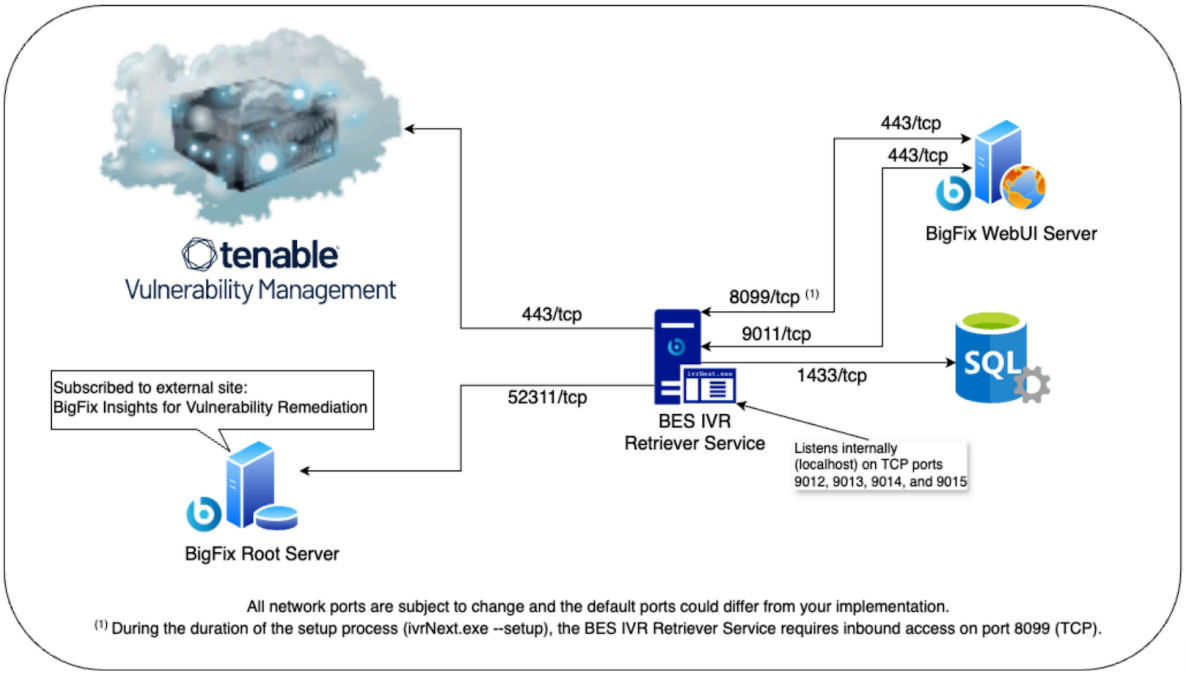
BigFix Insights for Vulnerability Remediation (IVR) v. 4.0.0

Contents

Chapter 1. 製品の概要

このモジュールでは、**IVR v.4.0.0** サービスのインストール、メンテナンス、および操作に関する包括的なガイダンスを提供します。IVR v.4.0.0 を使用するためのエンドツーエンド・ワークフロー全体についての詳細を説明します。



IVR4 は、脆弱性の検出と修復アクション間のギャップを埋めるように設計された高度なソリューションです。これにより、セキュリティーの脆弱性への対処のスピード、精度、効率が大幅に向上します。Tenable の脆弱性データと BigFix の修復機能を統合することで、IVR は合理化されたアプローチを提供し、組織がセキュリティー・リスクに迅速に対処できるようにします。

IVR4 システムの主な機能は次のとおりです。

- 向上した修復相関関係の脆弱性: これまでは、Tenable の脆弱性調査結果と BigFix の修復コンテンツの相関関係は CVE ID (Common Vulnerabilities and Exposures: 通脆弱性識別子) に基づいていましたが、それにより遅延や誤りが発生することがよくありました。この新しいアプローチにより、IVR4 ではより正確な相関関係のために **xref** タイプなどのさまざまな Tenable プラグイン属性を利用するルールベースのシステムが使用されています。さらに、IVR4 は、継続的に更新される Tenable プラグインと BigFix Fixlet 間の事前相関マッピングを提供するようになりました。この機能強化により、より迅速かつ正確な修復ガイダンスが実現します。
- アセットの相関関係の強化: これまでは、Tenable アセットは、IP アドレス、MAC アドレス、またはホスト名に基づいて BigFix のデバイスと照合されていました。多くの場合、この方法では IP

アドレスや複数のネットワーク・アダプターを使用しているデバイスを変更することで問題が発生します。新しいリリースでは、IVR4 は Tenable が提供する **BigFix** アセット **ID** を直接活用できるため、アセットの相関関係の精度と速度が向上します。この新しい方法では、仮想化や、動的または複数のネットワーク接続を持つデバイスに関連する課題をなくすことができます。

- インフラストラクチャー要件の削減: IVR の以前のバージョンでの重要な課題の 1 つは、特に大規模な環境での大規模なインフラストラクチャーの必要性でした。お客様は、追加の SQL データベース、ETL 構成、およびリソース管理が含まれていた **BigFix Insights** コンポーネントと **IVR** サービスの両方をデプロイして保守する必要がありました。新しい IVR4 アーキテクチャーにより、IVR サービスは BigFix Insights から完全に切り離されるため、デプロイメント・プロセスが簡素化され、インフラストラクチャー全体の設置面積が削減されます。これにより、お客様の価値創出までの時間が短縮されるとともに、リソース要件が軽減され、データの適時性が向上し、運用コストが削減されます。

Chapter 2. システム要件

BigFix IVR Retriever サービスの前提条件とシステム要件について詳しくは、こちらをご覧ください。

ソフトウェア要件

ソフトウェア要件	
BigFix コンポーネントの要件	• BigFