql);

drop schema ivr;


DROP TABLE IF EXISTS [ivr].[vulnerability_fixlet_nexus]DROP TABLE IF EXISTS

[ivr].[findings]

DROP TABLE IF EXISTS [ivr].[vulnerabilities]DROP TABLE IF EXISTS

[ivr].[global_computer_values]

DROP TABLE IF EXISTS [ivr].[schema]DROP TABLE IF EXISTS [ivr].[analysis_calendar]

DROP FUNCTION IF EXISTS [ivr].[rtrim_non_ascii]DROP schema IF EXISTS [ivr]
```

注:
IVR テーブルが配置されている関連データベースを選択してください。

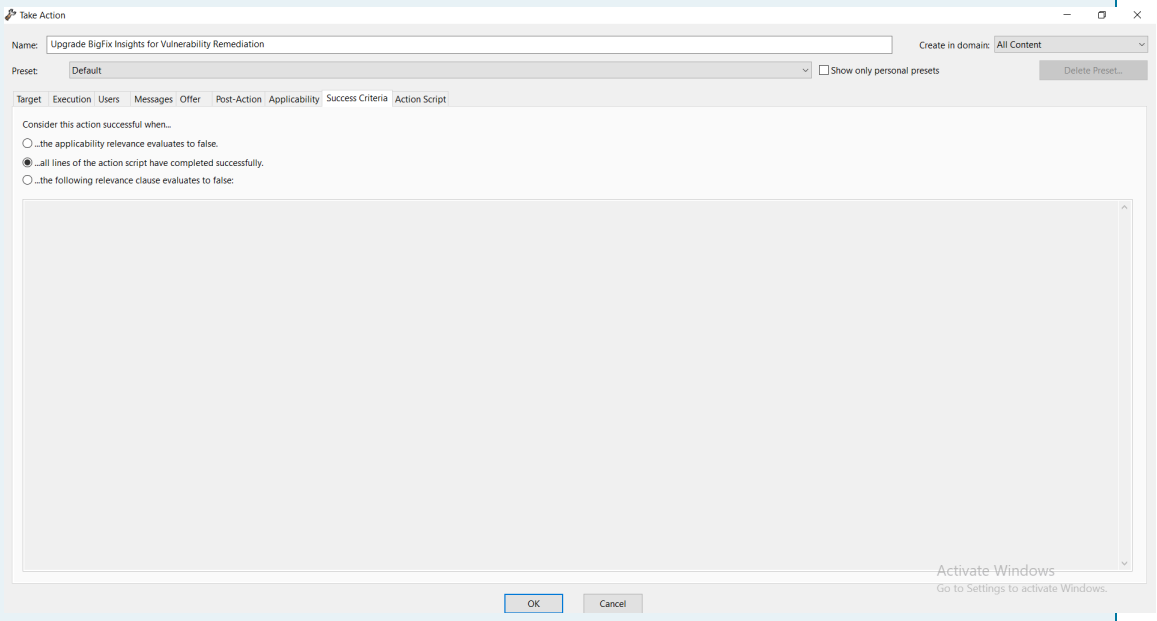
BigFix Insights for Vulnerability Remediation のアップグレード

Fixlet は、BigFix Insights for Vulnerability Remediation サービスを最新バージョンにアップグレードします。アップグレードを開始するには、BigFix Insights ユーザー資格情報と脆弱性管理データ・ソース資格情報を入力する必要があります。



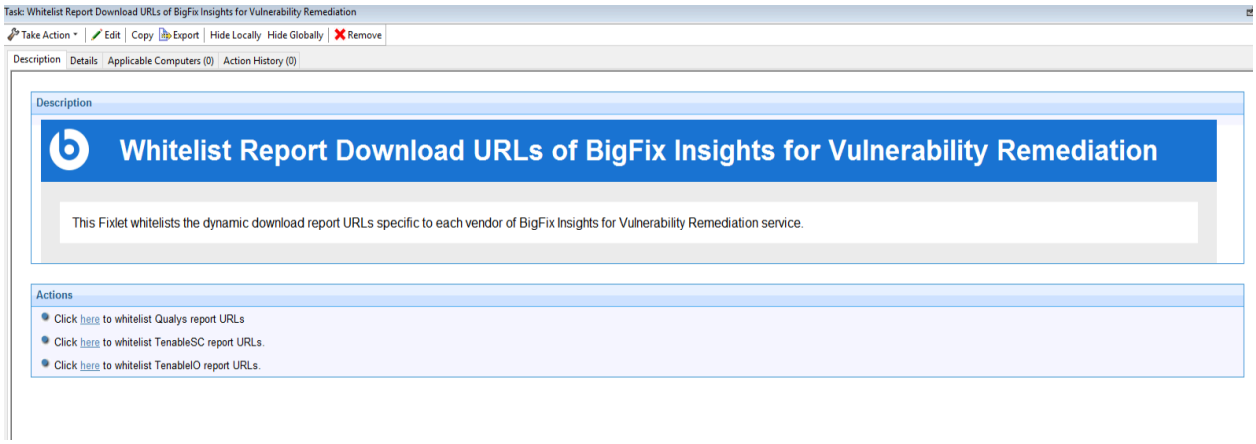
注:

Fixlet をインストールする前に、「成功基準」タブに移動し、「アクション・スクリプトのすべての行が正常に完了しました」を選択します。



BigFix Insights for Vulnerability Remediation のホワイトリスト・レポートのダウンロード **URL**

この Fixlet は、BigFix Insights for Vulnerability Remediation サービスの各ベンダーに固有の動的ダウンロード・レポートの URL をホワイトリストに登録します。



第 7 章. IVR 構成ファイルの更新と検証

IVR 構成を更新および検証することができます。

> 注:
> 構成ファイルを変更すると、現在のデータ・フロー構成 (ハッシュの生成元) に関連付けられているすべての IVR データが削除されます。さらに、既存のデータ・フロー構成に関連付けられていないすべてのデータが削除されます。詳しくは、PurgeFindingsOnExecutionOfDataflow 設定を参照してください。

構成ファイルの更新

1. ターゲット・サーバーにログインします。
2. 製品インストール・ディレクトリーに移動します。
3. テキスト・エディターで `DataFlowsConfig.xml` ファイルを開きます。
4. 構成を更新します。詳しくは、構成設定を参照してください。

構成ファイルの検証

1. CLI (コマンド行インターフェース) を開き、`BFIVR.exe --ValidateConfiguration` コマンドを実行します。
2. BigFix Insights for Vulnerability Remediation を再起動して、新しい構成をインポートします。正常に完了すると、「*Configuration verified successfully*」というメッセージが表示されます。

第 8 章. IVR の資格情報の更新

IVR の資格情報を更新できます。

1. コマンド行インターフェース (CLI) を開き、BFIVR.exe --ProvideCredentials コマンドを実行します。
2. 画面の指示に従って、ユーザー名/アクセス・キーとパスワード/シークレット・キーを入力します。
3. データ・ソースにアクセスするには、更新されたユーザー名/アクセス・キーとパスワード/シークレット・キーの資格情報を入力します。

更新が完了すると、以下のメッセージが表示されます: `The entered credentials are encrypted successfully.`

第 9 章. ビジネス・インテリジェンス・レポート

このセクションを使用して、Power BI レポートと Tableau レポートについて理解してください。

IVR (BigFix Insights for Vulnerability Remediation) ソリューションのレポート作成機能は、アプリケーションの 3 つの主なユース・ケースに対応します。

- 脆弱性 (使用可能な **Fixlet** あり) - 修復に使用できる、一致する BigFix Fixlet を持つ脆弱性のリスト。レポートには、各脆弱性に関連する最新の Fixlet と、脆弱性に関連付けられた CVE エントリーがリストされます。
- 脆弱性 (使用可能な **Fixlet** なし) - 修復に使用可能な Fixlet がない脆弱性のリスト
- 脆弱性の不一致 - スキャン・システムが問題を特定したが、BigFix では問題の解決が宣言されている脆弱性のリスト。これは、主にスキャン・プロセスのタイミングの違いが原因で発生します。

レポートは、Power BI (Desktop、2020 年 5 月に BI Server 用に最適化) と Tableau バージョン 2020.4 以降の両方で作成されます。

Power BI レポート

Tableau レポート

Power BI レポート

このセクションを読むことで Power BI レポートの理解を深めることができます。

Power BI レポート対象:

- Qualys
- Tenable.io
- Tenable.sc

レポートは、Power BI (デスクトップ、BI Server 用に最適化、2020 年 5 月) で作成されます。

- レポートの違い: レポートの機能は、Power BI と Tableau でほぼ同じです。このセクションでは、レポートの相違点について詳しく説明します。
- ナビゲーション: 各視覚化はダッシュボード・ページに表示されます。ビジネス・プロセスに適用されない視覚化は、必要に応じて削除できます。

- Qualys 重要度

  重要度の値は、脆弱性に関連する相対的なセキュリティー上のリスクを測定するために、Qualys によって提供されます。この測定に含まれる要素は次のとおりです。

- 考えられる結果
- 複雑度
- 通常の条件下でエクスプロイトが行われる可能性
- ネットワーク・ロケーション
- アタッカーが必要とする権限
- 影響を受けるソフトウェアの普及度
- 既知の攻撃の存在

IVR データベースでは、情報は vulnerabilities.severity 列に格納されます。レポート集計テーブルは、数値スコアと、以下のマトリックスに対応する値 (該当する場合) の両方を返します。

表 2.

重大度値	レベル値
1	最小
2	中
3	重大
4	重大
5	至急

ベンダーによるこのトピックの詳細については、 を参照してください。 https://qualysguard.qualys.com/qwebhelp/fo_portal/knowledgebase/severity_levels.htm

- Tenable 重大度

脆弱性優先順位の評価 (VPR) 値は、脆弱性に関連する相対的なセキュリティー上のリスクを測定するために Tenable によって提供されます。この測定に含まれる要素は次のとおりです。

- 脆弱性の存続期間
- CVSSv3 の影響スコア
- 悪用コードの完成度
- 製品範囲
- 脅威のソース
- 脅威の強度
- 脅威の最新性

IVR データベースでは、情報は vulnerabilities.vendor_rating 列に格納されます。レポート集計テーブルは、数値スコアと、以下のマトリックスに対応する値 (該当する場合) の両方を返します。

表 3.

VPR 値	レベル値
9.0 ~ 10.0	重大
7.0 ~ 8.9	高
4.0 ~ 6.9	中
0.1 ~ 3.9	低

ベンダーによるこのトピックの詳細については、 を参照してください。 https://docs.tenable.com/tenablesc/Content/RiskMetrics.htm

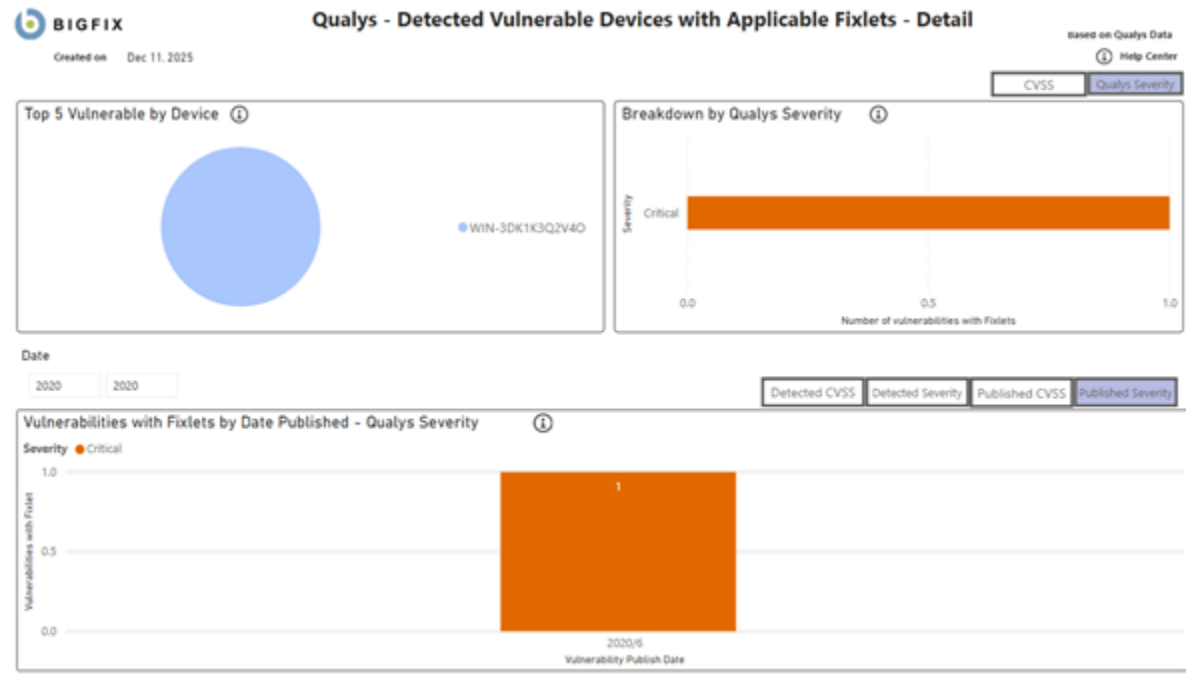
Qualys 用 Power BI レポート

このセクションを読むことで、Qualys 用 Power BI レポートの理解を深めることができます。

チャートの詳細:

- 脆弱性タイトル - 脆弱性タイトル
- 脆弱性 ID - 脆弱性に割り当てられた一意の識別子
- QID - Qualys ID。Qualys 脆弱性データベースの脆弱性に割り当てられた一意の識別子
- CVSS2 - Common Vulnerability Scoring System、バージョン 2
- Qualys 重大度 - 脆弱性に関連付けられたリスクのレベル。
- Qualys 重大度スコア - 脆弱性に割り当てられた数値。その脆弱性に関連付けられたリスクのレベルを示します。重大度スコアは、1 ~ 5 の範囲の数値で、5 が最も高い重大度を示します
- 重み付けされたスコア - cvss_base*applicable_computers に基づいて、「重み付けされたスコア」として算出された値
- 公開日 - 脆弱性に関する情報が最初に利用可能になった日付
- 検出日 - 脆弱性が最初に検出された日付
- 該当するデバイス - 脆弱性の影響を受けるデバイス

検出された脆弱性 (適用可能な **Fixlet** あり)



BIGFIX

Qualys -Detected Vulnerable Devices with Applicable Fixlets - Device Detail

* BigFix data

* Device Name: | DESKTOP-99268DV
* BigFix Computer: | 1
* IP Address: | 10.134.146.136
* OS: | Win10 10.0.19041.804 (2004)
* Type: | Server
* Groups: | Reports_Computer_Group
* Group Source Site:
* Last Report Time: | 2/11/2021 8:26:41 AM

Vulnerability Title	QID	CVE	CVSS2	CVSS3	Qualys Severity	Qualys Severity Score	Weighted Score	DeviceID	* Fixlet Title	* Fixlet ID	* Fixlet Site	* Fixlet Source ID	* Fi
CentOS Security Update for openssl (CESA-2014:1653)	122778	CVE-2014-3566	Medium	Low	Serious	3	0	14456361-1	3009008: Security Advisory: Vulnerability in SSL 3.0 Could Allow Information Disclosure - Disable Workaround for Client Software (Disable SSL 3.0 in Windows)	300900813	Patches for Windows	KB300900 8	Un
CentOS Security Update for openssl (CESA-2014:1653)	122778	CVE-2014-3566	Medium	Low	Serious	3	0	14456361-1	3009008: Security Advisory: Vulnerability in SSL 3.0 Could Allow Information Disclosure - Disable Workaround for IE Settings (Disable SSL 3.0 and enable TLS 1.0, TLS 1.1, and TLS 1.2 in Internet Explorer)	300900805	Patches for Windows	KB300900 8	Un
CentOS Security Update for openssl (CESA-2014:1653)	122778	CVE-2014-3566	Medium	Low	Serious	3	0	14456361-1	3009008: Security Advisory: Vulnerability in SSL 3.0 Could Allow Information Disclosure - Disable Workaround for IE Settings (Disable SSL 3.0 in Internet Explorer)	300900817	Patches for Windows	KB300900 8	Un
CentOS Security Update for openssl (CESA-2014:1653)	122778	CVE-2014-3566	Medium	Low	Serious	3	0	14456361-1	3009008: Security Advisory: Vulnerability in SSL 3.0 Could Allow Information Disclosure - Disable Workaround for Server Software (Disable SSL 3.0 in Windows)	300900809	Patches for Windows	KB300900 8	Un

BIGFIX

Qualys - Detected Vulnerable Devices with Applicable Fixlets - Device Detail

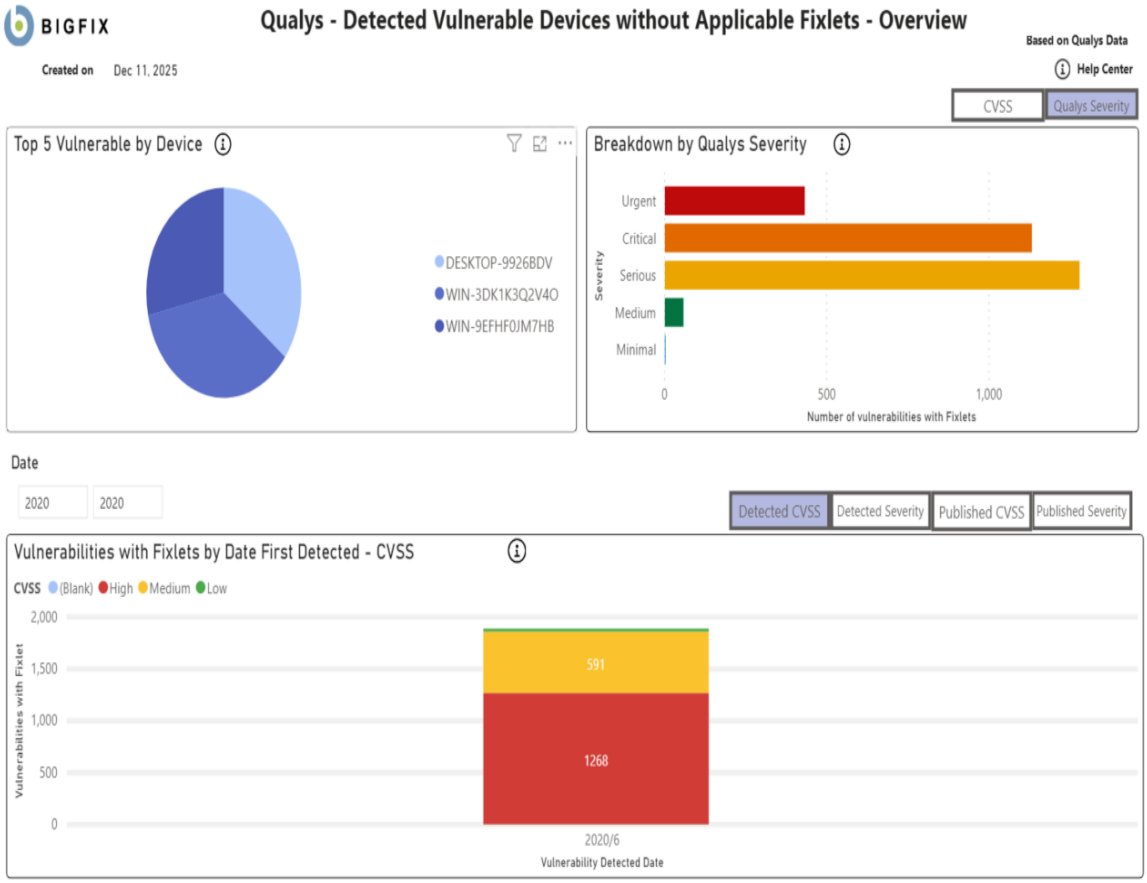
* BigFix data

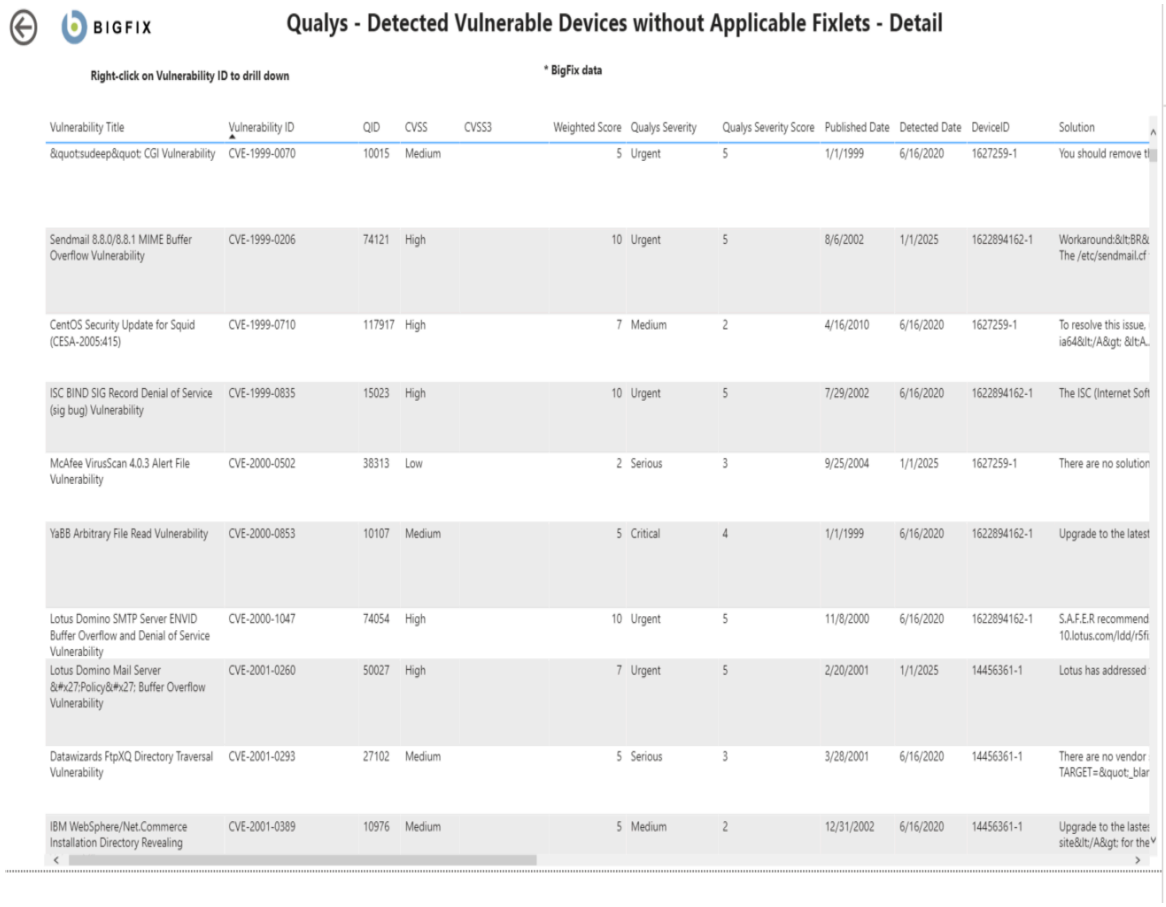
Vulnerability Title: | CentOS Security Update for openssl (CESA-2014:1653)
QID: | 110168
Published Date: | 9/8/2009
CVE: | CVE-2009-0901
CVSS: | High
Qualys Severity: | Critical
Qualys Severity Score: | 1
* Fixlet Title: | 3009008: Security Advisory: Vulnerability in SSL 3.0 Could A
* Fixlet ID: | 903505
* Fixlet Site: | Patches for Windows
* Fixlet Source ID: | KB2553374
* Fixlet Category: | Critical Updates
* Source Release Date: | 01/03/2018

Right-click on Device ID to drill down

Date Detected	BigFix Computer ID	Computer Name	OS	IP Address	Type	Group	Last Report Time
6/16/2020	1	DESKTOP-99268DV	Win10 10.0.19041.804 (2004)	10.134.146.207	Server	Reports_Computer_Group	2/11/2021 8:26:41 AM
1/1/2025	1	DESKTOP-99268DV	Win10 10.0.19041.804 (2004)	10.134.146.207	Server	Reports_Computer_Group	2/11/2021 8:26:41 AM
6/16/2020	3	WIN-3DK1K3Q2V4O	Win2019 10.0.17763.107 (1809)	10.134.146.184	Server	Reports_Computer_Group	2/16/2021 4:05:18 PM
1/1/2025	3	WIN-3DK1K3Q2V4O	Win2019 10.0.17763.107 (1809)	10.134.146.184	Server	Reports_Computer_Group	2/16/2021 4:05:18 PM
6/16/2020	2	WIN-9EFHF0JM7H8	Win2016 10.0.14393.1884 (1607)	10.134.146.136	Server	Reports_Computer_Group	2/16/2021 4:11:07 PM
1/1/2025	2	WIN-9EFHF0JM7H8	Win2016 10.0.14393.1884 (1607)	10.134.146.136	Server	Reports_Computer_Group	2/16/2021 4:11:07 PM

検出された脆弱性 (使用可能な **Fixlet** なし)





BIGFIX

Qualys - Detected Vulnerable Devices without Applicable Fixlets - Detail

Right-click on Vulnerability ID to drill down

*** BigFix data**

Vulnerability Title	Vulnerability ID	QID	CVSS	CVSS3	Weighted Score	Qualys Severity	Qualys Severity Score	Published Date	Detected Date	DeviceID	Solution
"sudeep" CGI Vulnerability	CVE-1999-0070	10015	Medium		5	Urgent	5	1/1/1999	6/16/2020	1627259-1	You should remove t
Sendmail 8.8.0/8.8.1 MIME Buffer Overflow Vulnerability	CVE-1999-0206	74121	High		10	Urgent	5	8/6/2002	1/1/2025	1622894162-1	Workaround:<BR& The /etc/sendmail.cf
CentOS Security Update for Squid (CESA-2005:415)	CVE-1999-0710	117917	High		7	Medium	2	4/16/2010	6/16/2020	1627259-1	To resolve this issue, ia64</A> <A...
ISC BIND SIG Record Denial of Service (sig bug) Vulnerability	CVE-1999-0835	15023	High		10	Urgent	5	7/29/2002	6/16/2020	1622894162-1	The ISC (Internet Soft
McAfee VirusScan 4.0.3 Alert File Vulnerability	CVE-2000-0502	38313	Low		2	Serious	3	9/25/2004	1/1/2025	1627259-1	There are no solution
YaBB Arbitrary File Read Vulnerability	CVE-2000-0853	10107	Medium		5	Critical	4	1/1/1999	6/16/2020	1622894162-1	Upgrade to the latest
Lotus Domino SMTP Server ENVID Buffer Overflow and Denial of Service Vulnerability	CVE-2000-1047	74054	High		10	Urgent	5	11/8/2000	6/16/2020	1622894162-1	S.A.F.E.R recommend 10.lotus.com/ldd/r5fi
Lotus Domino Mail Server 'Policy' Buffer Overflow Vulnerability	CVE-2001-0260	50027	High		7	Urgent	5	2/20/2001	1/1/2025	14456361-1	Lotus has addressed
Datawizards FtpXQ Directory Traversal Vulnerability	CVE-2001-0293	27102	Medium		5	Serious	3	3/28/2001	6/16/2020	14456361-1	There are no vendor TARGET="_blar
IBM WebSphere/Net.Commerce Installation Directory Revealing	CVE-2001-0389	10976	Medium		5	Medium	2	12/31/2002	6/16/2020	14456361-1	Upgrade to the laste site</A> for the

Qualys - Detected Vulnerable Devices without Applicable Fixlets - Device Detail

* BigFix data

Vulnerability Title: | "sudeep" CGI Vulnerability

QID: | 10005

Published Date: | 1/1/1999

CVE: | CVE-1999-0070

CVSS: | (Blank)

Qualys Severity: | Critical

Qualys Severity Score: | 1

Right-click on Device ID to drill down

Date Detected	BigFix Computer ID	Computer Name	OS	IP Address	Device Type	Last Report Time
6/16/2020	1627259-1	DESKTOP-9926BDV	Win10 10.0.19041.804 (2004)	10.134.146.207	Server	2/11/2021 8:26:41 AM
1/1/2025	1627259-1	DESKTOP-9926BDV	Win10 10.0.19041.804 (2004)	10.134.146.207	Server	2/11/2021 8:26:41 AM
6/16/2020	1622894162-1	WIN-3DK1K3Q2V4O	Win2019 10.0.17763.107 (1809)	10.134.146.184	Server	2/16/2021 4:05:18 PM
1/1/2025	1622894162-1	WIN-3DK1K3Q2V4O	Win2019 10.0.17763.107 (1809)	10.134.146.184	Server	2/16/2021 4:05:18 PM
6/16/2020	14456361-1	WIN-9EFHF0JM7HB	Win2016 10.0.14393.1884 (1607)	10.134.146.136	Server	2/16/2021 4:11:07 PM
1/1/2025	14456361-1	WIN-9EFHF0JM7HB	Win2016 10.0.14393.1884 (1607)	10.134.146.136	Server	2/16/2021 4:11:07 PM

BIGFIX

Qualys -Detected Vulnerable Devices without Applicable Fixlets - Device Detail

* BigFix data

*** Device Name:** DESKTOP-9926BDV

*** BigFix Computer** 14456361-1

*** IP Address:** 10.134.146.136

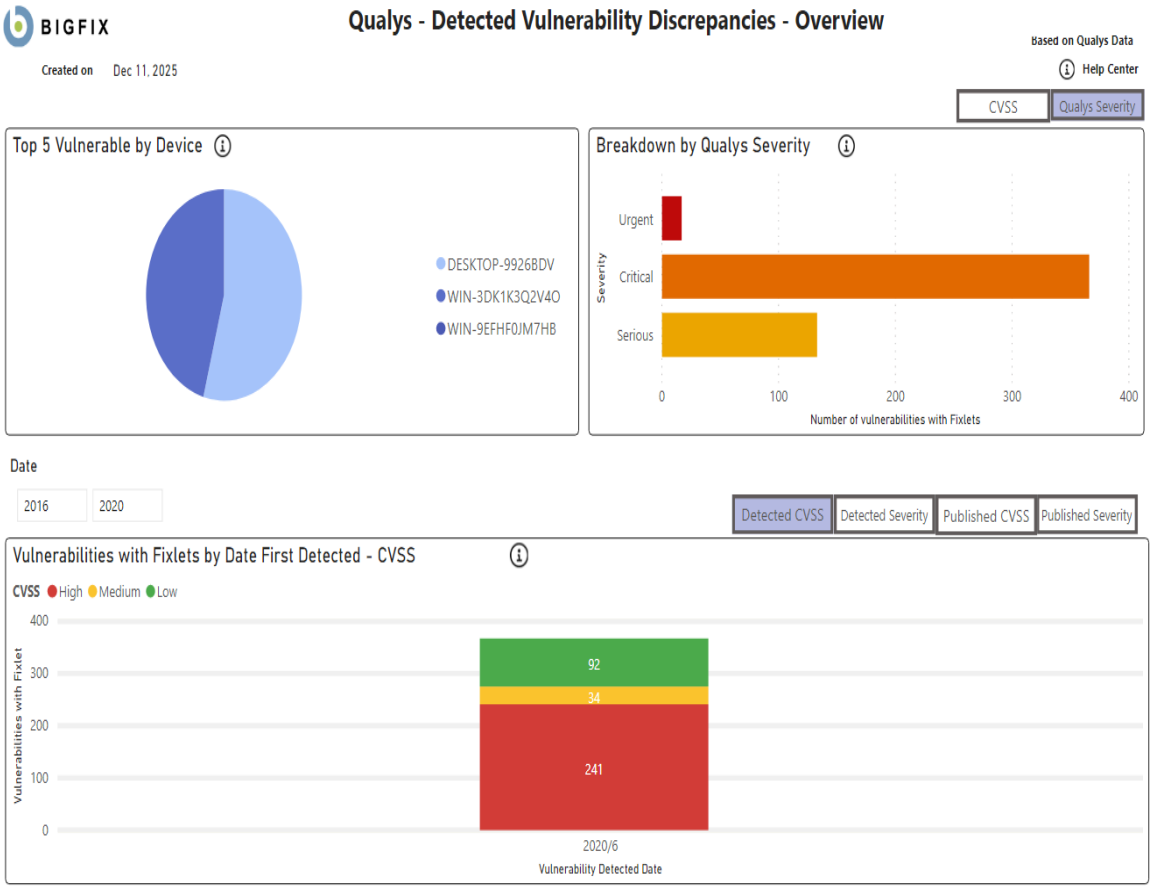
*** OS:** Win10 10.0.19041.804 (2004)

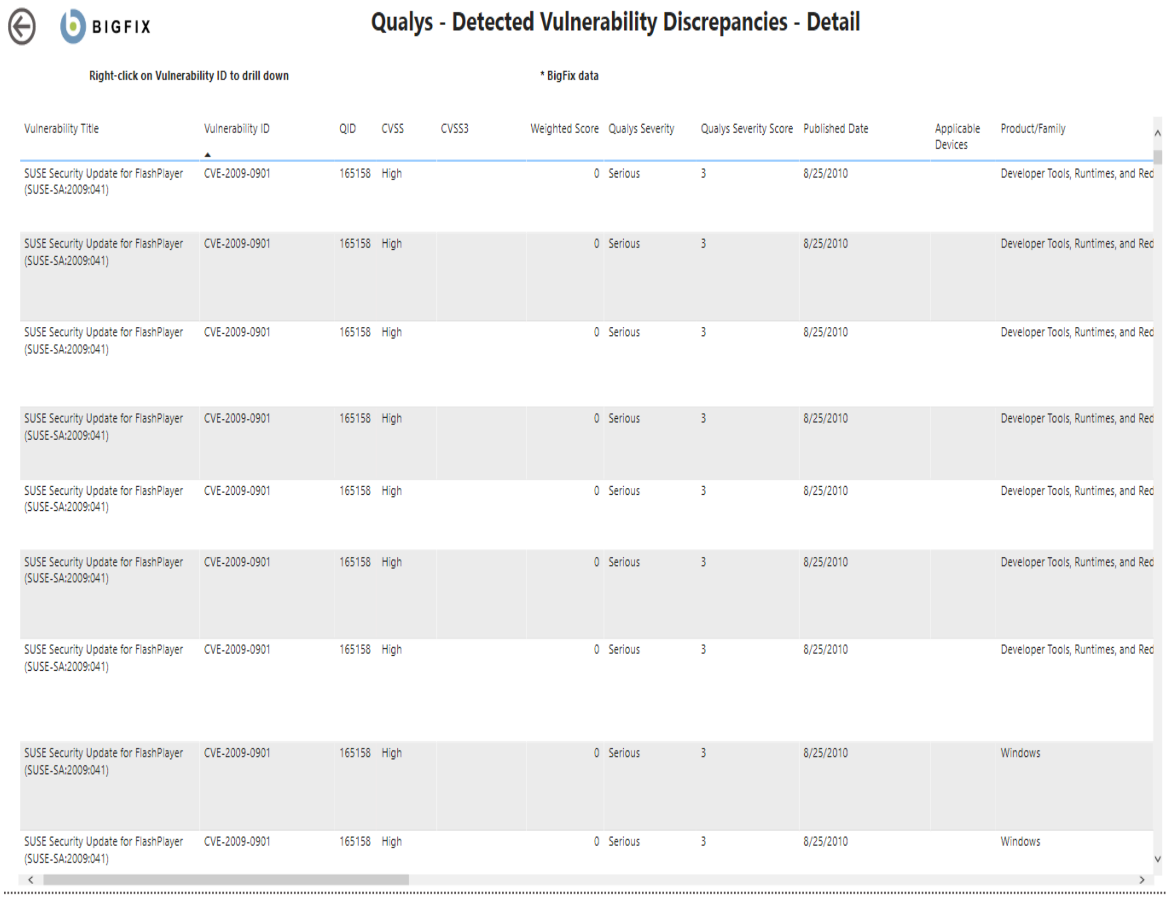
*** Type:** Server

*** Last Report Time:** 2/11/2021 8:26:41 AM

Vulnerability Title	QID	CVE	CVSS2	Qualys Severity	Qualys Severity Score	Detected Date
"sudeep" CGI Vulnerability	10015	CVE-1999-0070	Medium	Urgent	5	6/16/2020
Sendmail 8.8.0/8.8.1 MIME Buffer Overflow Vulnerability	74121	CVE-1999-0206	High	Urgent	5	1/1/2025
CentOS Security Update for Squid (CESA-2005:415)	117917	CVE-1999-0710	High	Medium	2	6/16/2020
ISC BIND SIG Record Denial of Service (sig bug) Vulnerability	15023	CVE-1999-0835	High	Urgent	5	6/16/2020
McAfee VirusScan 4.0.3 Alert File Vulnerability	38313	CVE-2000-0502	Low	Serious	3	1/1/2025
YaBB Arbitrary File Read Vulnerability	10107	CVE-2000-0853	Medium	Critical	4	6/16/2020
Lotus Domino SMTP Server ENVID Buffer Overflow and Denial of Service Vulnerability	74054	CVE-2000-1047	High	Urgent	5	6/16/2020
Lotus Domino Mail Server 'Policy' Buffer Overflow Vulnerability	50027	CVE-2001-0260	High	Urgent	5	1/1/2025
Datawizards FtpXQ Directory Traversal Vulnerability	27102	CVE-2001-0293	Medium	Serious	3	6/16/2020
IBM WebSphere/Net.Commerce Installation Directory Revealing Vulnerability	10976	CVE-2001-0389	Medium	Medium	2	6/16/2020
Multiple Oracle 8i Listener Vulnerabilities	19055	CVE-2001-0498	High	Critical	4	6/16/2020
Multiple Oracle 8i Listener Vulnerabilities	19055	CVE-2001-0499	High	Critical	4	6/16/2020
Cisco IOS HTTP Configuration Arbitrary Administrative Access Vulnerability	43005	CVE-2001-0537	High	Critical	4	6/16/2020
Drummon Miles A1Stats Directory Traversal Vulnerability	10340	CVE-2001-0561	High	Serious	3	6/16/2020
iPlanet Calendar Server Plaintext Admin Password Vulnerability	86154	CVE-2001-0620	Low	Urgent	5	1/1/2025
Dream Catchers Post-It! CGI Remote Arbitrary Command Execution Vulnerability	10431	CVE-2001-0844	High	Urgent	5	1/1/2025
Hassan Consulting Shopping Cart Arbitrary Command Execution Vulnerability	23013	CVE-2001-0985	High	Urgent	5	1/1/2025
Red Hat PHP SafeMode Arbitrary File Execution Vulnerability	115006	CVE-2001-1246	High	Urgent	5	6/16/2020
Ipswitch IMail Server Path Disclosure Vulnerability	74094	CVE-2001-1282	Medium	Serious	3	6/16/2020
Horde IMP Cross Site Scripting Vulnerability	11014	CVE-2002-0181	High	Serious	3	1/1/2025
CSSearch Remote Command Execution Vulnerability	10850	CVE-2002-0495	High	Urgent	5	1/1/2025
Hosting Controller Default Account Vulnerability	10674	CVE-2002-0774	High	Serious	3	6/16/2020
W3C Jigsaw Device Name Path Disclosure Vulnerability	86370	CVE-2002-1052	Medium	Medium	2	6/16/2020
Microsoft Data Access Components RDS Enabled	86432	CVE-2002-1142	High	Minimal	1	6/16/2020
Apache 2 WebDAV CGI POST Request Information Disclosure Vulnerability	86512	CVE-2002-1156	Medium	Critical	4	1/1/2025

脆弱性の不一致


BIGFIX
Qualys - Detected Vulnerability Discrepancies - Overview
Created on Dec 11, 2025
Based on Qualys Data
Help Center
CVSS
Qualys Severity
Top 5 Vulnerable by Device
DESKTOP-9926BDV
WIN-3DK1K3Q2V4O
WIN-9EFHF0JM7HB
Breakdown by Qualys Severity
Urgent
Critical
Serious
Severity
0
100
200
300
400
Number of vulnerabilities with Fixlets
Date
2016
2020
Detected CVSS
Detected Severity
Published CVSS
Published Severity
Vulnerabilities with Fixlets by Date First Detected - CVSS
CVSS High Medium Low
400
300
200
100
0
Vulnerabilities with Fixlet
92
34
241
2020/6
Vulnerability Detected Date



BIGFIX

Qualys - Detected Vulnerability Discrepancies - Detail

Right-click on Vulnerability ID to drill down

* BigFix data

Vulnerability Title	Vulnerability ID	QID	CVSS	CVSS3	Weighted Score	Qualys Severity	Qualys Severity Score	Published Date	Applicable Devices	Product/Family
SUSE Security Update for FlashPlayer (SUSE-SA:2009:041)	CVE-2009-0901	165158	High		0	Serious	3	8/25/2010		Developer Tools, Runtimes, and Red
SUSE Security Update for FlashPlayer (SUSE-SA:2009:041)	CVE-2009-0901	165158	High		0	Serious	3	8/25/2010		Developer Tools, Runtimes, and Red
SUSE Security Update for FlashPlayer (SUSE-SA:2009:041)	CVE-2009-0901	165158	High		0	Serious	3	8/25/2010		Developer Tools, Runtimes, and Red
SUSE Security Update for FlashPlayer (SUSE-SA:2009:041)	CVE-2009-0901	165158	High		0	Serious	3	8/25/2010		Developer Tools, Runtimes, and Red
SUSE Security Update for FlashPlayer (SUSE-SA:2009:041)	CVE-2009-0901	165158	High		0	Serious	3	8/25/2010		Developer Tools, Runtimes, and Red
SUSE Security Update for FlashPlayer (SUSE-SA:2009:041)	CVE-2009-0901	165158	High		0	Serious	3	8/25/2010		Developer Tools, Runtimes, and Red
SUSE Security Update for FlashPlayer (SUSE-SA:2009:041)	CVE-2009-0901	165158	High		0	Serious	3	8/25/2010		Developer Tools, Runtimes, and Red
SUSE Security Update for FlashPlayer (SUSE-SA:2009:041)	CVE-2009-0901	165158	High		0	Serious	3	8/25/2010		Windows
SUSE Security Update for FlashPlayer (SUSE-SA:2009:041)	CVE-2009-0901	165158	High		0	Serious	3	8/25/2010		Windows

Qualys - Detected Vulnerability Discrepancies - Device Detail

* BigFix data

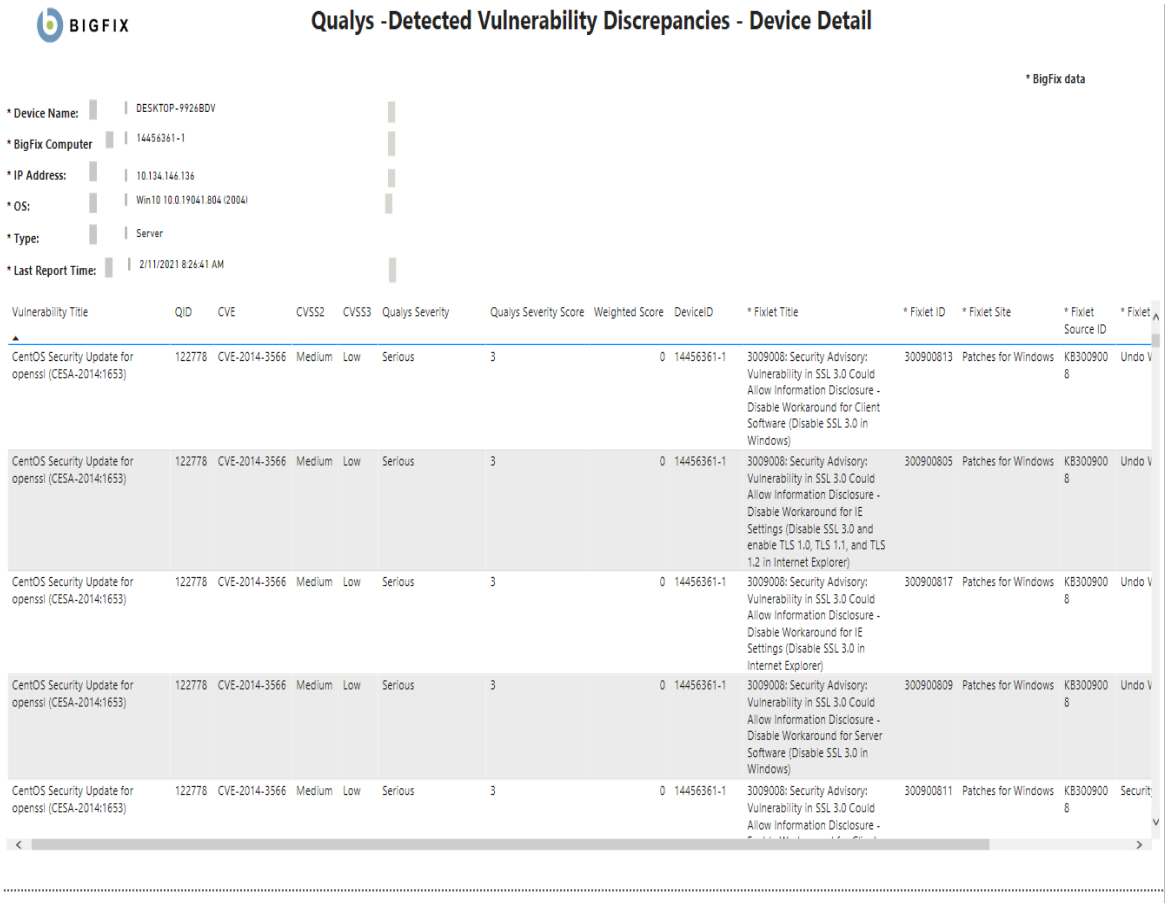
Vulnerability Title: CentOS Security Update for openssl (CESA-2014:1653)
QID: 110168
Published Date: 9/8/2009

CVE: CVE-2009-0901
CVSS: High
Qualys Severity: Critical
Qualys Severity Score: 3

*** Fixlet Title:** 3009008: Security Advisory: Vulnerability in SSL 3.0 Could A
*** Fixlet ID:** 903505
*** Fixlet Site:** Patches for Windows
*** Fixlet Source ID:** KB2553374
*** Fixlet Category:** Critical Updates
*** Source Release Date:** 01/03/2018

Right-click on Device ID to drill down

Date Detected	BigFix Computer ID	Computer Name	OS	IP Address	Type	Last Report Time
6/16/2020	1627259-1	DESKTOP-9926BDV	Win10 10.0.19041.804 (2004)	10.134.146.207	Server	2/11/2021 8:26:41 AM
1/1/2025	1627259-1	DESKTOP-9926BDV	Win10 10.0.19041.804 (2004)	10.134.146.207	Server	2/11/2021 8:26:41 AM
6/16/2020	1622894162-1	WIN-3DK1K3Q2V4O	Win2019 10.0.17763.107 (1809)	10.134.146.184	Server	2/16/2021 4:05:18 PM
1/1/2025	1622894162-1	WIN-3DK1K3Q2V4O	Win2019 10.0.17763.107 (1809)	10.134.146.184	Server	2/16/2021 4:05:18 PM
6/16/2020	14456361-1	WIN-9EFHF0JM7HB	Win2016 10.0.14393.1884 (1607)	10.134.146.136	Server	2/16/2021 4:11:07 PM
1/1/2025	14456361-1	WIN-9EFHF0JM7HB	Win2016 10.0.14393.1884 (1607)	10.134.146.136	Server	2/16/2021 4:11:07 PM



BIGFIX

Qualys -Detected Vulnerability Discrepancies - Device Detail

* BigFix data

* Device Name: DESKTOP-9926BDV
* BigFix Computer 14456361-1
* IP Address: 10.134.146.136
* OS: Win10 10.0.19041.804 (2004)
* Type: Server
* Last Report Time: 2/11/2021 8:26:41 AM

Vulnerability Title	QID	CVE	CVSS2	CVSS3	Qualys Severity	Qualys Severity Score	Weighted Score	DeviceID	* Fixlet Title	* Fixlet ID	* Fixlet Site	* Fixlet Source ID	* Fixlet
CentOS Security Update for openssl (CESA-2014:1653)	122778	CVE-2014-3566	Medium	Low	Serious	3	0	14456361-1	3009008: Security Advisory: Vulnerability in SSL 3.0 Could Allow Information Disclosure - Disable Workaround for Client Software (Disable SSL 3.0 in Windows)	300900813	Patches for Windows	KB3009008	Undo V
CentOS Security Update for openssl (CESA-2014:1653)	122778	CVE-2014-3566	Medium	Low	Serious	3	0	14456361-1	3009008: Security Advisory: Vulnerability in SSL 3.0 Could Allow Information Disclosure - Disable Workaround for IE Settings (Disable SSL 3.0 and enable TLS 1.0, TLS 1.1, and TLS 1.2 in Internet Explorer)	300900805	Patches for Windows	KB3009008	Undo V
CentOS Security Update for openssl (CESA-2014:1653)	122778	CVE-2014-3566	Medium	Low	Serious	3	0	14456361-1	3009008: Security Advisory: Vulnerability in SSL 3.0 Could Allow Information Disclosure - Disable Workaround for IE Settings (Disable SSL 3.0 in Internet Explorer)	300900817	Patches for Windows	KB3009008	Undo V
CentOS Security Update for openssl (CESA-2014:1653)	122778	CVE-2014-3566	Medium	Low	Serious	3	0	14456361-1	3009008: Security Advisory: Vulnerability in SSL 3.0 Could Allow Information Disclosure - Disable Workaround for Server Software (Disable SSL 3.0 in Windows)	300900809	Patches for Windows	KB3009008	Undo V
CentOS Security Update for openssl (CESA-2014:1653)	122778	CVE-2014-3566	Medium	Low	Serious	3	0	14456361-1	3009008: Security Advisory: Vulnerability in SSL 3.0 Could Allow Information Disclosure -	300900811	Patches for Windows	KB3009008	Securit

Tenable.io 用 Power BI レポート

このセクションを読むことで、Tenable.io 用 Power BI レポートの理解を深めることができます。

BigFix Insights for Vulnerability Remediation で、Tenable.io の脆弱性データを利用できます。Tenable Lumin が使用可能な場合、BigFix Insights for Vulnerability Remediation は、次の資産の優先順位付けデータも利用します。

- 資産の重大度の評価 (ACR): デバイス・タイプ、デバイスの目的、インターネットへのネットワーク・ロケーション/近接度に基づく資産の相対的な重要度を表す 1 ~ 10 の評価。
- 資産露出スコア (AES): ACR および VPR (脆弱性優先順位の評価) を 1 つのスコアに結合して資産の相対的な露出を表すメトリック。

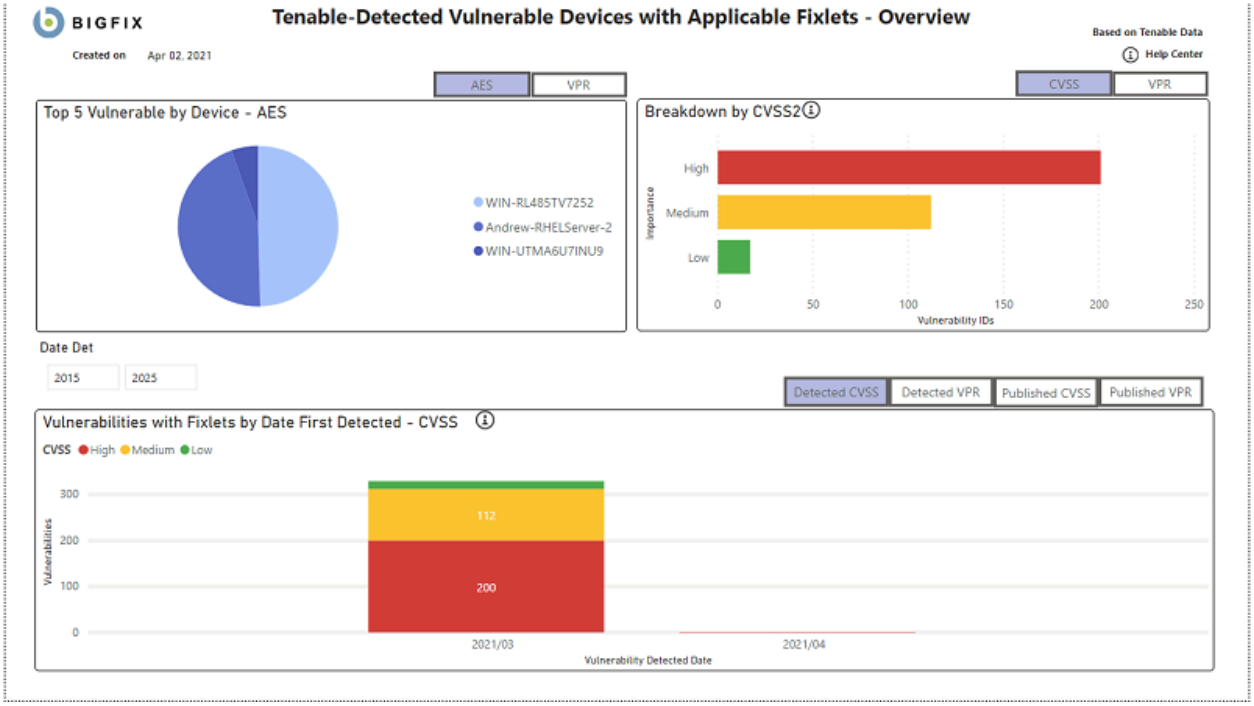
詳しくは、次のリンク先を参照してください。Lumin メトリック

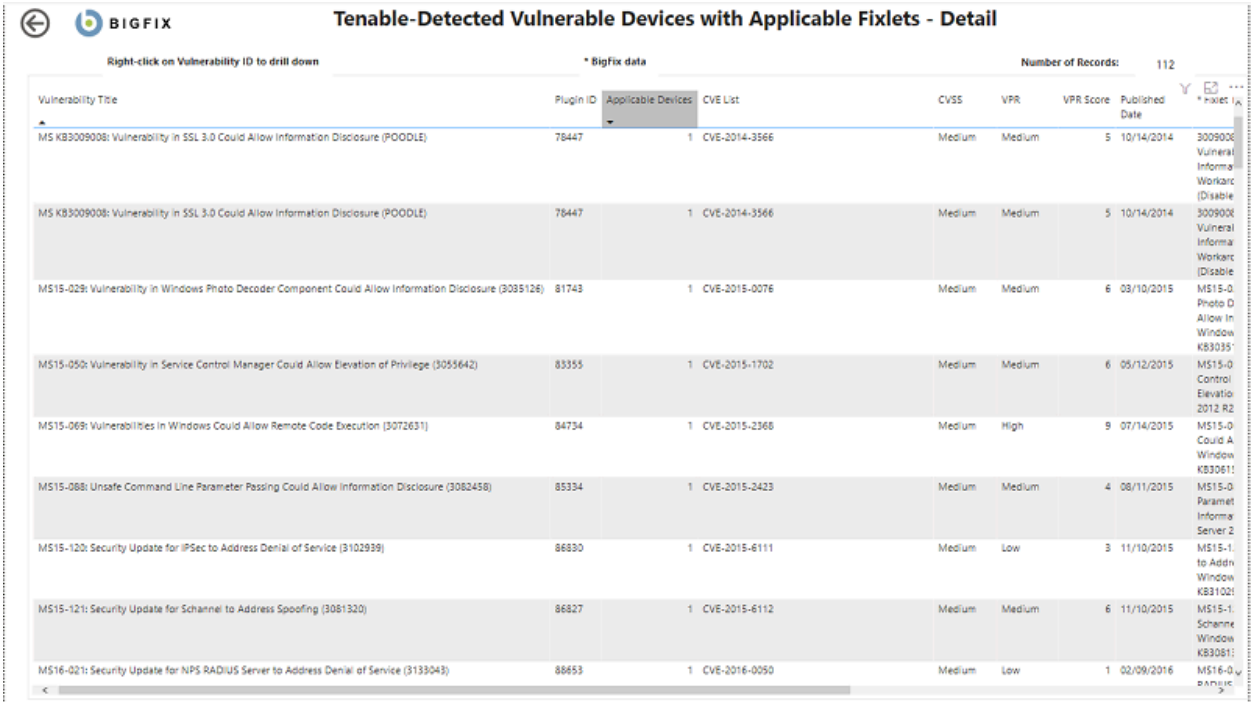
さらに、Tenable.io の場合にのみ、BigFix はエンドポイント資産データを Tenable.io に送信して、管理対象外の可能性がある資産を表示できるようにします。

チャートの詳細:

- 脆弱性タイトル - 脆弱性タイトル
- PluginID - 脆弱性の検出に割り当てられた一意の識別子
- 該当デバイス - Tenable によってスキャンされ、脆弱性が特定されたデバイス
- CVE リスト - CVE のリスト
- CVSS2 - (Common Vulnerability Scoring System バージョン 2)、セキュリティーの脆弱性の重大度と潜在的な影響を評価するために使用されるスコアリング・システム。
- CVSS3 - (Common Vulnerability Scoring System バージョン 3)、スコアリング・システムの更新バージョン
- VPR - 脆弱性優先順位の評価
- VPR スコア - 0 ~ 10 の範囲の数値。10 が最も高い優先度を示します
- 検出日 - 脆弱性が最初に検出された日付
- 公開日 - 脆弱性に関する情報が最初に利用可能になった日付
- ACR - 資産の重大度の評価: デバイス・タイプ、デバイスの目的、インターネットへのネットワーク・ロケーション/近接度に基づく資産の相対的な重要度を表す 1 ~ 10 の評価。
- AES - 資産露出スコア: ACR および VPR (脆弱性優先順位の評価) を 1 つのスコアに結合して資産の相対的な露出を表すメトリック。

検出された脆弱性 (適用可能な **Fixlet** あり)





BIGFIX

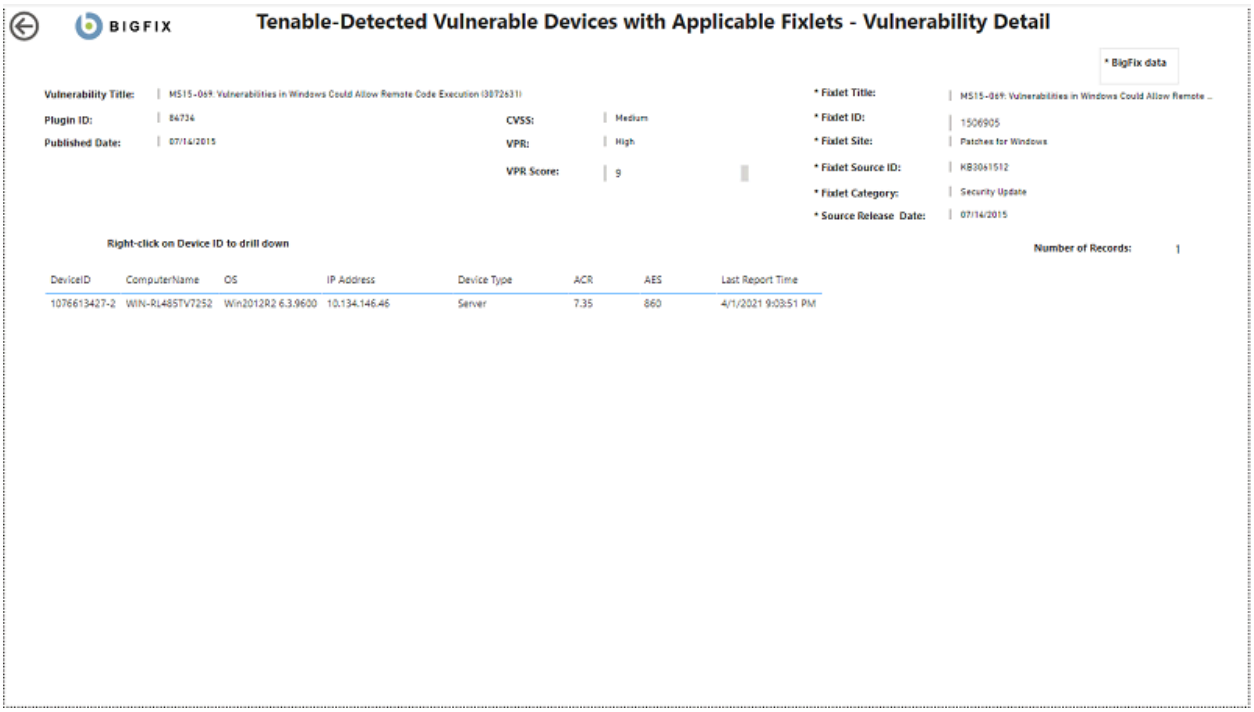
Tenable-Detected Vulnerable Devices with Applicable Fixlets - Detail

Right-click on Vulnerability ID to drill down

* BigFix data

Number of Records: 112

Vulnerability Title	Plugin ID	Applicable Devices	CVE List	CVSS	VPR	VPR Score	Published Date	* Fixlet
MS KB3009008: Vulnerability in SSL 3.0 Could Allow Information Disclosure (POODLE)	78447	1	CVE-2014-3566	Medium	Medium	5	10/14/2014	3009008 Vulnerat Informa Workarc (Disable
MS KB3009008: Vulnerability in SSL 3.0 Could Allow Information Disclosure (POODLE)	78447	1	CVE-2014-3566	Medium	Medium	5	10/14/2014	3009008 Vulnerat Informa Workarc (Disable
MS15-029: Vulnerability in Windows Photo Decoder Component Could Allow Information Disclosure (3035126)	81743	1	CVE-2015-0076	Medium	Medium	6	03/10/2015	MS15-0 Photo D Allow In Window KB3035
MS15-050: Vulnerability in Service Control Manager Could Allow Elevation of Privilege (3055642)	83355	1	CVE-2015-1702	Medium	Medium	6	05/12/2015	MS15-0 Control Elevatio 2012 R2
MS15-069: Vulnerabilities in Windows Could Allow Remote Code Execution (3072631)	84734	1	CVE-2015-2368	Medium	High	9	07/14/2015	MS15-0 Could A Window KB3061
MS15-088: Unsafe Command Line Parameter Passing Could Allow Information Disclosure (3082458)	85334	1	CVE-2015-2423	Medium	Medium	4	08/11/2015	MS15-0 Paramet Informa Server 2
MS15-120: Security Update for IPSec to Address Denial of Service (3102939)	86830	1	CVE-2015-6111	Medium	Low	3	11/10/2015	MS15-1 to Addr Window KB3102
MS15-121: Security Update for Schannel to Address Spoofing (3081320)	86827	1	CVE-2015-6112	Medium	Medium	6	11/10/2015	MS15-1 Schanne Window KB3081
MS16-021: Security Update for NPS RADIUS Server to Address Denial of Service (3133043)	88653	1	CVE-2016-0050	Medium	Low	1	02/09/2016	MS16-0 RADIUS



BIGFIX

Tenable-Detected Vulnerable Devices with Applicable Fixlets - Vulnerability Detail

* BigFix data

Vulnerability Title: MS15-069: Vulnerabilities in Windows Could Allow Remote Code Execution (3072631)

Plugin ID: 84734

Published Date: 07/14/2015

CVSS: Medium

VPR: High

VPR Score: 9

*** Fixlet Title:** MS15-069: Vulnerabilities in Windows Could Allow Remote ...

*** Fixlet ID:** 1506905

*** Fixlet Site:** Patches for Windows

*** Fixlet Source ID:** KB3061512

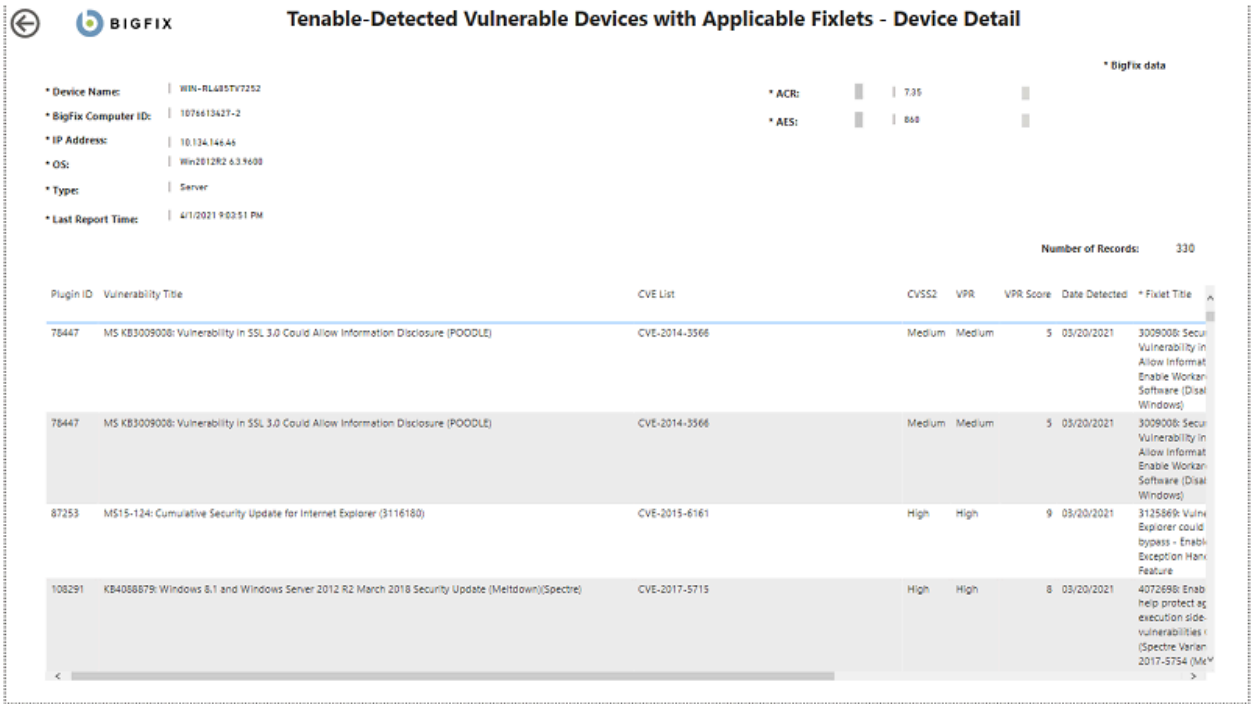
*** Fixlet Category:** Security Update

*** Source Release Date:** 07/14/2015

Right-click on Device ID to drill down

Number of Records: 1

DeviceID	ComputerName	OS	IP Address	Device Type	ACR	AES	Last Report Time
1076613427-2	WIN-RL48STV7252	Win2012R2 6.3.9600	10.134.146.46	Server	7.35	860	4/1/2021 9:03:51 PM



BIGFIX

Tenable-Detected Vulnerable Devices with Applicable Fixlets - Device Detail

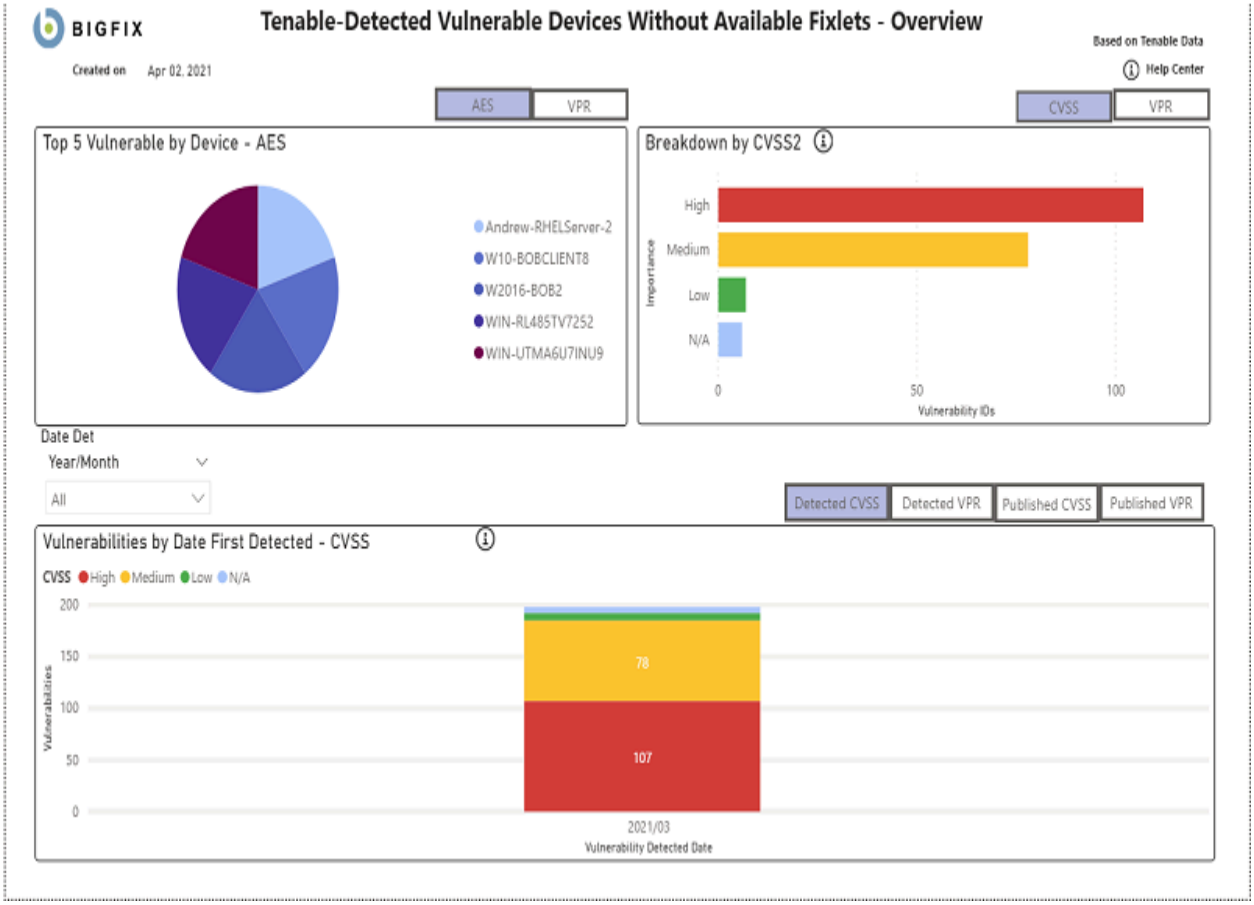
* BigFix data

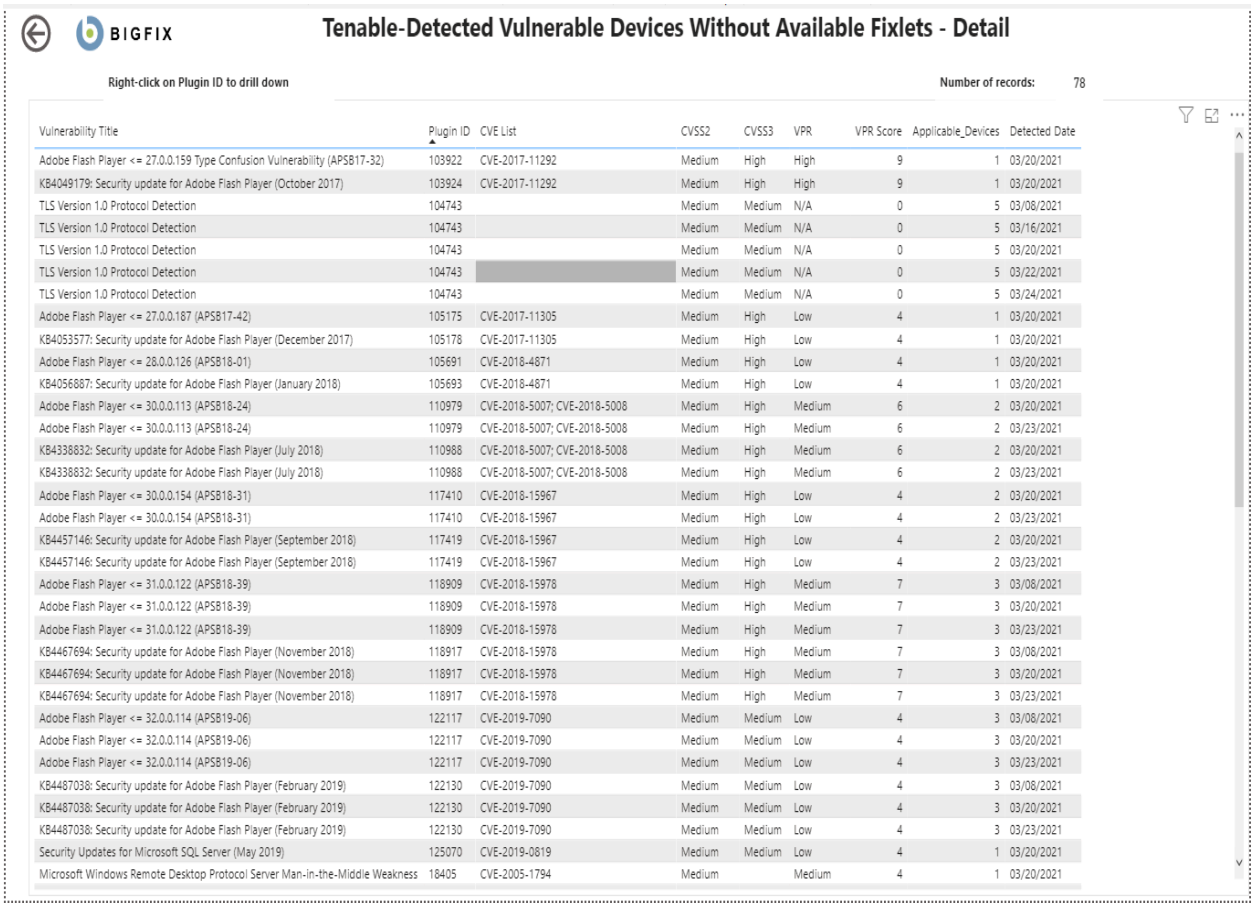
* Device Name:	WIN-RL685TV7252	* ACR:	7.35
* BigFix Computer ID:	1076613627-2	* AES:	868
* IP Address:	10.134.146.46		
* OS:	Win2012R2 6.3.9600		
* Type:	Server		
* Last Report Time:	4/1/2021 9:03:51 PM		

Number of Records: 330

Plugin ID	Vulnerability Title	CVE List	CVSS2	VPR	VPR Score	Date Detected	* Fixlet Title
78447	MS KB3009008: Vulnerability in SSL 3.0 Could Allow Information Disclosure (POODLE)	CVE-2014-3566	Medium	Medium	5	03/20/2021	3009008: Secu Vulnerability in Allow Informat Enable Workar Software (Disal Windows)
78447	MS KB3009008: Vulnerability in SSL 3.0 Could Allow Information Disclosure (POODLE)	CVE-2014-3566	Medium	Medium	5	03/20/2021	3009008: Secu Vulnerability in Allow Informat Enable Workar Software (Disal Windows)
87253	MS15-124: Cumulative Security Update for Internet Explorer (3116180)	CVE-2015-6161	High	High	9	03/20/2021	3125869: Vuln Explorer could bypass - Enabl Exception Har Feature
108291	KB4088879: Windows 8.1 and Windows Server 2012 R2 March 2018 Security Update (Meltdown)(Spectre)	CVE-2017-5715	High	High	8	03/20/2021	4072698: Enab help protect ag execution side- vulnerabilities ((Spectre Varian 2017-5754 (Me

検出された脆弱性 (使用可能な **Fixlet** なし)





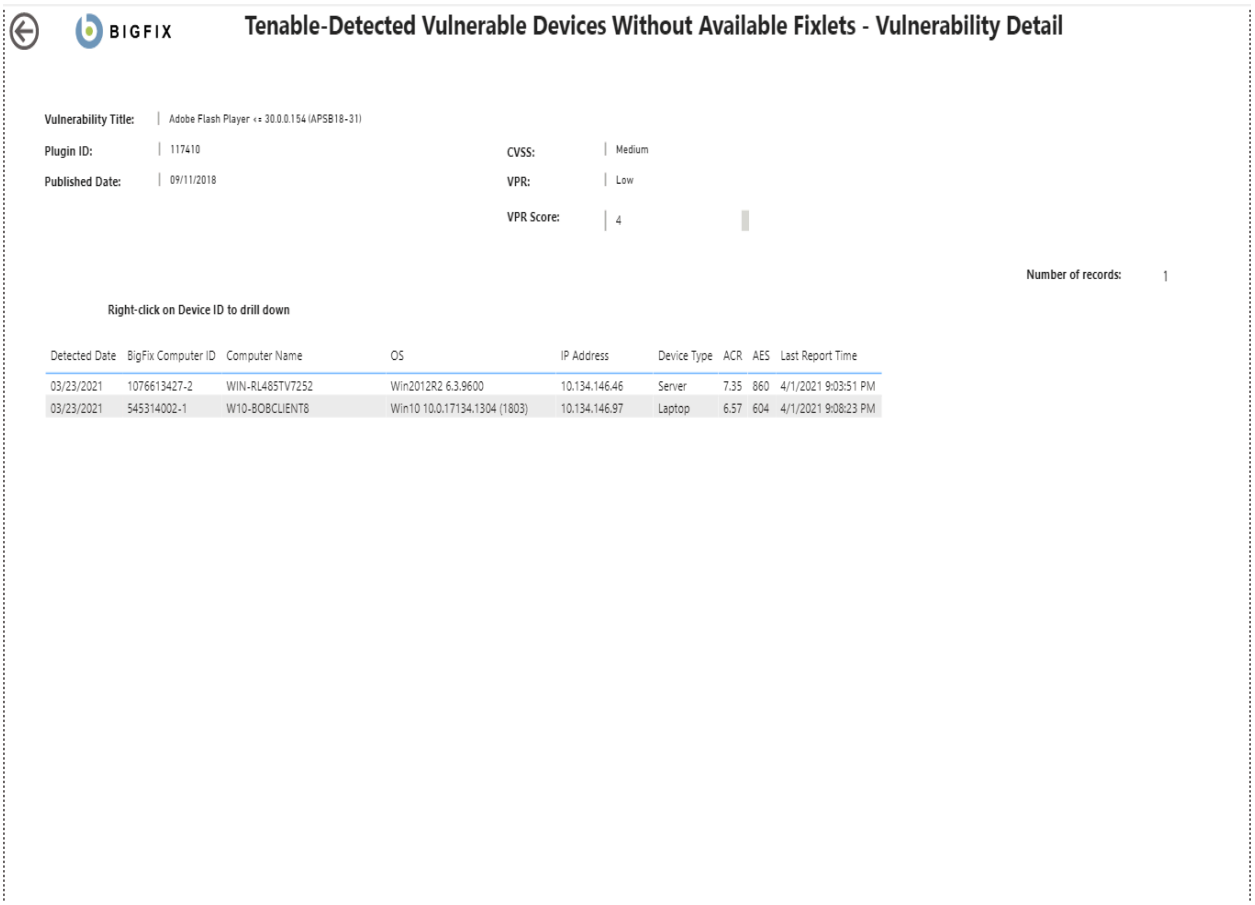
BIGFIX

Tenable-Detected Vulnerable Devices Without Available Fixlets - Detail

Right-click on Plugin ID to drill down

Number of records: 78

Vulnerability Title	Plugin ID	CVE List	CVSS2	CVSS3	VPR	VPR Score	Applicable_Devices	Detected Date
Adobe Flash Player <= 27.0.0.159 Type Confusion Vulnerability (APSB17-32)	103922	CVE-2017-11292	Medium	High	High	9	1	03/20/2021
KB4049179: Security update for Adobe Flash Player (October 2017)	103924	CVE-2017-11292	Medium	High	High	9	1	03/20/2021
TLS Version 1.0 Protocol Detection	104743		Medium	Medium	N/A	0	5	03/08/2021
TLS Version 1.0 Protocol Detection	104743		Medium	Medium	N/A	0	5	03/16/2021
TLS Version 1.0 Protocol Detection	104743		Medium	Medium	N/A	0	5	03/20/2021
TLS Version 1.0 Protocol Detection	104743		Medium	Medium	N/A	0	5	03/22/2021
TLS Version 1.0 Protocol Detection	104743		Medium	Medium	N/A	0	5	03/24/2021
Adobe Flash Player <= 27.0.0.187 (APSB17-42)	105175	CVE-2017-11305	Medium	High	Low	4	1	03/20/2021
KB4053577: Security update for Adobe Flash Player (December 2017)	105178	CVE-2017-11305	Medium	High	Low	4	1	03/20/2021
Adobe Flash Player <= 28.0.0.126 (APSB18-01)	105691	CVE-2018-4871	Medium	High	Low	4	1	03/20/2021
KB4056887: Security update for Adobe Flash Player (January 2018)	105693	CVE-2018-4871	Medium	High	Low	4	1	03/20/2021
Adobe Flash Player <= 30.0.0.113 (APSB18-24)	110979	CVE-2018-5007; CVE-2018-5008	Medium	High	Medium	6	2	03/20/2021
Adobe Flash Player <= 30.0.0.113 (APSB18-24)	110979	CVE-2018-5007; CVE-2018-5008	Medium	High	Medium	6	2	03/23/2021
KB4338832: Security update for Adobe Flash Player (July 2018)	110988	CVE-2018-5007; CVE-2018-5008	Medium	High	Medium	6	2	03/20/2021
KB4338832: Security update for Adobe Flash Player (July 2018)	110988	CVE-2018-5007; CVE-2018-5008	Medium	High	Medium	6	2	03/23/2021
Adobe Flash Player <= 30.0.0.154 (APSB18-31)	117410	CVE-2018-15967	Medium	High	Low	4	2	03/20/2021
Adobe Flash Player <= 30.0.0.154 (APSB18-31)	117410	CVE-2018-15967	Medium	High	Low	4	2	03/23/2021
KB4457146: Security update for Adobe Flash Player (September 2018)	117419	CVE-2018-15967	Medium	High	Low	4	2	03/20/2021
KB4457146: Security update for Adobe Flash Player (September 2018)	117419	CVE-2018-15967	Medium	High	Low	4	2	03/23/2021
Adobe Flash Player <= 31.0.0.122 (APSB18-39)	118909	CVE-2018-15978	Medium	High	Medium	7	3	03/08/2021
Adobe Flash Player <= 31.0.0.122 (APSB18-39)	118909	CVE-2018-15978	Medium	High	Medium	7	3	03/20/2021
Adobe Flash Player <= 31.0.0.122 (APSB18-39)	118909	CVE-2018-15978	Medium	High	Medium	7	3	03/23/2021
KB4467694: Security update for Adobe Flash Player (November 2018)	118917	CVE-2018-15978	Medium	High	Medium	7	3	03/08/2021
KB4467694: Security update for Adobe Flash Player (November 2018)	118917	CVE-2018-15978	Medium	High	Medium	7	3	03/20/2021
KB4467694: Security update for Adobe Flash Player (November 2018)	118917	CVE-2018-15978	Medium	High	Medium	7	3	03/23/2021
Adobe Flash Player <= 32.0.0.114 (APSB19-06)	122117	CVE-2019-7090	Medium	Medium	Low	4	3	03/08/2021
Adobe Flash Player <= 32.0.0.114 (APSB19-06)	122117	CVE-2019-7090	Medium	Medium	Low	4	3	03/20/2021
Adobe Flash Player <= 32.0.0.114 (APSB19-06)	122117	CVE-2019-7090	Medium	Medium	Low	4	3	03/23/2021
KB4487038: Security update for Adobe Flash Player (February 2019)	122130	CVE-2019-7090	Medium	Medium	Low	4	3	03/08/2021
KB4487038: Security update for Adobe Flash Player (February 2019)	122130	CVE-2019-7090	Medium	Medium	Low	4	3	03/20/2021
KB4487038: Security update for Adobe Flash Player (February 2019)	122130	CVE-2019-7090	Medium	Medium	Low	4	3	03/23/2021
Security Updates for Microsoft SQL Server (May 2019)	125070	CVE-2019-0819	Medium	Medium	Low	4	1	03/20/2021
Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	18405	CVE-2005-1794	Medium		Medium	4	1	03/20/2021



BIGFIX

Tenable-Detected Vulnerable Devices Without Available Fixlets - Vulnerability Detail

Vulnerability Title: Adobe Flash Player <= 30.0.0.154 (APSB18-31)

Plugin ID: 117410

Published Date: 09/11/2018

CVSS: Medium

VPR: Low

VPR Score: 4

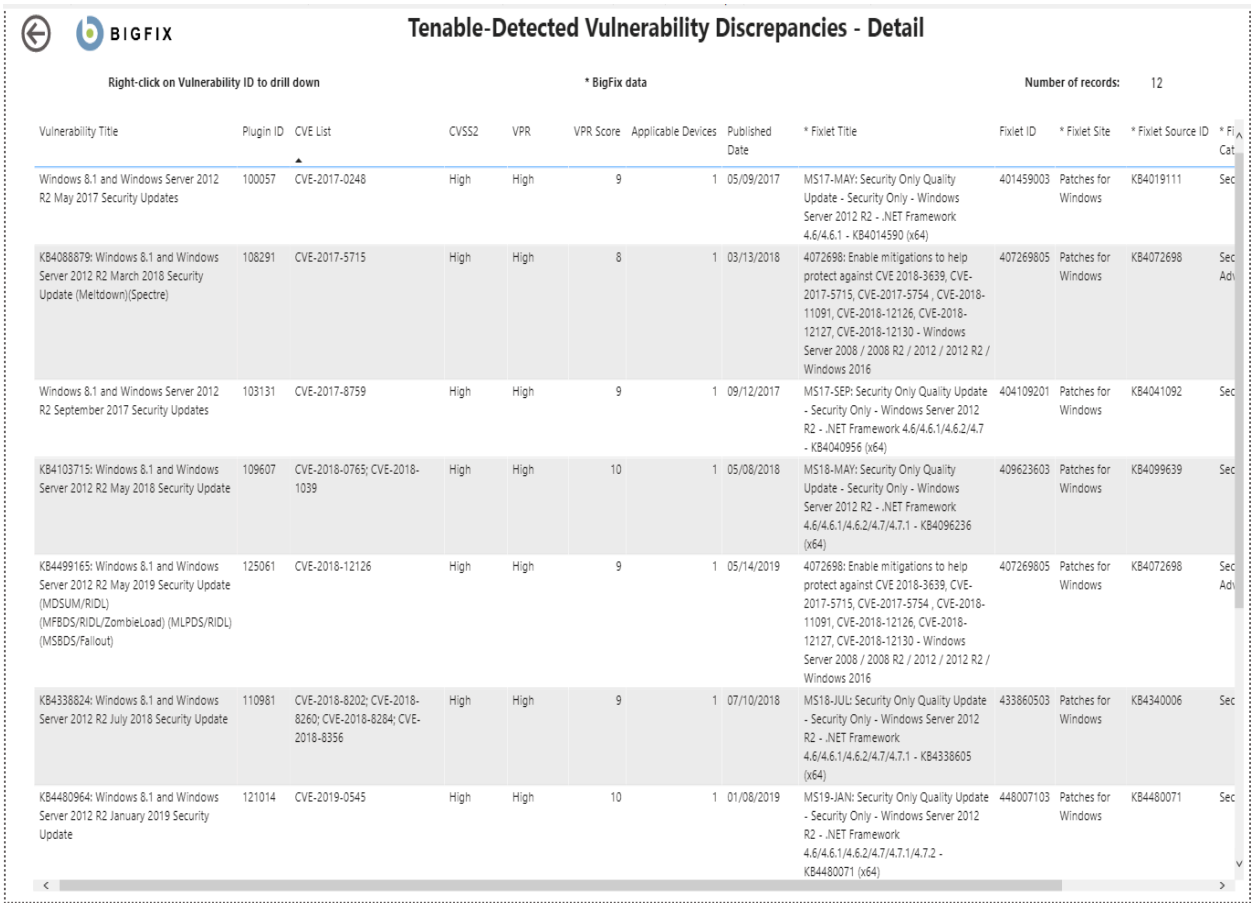
Number of records: 1

Right-click on Device ID to drill down

Detected Date	BigFix Computer ID	Computer Name	OS	IP Address	Device Type	ACR	AES	Last Report Time
03/23/2021	1076613427-2	WIN-RL485TV7252	Win2012R2 6.3.9600	10.134.146.46	Server	7.35	860	4/1/2021 9:03:51 PM
03/23/2021	545314002-1	W10-BOBCLIENT8	Win10 10.0.17134.1304 (1803)	10.134.146.97	Laptop	6.57	604	4/1/2021 9:08:23 PM

脆弱性の不一致


BIGFIX
Tenable-Detected Vulnerability Discrepancies - Overview
Based on Tenable Data
Created on Apr 02, 2021
Help Center
AES
VPR
CVSS
VPR
Top 5 Vulnerable by Device - AES
WIN-RL485TV7252
WIN-UTMA6U7INU9
Breakdown by VPR
High
Medium
Low
Severity
0
2
4
6
8
Vulnerability IDs
Date Pub
Year/Month
All
Detected CVSS
Detected VPR
Published CVSS
Published VPR
Vulnerabilities with Fixlets by Date First Detected - CVSS
CVSS High Medium
2
12
10
5
0
Vulnerabilities
2021/03
Vulnerability Detected Date

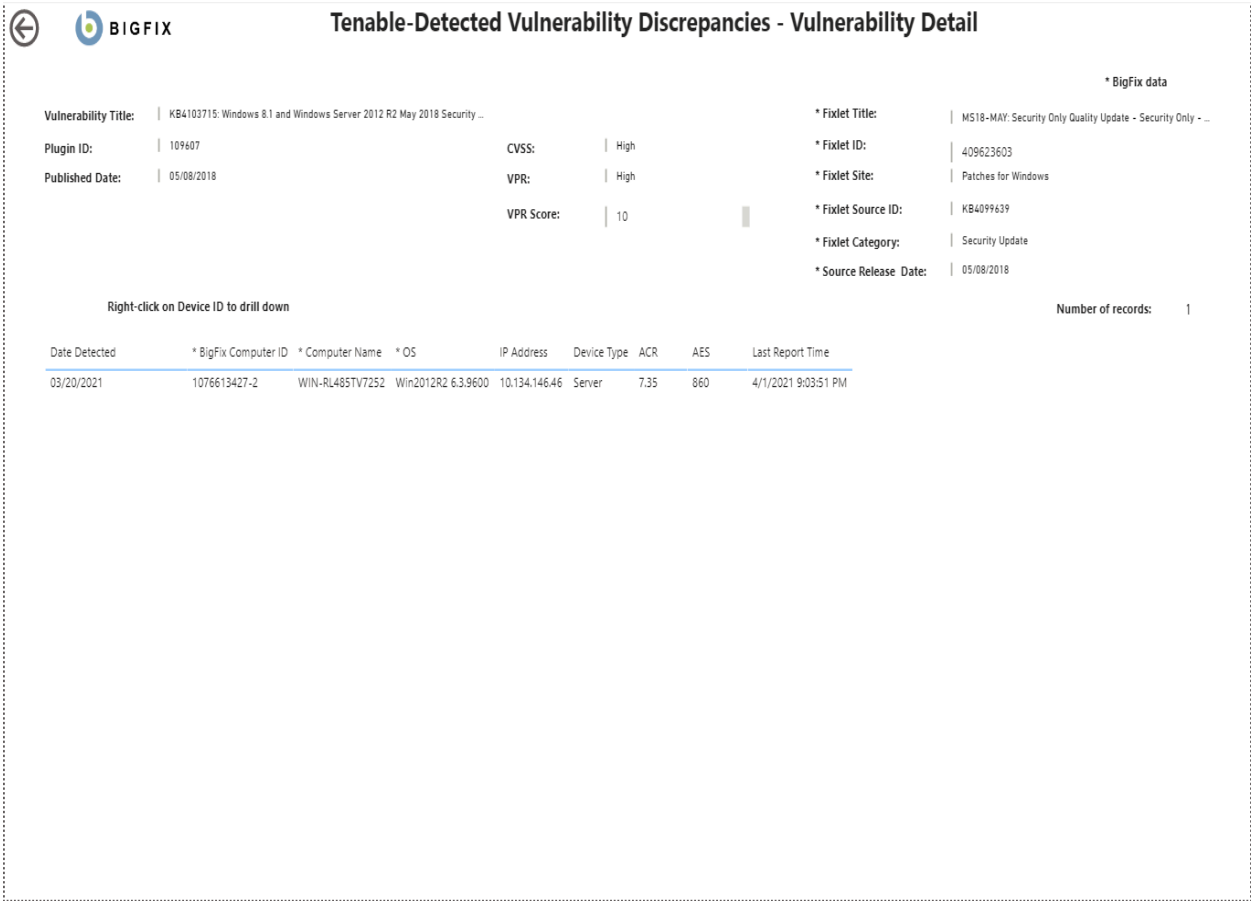


BIGFIX

Tenable-Detected Vulnerability Discrepancies - Detail

Right-click on Vulnerability ID to drill down | *** BigFix data** | **Number of records:** 12

Vulnerability Title	Plugin ID	CVE List	CVSS2	VPR	VPR Score	Applicable Devices	Published Date	* Fixlet Title	Fixlet ID	* Fixlet Site	* Fixlet Source ID	* Fi... Cat...
Windows 8.1 and Windows Server 2012 R2 May 2017 Security Updates	100057	CVE-2017-0248	High	High	9	1	05/09/2017	MS17-MAY: Security Only Quality Update - Security Only - Windows Server 2012 R2 - .NET Framework 4.6/4.6.1 - KB4014590 (x64)	401459003	Patches for Windows	KB4019111	Sec...
KB4088879: Windows 8.1 and Windows Server 2012 R2 March 2018 Security Update (Meltdown)(Spectre)	108291	CVE-2017-5715	High	High	8	1	03/13/2018	4072698: Enable mitigations to help protect against CVE 2018-3639, CVE-2017-5715, CVE-2017-5754 , CVE-2018-11091, CVE-2018-12126, CVE-2018-12127, CVE-2018-12130 - Windows Server 2008 / 2008 R2 / 2012 / 2012 R2 / Windows 2016	407269805	Patches for Windows	KB4072698	Sec... Adv...
Windows 8.1 and Windows Server 2012 R2 September 2017 Security Updates	103131	CVE-2017-8759	High	High	9	1	09/12/2017	MS17-SEP: Security Only Quality Update - Security Only - Windows Server 2012 R2 - .NET Framework 4.6/4.6.1/4.6.2/4.7 - KB4040956 (x64)	404109201	Patches for Windows	KB4041092	Sec...
KB4103715: Windows 8.1 and Windows Server 2012 R2 May 2018 Security Update	109607	CVE-2018-0765; CVE-2018-1039	High	High	10	1	05/08/2018	MS18-MAY: Security Only Quality Update - Security Only - Windows Server 2012 R2 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1 - KB4096236 (x64)	409623603	Patches for Windows	KB4099639	Sec...
KB4499165: Windows 8.1 and Windows Server 2012 R2 May 2019 Security Update (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)	125061	CVE-2018-12126	High	High	9	1	05/14/2019	4072698: Enable mitigations to help protect against CVE 2018-3639, CVE-2017-5715, CVE-2017-5754 , CVE-2018-11091, CVE-2018-12126, CVE-2018-12127, CVE-2018-12130 - Windows Server 2008 / 2008 R2 / 2012 / 2012 R2 / Windows 2016	407269805	Patches for Windows	KB4072698	Sec... Adv...
KB4338824: Windows 8.1 and Windows Server 2012 R2 July 2018 Security Update	110981	CVE-2018-8202; CVE-2018-8260; CVE-2018-8264; CVE-2018-8356	High	High	9	1	07/10/2018	MS18-JUL: Security Only Quality Update - Security Only - Windows Server 2012 R2 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1 - KB4338605 (x64)	433860503	Patches for Windows	KB4340006	Sec...
KB4480964: Windows 8.1 and Windows Server 2012 R2 January 2019 Security Update	121014	CVE-2019-0545	High	High	10	1	01/08/2019	MS19-JAN: Security Only Quality Update - Security Only - Windows Server 2012 R2 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4480071 (x64)	448007103	Patches for Windows	KB4480071	Sec...



BIGFIX

Tenable-Detected Vulnerability Discrepancies - Vulnerability Detail

Vulnerability Title: KB4103715: Windows 8.1 and Windows Server 2012 R2 May 2018 Security ...
Plugin ID: 109607
Published Date: 05/08/2018
CVSS: High
VPR: High
VPR Score: 10

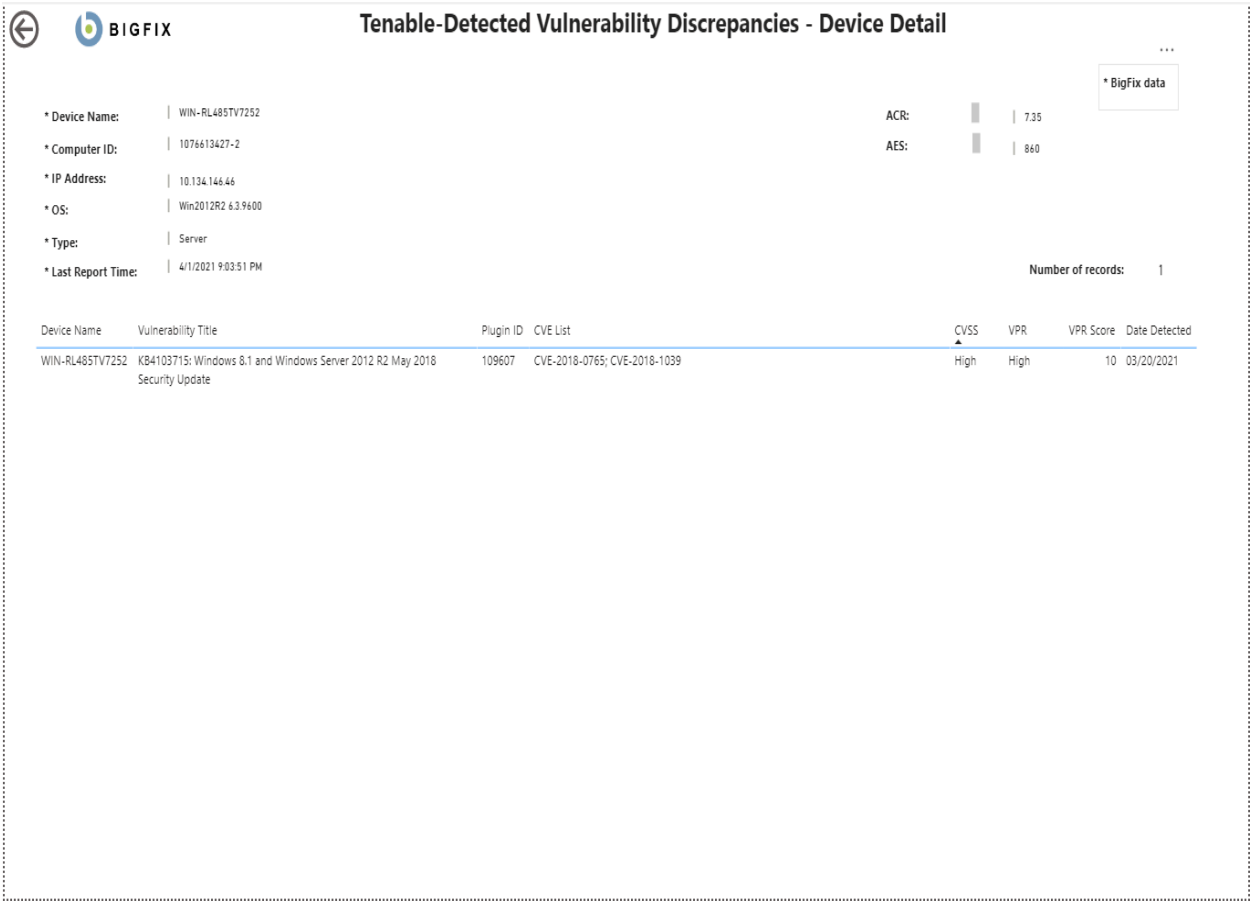
*** BigFix data**

*** Fixlet Title:** MS18-MAY: Security Only Quality Update - Security Only - ...
*** Fixlet ID:** 409623603
*** Fixlet Site:** Patches for Windows
*** Fixlet Source ID:** KB4099639
*** Fixlet Category:** Security Update
*** Source Release Date:** 05/08/2018

Right-click on Device ID to drill down

Number of records: 1

Date Detected	* BigFix Computer ID	* Computer Name	* OS	IP Address	Device Type	ACR	AES	Last Report Time
03/20/2021	1076613427-2	WIN-RL485TV7252	Win2012R2 6.3.9600	10.134.146.46	Server	7.35	860	4/1/2021 9:03:51 PM



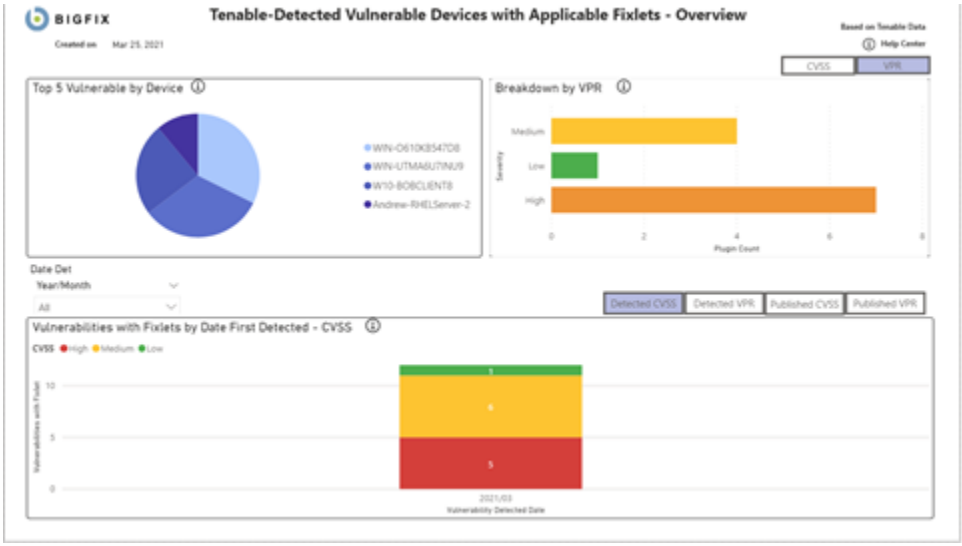
Tenable.sc 用 Power BI レポート

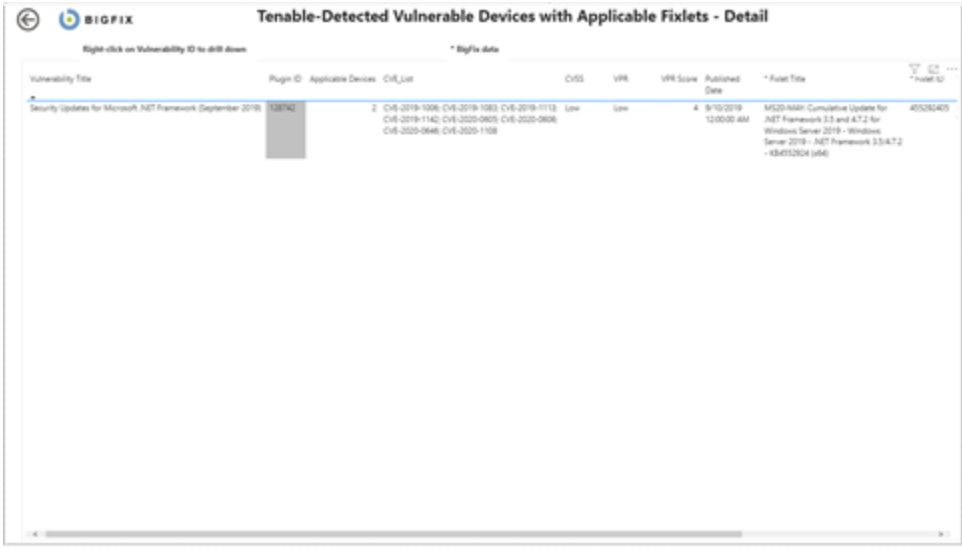
このセクションを読むことで、Tenable.sc 用 Power BI レポートの理解を深めることができます。

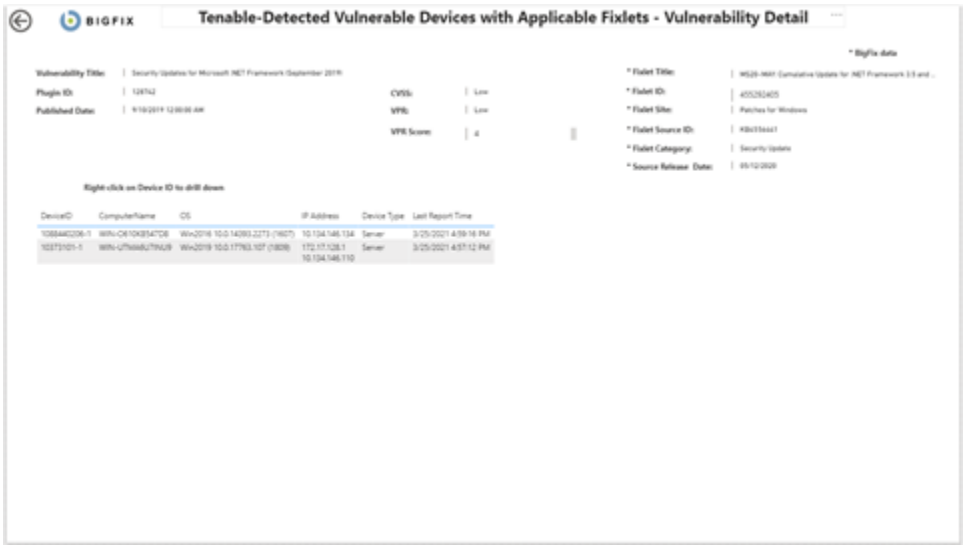
チャートの詳細:

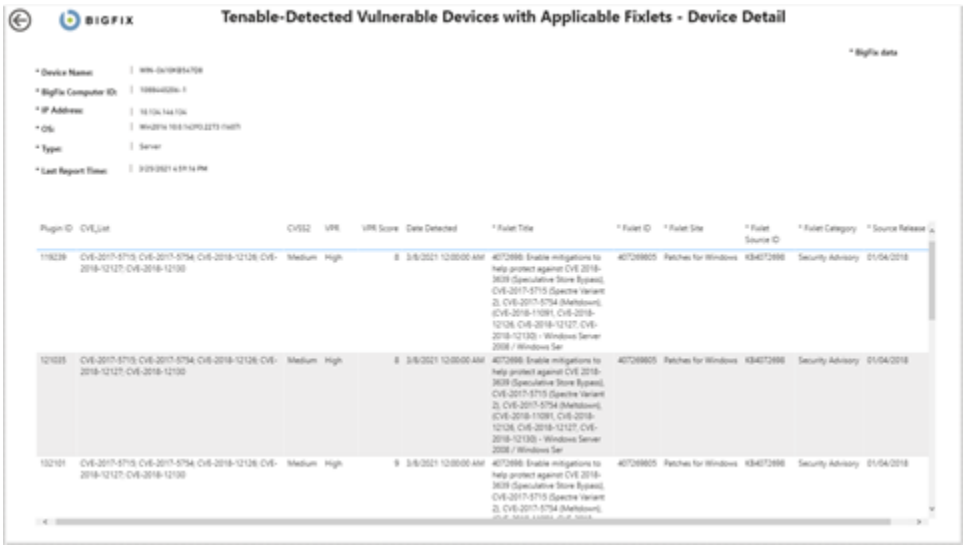
- 脆弱性タイトル - 脆弱性タイトル
- PluginID - 脆弱性の検出に割り当てられた一意の識別子
- 該当デバイス - Tenable によってスキャンされ、脆弱性が特定されたデバイス
- CVE リスト - CVE のリスト
- CVSS2 - (Common Vulnerability Scoring System バージョン 2)、セキュリティーの脆弱性の重大度と潜在的な影響を評価するために使用されるスコアリング・システム。
- CVSS3 - (Common Vulnerability Scoring System バージョン 3)、スコアリング・システムの更新バージョン
- VPR - 脆弱性優先順位の評価
- VPR スコア - 0 ~ 10 の範囲の数値。10 が最も高い優先度を示します
- 検出日 - 脆弱性が最初に検出された日付
- 公開日 - 脆弱性に関する情報が最初に利用可能になった日付

検出された脆弱性 (適用可能な **Fixlet** あり)

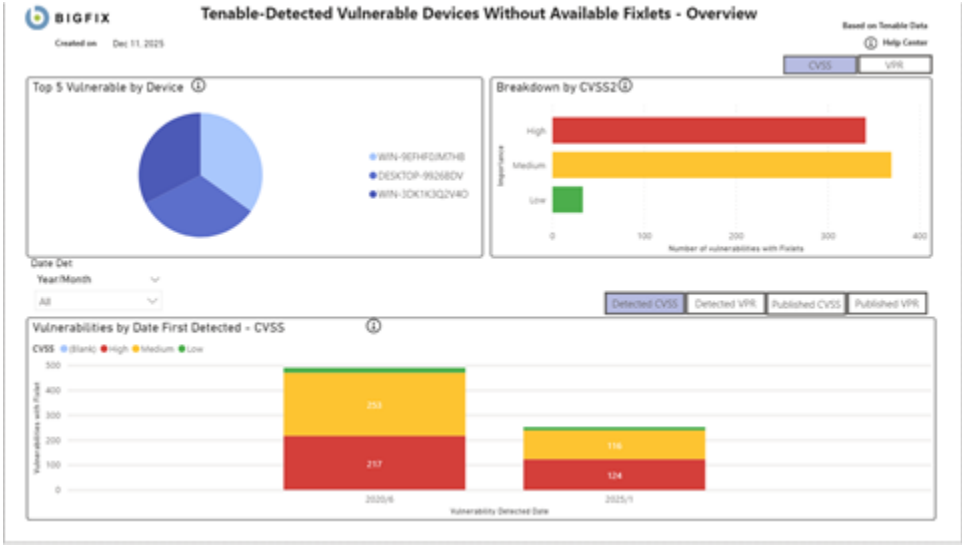


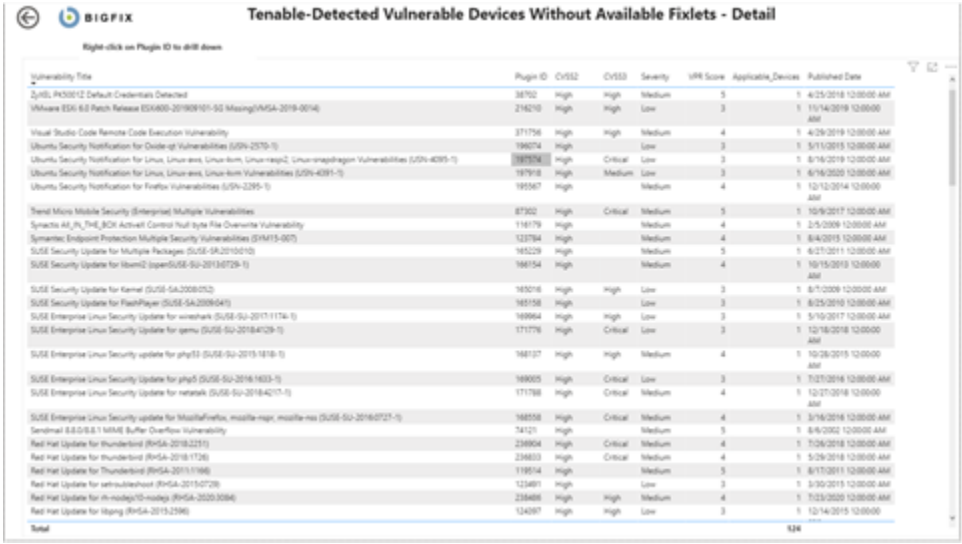



BIGFIX
Tenable-Detected Vulnerable Devices with Applicable Fixlets - Vulnerability Detail
* BigFix data
Vulnerability Title:
Plugin ID:
Published Date:
CVSS:
VPR:
VPR Score:
* Fixlet Title:
* Fixlet ID:
* Fixlet Site:
* Fixlet Source ID:
* Fixlet Category:
* Source Release Date:
Right-click on Device ID to drill down
DeviceID
ComputerName
OS
IP Address
Device Type
Last Report Time


BIGFIX
Tenable-Detected Vulnerable Devices with Applicable Fixlets - Device Detail
* BigFix data
* Device Name:
* BigFix Computer ID:
* IP Address:
* OS:
* Type:
* Last Report Time:
Plugin ID
CVE_List
CVSS2
VPR
VPR Score
Date Detected
* Fixlet Title
* Fixlet ID
* Fixlet Site
* Fixlet Source ID
* Fixlet Category
* Source Release

検出された脆弱性 (使用可能な **Fixlet** なし)

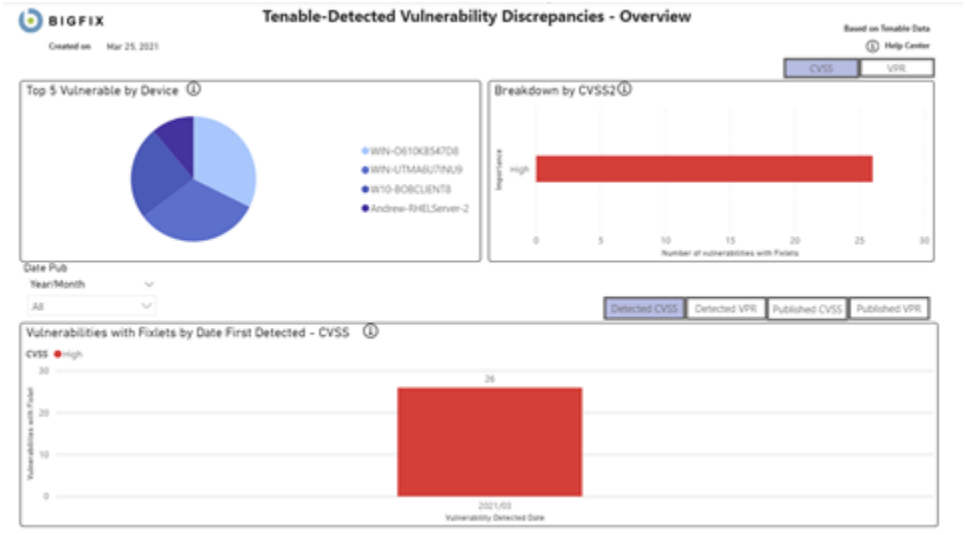


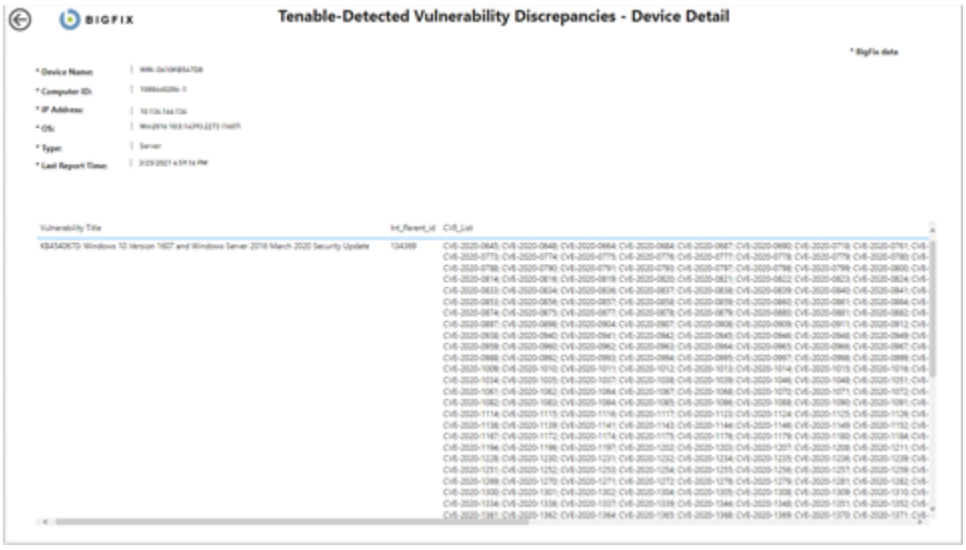



BIGFIX
Tenable-Detected Vulnerable Devices Without Available Fixlets - Device Detail
* BigFix data
* Device Name:
* Computer ID:
* IP Address:
* OS:
* Type:
* Last Report Time:
Vulnerability Title
Plugin ID
CVSS
VPR
VPR Score
Date Detected
Ubuntu Security Notification for Linux, Linux-aws, Linux-kvm, Linux-raspi2, Linux-snapdragon Vulnerabilities (USN-4095-1)
197574
High
Low
3
1/1/2025 12:00:00 AM


BIGFIX
Tenable-Detected Vulnerable Devices Without Available Fixlets - Vulnerability Detail
Vulnerability Title:
Plugin ID:
Published Date:
CVSS:
VPR:
VPR Score:
Right-click on Device ID to drill down
Date Detected
BigFix Computer ID
Computer Name
OS
IP Address
Device Type
Last Report Time
1/1/2025 12:00:00 AM
1622894162-1
WIN-3DK1KQ2V4O
Win2019 10.0.17763.107 (1809)
10.134.146.184
Server
2/16/2021 4:05:18 PM

脆弱性の不一致


BIGFIX
Tenable-Detected Vulnerability Discrepancies - Overview
Created on Mar 25, 2021
Based on Tenable Data
Help Center
CVSS
VPR
Top 5 Vulnerable by Device
WIN-O610KB547D8
WIN-UTMA6UTINU9
W10-BOBCLIENT8
Andrew-RHELServer-2
Breakdown by CVSS2
High
Importance
0
5
10
15
20
25
30
Number of vulnerabilities with Fixlets
Date Pub
Year/Month
All
Detected CVSS
Detected VPR
Published CVSS
Published VPR
Vulnerabilities with Fixlets by Date First Detected - CVSS
CVSS High
30
20
10
0
Vulnerabilities with Fixlet
26
2021/03
Vulnerability Detected Date


BIGFIX
Tenable-Detected Vulnerability Discrepancies - Device Detail
* BigFix data
* Device Name:
* Computer ID:
* IP Address:
* OS:
* Type:
* Last Report Time:
Vulnerability Title
Int_Parent_id
CVE_List
KB4540670: Windows 10 Version 1607 and Windows Server 2016 March 2020 Security Update
134389


BIGFIX
Tenable-Detected Vulnerability Discrepancies - Vulnerability Detail
* BigFix data
Vulnerability Title:
Plugin ID:
Published Date:
CVSS:
VPR:
VPR Score:
* Fixlet Title:
* Fixlet ID:
* Fixlet Site:
* Fixlet Source ID:
* Fixlet Category:
* Source Release Date:
Right-click on Device ID to drill down
Date Detected
* BigFix Computer ID
* Computer Name
* OS
IP Address
Device Type
Last Report Time

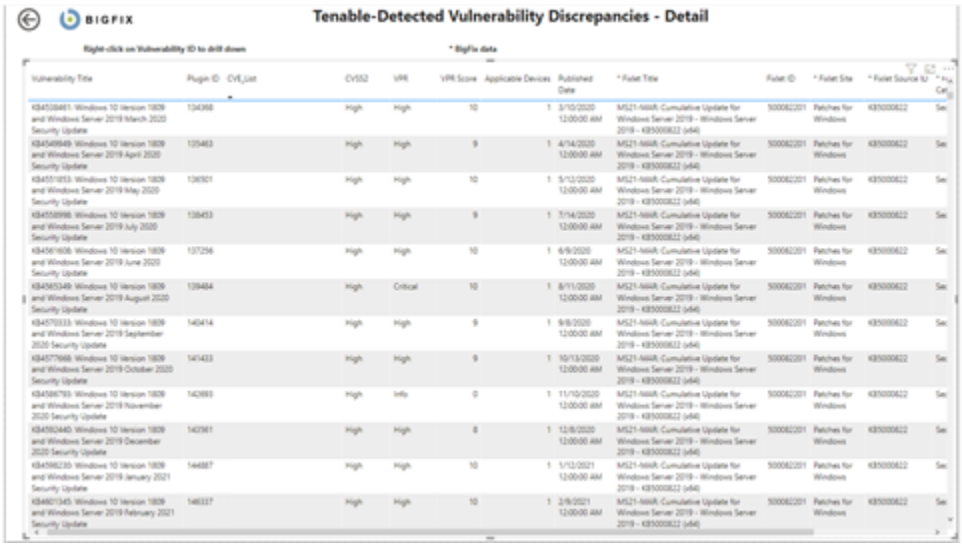


Tableau レポート

このセクションを読むことで、Tableau レポートの理解を深めることができます。

Tableau のレポート対象:

- Qualys
- Tenable.io
- Tenable.sc

レポートは Tableau バージョン 2020 4 以降で生成されます。

- レポートの違い: レポートの機能は、Power BI と Tableau でほぼ同じです。このセクションでは、レポートの相違点について詳しく説明します。
- ナビゲーション: 各視覚化はダッシュボード・ページに表示されます。ビジネス・プロセスに適用されない視覚化は、必要に応じて削除できます

- Qualys 重要度

  重要度の値は、脆弱性に関連する相対的なセキュリティー上のリスクを測定するために、Qualys によって提供されます。この測定に含まれる要素は次のとおりです。

  - 考えられる結果
  - 複雑度
  - 通常の条件下でエクスプロイトが行われる可能性
  - ネットワーク・ロケーション
  - アタッカーが必要とする権限

- 影響を受けるソフトウェアの普及度
- 既知の攻撃の存在

IVR データベースでは、情報は vulnerabilities.severity 列に格納されます。レポート集計テーブルは、数値スコアと、以下のマトリックスに対応する値 (該当する場合) の両方を返します。

表 4.

重大度値	レベル値
1	最小
2	中
3	重大
4	重大
5	至急

ベンダーによるこのトピックの詳細については、 を参照してください。 https://qualysguard.qualys.com/qwebhelp/fo_portal/knowledgebase/severity_levels.htm

- Tenable 重大度

脆弱性優先順位の評価 (VPR) 値は、脆弱性に関連する相対的なセキュリティー上のリスクを測定するために Tenable によって提供されます。この測定に含まれる要素は次のとおりです。

- 脆弱性の存続期間
- CVSSv3 の影響スコア
- 悪用コードの完成度
- 製品範囲
- 脅威のソース
- 脅威の強度
- 脅威の最新性

IVR データベースでは、情報は vulnerabilities.vendor_rating 列に格納されます。レポート集計テーブルは、数値スコアと、以下のマトリックスに対応する値 (該当する場合) の両方を返します。

表 5.

VPR 値	レベル値
9.0 ~ 10.0	重大
7.0 ~ 8.9	高

VPR 値	レベル値
4.0 ~ 6.9	中
0.1 ~ 3.9	低

ベンダーによるこのトピックの詳細については、 を参照してください。 https://docs.tenable.com/tenablesc/Content/RiskMetrics.htm

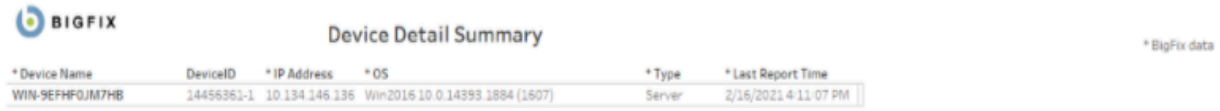
Qualys 用 Tableau レポート

このセクションを読むことで Qualys 用 Tableau レポートの理解を深めることができます。

チャートの詳細:

- 脆弱性タイトル - 脆弱性タイトル
- 脆弱性 ID - 脆弱性に割り当てられた一意の識別子
- デバイス名 - デバイスの名前
- 重大度 - 脆弱性に関連付けられたリスクのレベル。重大度評価の範囲は 1 ~ 5 です
- 検出日 - 脆弱性が最初に検出された日付
- CVSS2 - Common Vulnerability Scoring System バージョン 2
- 該当するデバイス - 脆弱性の影響を受けるデバイス

検出された脆弱性 (適用可能な **Fixlet** あり)

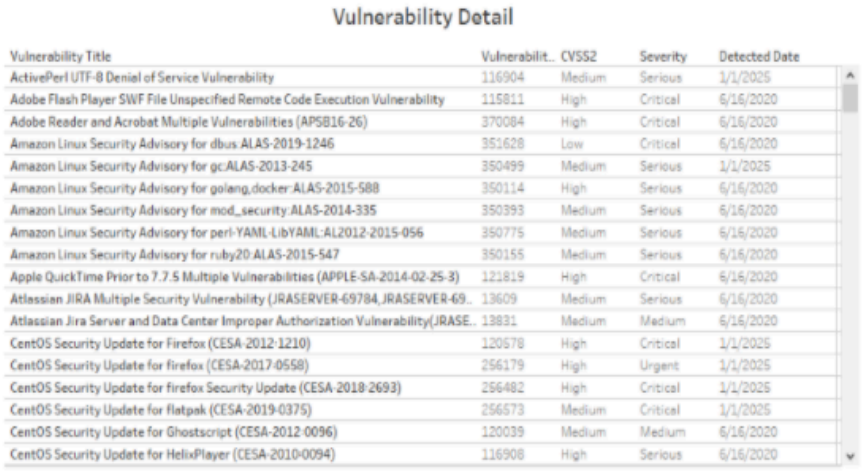


BIGFIX

Device Detail Summary

* BigFix data

* Device Name	DeviceID	* IP Address	* OS	* Type	* Last Report Time
WIN-9EFHF0JM7HB	14456361-1	10.134.146.136	Win2016 10.0.14393.1884 (1607)	Server	2/16/2021 4:11:07 PM



Vulnerability Detail

Vulnerability Title	Vulnerabilit..	CVSS2	Severity	Detected Date
ActivePerl UTF-8 Denial of Service Vulnerability	116904	Medium	Serious	1/1/2025
Adobe Flash Player SWF File Unspecified Remote Code Execution Vulnerability	115811	High	Critical	6/16/2020
Adobe Reader and Acrobat Multiple Vulnerabilities (APSB16-26)	370084	High	Critical	6/16/2020
Amazon Linux Security Advisory for dbus:ALAS-2019-1246	351628	Low	Critical	6/16/2020
Amazon Linux Security Advisory for gc:ALAS-2013-245	350499	Medium	Serious	1/1/2025
Amazon Linux Security Advisory for golang,docker:ALAS-2015-588	350114	High	Serious	6/16/2020
Amazon Linux Security Advisory for mod_security:ALAS-2014-335	350393	Medium	Serious	6/16/2020
Amazon Linux Security Advisory for perl-YAML-LibYAML:AL2012-2015-056	350775	Medium	Serious	6/16/2020
Amazon Linux Security Advisory for ruby20:ALAS-2015-547	350155	Medium	Serious	6/16/2020
Apple QuickTime Prior to 7.7.5 Multiple Vulnerabilities (APPLE-SA-2014-02-25-3)	121819	High	Critical	6/16/2020
Atlassian JIRA Multiple Security Vulnerability (JRASERVER-69784,JRASERVER-69..	13609	Medium	Serious	6/16/2020
Atlassian Jira Server and Data Center Improper Authorization Vulnerability(JRASE..	13831	Medium	Medium	6/16/2020
CentOS Security Update for Firefox (CESA-2012:1210)	120578	High	Critical	1/1/2025
CentOS Security Update for firefox (CESA-2017:0558)	256179	High	Urgent	1/1/2025
CentOS Security Update for firefox Security Update (CESA-2018:2693)	256482	High	Critical	1/1/2025
CentOS Security Update for flatpak (CESA-2019:0375)	256573	Medium	Critical	1/1/2025
CentOS Security Update for Ghostscript (CESA-2012:0096)	120039	Medium	Medium	6/16/2020
CentOS Security Update for HelixPlayer (CESA-2010:0094)	116908	High	Serious	6/16/2020

BIGFIX

Vulnerability Device Summary

*BigFix Data

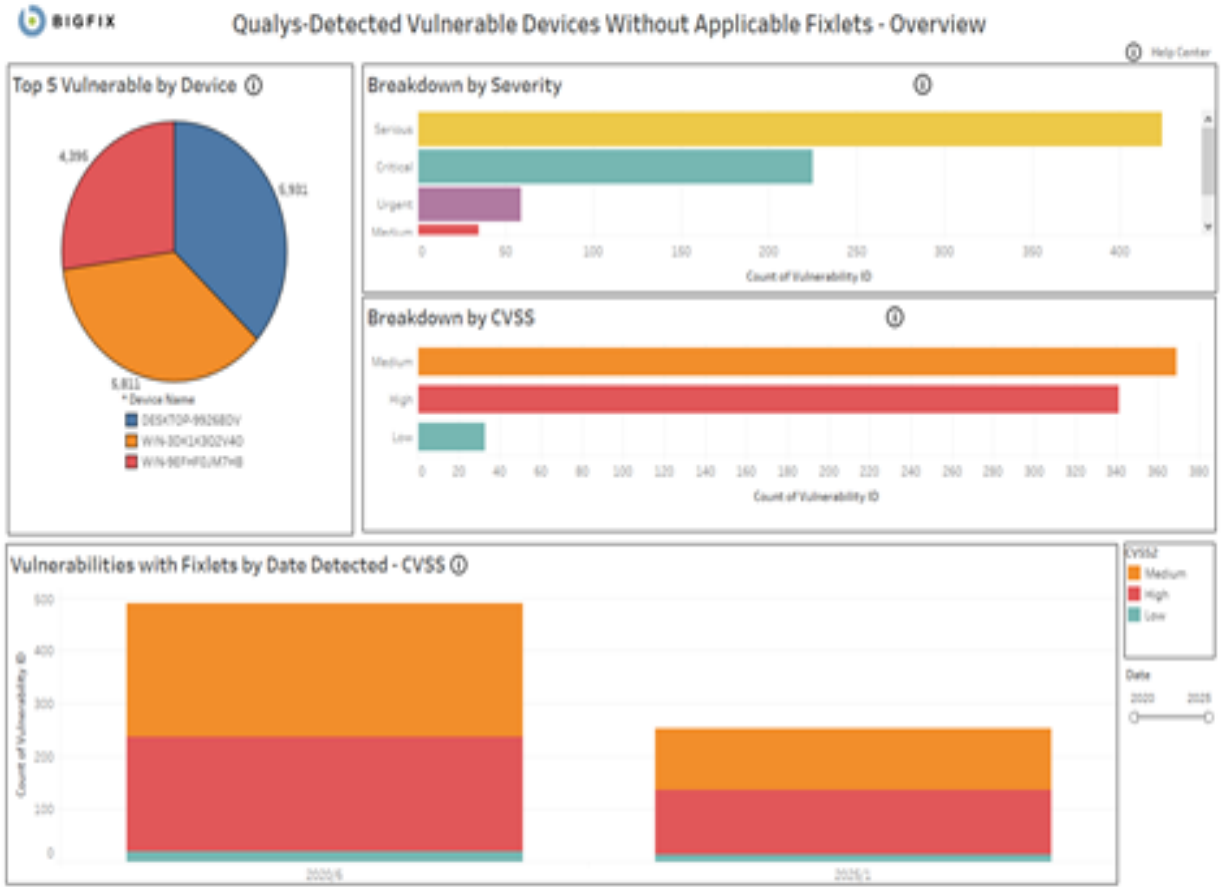
Vulnerabilit..	Vulnerabilit..	CVE List	Year of Pub..	CVSS2	Severity	* Fixlet Title	* Fixlet ID	* Fixlet Site	* Fixlet Sou..	* Fixlet Category	* Source Release Da..
Adobe Flas..	137253	CVE-2020-3..	2020	High	Critical	MS20-OCT Security Update for Adobe Flash Player fo..	468032615	Patches for Windo..	KB4580325	Security Update	10/13/2020

Right-click on Device ID to drill down

Vulnerability Device Detail

Detected Date	DeviceID	* Device Name	* OS	* IP Address	* Type	* Last Report Time
3/8/2021	10373101-1	WIN-UTM66L7T6L9	Win2019 10.0.17763.107 (..	172.17.128.1..	Server	3/25/2021 4:57:12 PM
	5453140002-1	W10-BOBCL-ENT8	Win10 10.0.17134.1304 (1..	10.134.146.97	Laptop	3/25/2021 4:54:11 PM

検出された脆弱性 (使用可能な **Fixlet** なし)



BIGFIX

Right-click on Vulnerability ID to dr..

* BigFix data

Vulnerability List

Vulnerability Title	Vulnerability ID	CVSS2	Severity	Applicable_Devices	Year of Published Date
Amazon Linux Security Advisory for dbus: ALAS-2019-1246	181628	Low	Critical	1	2019
Amazon Linux Security Advisory for quagga: ALAS-2012-070	180877	Low	Serious	1	2016
Atlassian Fisheye and Crucible Cross-Site Scripting Vulnerability ...	13427	Low	Serious	1	2019
CentOS Security Update for libvirt (CESA-2012:1202)	120574	Low	Medium	1	2012
CentOS Security Update for libvirt: test (CESA-2011:0478)	119287	Low	Serious	1	2011
CentOS Security Update for OpenSSH (CESA-2007:0292)	117847	Low	Medium	1	2010
CentOS Security Update for PAM (CESA-2007:0401)	117815	Low	Serious	1	2010
CentOS Security Update for qemu-kvm (CESA-2017:1896)	296277	Low	Critical	1	2017
CentOS Security Update for util-linux-ng (CESA-2013:0517)	121109	Low	Serious	1	2013
Debian Security Update for mailman (DSA 4246-1)	176429	Low	Serious	1	2018
Drupal core File Module Cross Site Scripting Vulnerability (SA-C...	13463	Low	Serious	1	2019
Fedora Security Update for libumberd (FEDORA-2015-11865)	134023	Low	Serious	1	2015
Fedora Security Update for qemu (FEDORA-2016-2b264eb6ad)	276023	Low	Serious	1	2016
Fedora Security Update for xlogmins (FEDORA-2014-1482)	122991	Low	Serious	1	2014
Fedora Security Update for sudo (FEDORA-2015-2247)	123347	Low	Serious	1	2015
Fedora Security Update for xen (FEDORA-2016-da6b1d277b)	274264	Low	Serious	1	2016
iPlanet Calendar Server Plaintext Admin Password Vulnerability	86184	Low	Urgent	1	2001
McAfee VirusScan 4.0.3 Alert File Vulnerability	38313	Low	Serious	1	2004
OpenSuSE Security Update for libvirt (openSUSE-SU-2014:0810-...	184706	Low	Serious	1	2014
OpenSuSE Security Update for ihvm (openSUSE-SU-2015:0295-1)	187600	Low	Serious	1	2015
OpenSuSE Security Update for XWayland (openSUSE-SU-2015:1...	187944	Low	Serious	1	2015
Oracle Enterprise Linux Security Update for libgcrypt (ELSA-201...	186707	Low	Serious	1	2014
Oracle Enterprise Linux Security Update for qemu-kvm (ELSA-20...	188022	Low	Medium	1	2019
PostNuke Cross Site Scripting Vulnerability	12643	Low	Serious	1	2002
Red Hat Update for OpenShift Container Platform 4.5.4 jenkins-...	298830	Low	Serious	1	2020
Skype Technologies Skype URI Handling Remote File Download V...	38647	Low	Serious	1	2006
SUSE Enterprise Linux Security Update for dbus-1 (SUSE-SU-201...	167211	Low	Serious	1	2014
SUSE Enterprise Linux Security Update for libapr1 (SUSE-SU-201...	171132	Low	Serious	1	2018
SUSE Enterprise Linux Security Update for Wireshark (SUSE-SU-...	165499	Low	Serious	1	2012
SUSE Security Update for libgd4 (openSUSE-SU-2013:0404-1)	165870	Low	Medium	1	2013

BIGFIX

Vulnerability Device Summary

* BigFix data

Vulnerability Title	Vulnerability ID	Year of Pub..	CVSS2	Severity
CentOS Security Update for libvirt (CESA-2012:1202)	120574	2012	Low	Medium

Right-click on Device ID to drill down

Vulnerability Device Detail

Detected Date	DeviceID	* Device Name	* OS	* IP Address	* Type	* Last Report Time
6/16/2020	14456361-1	WIN-9EFHF0JM7HB	Win2016 10.0.14393.1884 ...	10.134.146.136	Server	2/16/2021 4:11:07 PM

Device Detail Summary

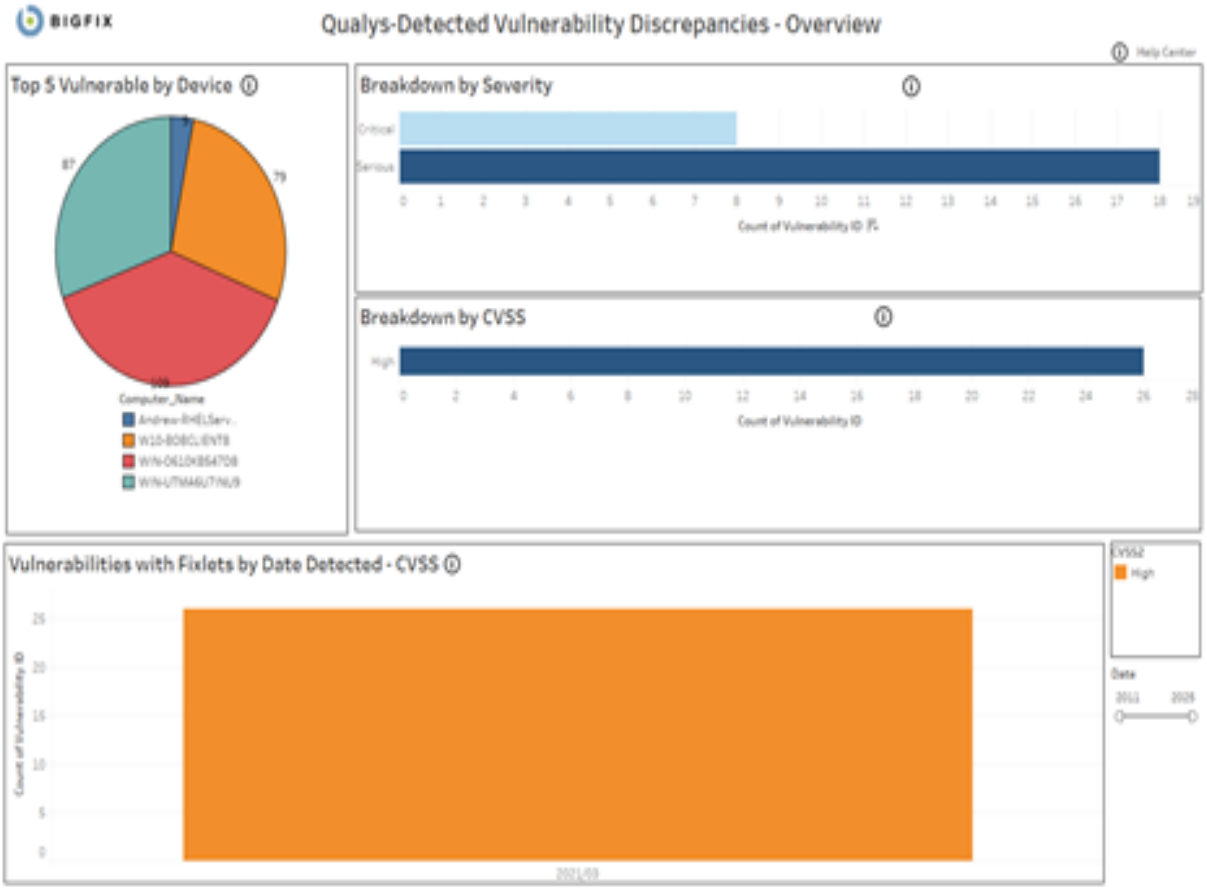
* BigFix data

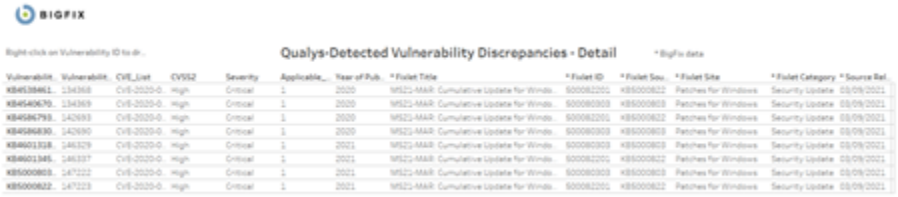
* Device Name	DeviceID	* IP Address	* OS	* Type	* Last Report Time
WIN-9EFHF0JM7HB	14456361-1	10.134.146.136	Win2016 10.0.14393.1884 (1607)	Server	2/16/2021 4:11:07 PM

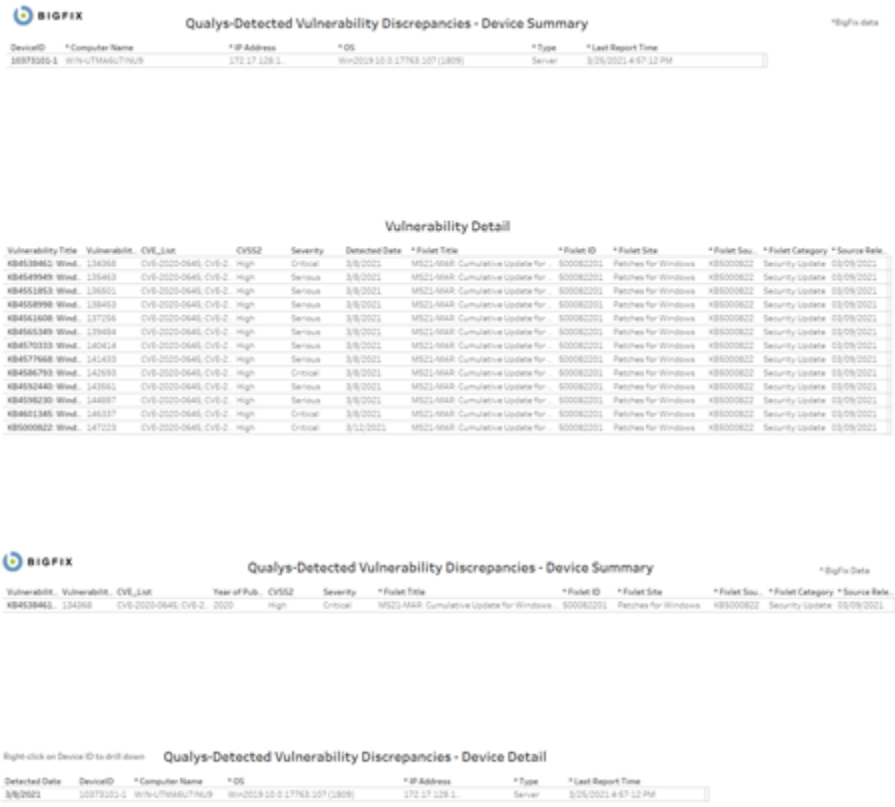
Vulnerability Detail

Vulnerability Title	Vulnerabilit..	CVSS2	Severity	Detected Date
ActivePerl UTF-8 Denial of Service Vulnerability	116904	Medium	Serious	1/1/2025
Adobe Flash Player SWF File Unspecified Remote Code Execution Vulnerability	115811	High	Critical	6/16/2020
Adobe Reader and Acrobat Multiple Vulnerabilities (APSB16-26)	370084	High	Critical	6/16/2020
Amazon Linux Security Advisory for dbus:ALAS-2019-1246	351628	Low	Critical	6/16/2020
Amazon Linux Security Advisory for gc:ALAS-2013-245	350499	Medium	Serious	1/1/2025
Amazon Linux Security Advisory for golang,docker:ALAS-2015-588	350114	High	Serious	6/16/2020
Amazon Linux Security Advisory for mod_security:ALAS-2014-335	350393	Medium	Serious	6/16/2020
Amazon Linux Security Advisory for perl-YAML-LibYAML:AL2012-2015-056	350775	Medium	Serious	6/16/2020
Amazon Linux Security Advisory for ruby20:ALAS-2015-547	350155	Medium	Serious	6/16/2020
Apple QuickTime Prior to 7.7.5 Multiple Vulnerabilities (APPLE-SA-2014-02-25-3)	121819	High	Critical	6/16/2020
Atlassian JIRA Multiple Security Vulnerability (JRASERVER-69784,JRASERVER-69..	13609	Medium	Serious	6/16/2020
Atlassian Jira Server and Data Center Improper Authorization Vulnerability(JRASE..	13831	Medium	Medium	6/16/2020
CentOS Security Update for Firefox (CESA-2012:1210)	120578	High	Critical	1/1/2025
CentOS Security Update for firefox (CESA-2017:0558)	256179	High	Urgent	1/1/2025
CentOS Security Update for firefox Security Update (CESA-2018:2693)	256482	High	Critical	1/1/2025
CentOS Security Update for flatpak (CESA-2019:0375)	256573	Medium	Critical	1/1/2025
CentOS Security Update for Ghostscript (CESA-2012:0096)	120039	Medium	Medium	6/16/2020
CentOS Security Update for HelixPlayer (CESA-2010:0094)	116908	High	Serious	6/16/2020

脆弱性の不一致


BIGFIX
Qualys-Detected Vulnerability Discrepancies - Overview
Help Center
Top 5 Vulnerable by Device
87
79
109
Computer_Name
Andrew-RHELServ...
W10-BOBCL-ENT8
WIN-06L0KB54TO8
WIN-UTM46UTN6J9
Breakdown by Severity
Critical
Serious
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19
Count of Vulnerability ID
Breakdown by CVSS
High
0 2 4 6 8 10 12 14 16 18 20 22 24 26 28
Count of Vulnerability ID
Vulnerabilities with Fixlets by Date Detected - CVSS
Count of Vulnerability ID
25
20
15
10
5
0
2021-09
CVSS2
High
Date
2011
2021


BIGFIX
Qualys-Detected Vulnerability Discrepancies - Detail



Tenable.io 用 Tableau レポート

このセクションを読むことで、Tenable.io 用 Tableau レポートの理解を深めることができます。

BigFix Insights for Vulnerability Remediation で、Tenable.io の脆弱性データを利用できるようになりました。Tenable Lumin が使用可能な場合、BigFix Insights for Vulnerability Remediation は、次の資産の優先順位付けデータも利用します。

- 資産の重大度の評価 (ACR): デバイス・タイプ、デバイスの目的、インターネットへのネットワーク・ロケーション/近接度に基づく資産の相対的な重要度を表す 1～10 の評価。
- 資産露出スコア (AES): ACR および VPR (脆弱性優先順位の評価) を 1 つのスコアに結合して資産の相対的な露出を表すメトリック。

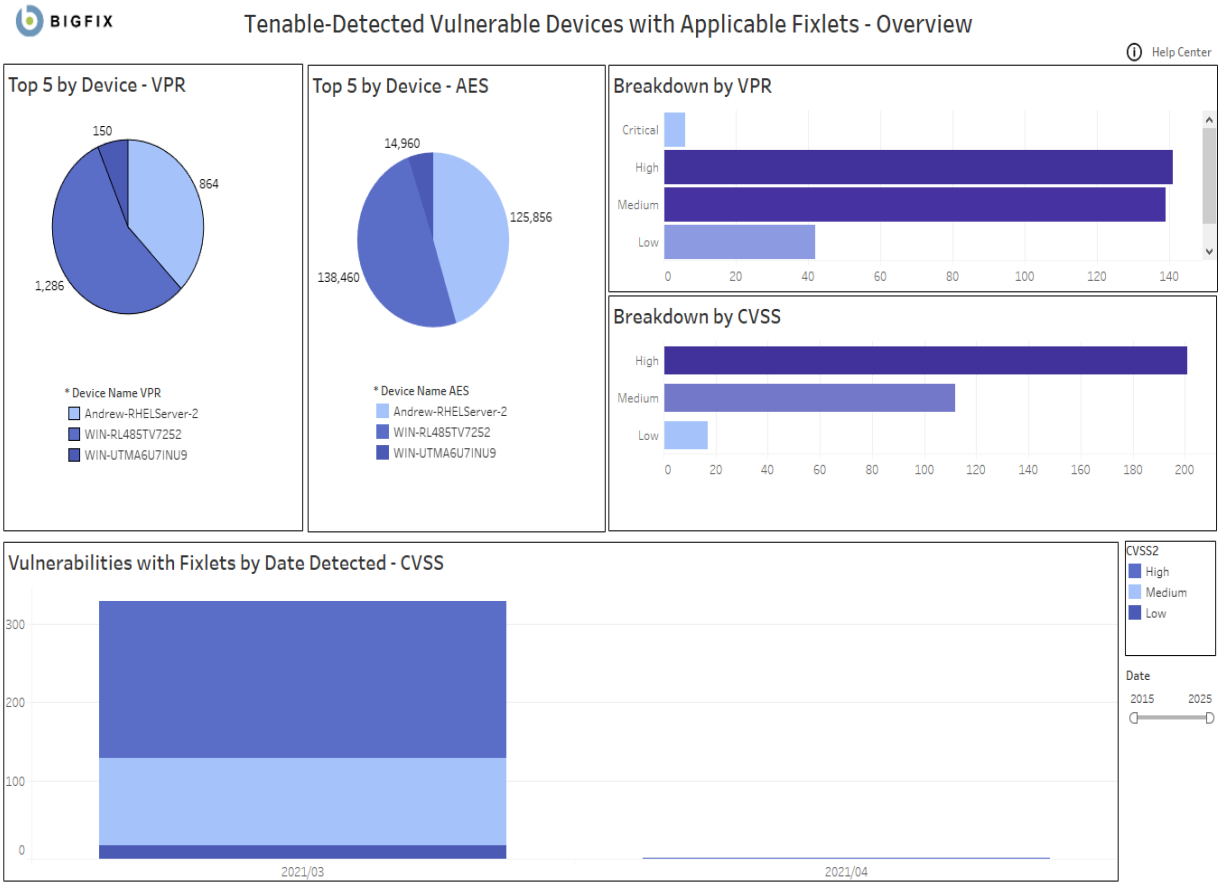
詳しくは、次のリンク先を参照してください。Lumin メトリック

さらに、Tenable.io の場合にのみ、BigFix はエンドポイント資産データを Tenable.io に送信して、管理対象外の可能性がある資産を表示できるようにします。

チャートの詳細:

- 脆弱性タイトル - 脆弱性タイトル
- PluginID - 脆弱性の検出に割り当てられた一意の識別子
- 該当デバイス - Tenable によってスキャンされ、脆弱性が特定されたデバイス
- CVE リスト - CVE のリスト
- CVSS2 - (Common Vulnerability Scoring System バージョン 2)、セキュリティーの脆弱性の重大度と潜在的な影響を評価するために使用されるスコアリング・システム。
- CVSS3 - (Common Vulnerability Scoring System バージョン 3)、スコアリング・システムの更新バージョン
- VPR - 脆弱性優先順位の評価
- VPR スコア - 0 ~ 10 の範囲の数値。10 が最も高い優先度を示します
- 検出日 - 脆弱性が最初に検出された日付
- 公開日 - 脆弱性に関する情報が最初に利用可能になった日付
- ACR - 資産の重大度の評価: デバイス・タイプ、デバイスの目的、インターネットへのネットワーク・ロケーション/近接度に基づく資産の相対的な重要度を表す 1 ~ 10 の評価。
- AES - 資産露出スコア: ACR および VPR (脆弱性優先順位の評価) を 1 つのスコアに結合して資産の相対的な露出を表すメトリック。

検出された脆弱性 (適用可能な **Fixlet** あり)



BIGFIX

Right-click on Plugin ID to drill down

Vulnerability List - 139 Rows

*BigFix data

Vulnerability Title	Pulgin ID	Applicable Devices	CVE List	CVSS2	CVSS3	VPR	VPR Score	Total VPR S..	Detected D..	Published D..	Product/I
MS KB3009008: Vulnerability in SSL 3.0 Could Allow Information Disclosure (POODLE)	78447	1	CVE-2014-3566	Medium		Medium	4.9	5	3/20/2021	10/14/2014	Windows
MS15-006: Vulnerability in Windows Error Rep..	80495	1	CVE-2015-0001	Low		Medium	4.2	4	3/20/2021	01/13/2015	Windows
MS15-014: Vulnerability in Group Policy Could ..	81267	1	CVE-2015-0009	Low		Medium	4.4	4	3/20/2021	02/10/2015	Windows
MS15-029: Vulnerability in Windows Photo De..	81743	1	CVE-2015-0076	Medium		Medium	5.7	6	3/20/2021	03/10/2015	Windows
MS15-050: Vulnerability in Service Control Ma..	83355	1	CVE-2015-1702	Medium		Medium	5.9	6	3/20/2021	05/12/2015	Windows
MS15-060: Vulnerability in Microsoft Common ..	84056	1	CVE-2015-1756	High		Medium	6.7	7	3/20/2021	06/09/2015	Windows
MS15-082: Vulnerability in RDP Could Allow Re..	85332	1	CVE-2015-2472	High		Medium	5.9	6	3/20/2021	08/11/2015	Windows
MS15-088: Unsafe Command Line Parameter P..	85334	1	CVE-2015-2423	Medium		Medium	4.2	4	3/20/2021	08/11/2015	Windows
MS15-089: Vulnerability in WebDAV Could Allo..	85323	1	CVE-2015-2476	Low		Medium	4.4	4	3/20/2021	08/11/2015	Windows
MS15-119: Security Update for Winsock to Ad..	86826	1	CVE-2015-2478	High		Medium	5.9	6	3/20/2021	11/10/2015	Windows
MS15-121: Security Update for Schannel to Ad..	86827	1	CVE-2015-6112	Medium		Medium	5.5	6	3/20/2021	11/10/2015	Windows
MS15-133: Security Update for Windows PGM ..	87262	1	CVE-2015-6126	High		Medium	5.9	6	3/20/2021	12/08/2015	Windows
MS16-013: Security Update for Windows Jour..	88645	1	CVE-2016-0038	High	High	Medium	6.7	7	3/20/2021	02/09/2016	Windows
MS16-027: Security Update for Windows Media to Address Remote Code Execution (3143146)	89750	1	CVE-2016-0098	High	High	Medium	6.7	7	3/20/2021	03/08/2016	Windows
			CVE-2016-0101	High	High	Medium	6.7	7	3/20/2021	03/08/2016	Windows
MS16-033: Security Update for Windows USB ..	89779	1	CVE-2016-0133	High	Medium	Medium	6.7	7	3/20/2021	03/08/2016	Windows
MS16-047: Security Update for SAM and LSAD ..	90510	1	CVE-2016-0128	Medium	Medium	Medium	6	6	3/20/2021	03/23/2016	Windows
MS16-067: Security Update for Volume Manag..	91016	1	CVE-2016-0190	Low	Medium	Medium	4.4	4	3/20/2021	05/10/2016	Windows
MS16-072: Security Update for Group Policy (3..	91600	1	CVE-2016-3223	High	High	Medium	6.7	7	3/20/2021	06/14/2016	Windows
MS16-076: Security Update for Netlogon (316..	91604	1	CVE-2016-3228	High	High	Medium	6.7	7	3/20/2021	06/14/2016	Windows
MS16-087: Security Update for Windows Print ..	92018	1	CVE-2016-3238	High	High	Medium	6.7	7	3/20/2021	07/12/2016	Windows
MS16-124: Security Update for Windows Regis..	94013	1	CVE-2016-0070; CVE-2016-0073..	Medium	Medium	Medium	6.6	7	3/20/2021	10/11/2016	Windows
MS16-134: Security Update for Common Log Fi..	94635	1	CVE-2016-0026; CVE-2016-3332..	High	High	Medium	5.9	6	3/20/2021	11/08/2016	Windows
MS16-137: Security Update for Windows Auth..	94638	1	CVE-2016-7237; CVE-2016-7238	High	High	Medium	5.9	6	3/20/2021	11/08/2016	Windows
MS16-149: Security Update for Microsoft Win..	95813	1	CVE-2016-7219; CVE-2016-7292	High	High	Medium	5.9	6	3/20/2021	11/17/2016	Windows
RHEL 7 : avahi (RHSA-2020:1176)	135048	1	CVE-2017-6519	Medium	Critical	Medium	5.2	5	3/11/2021	03/03/2015	Null
RHEL 7 : bash (RHSA-2020:1113)	135062	1	CVE-2019-9924	High	High	Medium	6.7	7	3/11/2021	03/22/2019	Null
RHEL 7 : bind (RHSA-2020:2344)	137082	1	CVE-2020-8616; CVE-2020-8617	Medium	High	Medium	6	6	3/11/2021	05/19/2020	Null
RHEL 7 : cpio (RHSA-2020:3908)	141056	1	CVE-2019-14866	Medium	High	Medium	6.7	7	3/11/2021	01/07/2020	Null

BIGFIX

Vulnerability Device Summary

*BigFix Data

Vulnerabilit..	Pulgin ID	CVE List	CVSS2	CVSS3	VPR	VPR Score	Total VPR S..	Detected D..	Published D..	Product/Fa..	* Fixlet Title	* Fixlet ID	* Fixle
MS15-050: ..	83355	CVE-2015-1..	Medium		Medium	5.9	6	3/20/2021	05/12/2015	Windows	MS15-050: Vulnerability in Service Control Manager ..	1505015	Patch

Right-click on Device ID to drill down

Vulnerability Device Detail - 1 Rows

Detected Date	DeviceID	* Device Name Detail	* OS	* IP Address	* Type	ACR	AES	* Last Report Time
3/20/2021	1076613427-2	WIN-RL485TV7252	Win2012R2 6.3.9600	10.134.146.46	Server	7.35	860	4/1/2021 9:03:51 PM

BIGFIX

Device Detail Summary

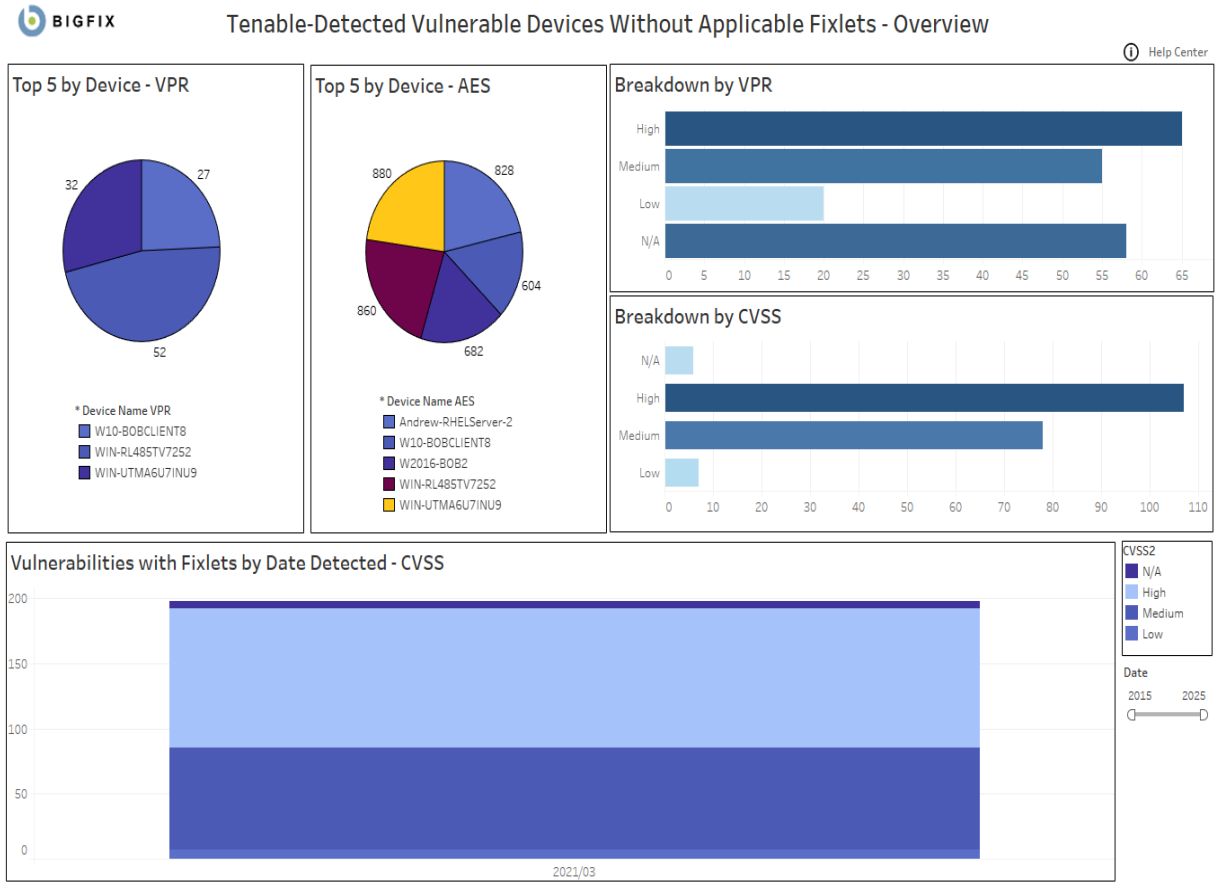
* BigFix data

DeviceID	* Device Name Det..	* IP Address	* OS	* Type	ACR	AES	* Last Report Time
1076613427-2	WIN-RL485TV7252	10.134.146.46	Win2012R2 6.3.9600	Server	7.35	860	4/1/2021 9:03:51 PM

Vulnerability Detail - 161 Rows

Vulnerability Title	Pulgin ID	CVE List	CVSS2	CVSS3	VPR	VPR Score	Total VPR S..	Detected Date	Published D..	Product/Fa..	* Fixlet Title	* Fixlet ID	* F
KB4088879: Wind..	108291	CVE-2017-5..	High	High	High	8.4	8	3/20/2021	03/13/2018	Windows	4072698: Enable mitigations to help pr..	407269801	Pat
KB4093115: Wind..	108965	CVE-2018-0..	High	High	High	9	9	3/20/2021	04/10/2018	Windows	MS18-APR: Security Only Quality Updat..	409311501	Pat
KB4103715: Wind..	109607	CVE-2018-0..	High	High	High	9.8	10	3/20/2021	05/08/2018	Windows	MS18-MAY: Security Only Quality Upda..	410371501	Pat
KB4338824: Wind..	110981	CVE-2018-8..	High	High	High	9	9	3/20/2021	07/10/2018	Windows	MS18-JUL: Security Only Quality Updat..	433882403	Pat
KB4457143: Wind..	117412	CVE-2018-8..	High	Critical	High	9	9	3/20/2021	09/11/2018	Windows	MS18-SEP: Security Only Quality Updat..	445714303	Pat
KB4462941: Wind..	118002	CVE-2018-8..	High	High	High	9.6	10	3/20/2021	10/09/2018	Windows	MS18-OCT: Security Only Quality Updat..	446294101	Pat
KB4467703: Wind..	118918	CVE-2018-8..	High	Critical	High	8.9	9	3/20/2021	11/13/2018	Windows	MS18-NOV: Security Only Quality Upda..	446770303	Pat
KB4471322: Windows 8.1 and ..	119583	CVE-2018-8..	High	Critical	High	9.4	9	3/20/2021	12/11/2018	Windows	MS18-DEC: Security Only Quality Updat..	447132201	Pat
		CVE-2018-8..	High	Critical	High	9.4	9	3/20/2021	12/11/2018	Windows	MS18-DEC: Security Only Quality Updat..	447049903	Pat
KB4480964: Wind..	121014	CVE-2019-0..	High	High	High	9.8	10	3/20/2021	01/08/2019	Windows	MS19-JAN: Security Only Quality Updat..	448096401	Pat
KB4487028: Windows 8.1 and ..	122120	CVE-2019-0..	High	High	High	8.9	9	3/20/2021	02/12/2019	Windows	MS19-FEB: Security Only Quality Updat..	448702801	Pat
		CVE-2019-0..	High	High	High	8.9	9	3/20/2021	02/12/2019	Windows	MS20-OCT: Security and Quality Rollup ..	457896201	Pat
KB4489883: Wind..	122784	CVE-2019-0..	High	High	High	8.4	8	3/20/2021	03/12/2019	Windows	MS19-MAR: Security Only Quality Upda..	448988301	Pat
KB4493467: Wind..	123940	CVE-2019-0..	High	High	High	9.5	10	3/20/2021	04/09/2019	Windows	MS19-APR: Security Only Quality Updat..	449346701	Pat
KB4499165: Wind..	125061	CVE-2019-0..	High	High	High	8.9	9	3/20/2021	05/14/2019	Windows	MS19-MAY: Security Only Quality Upda..	449916503	Pat
KB4503290: Wind..	125818	CVE-2019-0..	High	High	High	9.8	10	3/20/2021	06/11/2019	Windows	MS19-JUN: Security Only Quality Updat..	450329003	Pat
KB4507457:	126570	CVE-2019-0..	High	High	High	9	9	3/20/2021	07/09/2019	Windows	MS19-JUL: Security Only Quality Updat..	450745701	Pat

検出された脆弱性 (使用可能な **Fixlet** なし)



BIGFIX

Right-click on Plugin ID to drill down

* BigFix data

Vulnerability List - 107 Rows

Vulnerability Title	Plugin ID	Applicable Devices	CVE List	CVSS2	CVSS3	VPR	VPR
Adobe Flash Player <= 23.0.0.207 Multiple Vulnerabilities (APSB16-39)	95762	1	CVE-2016-7867; CVE-2016-7868; CVE-2016-7869; CVE-2016-7870; C..	High	Critical	High	8.9
Adobe Flash Player <= 24.0.0.186 Multiple Vulnerabilities (APSB17-02)	96388	1	CVE-2017-2925; CVE-2017-2926; CVE-2017-2927; CVE-2017-2928; C..	High	Critical	High	8.9
Adobe Flash Player <= 24.0.0.194 Multiple Vulnerabilities (APSB17-04)	97142	1	CVE-2017-2982; CVE-2017-2984; CVE-2017-2985; CVE-2017-2986; C..	High	Critical	High	8.9
Adobe Flash Player <= 25.0.0.127 Multiple Vulnerabilities (APSB17-10)	99283	1	CVE-2017-3058; CVE-2017-3059; CVE-2017-3060; CVE-2017-3061; C..	High	Critical	High	7.4
Adobe Flash Player <= 25.0.0.148 Multiple Vulnerabilities (APSB17-15)	100052	1	CVE-2017-3068; CVE-2017-3069; CVE-2017-3070; CVE-2017-3071; C..	High	Critical	High	8.9
Adobe Flash Player <= 25.0.0.171 Multiple Vulnerabilities (APSB17-17)	100756	1	CVE-2017-3075; CVE-2017-3076; CVE-2017-3077; CVE-2017-3078; C..	High	Critical	High	8.9
Adobe Flash Player <= 26.0.0.131 Multiple Vulnerabilities (APSB17-21)	101362	1	CVE-2017-3080; CVE-2017-3099; CVE-2017-3100	High	Critical	High	8.9
Adobe Flash Player <= 26.0.0.137 Multiple Vulnerabilities (APSB17-23)	102262	1	CVE-2017-3085; CVE-2017-3106	High	High	Medium	6.7
Adobe Flash Player <= 26.0.0.151 Multiple Vulnerabilities (APSB17-28)	103124	1	CVE-2017-11281; CVE-2017-11282	High	Critical	High	8.9
Adobe Flash Player <= 27.0.0.183 (APSB17-33)	104544	1	CVE-2017-11213; CVE-2017-11215; CVE-2017-11225; CVE-2017-311..	High	Critical	Medium	6.7
Adobe Flash Player <= 28.0.0.137 Use-after-free Remote Code Execution (A..	106606	1	CVE-2018-4877; CVE-2018-4878	High	Critical	High	9.6
Adobe Flash Player <= 28.0.0.161 (APSB18-05)	108281	1	CVE-2018-4919; CVE-2018-4920	High	Critical	Medium	6.7
Adobe Flash Player <= 29.0.0.113 (APSB18-08)	108958	1	CVE-2018-4932; CVE-2018-4933; CVE-2018-4934; CVE-2018-4935; C..	High	Critical	High	8.9
Adobe Flash Player <= 29.0.0.171 (APSB18-19)	110397	1	CVE-2018-4945; CVE-2018-5000; CVE-2018-5001; CVE-2018-5002	High	Critical	High	9.2
Adobe Flash Player <= 30.0.0.134 (APSB18-25)	111683	2	CVE-2018-12824; CVE-2018-12825; CVE-2018-12826; CVE-2018-12827; CVE-2018-12828	High	Critical	Medium	6.7
Adobe Flash Player <= 31.0.0.148 (APSB18-44)	119094	3	CVE-2018-15981	High	Critical	Medium	5.9
Adobe Flash Player <= 31.0.0.153 (APSB18-42)	119462	3	CVE-2018-15982; CVE-2018-15983	High	Critical	High	9.7
Adobe Flash Player <= 32.0.0.156 (APSB19-19)	123938	3	CVE-2019-7096; CVE-2019-7108	High	Critical	Medium	5.9
Adobe Flash Player Unsupported Version Detection	59196	3	Null	High		N/A	0
KB4018483: Security update for Adobe Flash Player (April 2017)	99290	1	CVE-2017-3058; CVE-2017-3059; CVE-2017-3060; CVE-2017-3061; C..	High	Critical	High	7.4
KB4020821: Security update for Adobe Flash Player (May 2017)	100062	1	CVE-2017-3068; CVE-2017-3069; CVE-2017-3070; CVE-2017-3071; C..	High	Critical	High	8.9

BIGFIX

Vulnerability Device Summary

*BigFix data

Vulnerability Title	Plugin ID	CVE List	CVSS2	CVSS3	VPR	VPR Score	Published D..	Solution
Adobe Flash Player <= 26.0.0.151 Multiple Vulnerabilities (APSB17-28)	103124	CVE-2017-11281; CVE-2017-11282	High	Critical	High	8.9	09/12/2017	Upgrade to Adobe Fla

Right-click on Device ID to drill down

Vulnerability Device Detail - 1 Rows

*Device Name Detail	Device ID	*OS	*IP Address	*Type	ACR	AES	*Last Report Time
WIN-RL485TV7252	1076613427-2	Win2012R2 6.3.9600	10.134.146.46	Server	7.35	860	4/1/2021 9:03:51 PM

BIGFIX

Device Detail Summary

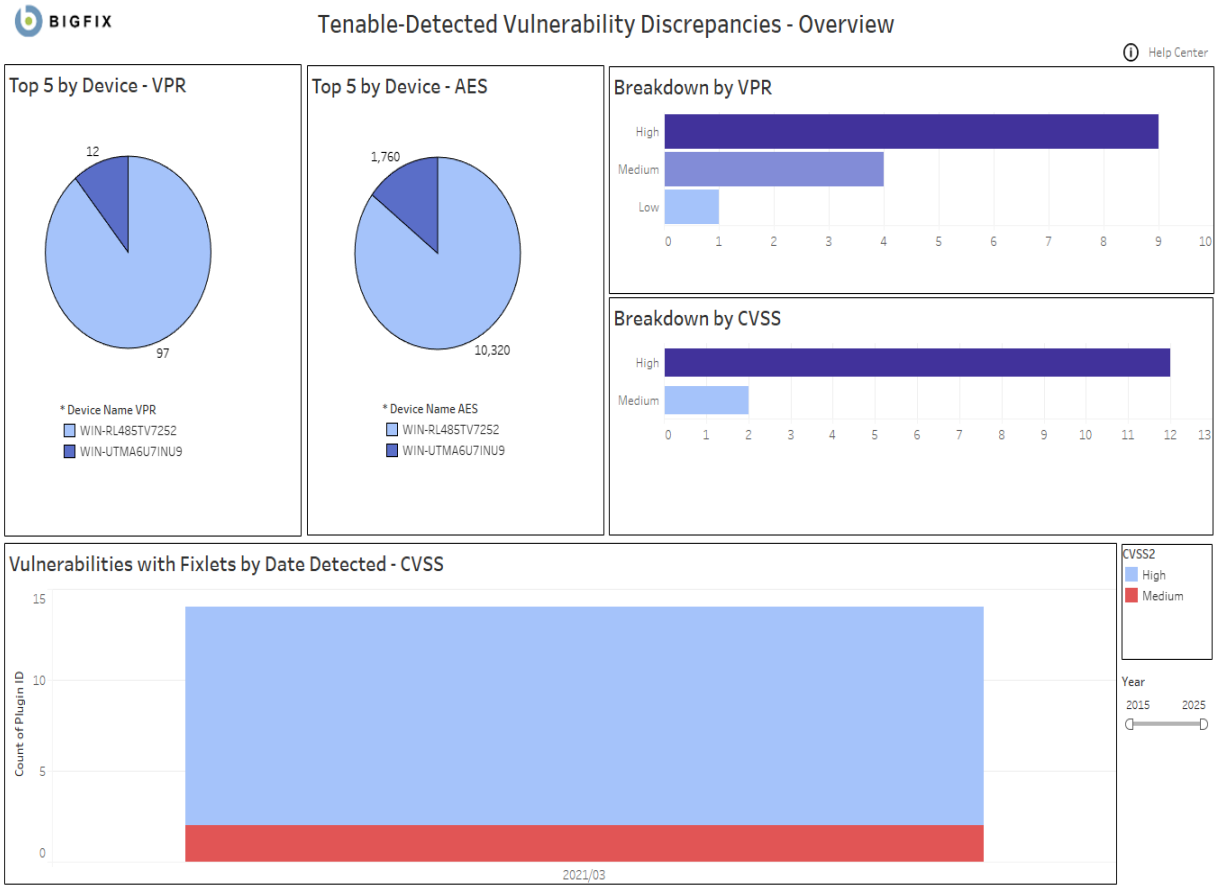
* BigFix data

* Device Name Detail	Device ID	* IP Address	* OS	* Type	ACR	AES	* Last Report Time
WIN-RL485TV7252	1076613427-2	10.134.146.46	Win2012R2 6.3.9600	Server	7.35	860	4/1/2021 9:03:51 PM

Vulnerability Detail - 178 Rows

Vulnerability Title	Plugin ID	CVE List	CVSS2	CVSS3	VPR	VPR Score	Publi
Adobe Flash Player <= 23.0.0.207 Multiple Vulnerabilities (APSB16-39)	95762	CVE-2016-7867; CVE-2016-7868; CVE-2016-7869; CVE-2016-7..	High	Critical	High	8.9	12/13
Adobe Flash Player <= 24.0.0.186 Multiple Vulnerabilities (APSB17-02)	96388	CVE-2017-2925; CVE-2017-2926; CVE-2017-2927; CVE-2017-2..	High	Critical	High	8.9	01/10
Adobe Flash Player <= 24.0.0.194 Multiple Vulnerabilities (APSB17-04)	97142	CVE-2017-2982; CVE-2017-2984; CVE-2017-2985; CVE-2017-2..	High	Critical	High	8.9	02/14
Adobe Flash Player <= 25.0.0.127 Multiple Vulnerabilities (APSB17-10)	99283	CVE-2017-3058; CVE-2017-3059; CVE-2017-3060; CVE-2017-3..	High	Critical	High	7.4	04/11
Adobe Flash Player <= 25.0.0.148 Multiple Vulnerabilities (APSB17-15)	100052	CVE-2017-3068; CVE-2017-3069; CVE-2017-3070; CVE-2017-3..	High	Critical	High	8.9	05/09
Adobe Flash Player <= 25.0.0.171 Multiple Vulnerabilities (APSB17-17)	100756	CVE-2017-3075; CVE-2017-3076; CVE-2017-3077; CVE-2017-3..	High	Critical	High	8.9	06/13
Adobe Flash Player <= 26.0.0.131 Multiple Vulnerabilities (APSB17-21)	101362	CVE-2017-3080; CVE-2017-3099; CVE-2017-3100	High	Critical	High	8.9	07/01
Adobe Flash Player <= 26.0.0.137 Multiple Vulnerabilities (APSB17-23)	102262	CVE-2017-3085; CVE-2017-3106	High	High	Medium	6.7	08/08
Adobe Flash Player <= 26.0.0.151 Multiple Vulnerabilities (APSB17-28)	103124	CVE-2017-11281; CVE-2017-11282	High	Critical	High	8.9	09/12
Adobe Flash Player <= 27.0.0.159 Type Confusion Vulnerability (APSB17-32)	103922	CVE-2017-11292	Medium	High	High	8.9	10/16
Adobe Flash Player <= 27.0.0.183 (APSB17-33)	104544	CVE-2017-11213; CVE-2017-11215; CVE-2017-11225; CVE-201..	High	Critical	Medium	6.7	11/14
Adobe Flash Player <= 27.0.0.187 (APSB17-42)	105175	CVE-2017-11305	Medium	High	Low	3.6	12/12
Adobe Flash Player <= 28.0.0.126 (APSB18-01)	105691	CVE-2018-4871	Medium	High	Low	3.6	01/09
Adobe Flash Player <= 28.0.0.137 Use-after-free Remote Code Execution (APSA18-01) ..	106606	CVE-2018-4877; CVE-2018-4878	High	Critical	High	9.6	02/01
Adobe Flash Player <= 28.0.0.161 (APSB18-05)	108281	CVE-2018-4919; CVE-2018-4920	High	Critical	Medium	6.7	03/13
Adobe Flash Player <= 29.0.0.113 (APSB18-08)	108958	CVE-2018-4932; CVE-2018-4933; CVE-2018-4934; CVE-2018-4..	High	Critical	High	8.9	04/10
Adobe Flash Player <= 29.0.0.171 (APSB18-19)	110397	CVE-2018-4945; CVE-2018-5000; CVE-2018-5001; CVE-2018-5..	High	Critical	High	9.2	06/07

脆弱性の不一致


BIGFIX
Tenable-Detected Vulnerability Discrepancies - Overview
Help Center
Top 5 by Device - VPR
12
97
* Device Name VPR
WIN-RL485TV7252
WIN-UTMA6U7INU9
Top 5 by Device - AES
1,760
10,320
* Device Name AES
WIN-RL485TV7252
WIN-UTMA6U7INU9
Breakdown by VPR
High
Medium
Low
0 1 2 3 4 5 6 7 8 9 10
Breakdown by CVSS
High
Medium
0 1 2 3 4 5 6 7 8 9 10 11 12 13
Vulnerabilities with Fixlets by Date Detected - CVSS
Count of Plugin ID
15
10
5
0
2021/03
CVSS2
High
Medium
Year
2015
2025

Right-click on Plugin ID to drill down

Vulnerability Discrepancies List - 4 Rows

* BigFix data

Vulnerability Title	Plugin ID	Applicable ..	CVE List	CVSS2	CVSS3	VPR	VPR Score	Detected D..	Published D..	Product/Fa..	* Fixlet Title	* Fixl
Adobe Flash Player <= 32.0.0.371 (APSB20-30)	137253	1	CVE-2020-9..	High	Critical	Medium	5.9	3/8/2021	06/09/2020	Windows	MS20-OCT: Security Update for Adobe Flas..	4580
								3/20/2021	06/09/2020	Windows	MS20-OCT: Security Update for Adobe Flas..	4580
KB4537759: Security update for Adobe Flash Player (February 2020)	133618	1	CVE-2020-3..	High	High	Medium	5.9	3/8/2021	02/11/2020	Windows	MS20-OCT: Security Update for Adobe Flas..	4580
								3/20/2021	02/11/2020	Windows	MS20-OCT: Security Update for Adobe Flas..	4580

BIGFIX

Vulnerability Discrepancies Device Summary

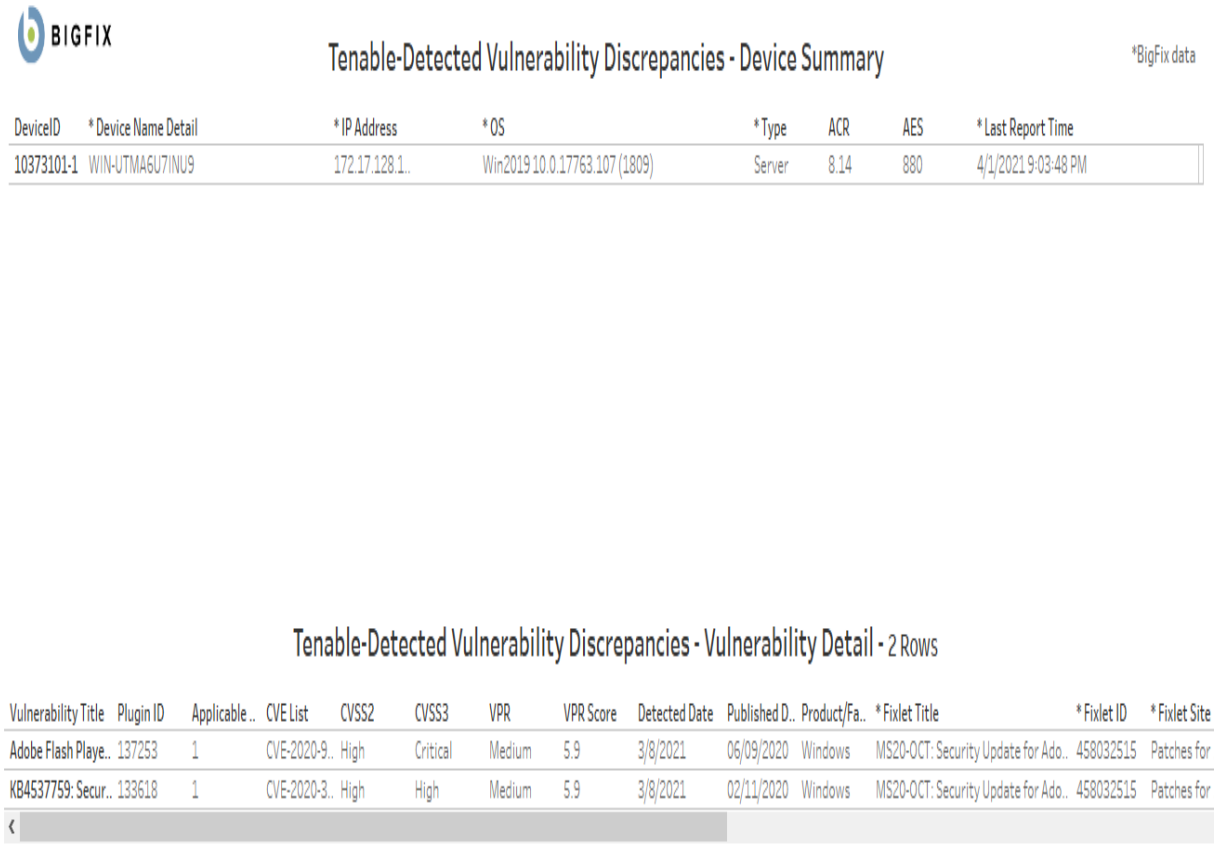
*BigFix Data

Vulnerability Title	Plugin ID	Applicable ..	CVE List	CVSS2	CVSS3	VPR	VPR Score	Detected D..	Published D..	Product/Fa..	*Fixlet Title
KB4537759: Security update for Adobe Flash Player (February 2020)	133618	1	CVE-2020-3757	High	High	Medium	5.9	3/8/2021	02/11/2020	Windows	MS20-OCT: Security Update
								3/20/2021	02/11/2020	Windows	MS20-OCT: Security Update

Right-click on Device Name to drill down

Vulnerability Discrepancies Device Detail - 2 Rows

Detected Date	DeviceID	*Device Name Detail	*OS	*IP Address	*Type	ACR	AES	*Last Report Time
3/8/2021	10373101-1	WIN-UTMA6U7INU9	Win2019 10.0.17763.107 (1809)	172.17.128.1..	Server	8.14	880	4/1/2021 9:03:48 PM
3/20/2021	1076613427-2	WIN-RL48STV7252	Win2012R2 6.3.9600	10.134.146.46	Server	7.35	860	4/1/2021 9:03:51 PM



BIGFIX

Tenable-Detected Vulnerability Discrepancies - Device Summary

*BigFix data

DeviceID	* Device Name Detail	* IP Address	* OS	* Type	ACR	AES	* Last Report Time
10373101-1	WIN-UTMA6U7INU9	172.17.128.1..	Win2019 10.0.17763.107 (1809)	Server	8.14	880	4/1/2021 9:03:48 PM

Tenable-Detected Vulnerability Discrepancies - Vulnerability Detail - 2 Rows

Vulnerability Title	Plugin ID	Applicable ..	CVE List	CVSS2	CVSS3	VPR	VPR Score	Detected Date	Published D..	Product/Fa..	* Fixlet Title	* Fixlet ID	* Fixlet Site
Adobe Flash Playe..	137253	1	CVE-2020-9..	High	Critical	Medium	5.9	3/8/2021	06/09/2020	Windows	MS20-OCT: Security Update for Ado..	458032515	Patches for ..
KB4537759: Secur..	133618	1	CVE-2020-3..	High	High	Medium	5.9	3/8/2021	02/11/2020	Windows	MS20-OCT: Security Update for Ado..	458032515	Patches for ..

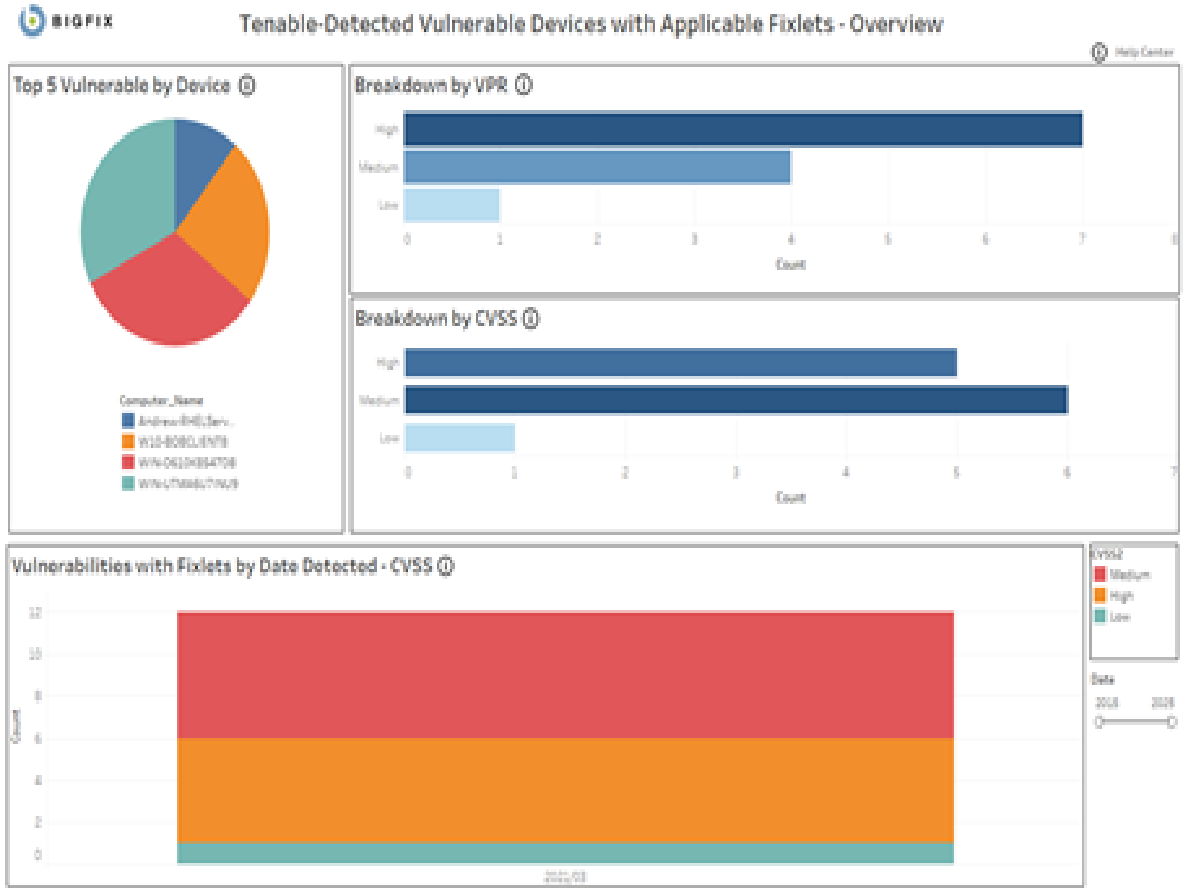
Tenable.sc 用 Tableau レポート

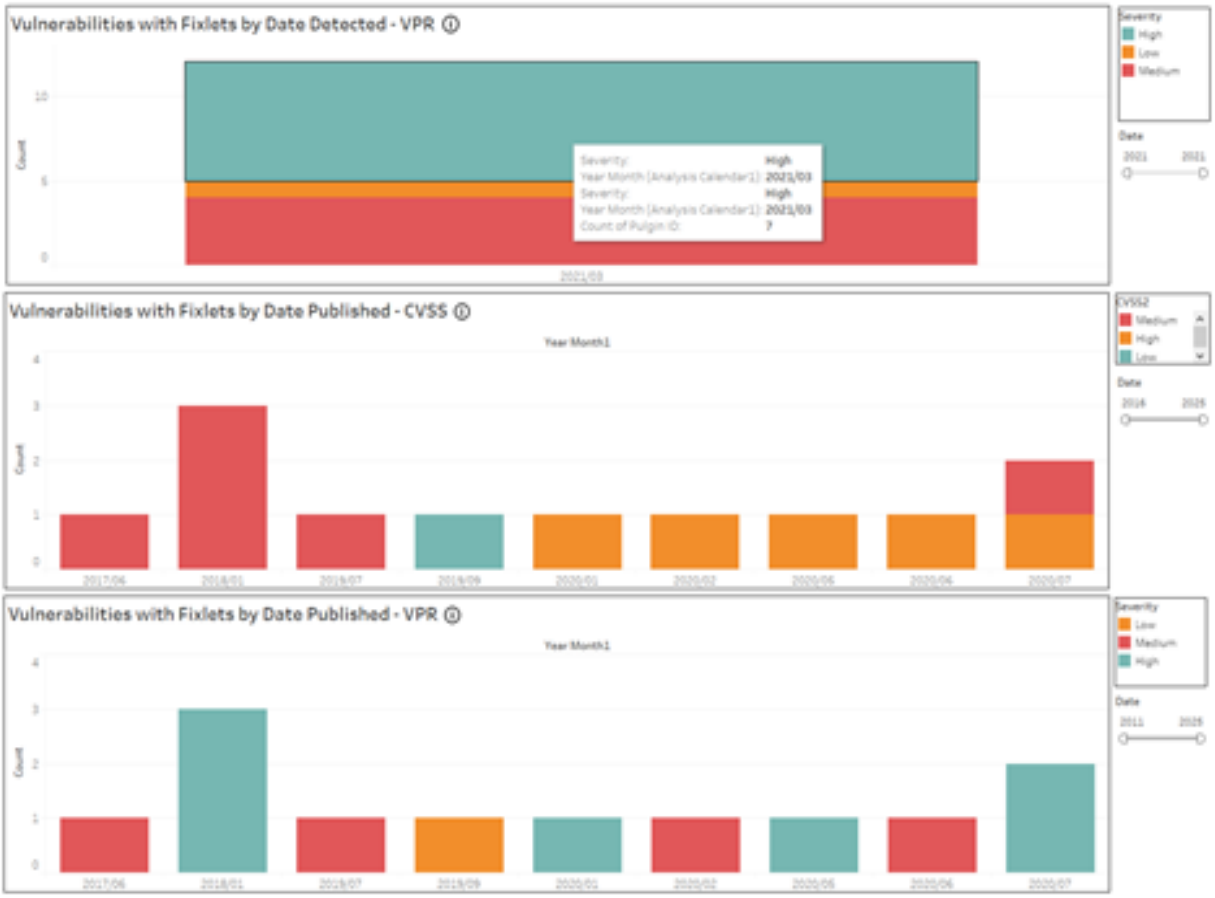
このセクションを読むことで、Tenable.sc 用 Tableau レポートの理解を深めることができます。

チャートの詳細:

- 脆弱性タイトル - 脆弱性タイトル
- PluginID - 脆弱性の検出に割り当てられた一意の識別子
- 該当デバイス - Tenable によってスキャンされ、脆弱性が特定されたデバイス
- CVE リスト - CVE のリスト
- CVSS2 - (Common Vulnerability Scoring System バージョン 2)、セキュリティーの脆弱性の重大度と潜在的な影響を評価するために使用されるスコアリング・システム。
- CVSS3 - (Common Vulnerability Scoring System バージョン 3)、スコアリング・システムの更新バージョン
- VPR - 脆弱性優先順位の評価
- VPR スコア - 0 ~ 10 の範囲の数値。10 が最も高い優先度を示します
- 検出日 - 脆弱性が最初に検出された日付
- 公開日 - 脆弱性に関する情報が最初に利用可能になった日付

検出された脆弱性 (適用可能な **Fixlet** あり)





BIGFIX

Tenable-Detected Vulnerability List - Detail

Right-click on Plugin ID to drill down

* BigFix data

Vulnerabilit..	Plugin ID	CVE_List	CVSS2	Severity	Applicable Devices	Year of Pub..	* Fixlet Title	* Fixlet ID	* Fixlet Sou..	* Fixlet Site	* Fixlet Category	* Source Rel..
Adobe Flas..	137253	CVE-2020-3757..	High	Medium	2	2020	MS20-OCT: Security Update for A..	468032515	KB4580325	Patches for Windows	Security Update	10/13/2020
KB4537759..	139618	CVE-2020-3757..	High	Medium	2	2020	MS20-OCT: Security Update for A..	468032515	KB4580325	Patches for Windows	Security Update	10/13/2020
KB4551853..	136501	CVE-2019-1006..	High	High	1	2020	MS20-MAY: Cumulative Update f..	465292405	KB4556441	Patches for Windows	Security Update	06/12/2020
KB4558998..	136463	CVE-2020-1346	High	High	1	2020	MS21-MAR: Servicing Stack Upd..	500085901	KB5000859	Patches for Windows	Security Update	03/09/2021
Security Up..	132999	CVE-2019-1006..	High	High	2	2020	MS20-MAY: Cumulative Update f..	465292405	KB4556441	Patches for Windows	Security Update	06/12/2020

BIGFIX

Device Detail Summary

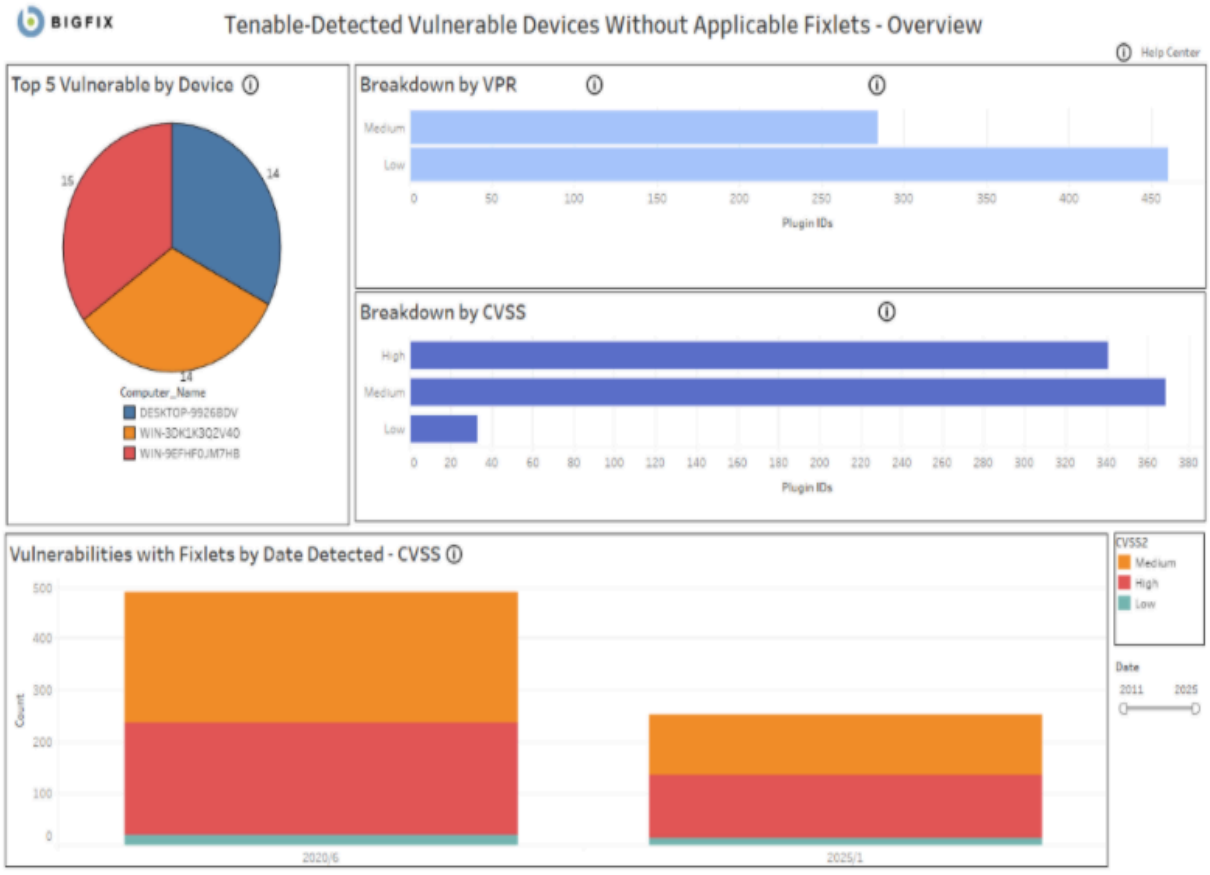
* BigFix data

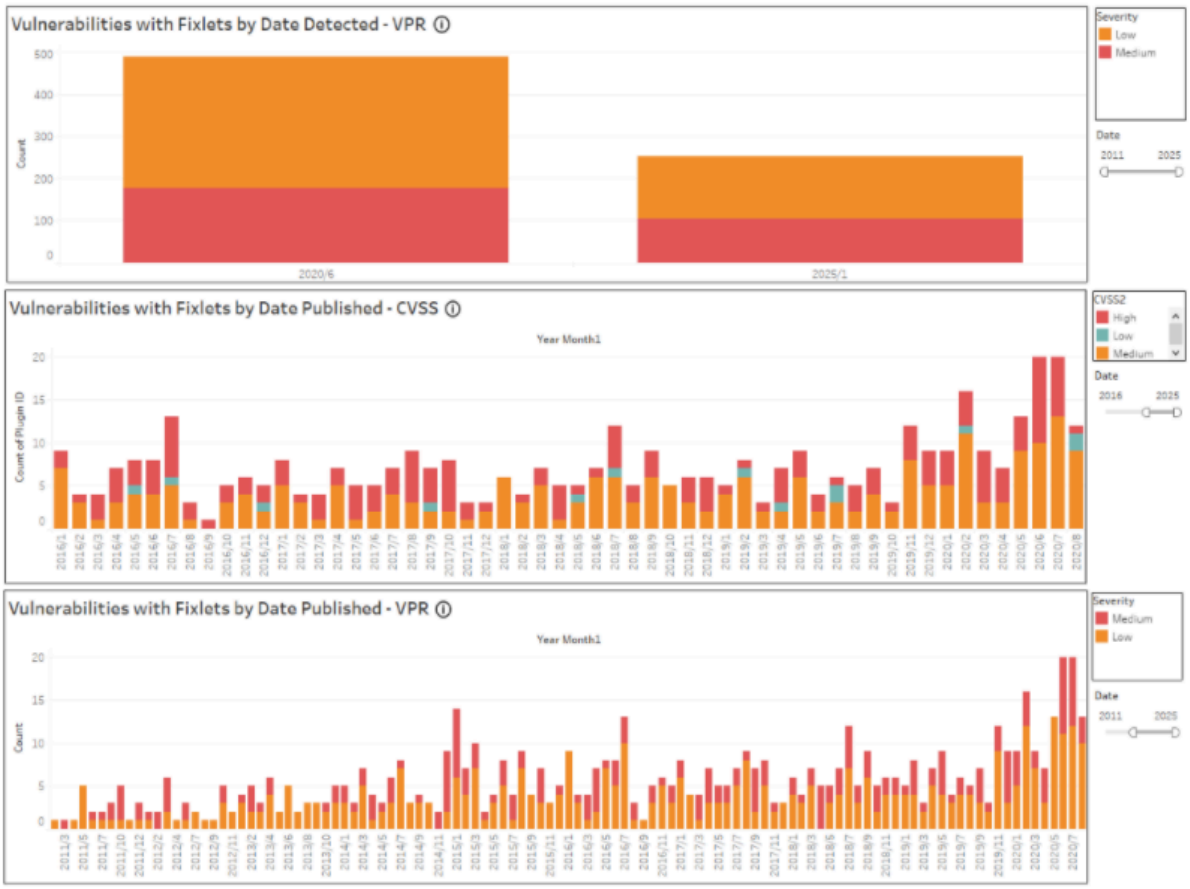
DeviceID	* Device Name	* IP Address	* OS	* Type	* Last Report Time
10373101-1	WIN-UTN46U7NU9	172.17.128.1..	Win2019 10.0.17763.107..	Server	3/26/2021 4:57:12 PM

Vulnerability Detail

Vulnerability Title	Plugin ID	CVE_List	CVSS2	Severity	Detected Date	* Fixlet Title	* Fixlet ID	* Fixlet Site	* Fixlet Sou..	* Fixlet Category	* Source Rel..
Adobe Flash Playe..	137253	CVE-2020-3757..	High	Medium	3/8/2021	MS20-OCT: Security Update for Adobe F..	468032515	Patches for Windows	KB4580325	Security Update	10/13/2020
KB4537759: Secur..	139618	CVE-2020-3757..	High	Medium	3/8/2021	MS20-OCT: Security Update for Adobe F..	468032515	Patches for Windows	KB4580325	Security Update	10/13/2020
KB4551853: Wind..	136501	CVE-2019-1006..	High	High	3/8/2021	MS20-MAY: Cumulative Update for .NE..	465292405	Patches for Windows	KB4556441	Security Update	06/12/2020
KB4558998: Wind..	136463	CVE-2020-1346	High	High	3/8/2021	MS21-MAR: Servicing Stack Update for ..	500085901	Patches for Windows	KB5000859	Security Update	03/09/2021
Security Updates ..	132999	CVE-2019-1006..	High	High	3/8/2021	MS20-MAY: Cumulative Update for .NE..	465292405	Patches for Windows	KB4556441	Security Update	06/12/2020
Security Updates ..	126600	CVE-2019-1006..	Medium	Medium	3/8/2021	MS20-MAY: Cumulative Update for .NE..	465292405	Patches for Windows	KB4556441	Security Update	06/12/2020
Security Updates ..	136464	CVE-2020-1046..	Medium	High	3/8/2021	MS20-OCT: Cumulative Update for .NET..	467896603	Patches for Windows	KB4579976	Security Update	10/13/2020
Security Updates ..	128742	CVE-2019-1006..	Low	Low	3/8/2021	MS20-MAY: Cumulative Update for .NE..	465292405	Patches for Windows	KB4556441	Security Update	06/12/2020
Windows Specula..	132101	CVE-2017-5715..	Medium	High	3/8/2021	4072698: Enable mitigations to help pr..	407269805	Patches for Windows	KB4072698	Security Advisо..	01/04/2018

検出された脆弱性 (使用可能な **Fixlet** なし)





BIGFIX

Right-click on Plugin ID to drill down

* BigFix data

Vulnerability List

Vulnerability Title	Plugin ID	CVSS2	Severity	Applicable_...	Year of Pub...
Amazon Linux Security Advisory for dbus:ALAS-2019-1246	351628	Low	Medium	1	2019
Amazon Linux Security Advisory for quagga:ALAS-2012-070	350677	Low	Low	1	2016
Atlassian Fisheye and Crucible Cross-Site Scripting Vulnerability (CRUC-8381,FE-7163,CRUC-8380,FE-...	13422	Low	Low	1	2019
CentOS Security Update for libvirt (CESA-2012:1202)	120674	Low	Low	1	2012
CentOS Security Update for libvirt.test (CESA-2011:0478)	119287	Low	Low	1	2011
CentOS Security Update for OpenSSH (CESA-2007:0257)	117547	Low	Low	1	2010
CentOS Security Update for PAM (CESA-2007:0465)	117515	Low	Low	1	2010
CentOS Security Update for qemu-kvm (CESA-2017:1856)	256277	Low	Medium	1	2017
CentOS Security Update for util-linux-ng (CESA-2013:0517)	121109	Low	Low	1	2013
Debian Security Update for mailman (DSA 4246-1)	176429	Low	Low	1	2018
Drupal core File Module Cross Site Scripting Vulnerability (SA-CORE-2019-004)	13453	Low	Low	1	2019
Fedora Security Update for libunwind (FEDORA-2015-11465)	124023	Low	Low	1	2015
Fedora Security Update for qemu (FEDORA-2016-1b264ab4a4)	276023	Low	Low	1	2016
Fedora Security Update for slapi-nis (FEDORA-2014-1442)	122951	Low	Low	1	2015
Fedora Security Update for sudo (FEDORA-2015-2247)	123347	Low	Low	1	2015
Fedora Security Update for xen (FEDORA-2016-da6b1d277b)	276264	Low	Low	1	2016
iPlanet Calendar Server Plaintext Admin Password Vulnerability	86154	Low	Medium	1	2001
McAfee VirusScan 4.0.3 Alert File Vulnerability	38313	Low	Low	1	2004
OpenSuSE Security Update for libvirt (openSUSE-SU-2014:0010-1)	166705	Low	Low	1	2014
OpenSuSE Security Update for llvm (openSUSE-SU-2015:0245-1)	167600	Low	Low	1	2015
OpenSuSE Security Update for XWayland (openSUSE-SU-2015:1095-1)	167944	Low	Low	1	2015
Oracle Enterprise Linux Security Update for libgcrypt (ELSA-2013-1457)	156707	Low	Low	1	2014
Oracle Enterprise Linux Security Update for qemu-kvm (ELSA-2019-1650)	158022	Low	Low	1	2019
PostNuke Cross Site Scripting Vulnerability	10543	Low	Low	1	2002
Red Hat Update for OpenShift Container Platform 4.5.4 jenkins-2-plugins (RHSA-2020:3207)	238533	Low	Low	1	2020
Skype Technologies Skype URI Handling Remote File Download Vulnerability	38547	Low	Low	1	2006
SUSE Enterprise Linux Security Update for dbus-1 (SUSE-SU-2014:0846-1)	167211	Low	Low	1	2014
SUSE Enterprise Linux Security Update for libapr1 (SUSE-SU-2018:1322-1)	171132	Low	Low	1	2018
SUSE Enterprise Linux Security Update for Wireshark (SUSE-SU-2012:0792-1)	165499	Low	Low	1	2012
SUSE Security Update for libqt4 (openSUSE-SU-2013:0404-1)	165870	Low	Low	1	2013

BIGFIX

Device Detail Summary

* BigFix data

* Device Name	DeviceID	* IP Address	* OS	* Type	* Last Report Time
WIN-9EFHF0JM7HB	14456361-1	10.134.146.136	Win2016 10.0.14393.188..	Server	2/16/2021 4:11:07 PM

Vulnerability Detail

Vulnerability Title	Plugin ID	CVSS2	Severity	Detected Date
ActivePerl UTF-8 Denial of Service Vulnerability	116904	Medium	Low	1/1/2025
Adobe Flash Player SWF File Unspecified Remote Code Execution Vulnerability	115811	High	Medium	6/16/2020
Adobe Reader and Acrobat Multiple Vulnerabilities (APSB16-26)	370084	High	Medium	6/16/2020
Amazon Linux Security Advisory for dbus:ALAS-2019-1246	351628	Low	Medium	6/16/2020
Amazon Linux Security Advisory for gc:ALAS-2013-245	350499	Medium	Low	1/1/2025
Amazon Linux Security Advisory for golang,docker:ALAS-2015-588	350114	High	Low	6/16/2020
Amazon Linux Security Advisory for mod_security:ALAS-2014-335	350393	Medium	Low	6/16/2020
Amazon Linux Security Advisory for perl-YAML-LibYAML:AL2012-2015-056	350775	Medium	Low	6/16/2020
Amazon Linux Security Advisory for ruby20:ALAS-2015-547	350155	Medium	Low	6/16/2020
Apple QuickTime Prior to 7.7.5 Multiple Vulnerabilities (APPLE-SA-2014-02-25-3)	121819	High	Medium	6/16/2020
Atlassian JIRA Multiple Security Vulnerability (JRASERVER-69784,JRASERVER-69783,JRASERVER-69782,JRASERVER-..	13609	Medium	Low	6/16/2020
Atlassian Jira Server and Data Center Improper Authorization Vulnerability(JRASERVER-70526)	13831	Medium	Low	6/16/2020
CentOS Security Update for Firefox (CESA-2012:1210)	120578	High	Medium	1/1/2025
CentOS Security Update for firefox (CESA-2017:0558)	256179	High	Medium	1/1/2025
CentOS Security Update for firefox Security Update (CESA-2018:2693)	256482	High	Medium	1/1/2025
CentOS Security Update for flatpak (CESA-2019:0375)	256573	Medium	Medium	1/1/2025
CentOS Security Update for Ghostscript (CESA-2012:0096)	120039	Medium	Low	6/16/2020
CentOS Security Update for HelixPlayer (CESA-2010:0094)	116908	High	Low	6/16/2020

BIGFIX

Vulnerability Device Summary

* BigFix data

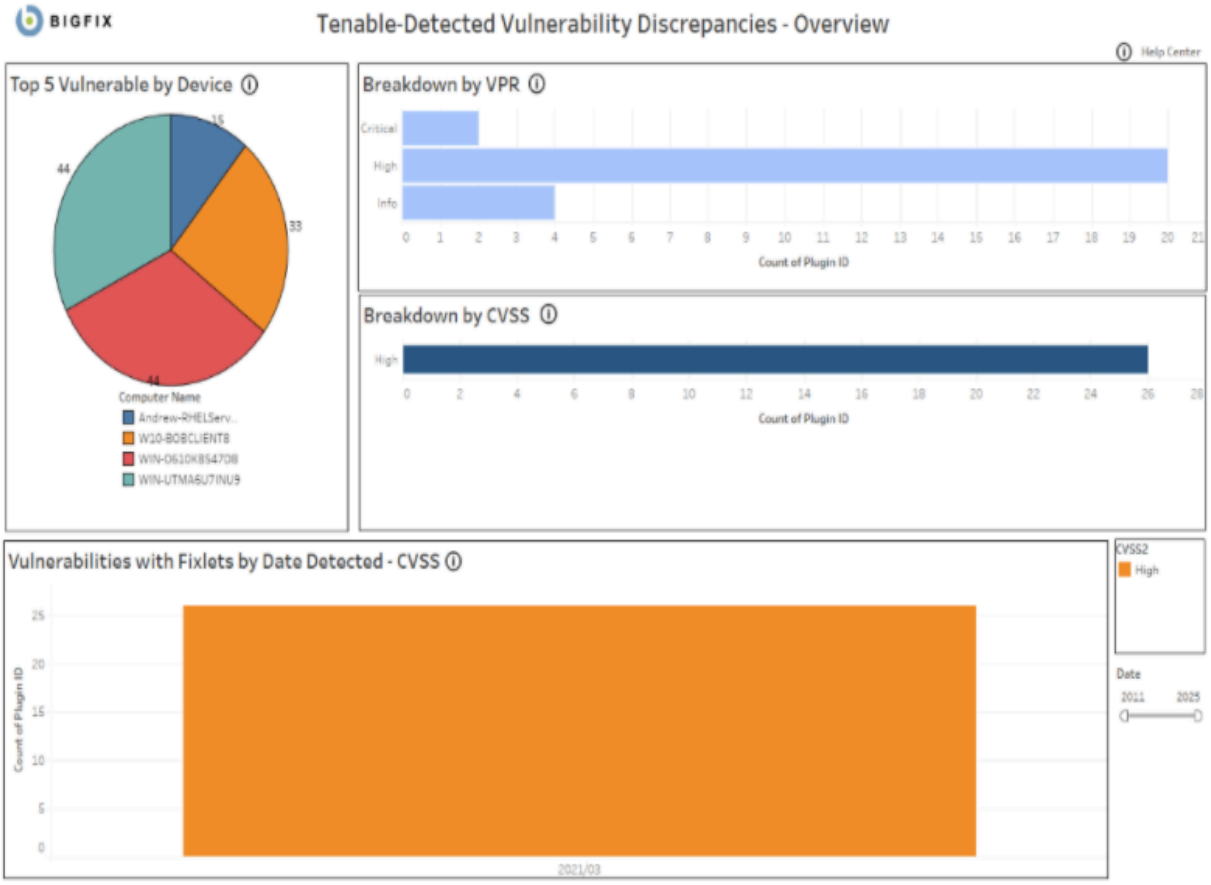
Vulnerability Title	Plugin ID	Year of Pub..	CVSS2	Severity
Amazon Linux Security Advisory for dbus:ALAS-2019-1246	351628	2019	Low	Medium

Vulnerability Device Detail

Right-click on Device ID to drill down

Detected Date	Device ID	* Device Name	* OS	* IP Address	* Type	* Last Report Time	Plugin_ID
6/16/2020	14456361-1	WIN-9EFHF0JM7HB	Win2016 10.0.14393.1884 ..	10.134.146.136	Server	2/16/2021 4:11:07 PM	351628

脆弱性の不一致


BIGFIX
Tenable-Detected Vulnerability Discrepancies - Overview
Help Center
Top 5 Vulnerable by Device
16
44
33
44
Computer Name
Andrew-RHELServ...
W10-BOBCLIENT8
WIN-O610K8547D8
WIN-UTMA6U7INU9
Breakdown by VPR
Critical
High
Info
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21
Count of Plugin ID
Breakdown by CVSS
High
0 2 4 6 8 10 12 14 16 18 20 22 24 26 28
Count of Plugin ID
Vulnerabilities with Fixlets by Date Detected - CVSS
25
20
15
10
5
0
Count of Plugin ID
2021/03
CVSS2
High
Date
2011
2025

BIGFIX

Right-click on Plugin ID to drill down

Tenable-Detected Vulnerability Discrepancies - Detail * BigFix data

Vulnerabilit..	Plugin ID	CVE_List	CVSS2	Severity	Applicable_..	Year of Pub..	* Fixlet Title	* Fixlet ID	* Fixlet Sou..	* Fixlet Site	* Fixlet Category	* Source Rel..
KB4586793..	142693	CVE-2020-0..	High	Info	1	2020	MS21-MAR: Cumulative Update for Windo..	S00082201	KB5000822	Patches for Windows	Security Update	03/09/2021
KB4586830..	142690	CVE-2020-0..	High	Info	1	2020	MS21-MAR: Cumulative Update for Windo..	S00080303	KB5000803	Patches for Windows	Security Update	03/09/2021
KB5000803..	147222	CVE-2020-0..	High	Info	1	2021	MS21-MAR: Cumulative Update for Windo..	S00080303	KB5000803	Patches for Windows	Security Update	03/09/2021
KB5000822..	147223	CVE-2020-0..	High	Info	1	2021	MS21-MAR: Cumulative Update for Windo..	S00082201	KB5000822	Patches for Windows	Security Update	03/09/2021

BIGFIX

Tenable-Detected Vulnerability Discrepancies - Device Summary

*BigFix data

DeviceID	* Device Name	* IP Address	* OS	* Type	* Last Report Time
10373101-1	WIN-UTMA6U7INU9	172.17.128.1..	Win2019 10.0.17763.107 (1809)	Server	3/25/2021 4:57:12 PM

Tenable-Detected Vulnerability Discrepancies - Vulnerability Detail

Vulnerability Title	Plugin ID	CVE_List	CVSS2	Severity	Detected Date	* Fixlet Title	* Fixlet ID	* Fixlet Site	* Fixlet Sou..	* Fixlet Category	* Source Rele..
KB4538461: Wind..	134368	CVE-2020-0645; CVE-2..	High	High	3/8/2021	MS21-MAR: Cumulative Update for ...	500082201	Patches for Windows	KB5000822	Security Update	03/09/2021
KB4549949: Wind..	135463	CVE-2020-0645; CVE-2..	High	High	3/8/2021	MS21-MAR: Cumulative Update for ...	500082201	Patches for Windows	KB5000822	Security Update	03/09/2021
KB4551853: Wind..	136501	CVE-2020-0645; CVE-2..	High	High	3/8/2021	MS21-MAR: Cumulative Update for ...	500082201	Patches for Windows	KB5000822	Security Update	03/09/2021
KB4558998: Wind..	138453	CVE-2020-0645; CVE-2..	High	High	3/8/2021	MS21-MAR: Cumulative Update for ...	500082201	Patches for Windows	KB5000822	Security Update	03/09/2021
KB4561608: Wind..	137256	CVE-2020-0645; CVE-2..	High	High	3/8/2021	MS21-MAR: Cumulative Update for ...	500082201	Patches for Windows	KB5000822	Security Update	03/09/2021
KB4565349: Wind..	139484	CVE-2020-0645; CVE-2..	High	Critical	3/8/2021	MS21-MAR: Cumulative Update for ...	500082201	Patches for Windows	KB5000822	Security Update	03/09/2021
KB4570333: Wind..	140414	CVE-2020-0645; CVE-2..	High	High	3/8/2021	MS21-MAR: Cumulative Update for ...	500082201	Patches for Windows	KB5000822	Security Update	03/09/2021
KB4577668: Wind..	141433	CVE-2020-0645; CVE-2..	High	High	3/8/2021	MS21-MAR: Cumulative Update for ...	500082201	Patches for Windows	KB5000822	Security Update	03/09/2021
KB4586793: Wind..	142693	CVE-2020-0645; CVE-2..	High	Info	3/8/2021	MS21-MAR: Cumulative Update for ...	500082201	Patches for Windows	KB5000822	Security Update	03/09/2021
KB4592440: Wind..	143561	CVE-2020-0645; CVE-2..	High	High	3/8/2021	MS21-MAR: Cumulative Update for ...	500082201	Patches for Windows	KB5000822	Security Update	03/09/2021
KB4598230: Wind..	144887	CVE-2020-0645; CVE-2..	High	High	3/8/2021	MS21-MAR: Cumulative Update for ...	500082201	Patches for Windows	KB5000822	Security Update	03/09/2021
KB4601345: Wind..	146337	CVE-2020-0645; CVE-2..	High	High	3/8/2021	MS21-MAR: Cumulative Update for ...	500082201	Patches for Windows	KB5000822	Security Update	03/09/2021
KB5000822: Wind..	147223	CVE-2020-0645; CVE-2..	High	Info	3/12/2021	MS21-MAR: Cumulative Update for ...	500082201	Patches for Windows	KB5000822	Security Update	03/09/2021

BIGFIX

Tenable-Detected Vulnerability Discrepancies - Device Summary

* BigFix Data

Vulnerabilit..	Plugin ID	CVE_List	Year of Pub..	CVSS2	Severity	* Fixlet Title	* Fixlet ID	* Fixlet Site	* Fixlet Sou..	* Fixlet Category	* Source Rele..
KB4586793..	142693	CVE-2020-0645; CVE-2..	2020	High	Info	MS21-MAR: Cumulative Update for Windows ...	500082201	Patches for Windows	KB5000822	Security Update	03/09/2021

Right-click on Device ID to drill down

Tenable-Detected Vulnerability Discrepancies - Device Detail

Detected Date	DeviceID	* Device Name	* OS	* IP Address	* Type	* Last Report Time
3/8/2021	10373101-1	WIN-UTMA6U7INU9	Win2019 10.0.17763.107 (1809)	172.17.128.1..	Server	3/25/2021 4:57:12 PM

第 10 章. 参照

以下のトピックでは、構成ファイルおよび設定、パッケージに付属の CLI の操作方法について説明します。また、トラブルシューティング目的でログ・ファイルを使用する方法についても説明します。

構成ファイル

データ・フロー・サービスは、`DataflowsConfig.xml` 構成ファイルを使用します。このファイルは、デフォルトのインストール・パスにあります。C:\Program Files (x86)\BigFix Enterprise\Dataflow。ファイルには、データ・ソース、データ・フロー、設定の 3 つのセクションがあります。ファイル内のタグと属性名は、すべて小文字にする必要があります。起動時に構成ファイルを検証するために使用できる `DataFlowsConfig.xsd` ファイルもあります。

<datasources>

この`<datasources>`構成ファイルのタグは、ソリューションが対話するように構成されているさまざまなデータ・ソースの集合を表します。構成を有効にするには、少なくとも 2 つのデータ・ソースが必要です。この`<datasourcename>`属性は固有でなければなりません。

この`<データ・ソース>`タグは、 構成ドキュメントの`<datasources>`タグの子ノードであり、単一のデータ・ソースの構成情報を表します。

表 6. 構成ファイルの属性の詳細

属性名	デフォルト値	必須	説明
datasourcename	該当なし	あり	この属性は、データ・ソースを一意的に識別するために使用されます。この属性を使用すると、データ・ソースを各データ・フロー内の特定のアダプターにマッピングできます。 注: datasourcename 属性の値

表 6. 構成ファイルの属性の詳細 (続く)

属性名	デフォルト値	必須	説明
			は、Tenable の場合は「TenableSC」または「TenableIO」でなければなりません。例: <datasource datasourcename="TenableIO" .../>
connectionstring	該当なし	あり	それぞれのデータ・ソースの URL。 例: `https://[QualysAPIURL],https://[TenableAPI_URL]:443` 注: Tenable.io では、ポート番号は必要ありません。例: https://cloud.tenable.com
username	該当なし	システム生成	この属性は、ProvideCredentials コマンドを使用して管理されます。データは、構成ファイル

表 6. 構成ファイルの属性の詳細 (続く)

属性名	デフォルト値	必須	説明
			に保持される前に暗号化されます。
password	該当なし	システム生成	この属性は、ProvideCredentials コマンドを使用して管理されます。データは、構成ファイルに保持される前に暗号化されます。
verifycert	True	なし	この属性は、このデータ・ソースでの SSL 証明書検証を有効または無効にします。 **Tenable.sc**: verifycert が true に設定されている場合、証明機関 (CA) の証明書に以下のものが含まれていることを確認します。 • ルート証明書 • 中間証明書 Tenable.sc のデフォルト値は False です
proxy_host	該当なし	あり	この属性は、プロキシー・サーバー・ホストとポート番号 (形式: HTTP:// または HTTPS://

表 6. 構成ファイルの属性の詳細 (続く)

属性名	デフォルト値	必須	説明
			proxy_host:proxy_port) を提供します。
proxy_username	該当なし	オプション	この属性は、configureproxy コマンドを使用して管理されます。データは、構成ファイルに保持される前に暗号化されます。
proxy_password	該当なし	オプション	この属性は、configureproxy コマンドを使用して管理されます。データは、構成ファイルに保持される前に暗号化されます。

注:
プロキシーで verifycert が True に設定されている場合は、プロキシー・マシン証明書がマシンのクライアントに追加されていることを確認します。

<dataflows>

この`<dataflows>`構成ファイルのタグは、ソリューションが実行するように構成されているさまざまなデータ・フローの集合を表します。

各`<dataflow>`タグは、あるシステムから別のシステムへのデータ・フローのインスタンスを表し、SourceAdapter タグと TargetAdapter タグで構成されます。

表 7. 構成ファイルの属性の詳細。

属性名	必須	説明
displayname	あり	この属性は、個々のデータ・フローを記述するために使用されます。

表 7. 構成ファイルの属性の詳細。 (続く)

属性名	必須	説明
datatype	あり	asset (Asset Exchange の場合のみ)/検出結果 (その他すべてのデータ・フローの場合)
schedule*	あり	スケジュールの詳細については、こちらを参照してください。

Schedule*

cron 時刻ストリング形式: cron 時刻ストリング形式は、cron によって時間間隔に変換される 5 つのフィールドで構成されます。次に cron はこの間隔を使用して、データ・フローをスケジュールする頻度を決定します。5 つプレース値では、分、時、月の日付、月、曜日をそれぞれ指定します。

文字	記述子	許容される値
1	分	**0 ~ 59**、または *** (特定の値なし)
2	時間	**0 ~ 23**、または *** (任意の値)時刻はローカル・サーバーの時刻です。
3	日	**1 ~ 31**、または *** (特定の値なし)
4	月	**1 ~ 12**、または *** (特定の値なし)
5	曜日	**0 ~ 7** (0 と 7 はどちらも日曜日を表す)、または *** (特定の値なし)

ユースケースの例:

- 毎時間、正時から特定の分数が過ぎた後に、データ・フローを実行する。
- 毎週月曜日のローカル・サーバー時刻の特定の時刻にデータ・フローを実行する。
- 5 分ごとにデータ・フローを実行する。
- 2 時間ごとに正時にデータ・フローを実行する。

例 1: `0 10 15 * *` の cron 時刻ストリングは、毎月 15 日のローカル・サーバー時刻の午前 10:00 にコマンドを実行します。

例 2: `10/30 10 * * *` の cron 時刻ストリングは、毎日 10 時 10 分とその後 30 分ごとにコマンドを実行します。

> 注:
> データ・フロー・サービスの開始直後にデータ・フローを実行する必要がある場合は、スケジューラー値を現在時刻の 1 分後に構成する必要があります。例えば、現在時刻が 11:35:30 の場合、スケジューラーを 36 11 * * * に構成します。

> 注:
> 統合を最初にテストするときには、スケジューラーで「今すぐ」を使用でき、データ・フローの実行を手動でテストできます。構成が機能したら、都合に合わせてスケジュールを構成します。例: schedule = "now"。

<sourceadapter>

この`<sourceadapter>`タグは、データの抽出元のソース・システムを識別します。少なくとも 1 つのプロパティーが有効なプロパティー・コレクションを含める必要があります。

表 8. 構成ファイルの属性の詳細

属性名	必須	説明
displayname	あり	この属性は、このアダプター構成を記述するために使用されます。
adapterclass	あり	qualys 、 tenable、 insight (Asset Exchange の場合のみ) この属性は、データ・ソースからデータを抽出する際に使用されるアダプターを決定します。
datasourcename	あり	この属性値は、データ・ソース・コレクションで定義されているデータ・ソー

表 8. 構成ファイルの属性の詳細 (続く)

属性名	必須	説明
		スの名前と一致する必要があります。これは、アダプターに接続情報を提供するために使用されます。

<targetadapter>

この`<targetadapter>`タグは、データがロードされるターゲット・システムを識別します。少なくとも 1 つのプロパティーが有効なプロパティー・コレクションを含める必要があります。

表 9. 構成ファイルの属性の詳細

属性名	必須	説明
displayname	あり	この属性は、このアダプター構成を記述するために使用されます。
adapterclass	あり	insight、tenable この属性は、データ・ソースからデータを抽出する際に使用されるアダプターを決定します。
datasourcename	あり	この属性値は、データ・ソース・コレクションで定義されているデータ・ソースの名前と一致する必要があります。これは、アダプターに接続情報を提供するために使用されます。

<device_properties>

この`<device_properties>`タグは、特定のアダプター内のプロパティーのコレクションを表します。このコレクション内の各プロパティーは、対応するターゲット・アダプターまたはソース・アダプター内のコレクションへの位置によってマッピングされます。ターゲッ

ト・アダプター・デバイスとソース・アダプター・デバイスは、<identityproperty> タグの weight 属性でマッピングされます。

```
<dataflows>
    <dataflow displayname="Endpoint data from Qualys To Bigfix Insights" datatype="finding" schedule="0 */2 * * *">
        <dataflowdescription/>
        <sourceadapter displayname="Qualys Adapter" adapterclass="qualys" datasourcename="QualysAPI">
            <device_properties>
                <identityproperty displayname="IP Address" propertyname="IP" datatype="string" weight="20"/>
                <property displayname="Computer Name" propertyname="DNS" datatype="string"/>
                <property displayname="Operating System" propertyname="OS" datatype="string"/>
            </device_properties>
        </sourceadapter>

        <targetadapter displayname="BigFix Insight Adapter" adapterclass="insight" datasourcename="BigfixINSIGHT">
            <device_properties>
                <identityproperty displayname="IP Address" propertyname="IP Address" datatype="string" weight="20"/>
                <property displayname="Computer Name" propertyname="Computer Name" datatype="string"/>
                <property displayname="Operating System" propertyname="OS" datatype="string"/>
            </device_properties>
        </targetadapter>
    </dataflow>
</dataflows>
```

注:

デフォルトでは、Tenable.io には、Tenable.io データ・フローと Asset Exchange データ・フローの 2 つのデータ・フローがあります。Asset Exchange データ・フローを無効にするには、AE データ・フローを含む XML ファイルの部分を削除します。重要: データ・フローは、コメント化するのではなく、XML ファイルから削除する必要があります。

```
<?xml version="1.0" ?><dataflowconfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="DataflowsConfig.xsd">
    <datasources>
        <datasource datasourcename="BigfixINSIGHT" connectionstring="DRIVER={ODBC Driver 17 for SQL Server};SERVER=;DATABASE=BFInsights" verifycert="false"  username="" password=""/>
        <datasource datasourcename="TenableIO" connectionstring="https://cloud.tenable.com" verifycert="false" accesskey="" secretkey="" pagesize="5000"/>
    </datasources>
    <dataflows>
        <dataflow displayname="Endpoint data from Tenable.io To BigFix Insights" datatype="finding" schedule="*/60 * * * *">
            <dataflowdescription/>
            <sourceadapter displayname="Tenable Adapter" adapterclass="tenable" datasourcename="TenableIO">
                <device_properties>
                    <identityproperty displayname="IP Address" propertyname="asset_ips" datatype="string" weight="20"/>
                    <property displayname="DNS Name" propertyname="asset_dns_names" datatype="string"/>
                    <property displayname="NetBIOS Name" propertyname="asset_netbios_names" datatype="string"/>
                </device_properties>
            </sourceadapter>
            <targetadapter displayname="BigFix Insights Adapter" adapterclass="insight" datasourcename="BigfixINSIGHT">
                <device_properties>
                    <identityproperty displayname="IP Address" propertyname="IP Address" datatype="string" weight="20"/>
                    <property displayname="DNS Name" propertyname="DNS Name" datatype="string"/>
                    <property displayname="NetBIOS Name" propertyname="BIOS" datatype="string"/>
                </device_properties>
            </targetadapter>
        </dataflow>
        <dataflow displayname="Asset Exchange from BigFix Insights To Tenable.io" datatype="asset" schedule="*/60 * * * *">
            <dataflowdescription/>
            <sourceadapter displayname="BigFix Insights Adapter" adapterclass="insight" datasourcename="BigfixINSIGHT">
                <device_properties>
                    <property displayname="IP Address" propertyname="IP Address" datatype="string"/>
                    <property displayname="MAC Address" propertyname="MAC Address" datatype="string"/>
                    <property displayname="DNS Name" propertyname="DNS Name" datatype="string"/>
                    <property displayname="Computer Name" propertyname="Computer Name" datatype="string"/>
                    <property displayname="Remote ID" propertyname="ID" datatype="string"/>
                </device_properties>
            </sourceadapter>
            <targetadapter displayname="Tenable Adapter" adapterclass="tenable" datasourcename="TenableIO">
                <device_properties>
                    <property displayname="IP Address" propertyname="ipv4" datatype="list"/>
                    <property displayname="MAC Address" propertyname="mac_address" datatype="list"/>
                    <property displayname="DNS Name" propertyname="fqdn" datatype="list"/>
                    <property displayname="Netbios Name" propertyname="netbios_name" datatype="string"/>
                    <property displayname="Remote ID" propertyname="bigfix_remote_id" datatype="string"/>
                </device_properties>
            </targetadapter>
        </dataflow>
    </dataflows>
    <settings>
        <setting key="MinimumConfidenceLevel" value="20"/>
        <setting key="NumberOfConcurrentDataflows" value="1"/>
        <setting key="LogLevel" value="INFO"/>
        <setting key="CacheRefreshLimit" value="10"/>
    <setting key="rest_api_response_timeout" value="120"/>
    <setting key="rest_api_read_timeout" value="300"/>
    </settings>
</dataflowconfig>
```

<property>

この`<property>`タグは、システムから抽出されるか、システムにロードされるデータの単一の列を表します。受信したデータの変換を容易にするためのシンプルな変換ロジックを含む場合があります。

表 10. 構成ファイルの属性の詳細

属性名	必須	説明
displayname	あり	この属性は、構成されるプロパティーを記述するために使用されます。
propertyname	あり	この属性は、各アダプターに固有の表記を使用して、対応する列を識別するために使用されます。
datatype	あり	タイプ: ストリング
重み	なし	この属性は、プロパティーに重みを割り当てます。これは、レコードの重み付け信頼度の一致に使用されます。タイプ: Int.

<settings>

この`<settings>`タグは、ソリューションの設定のコレクションを表します。設定の詳細なリストについては、「IVR ソリューションの構成設定」を参照してください。

表 11. 構成ファイルの属性の詳細

属性名	必須	説明
key	あり	この属性は、構成中の設定の名前です。
value	あり	この属性は、構成中の設定の値です。

IVR ソリューションの構成設定

構成ファイルで変更できる使用可能な設定のリスト。

設定名	データ型	デフォルト値	説明	指定可能な値	注釈
LogLevel	ストリング	DEBUG	サーバーの口ギング・レベルを設定します。	• INFO • DEBUG • ERROR	
Ivr_insight.workerUnit	Threads	8	同時に実行できるワーカー・プロセス (相関) の数を設定します。		
Logger.RetentionInDays	Int	5	保持するログの期間を示します。		
NumberOfConcurrentDataflows	Int	1	同時に実行できるデータ・フロー・プロセッサーの数を設定します。		
DataFlow.QueueRefreshInterval	Int	120	データ・フローが更新される時間間隔。		
MinimumConfidenceLevel	Int	20	レコードが一致するための最小基準。		
CacheRefreshLimit	Int	10	指定された時間間隔でキャッシュを更新するようにシステムを構成します。この設定を変更すると、データの鮮度が影響を受けるが、それと引き換えに		

設定名	データ型	デフォルト値	説明	指定可能な値	注釈
			データが効率的に処理されるようになる場合があります。		
qualys.batch_size	Int	10000	要求ごとに処理されるホスト・レコードの最大数を指定します。指定しない場合、`qualys.batch_size` は 10,000 件のホスト・レコードに設定されます。デフォルトより小さい値 (1 ~ 999) またはデフォルトより大きい値 (1001 ~ 10000000) を指定できます。		
PurgeFindingsOnExecutionOfDataflow		FALSE		true に設定すると、 は、現在のデータ・フロー構成 (ハッシュの生成元) に関連付けられた*無効な ivr データと、既存のデータ・フロー構成に関連付けられて*いない*すべてのデータのパー	

設定名	データ型	デフォルト値	説明	指定可能な値	注釈
				ジが試みられます。 *無効 - ユーザーがデータ・フローのプロパティーを変更すると、新しいハッシュが計算されます。IVR スキーマのデータは、派生元の構成ハッシュにリンクされます。 注: IVR サービスが開始されると、この設定に関係なくパージが実行され、すべての無効なデータ (つまり、ユーザーによって	

設定名	データ型	デフォルト値	説明	指定可能な値	注釈
				変更/変更されたデータ・フロー構成から計算されたハッシュにリンクされた IVR テーブル内のデータ) の自動削除が試みられます。	
rest_api_read_timeout	int	デフォルトでは、いずれのタイムアウトも設定されないため、状況に応じて値を構成することが重要です。	サーバーへの接続が確立されるまで BFIVR が待機する秒数。	例: <setting key="rest_api_read_timeout" value="5"/>	デフォルトの TCP パケット再送信ウィンドウである 3 の倍数より少し大きい接続タイムアウトを設定することをお勧めします。
rest_api_response_timeout	int		BFIVR がサーバーに接続され、HTTP 要求が送信されると、このタイムアウトは、サーバーがデータに応答するのを	例: <setting key="rest_api_response_timeout" value="5"/>	

設定名	データ型	デフォルト値	説明	指定可能な値	注釈
			ユーザーが待機する秒数です。		
ResponseFile	ブール値	FALSE	true に設定した場合: • Qualys の場合: qualys_response ファイルが作成されます • tenableSC の場合: tenableSc_response ファイルが作成されます • tenableIo の場合: tenableIo_response ファイルが作成されます	TRUE、FALSE	

コマンド行インターフェース

BigFix Insights for Vulnerability Remediation サービス実行可能ファイル (*BFIVR.exe*) には、コマンド行インターフェース (CLI) が備わっており、ソリューションのセットアップと実行に関連するいくつかの異なる機能を実行できます。これには、ネイティブ・システム・サービスとしてのソリューションのインストール、アンインストール、開始、停止が含まれます。これにより、BigFix console からサービスを開始する前に、データ・ソースの資格情報を安全に提供し、構成を検証できます。

BigFix Insights for Vulnerability Remediation コマンド引数

BFIVR.exe 実行可能ファイルは、デフォルトのデプロイメント・フォルダーにあります。サポートされているすべてのコマンドのリストを表示するには、コマンド・プロンプトで --Help または -h を入力します。

```
.\BFIVR.exe -h
usage: BFIVR.exe [-h] [--Install | --Uninstall | --Start | --Stop | --Run | --ProvideCredentials [PROVIDECREDENTIALS] | --ValidateConfiguration | --InitializeSchemas]
                 [--ConfigFilePath <FilePath>] [--UserName <UserName>] [--Password <Password>]

Integration Services Command-Line Help

optional arguments:
  -h, --help            show this help message and exit
  --Install             This command will install this application as a system servivce.
  --Uninstall           This command will uninstall this application as a system service.
  --Start               This command will start the system service.
  --Stop                This command will stop the system service.
  --Run                 This command will execute the application as a Console application
  --ProvideCredentials [PROVIDECREDENTIALS]
                        This command will securely ask for credentials for all configured datasources
  --ValidateConfiguration
                        This command will attempt to validate the Integration Services XML Configuration file
  --InitializeSchemas   This command will attempt to initialize the datasources configured within a dataflow.
  --ConfigFilePath <FilePath>
                        Use this argument to provide the path to the Configuration File to store Encrypted Credentials
  --UserName <UserName>
                        Use this argument to provide the username for the system service to authenticate with, during installation.
  --Password <Password>
                        Use this argument to provide the password for the system service to authenticate with, during installation.
```

表 12. コマンド行引数のリスト

コマンド	目的	追加情報
--ProvideCredentials <DataSourceName>	単一データ・ソースの資格情報を安全に取得する	
--provideCredentials	すべてのデータ・ソースの資格情報を安全に取得する	
--ValidateConfiguration	構成を検証する	
--InitializeSchemas	スキーマを初期化する	
--configureproxy	プロキシー・パラメーターを構成する	

注:
コマンド行パラメーター名では大文字と小文字が区別されます。

ログ

ログ・ファイルは、インストール・パスの logs フォルダー内にあります。ログは毎日更新されます。問題のトラブルシューティングを行う場合を除き、INFO をログ・レベルとしてソリューションを構成します。

Connections.[date].log

DEBUG を有効にすると、このログ・ファイルには、サード・パーティー・データ・ソースへの外部接続に関連する詳細なロギング情報が記録されます。

DataFlow.[date].log

DEBUG を有効にすると、このログ・ファイルには、各データフローの実行に関連する詳細なロギング情報が記録されます。ETL (抽出、変換、ロード) に関連する問題のデバッグに使用される基本インターフェースです。

Main.[date]log

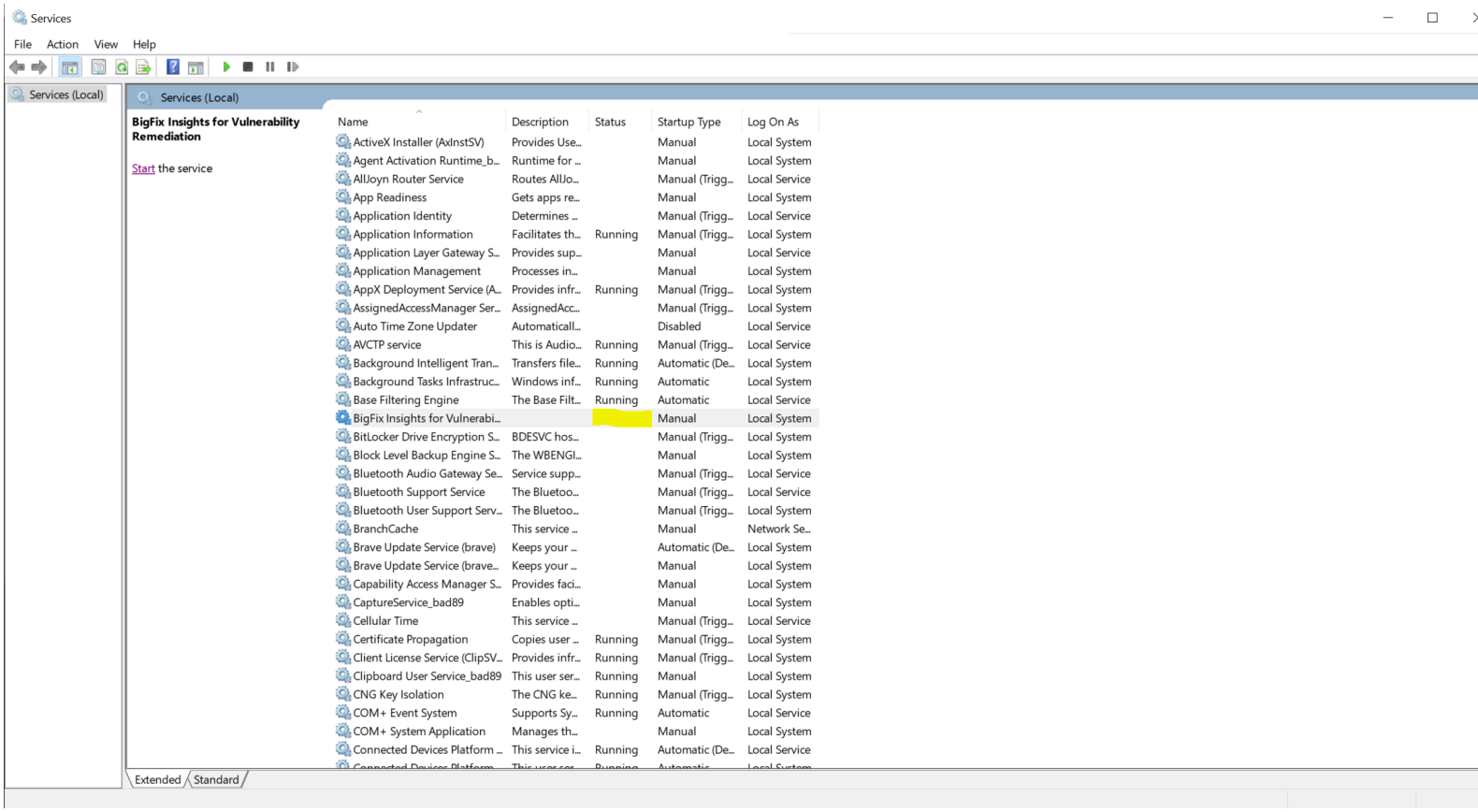
DEBUG を有効にすると、このログ・ファイルには、基本プロセスに関連する詳細なロギング情報が記録されます。サービスの開始と構成に関連する問題が表示されます。

IVR のトラブルシューティング

このトピックでは、IVR (BigFix Insights for Vulnerability Remediation) サービスで発生するさまざまな問題のトラブルシューティングについて説明します。

診断手順:

- サービス状態の Windows サービス・マネージャーを確認します。サービスは実行中の状態である必要があります。



- ログでエラーとタイムスタンプを確認します。ログは logs ディレクトリーにあります。

[DatetimeOfExecution] [ProcessID] [Method] [Message]

```
2021-03-20 23:13:27.730910  3896    DataFlowRunner  LogLevels.DEBUG Executing DataFlow Task : Endpoint data from Qualys To Bigfix Insights
2021-03-20 23:13:27.730910  3896    GetDataSource   LogLevels.DEBUG Read Single Datasource details: QualysAPI
2021-03-20 23:13:27.730910  3896    GetDataSource   LogLevels.DEBUG Read Single Datasource details: BigfixINSIGHT
2021-03-20 23:13:27.746534  3896    __init__    LogLevels.DEBUG DataFlow Initialized
2021-03-20 23:13:27.746534  3896    execute LogLevels.INFO  Starting DataFlow: Endpoint data from Qualys To Bigfix Insights
2021-03-20 23:13:27.746534  3896    validate_configuration  LogLevels.DEBUG Validating Configuration
2021-03-20 23:13:27.746534  3896    validate_configuration  LogLevels.DEBUG Source Adapter Validation: qualys
2021-03-20 23:13:27.762156  3896    ExecuteRESTCommand  LogLevels.INFO  Executing REST Command
```

表 13. DataFlow ログの詳細

メッセージ	説明
Executing DataFlow Task: Endpoint data from Qualys to BigFix Insights	データ・フローの開始を示します。

メッセージ	説明
Loading Qualys Data	Qualys データのロードを示します。
Loading Insights Data	Insights データのロードを示します。
RecordCaches Loaded In	Insights およびソース・アダプター (Qualys または Tenable) からデータを取得するのに要した時間を示します。
Processing Changes From Source Adapter	この時点で、変更を取得し、IVR テーブルの更新を準備します。ソース・アダプターからの変更が処理される時間が考慮され、IVR テーブルで更新されます。
Done Processing Devices	デバイス相関が完了したことを示します。
Updates Performed In	IVR テーブルにデータをスティックさせるのに要した時間を示します。
Saving RecordCaches	レコード・キャッシュが保存される最後のステップ。
DataFlowExecution Completed In	データ・フローの終了を示します。
Starting Dataflow: Endpoint data from Tenable.io to Bigfix Insights	データ・フローの開始を示します。
Connected to Tenable.io Server VERSION 6.9.1	Tenable データのロードが開始されようとしていることを示します。

- 冗長度の設定 - 詳しくは、リンクを参照してください。

cURL コマンドを使用した Qualys による IVR のトラブルシューティング

このトピックでは、cURL コマンドを使用した Qualys のトラブルシューティング手順を段階的に説明します。

前提条件

- cURL は、Windows マシンにインストールする必要があります。cURL をダウンロードするには、以下のサイトにアクセスしてください。cURL をダウンロードする

Windows への cURL のインストール

1. ダウンロードした ZIP ファイルをマシンの任意の場所に展開します。
2. システム・パスに cURL を追加します。
   a. 「PC」または「マイコンピュータ」を右クリックして、「プロパティ」を選択します。
   b. 右側の「高度なシステム設定」をクリックします。
   c. 「システムのプロパティ」ウィンドウの「詳細設定」タブで、「環境変数」ボタンをクリックします。
   d. 「システム環境変数」で、「Path」変数を見つけて選択し、「編集」をクリックします。
   e. 「新規」をクリックし、cURL を抽出したパスを追加して、「OK」をクリックします。
   f. すべてのウィンドウで「OK」をクリックして、変更を保存します。
3. コマンド・プロンプトを開いて、以下のコマンドを入力し、cURL のバージョンを確認します。

```
curl --version
```

トラブルシューティングの手順

1. アセットの抽出の確認

   アセットの抽出を確認するには、以下の cURL コマンドを実行します。

```
curl --location --request GET
 "https://qualysapi.qg3.apps.qualys.com/api/2.0/fo/asset/host/vm/detection/?action=list&truncation_limit=1"
 --header "X-Requested-With: QualysUVM" -u "username:password"
```

   注:
   - コマンド内の関連するルート URL を置き換えます (例: `https://qualysapi.qg3.apps.qualys.com`)
   - 「username」は、実際の Qualys のユーザー名とパスワードに置き換えます
   - このコマンドは、テスト用のため 1 つのアセットのみを抽出することに制限されています。

   解釈:
   - コマンドがデータを返した場合、Qualys API は正しくデータを取得しています。
   - コマンドが正しく実行されたにもかかわらず、IVR ログにデータが表示されない場合は、IVR サポートに連絡してください。
2. 脆弱性の抽出の確認

a. 以下の cURL コマンドを実行します。

```
curl --location --request GET

 "https://qualysapi.qg3.apps.qualys.com/api/2.0/fo/knowledge_base/vuln/?action=list" --header

 "X-Requested-With: IVR-QUALYS-ADAPTER" -u "username:password" -o output.txt
```

注:

- コマンド内の関連するルート URL を置き換えます
- 「username」は、実際の Qualys のユーザー名とパスワードに置き換えます
- 出力は、現在の作業ディレクトリーにある `output.txt` という名前のファイルに保存されます

解釈:

- `output.txt` に脆弱性の詳細が含まれている場合、Qualys API は正しくデータを取得しています
- コマンドが正しく実行されたにもかかわらず、IVR ログにデータが表示されない場合は、IVR サポートに連絡してください。

その他の注意事項

- Qualys アカウントで API アクセスが許可されていることを確認します。
- cURL コマンドのプレースホルダーを、Qualys アカウントおよび環境に固有の実際の値に置き換えます。

これらの手順に従って、Qualys API の機能を確認し、データ取得に関する問題を診断できます。問題が解決しない場合は、これらのテストの結果を IVR サポートにお問い合わせいただくことで、さらなるサポートを受けることができます。

既知の制限

BigFix Insights for Vulnerability Remediation の制限については、次のリストを参照してください。

警告:
BigFix Insights for Vulnerability Remediation サービスごとに 1 つ以上のデータ・フローを使用しないでください。

> **警告:**
> BigFix Insights for Vulnerability Remediation サービスは 1 台を超えるマシンにデプロイしないでください。

1. IVR(BigFix Insights for Vulnerability Remediation)1.1 は現在、1 つの BigFix データ・ソースのみを持つ BigFix Insights インスタンスを正式にサポートしています。
2. IVR Tenable.sc: セッション管理の許可を無効にする必要があります。詳しくは、Tenable.sc の構成設定を参照してください。
3. 現在、同じデータ・ソース・タイプであっても、マルチインスタンス・データ・フロー・サービスはサポートされていません。
4. PowerBI レポートと Tableau レポート: CSV ファイルにエクスポートできるレコードの最大数。
    - Tableau では 50,000 件のレコード
    - PowerBI では 30,000 件のレコード
5. Power BI: 内訳表示で重大度をソートすると、予測不能な結果が生じる場合があります。
    - 棒グラフのソート順が予測不能な順序に異なって表示されますが、データの機能には影響しません。
6. IVR Tenable.io: Tenable.io でアセットが削除された IVR.findings テーブルの検出結果は、検出結果/脆弱性自体が Tenable.io で更新されるまで削除されません。
7. Asset Exchange と Tenable.io を実行するには、Asset Exchange データ・フローと Tenable.io データ・フローの間でサービスを停止して再起動する必要があります。
8. Tenable.io: IP アドレスの多重度 - 特定のデバイス/アセットのプロパティー結果セットに複数の IPv4 アドレスが含まれている場合、このデバイス/アセットは相関されません。現在サポートされていません。
9. IVR Insights: 削除されたカスタム Fixlet は、IVR.vulnerability_fixlet_nexus テーブルに残ります。
10. 検出日/公開日の視覚化に対する「概要」ダッシュボードの「脆弱性リスト」へのドリルスルー・フィルターが正しく機能しない場合があります。

第 11 章. リリース・ ノート

リリース・ ノートでは、最新のアプリケーション更新など、BigFix Insights for Vulnerability Remediation の各バージョンに含まれる機能、更新、パッチについて説明しています。

IVR 2.0.3 リリース情報

BigFix Insights for Vulnerability Remediation アプリケーション (BigFix Lifecycle および Compliance サイトに含まれる) のバージョン 2.0.3 のリリースをお知らせします。このアプリケーションを使用すると、検出された脆弱性が適切な修復に自動的に関連付けられ、修復作業に集中するための優先順位付けデータが提供されるため、IT セキュリティー・ チームと運用チームはコラボレーションをより効果的に行うことができます。

このリリースの主な機能は次のとおりです。

- セキュリティの向上
- バグ修正
- Tenable.sc のユーザー・ エージェントのサポート

このリリースに関する追加情報:

- 「ライフサイクル」セクションまたは「コンプライアンス」セクションの「ライセンスの概要」ダッシュボードから、**BigFix Insights for Vulnerability Remediation** Fixlet サイトを見つけてください。

  サイトの有効化について詳しくは、https://help.hcltechsw.com/bigfix/10.0/platform/Platform/Console/c_license_overview_dashboard.html を参照してください。

- 公開済みサイト・ バージョン: 13

便利なリンク

- マニュアル: https://help.hcl-software.com/bigfix/10.0/integrations/Ecosystem/Install_Config/c_welcome.html
- Insights for Vulnerability Remediation のスキーマ: https://help.hcl-software.com/bigfix/10.0/integrations/Ecosystem/Schema/c_IVR_schema.html
- 詳しくは、製品ページ https://www.hcltechsw.com/bigfix/ivr-home を参照してください。

IVR 1.4 リリース情報

BigFix Insights for Vulnerability Remediation アプリケーション (BigFix Lifecycle および Compliance サイトに含まれる) のバージョン 1.4 のリリースをお知らせします。このアプリケーションを使用すると、検出された脆弱性が適切な修復に自動的に関連付けられ、修復作業に集中するための優先順位付けデータが提供されるため、IT セキュリティー・ チームと運用チームはコラボレーションをより効果的に行うことができます。

このリリースの主な機能は次のとおりです。

- Fixlet を使用した IVR のデプロイメント、構成、管理の簡素化
  - 単一の Fixlet を使用して IVR をデプロイしたり、IVR を構成したりして、より迅速かつ簡単に稼働状態にすることができるようになりました。詳しくは、本ドキュメントの「デプロイメントと構成」セクションを参照してください。
  - データ同期スケジュール、資格情報、サービス状態など、IVR の一般的な管理を簡素化するための、追加のタスクを使用できます。詳しくは、本ドキュメントの「IVR Fixlet とタスク」セクションを参照してください

このリリースに関する追加情報:

- 「ライフサイクル」セクションまたは「コンプライアンス」セクションの「ライセンスの概要」ダッシュボードから、**BigFix Insights for Vulnerability Remediation** Fixlet サイトを見つけてください。

  サイトの有効化について詳しくは、https://help.hcl-software.com/bigfix/10.0/platform/Platform/Console/c_license_overview_dashboard.html を参照してください。

- 公開済みサイト・ バージョン: 10

便利なリンク

- マニュアル: https://help.hcl-software.com/bigfix/10.0/integrations/Ecosystem/Install_Config/c_welcome.html
- Insights for Vulnerability Remediation のスキーマ: https://help.hcl-software.com/bigfix/10.0/integrations/Ecosystem/Schema/c_IVR_schema.html
- 詳しくは、製品ページ https://www.hcltechsw.com/bigfix/ivr-home を参照してください。

IVR 1.3 リリース情報

BigFix Insights for Vulnerability Remediation アプリケーション (BigFix Lifecycle および Compliance スイートに含まれる) のバージョン 1.3 のリリースをお知らせします。このアプリケーションを使用すると、検出された脆弱性が適切な修復に自動的に関連付けられ、修復作業に集中するための優先順位付けデータが提供されるため、IT セキュリティー・チームと運用チームはコラボレーションをより効果的に行うことができます。

このリリースの主な機能は次のとおりです。

- Tenable.sc バージョン 5.20.x のサポートが導入されました

このリリースに関する追加情報:

- 「ライフサイクル」セクションまたは「コンプライアンス」セクションの「ライセンスの概要」ダッシュボードから、**BigFix Insights for Vulnerability Remediation** Fixlet サイトを見つけてください。

  サイトの有効化について詳しくは、https://help.hcl-software.com/bigfix/10.0/platform/Platform/Console/c_license_overview_dashboard.html を参照してください。

- 公開済みサイト・バージョン: 9

便利なリンク

- マニュアル: https://help.hcltechsw.com/bigfix/10.0/integrations/Ecosystem/Install_Config/c_welcome.html
- Insights for Vulnerability Remediation のスキーマ: https://help.hcl-software.com/bigfix/10.0/integrations/Ecosystem/Schema/c_IVR_schema.html
- 詳しくは、製品ページ https://www.hcltechsw.com/bigfix/ivr-home を参照してください。

IVR 1.2 リリース情報

BigFix Insights for Vulnerability Remediation アプリケーション (BigFix Lifecycle および Compliance スイートに含まれる) のバージョン 1.2 のリリースをお知らせします。このアプリケーションを使用すると、検出された脆弱性が適切な修復に自動的に関連付けられ、修復作業に集中するための優先順位付けデータが提供されるため、IT セキュリティー・チームと運用チームはコラボレーションをより効果的に行うことができます。

このリリースの主な機能は次のとおりです。

- スケジューリングのサポートの向上
  - BigFix Insights for Vulnerability Remediation の詳細なスケジュールを定義して、データを同期・処理するタイミングをより適切に制御・管理できるようになりました。
- プロキシー・ サポート
  - BigFix Insights for Vulnerability Remediation から脆弱性管理製品への接続をプロキシー経由で設定できるようになったため、セキュリティーが向上されました。
- その他のマイナーな機能拡張とバグの修正

このリリースに関する追加情報:

- 「ライフサイクル」セクションまたは「コンプライアンス」セクションの「ライセンスの概要」ダッシュボードから **BigFix Insights for Vulnerability Remediation** Fixlet サイトを探してください。

  サイトの有効化について詳しくは、https://help.hcl-software.com/bigfix/10.0/platform/Platform/Console/c_license_overview_dashboard.html を参照してください。

便利なリンク

- マニュアル: https://help.hcl-software.com/bigfix/10.0/integrations/Ecosystem/Install_Config/c_welcome.html
- Insights for Vulnerability Remediation のスキーマ: https://help.hcl-software.com/bigfix/10.0/integrations/Ecosystem/Schema/c_IVR_schema.html
- 詳しくは、製品ページ https://www.hcltechsw.com/bigfix/ivr-home を参照してください。

付録 A. 用語集

この用語集は、BigFix の最新のクライアント管理ソフトウェアおよび製品の用語と定義を記載しています。

この用語集では次の相互参照が使用されています。

- 「を参照」は、非優先用語の場合は優先用語を、省略語の場合は省略していない形式を示すものです。
- 「も参照」は、関連する用語または対比される用語を示します。

A B C D E F G L M N O P R S T U V W

A

アクション **(action)**

1. 「Fixlet」を参照。
2. 操作タスクや管理用タスク (パッチのインストール、デバイスのリブートなど) を実行するアクション・スクリプト・コマンドのセット。

アクション・スクリプト **(Action Script)**

エンドポイントでアクションを実行するために使用する言語。

エージェント (agent)

「BigFix エージェント (BigFix agent)」を参照。

あいまいなソフトウェア **(ambiguous software)**

別の実行可能ファイルとよく似た実行可能ファイルがあるソフトウェア、またはカタログ内の複数の場所に存在するソフトウェア (スタンドアロン製品としての Microsoft Word と Microsoft Office にバンドルされた Microsoft Word が存在する場合など)。

監査パッチ **(audit patch)**

修正不能であり管理者の確認を要する状態を検出するために使用されるパッチ。監査パッチにはアクションが含まれず、監査パッチをデプロイすることはできない。

自動コンピューター・グループ **(automatic computer group)**

指定されたデバイスのプロパティーをグループ・メンバーシップに設定された基準と比較することにより、実行時にメンバーシップが決まるコンピューター・グループ。自動グループ内のデバイスのセットは動的である。これは、そのグループが変化する可能性があること、また実際に変化することを意味する。「コンピューター・グループ」も参照。

B

ベースライン **(baseline)**

一緒にデプロイされるアクションの集合。ベースラインは、通常、デプロイメントを単純化するため、またはアクションのセットが適用される順序を制御するために使用される。「デプロイメント・グループ (deployment group)」も参照。

BigFix エージェント **(BigFix agent)**

BigFix による管理とモニタリングを可能にするエンドポイント上の BigFix コード。

BigFix クライアント **(BigFix client)**

「BigFix エージェント (BigFix agent)」を参照。

BigFix コンソール **(BigFix console)**

プライマリー BigFix 管理インターフェース。このコンソールは、完全な機能セットを BigFix 管理者に提供する。

BYOD

独自のデバイスを持ち込む (BYOD) とは、従業員が個人所有のデバイスを使用して組織ネットワークに接続し、業務関連システムや潜在的に重要または機密データにアクセスすることを指します。

C

クライアント **(client)**

サーバーからのサービスを要求するソフトウェア・プログラムまたはコンピューター。サーバー (server) も参照。

クライアント時間 **(client time)**

BigFix クライアント・デバイス上のローカル時間。

クラウド

コンテナーまたは仮想マシンで実行されるコンピューターおよびストレージ・インスタンスまたはサービスのセット。

Common Vulnerabilities and Exposures 識別番号 **(CVE ID) (Common Vulnerabilities and Exposures Identification Number (CVE ID))**

National Vulnerability Database の特定のエントリーを識別する番号。ベンダーのパッチ文書には、通常、CVE ID が含まれる (CVE ID が使用可能な場合)。「National Vulnerability Database」も参照。

Common Vulnerabilities and Exposures (CVE) システム (Common Vulnerabilities and Exposures system (CVE))

米国連邦情報・技術局 (NIST) が保守する National Vulnerabilities Database (NVD) の一部である公式に知られたネットワーク脆弱性の参照。

コンポーネント **(component)**

複数のアクションを含むデプロイメント内の個々のアクション。「デプロイメント・グループ (deployment group)」も参照。

コンピューター・グループ **(computer group)**

関連するコンピューターのグループ。管理者はコンピューター・グループを作成して、システムを意味のあるカテゴリーに編成し、複数のコンピューターへのコンテンツのデプロイメントを容易にできる。「自動コンピューター・グループ」、「手動コンピューター・グループ 」も参照。

console (コンソール)

「BigFix コンソール」を参照。

コンテンツ **(content)**

データ、ルール、クエリー、基準、その他の指示を含むデジタル署名されたファイル。ネットワーク全体でのデプロイメント用にパッケージ化されている。BigFix エージェントはコンテンツ内の検出基準 (Relevance ステートメント) およびアクション指示 (アクション・スクリプト・ステートメント) を使用して、脆弱性を検出したりネットワーク・ポリシーを施行したりする。

コンテンツの関連度 **(content relevance)**

パッチまたはソフトウェアが 1 つ以上のデバイスへのデプロイメントに適しているかどうかの判定。「デバイスの関連度」も参照。

協定世界時 **(UTC) (Coordinated Universal Time (UTC))**

世界中で原子時計によって保持される国際標準時。

問題のあるパッチ **(corrupt patch)**

前のパッチで行われた修正が変更または危殆化された場合にオペレーターに警告するパッチ。この状況は、前のサービス・パックまたはアプリケーションがより新しいファイルを上書きし、パッチが適用されたファイルが現行ファイルではなくなった場合に発生する可能性がある。問題のあるパッチによって、この状態にフラグが立てられる。これを使用して、より新しいパッチを再適用することができる。

カスタム・コンテンツ **(custom content)**

ユーザーが独自のネットワークで使用するために作成した BigFix コード (カスタム・パッチやカスタム・ベースラインなど)。

CVE

「Common Vulnerabilities and Exposures システム」を参照。

CVE ID

「Common Vulnerabilities and Exposures 識別番号 」を参照。

D

データ・ストリーム **(data stream)**

パッケージ・データのソースとして機能する情報のストリング。

デフォルト・アクション **(default action)**

Fixlet のデプロイ時に実行されるように指定されたアクション。デフォルト・アクションが定義されていない場合、オペレーターには、いくつかのアクションから選択するか、単一アクション関する情報に基づく意思決定を行うように求めるプロンプトが出されます。

確定パッケージ **(definitive package)**

コンピューター上のソフトウェアの存在を識別するための主な方法となるデータのストリング。

適用 **(deploy)**

ソフトウェアのインストールやパッチの更新などの目的で、実行により操作やタスクを完了するために 1 つ以上のエンドポイントにコンテンツをディスパッチすること。

デプロイメント **(deployment)**

1 つ以上のエンドポイントにディスパッチされたコンテンツに関する情報 (ディスパッチされたコンテンツの特定のインスタンス)。

デプロイメント・グループ **(deployment group)**

オペレーターがデプロイメント用に複数のアクションを選択した場合、またはベースラインがデプロイされた場合に作成されたアクションの集合。「ベースライン」、「コンポーネント」、「デプロイメント・ウィンドウ」、「複数のアクション・グループ」も参照。

デプロイメント状態 **(deployment state)**

エンドポイント上で実行するデプロイメントの適格性。状態には、オペレーターによって設定されたパラメーター (「Start at 1AM, end at 3AM」など) が含まれる。

デプロイメント状況 **(deployment status)**

すべての対象デバイスの累積の結果。デプロイメントの成功のパーセンテージとして表示される。

デプロイメント・タイプ **(deployment type)**

デプロイメントに含まれるアクションが 1 つか複数かを示すもの。

デプロイメント期間 **(deployment window)**

デプロイメントのアクションが実行に適格である期間。例えば、Fixlet に 3 日間のデプロイメント期間があり、オフラインの適格デバイスがこの 3 日の期間内に BigFix に通信した場合、そのデバイスは Fixlet を取得します。この 3 日間の期限が切れた後にデバイスがオンラインに戻った場合、そのデバイスは Fixlet を取得しません。「デプロイメント・グループ (deployment group)」も参照。

デバイス **(device)**

BigFix が管理しているラップトップ、デスクトップ、サーバー、仮想マシンなどのエンドポイント。BigFix エージェントを実行しているエンドポイント。

デバイスの所有者 **(device holder)**

BigFix 管理対象コンピューターを使用する個人。

デバイス・プロパティー **(device property)**

BigFix によって収集されたデバイスに関する情報 (デバイスのハードウェア、オペレーティング・システム、ネットワーク状況、設定、BigFix クライアントに関する詳細を含む)。カスタム・プロパティーをデバイスに割り当てることもできる。

デバイスの関連度 **(device relevance)**

BigFix コンテンツの一部をデバイスに適用するか (パッチを適用する、ソフトウェアをインストールする、ベースラインを実行するなど) の判定。「コンテンツの関連度」も参照。

デバイスの結果 **(device result)**

特定のエンドポイントのデプロイメントの状態 (結果を含む)。

災害対策サーバー・アーキテクチャー **(Disaster Server** Architecture、DSA)

障害が発生した場合に備えて完全な冗長性を実現するために複数のサーバーをリンクするアーキテクチャー。

DSA

「災害対策サーバー・アーキテクチャー (DSA)」を参照。

動的に対象指定 **(dynamically targeted)**

コンピューター・グループを使用してデプロイメントを対象にすることに関連する。

E

エンドポイント **(endpoint)**

BigFix エージェントを実行するネットワーク・デバイス。

F

フィルター **(filter)**

項目のリストを、特定の属性の項目に絞ること。

Fixlet

操作またはタスクを実行するために一緒にバンドルされた Relevance ステートメントおよびアクション・スクリプト・ステートメントを含む BigFix コンテンツの一部。Fixlet は BigFix コンテンツの基本的なビルディング・ブロックである。Fixlet は、ネットワーク管理アクションやレポート・アクションを実行するために BigFix エージェントに指示を提供する。

フル・ディスク暗号化

項目のリストを、特定の属性の項目に絞ること。

G

グループ・デプロイメント **(group deployment)**

複数のアクションが 1 つ以上のデバイスにデプロイされたデプロイメントのタイプ。

H

ハイブリッド・クラウド

クラウド・サービスの異なるセット (通常はパブリック・クラウドとプライベート・クラウド) を最適に組み合わせて使用すること。

L

ロック済み **(locked)**

デバイスのロックが解除されるまで BigFix のアクションの大部分が実行できないエンドポイントの状態。

M

MAG

「複数アクション・グループ」を参照。

管理権限 **(management rights)**

指定されたコンピューターのグループへのコンソール・オペレーターの制限。サイト管理者またはマスター・オペレーターのみが管理権限を割り当てることができる。

マニュアル・コンピューター・グループ **(manual computer group)**

オペレーターによる選択によってメンバーシップが決まるコンピューター・グループ。マニュアル・グループ内のデバイスの組み合わせは静的で、従って変化しない。「コンピューター・グループ」も参照。

マスター・オペレーター **(master operator)**

管理権限を持つコンソール・オペレーター。マスター・オペレーターは、サイト管理者とほぼ同等のことを実行できるが、オペレーターを作成することはできない。

マストヘッド **(masthead)**

BigFix プロセス (Fixlet コンテンツへの URL など) のパラメーターを含むファイルの集合。BigFix エージェントは、サブスクライブされているマストヘッドに基づいてコンテンツを企業内に取り込む。

MCM と BigFix Mobile

ラップトップ (Windows、macOS) を管理する Modern Client Management と、モバイルデバイス (Android、iOS、iPadOS) を管理する BigFix Mobile の両方に共通する BigFix の機能を指す。

ミラー・サーバー **(mirror server)**

企業で直接の Web アクセスは許可していないが、代わりにパスワード・レベルの認証を必要とするプロキシー・サーバーを使用する場合に必要な BigFix サーバー。

マルチクラウド **(Multicloud)**

別個のクラウド・サービス・セットを使用すること。通常、複数ベンダーから提供され、特定のアプリケーション群は単一のクラウド・インスタンスに限定される。

複数アクション・グループ **(MAG) (multiple action group (MAG))**

ベースラインなどで複数のアクションが一緒にデプロイされたときに作成される BigFix オブジェクト。1 つの MAG には複数の Fixlet またはタスクが含まれる。「デプロイメント・グループ (deployment group)」も参照。

N

National Vulnerability Database (NVD)

米国連邦情報・技術局 (NIST) が保持する公式に知られた情報セキュリティーの脆弱性およびエクスポージャーのカタログ。「Common Vulnerabilities and Exposures 識別番号」も参照。

NVD

「National Vulnerability Database」を参照。

O

オファー **(offer)**

デバイスの所有者が、BigFix アクションに同意するか同意しないこと、および実行時に何らかの制御を行うことを可能にするデプロイメントのオプション。例えば、デバイス所有者が、ソフトウェア・アプリケーションをインストールするかインストールしないか、インストールを夜間に実行するか昼間に実行するかを決定できる。

無期限のデプロイメント **(open-ended deployment)**

終了日も有効期限もないデプロイメント。継続的に実行され、ネットワーク上のコンピューターが準拠しているかを検査するものなど。

オペレーター **(operator)**

BigFix WebUI または BigFix コンソールの一部を使用する個人。

P

パッチ **(patch)**

問題を修正するために、2 つのリリースの間にユーザーに提供される当面のソリューションとしてベンダー・ソフトウェアに追加されるコードの断片。

パッチ・カテゴリー **(patch category)**

バグ修正やサービス・パックなど、パッチのタイプおよび操作の一般領域の説明。

パッチの重大度 **(patch severity)**

ネットワークの脅威または脆弱性によってもたらされるリスクのレベル、およびそれに関連してそのパッチを適用する重要度。

R

リレー **(relay)**

特殊なサーバー・ソフトウェアを実行しているクライアント。リレーは、サーバーとクライアントの間の直接ダウンロードを最小限に抑え、アップストリーム・データを圧縮することにより、サーバーとネットワークの負荷を軽減する。

関連度 **(Relevance)**

指定のエンドポイントへのコンテンツの適用可能性を判別するために使用される BigFix クエリー言語。関連度では「はい」または「いいえ」の質問が行われ、その結果が評価される。関連度のクエリーの結果により、アクションを適用できるか、またはアクションを適用する必要があるかが決定される。関連度は Fixlet のアクション・スクリプトと対になっている。

S

SCAP

「Security Content Automation Protocol」を参照。

SCAP チェック **(SCAP check)**

Security Content Automation Protocol (SCAP) チェックリスト内の特定の構成チェック。チェック項目は XCCDF で記述されており、SCAP テンプレートに従って SCAP 列挙と SCAP マッピングを組み込む必要がある。

SCAP チェックリスト **(SCAP checklist)**

機械可読言語 (XCCDF) で記述された構成チェックリスト。Security Content Automation Protocol (SCAP) チェックリストは、NIST National Checklist Program に提出され、承認されている。これらは、SCAP 製品およびサービスとの互換性を確保するため、SCAP テンプレートにも準拠している。

SCAP コンテンツ **(SCAP Content)**

自動化 XML 形式で表されたセキュリティー・チェックリスト・データ、脆弱性および製品名関連の列挙、および列挙間のマッピングで構成されたリポジトリー。

SCAP 列挙 **(SCAP enumeration)**

すべて既知のセキュリティー関連ソフトウェア欠陥 (CVE)、既知のソフトウェア構成問題 (CCE)、および標準ベンダー名および製品名 (CPE) のリスト。

SCAP マッピング **(SCAP mapping)**

ソフトウェア欠陥および構成問題に対して標準ベースの影響の測定を提供する列挙の相互関係。

Security Content Automation Protocol (SCAP)

米国連邦情報・技術局 (NIST) による脆弱性およびコンプライアンスの自動化、測定、管理に使用される標準のセット。

サーバー **(server)**

他のソフトウェア・プログラムまたはコンピューターにサービスを提供するソフトウェア・プログラムまたはコンピューター。「クライアント」も参照。

署名パスワード **(signing password)**

デプロイメント用のアクションに署名するためにコンソール・オペレーターが使用するパスワード。

単一デプロイメント **(single deployment)**

単一のアクションが 1 つ以上のデバイスにデプロイされたデプロイメントのタイプ。

サイト **(site)**

BigFix コンテンツの集合。サイトは、同様のコンテンツを一緒にまとめる。

サイト管理者 **(site administrator)**

BigFix のインストール、新規コンソール・オペレーターの承認と作成に関する責任者。

ソフトウェア・パッケージ **(software package)**

デバイスにソフトウェア製品をインストールする Fixlet の集合。ソフトウェア・パッケージは、配布のためにオペレーターによって BigFix にアップロードされる。BigFix ソフトウェア・パッケージには、インストール・ファイル、ファイルをインストールするための Fixlet、およびパッケージに関する情報 (メタデータ) が含まれる。

SQL Server

Microsoft が提供する完全なデータベース・エンジン。取得して BigFix システムにインストールすると、基本的なレポート作成とデータ・ストレージを超えるニーズを実現できる。

標準デプロイメント **(standard deployment)**

単一の管理ドメインを持つワークグループおよび企業に適用される BigFix のデプロイメント。すべてのクライアント・コンピューターが単一の社内サーバーに直接アクセスできる設定を目的としている。

静的に対象指定 **(statistically targeted)**

デバイスまたはコンテンツの一部に対してデプロイメントを対象指定するために使用する方式に関連する。静的に対象指定されたデバイスは、オペレーターによって手動で選択されている。

置き換えられたパッチ **(superseded patch)**

以前のバージョンのパッチがより新しいバージョンによって置き換えられている場合にオペレーターに通知するパッチのタイプ。新しいパッチが以前のパッチと同じファイルを更新した場合に発生する。置き換えられたパッチは、より新しいパッチで修正可能な脆弱性にフラグを立てる。置き換えられたパッチはデプロイできない。

システムの電源状態 **(system power state)**

システムの全体的な電力使用量の定義。BigFix 電源管理がトラッキングする主な電源状態は、「アクティブ」、「アイドル」、「スタンバイ」または「休止状態」、「電源オフ」の 4 つです。

T

対象 **(target)**

デプロイメント用のコンテンツを選択するか、コンテンツを受け取るデバイスを選択することにより、コンテンツをデプロイメント内のデバイスとマッチングすること。

対象指定 **(targeting)**

デプロイメント内のエンドポイントを指定するために使用する方式。

タスク **(task)**

継続中の保守タスクを実行するためなど、再使用のために設計された Fixlet のタイプ。

U

UTC

「協定世界時 (Coordinated Universal Time)」を参照。

V

仮想プライベート・ネットワーク **(VPN) (virtual private network (VPN))**

パブリック・ネットワークまたはプライベート・ネットワークの既存フレームワーク上で企業のイントラネットを拡張したもの。VPN を使用すると、接続の 2 つのエンドポイント間で送信されるデータを保護できる。

VPN

「仮想プライベート・ネットワーク (virtual private network)」を参照。

脆弱性 **(vulnerability)**

オペレーティング・システム、システム・ソフトウェア、またはアプリケーション・ソフトウェア・コンポーネントでの機密漏れ。

W

Wake-from-Standby

アプリケーションが、Wake on LAN を必要とせずに、事前定義された時間にコンピューターを待機モードから起動できるようにするモード。

Wake on LAN

時間外の保守のためにユーザーがシステムをリモートで起動できるテクノロジー。Intel と IBM の Advanced Manageability Alliance の成果であり、Wired for Management Baseline Specification の一部である。このテクノロジーのユーザーは、リモートでサーバーを起動したりネットワーク経由でサーバーを制御したりできるため、ソフトウェアのインストール、アップグレード、ディスク・バックアップ、およびウィルス・スキャンを自動化して時間を節約できる。

WAN

「広域ネットワーク (wide area network)」を参照。

広域ネットワーク **(WAN) (wide area network (WAN))**

ローカル・エリア・ネットワーク (LAN) や大都市圏ネットワーク (MAN) で提供されるよりも大きい地理上の領域で、デバイス間の通信サービスを提供するネットワーク。

Notices

This information was developed for products and services offered in the US.

HCL may not offer the products, services, or features discussed in this document in other countries. Consult your local HCL representative for information on the products and services currently available in your area. Any reference to an HCL product, program, or service is not intended to state or imply that only that HCL product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any HCL intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-HCL product, program, or service.

HCL may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

HCL
330 Potrero Ave.
Sunnyvale, CA 94085
USA
Attention: Office of the General Counsel

For license inquiries regarding double-byte character set (DBCS) information, contact the HCL Intellectual Property Department in your country or send inquiries, in writing, to:

HCL
330 Potrero Ave.
Sunnyvale, CA 94085
USA
Attention: Office of the General Counsel

HCL TECHNOLOGIES LTD. PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. HCL may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-HCL websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this HCL product and use of those websites is at your own risk.

HCL may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

HCL
330 Potrero Ave.
Sunnyvale, CA 94085
USA
Attention: Office of the General Counsel

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by HCL under terms of the HCL Customer Agreement, HCL International Program License Agreement or any equivalent agreement between us.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

Information concerning non-HCL products was obtained from the suppliers of those products, their published announcements or other publicly available sources. HCL has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-HCL products. Questions on the capabilities of non-HCL products should be addressed to the suppliers of those products.

Statements regarding HCL's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to HCL, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. HCL, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS," without warranty of any kind. HCL shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as follows:
© (your company name) (year).
Portions of this code are derived from HCL Ltd. Sample Programs.

Trademarks

HCL Technologies Ltd. and HCL Technologies Ltd. logo, and hcl.com are trademarks or registered trademarks of HCL Technologies Ltd., registered in many jurisdictions worldwide.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other product and service names might be trademarks of HCL or other companies.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the HCL website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of HCL.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of HCL.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

HCL reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by HCL, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

HCL MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.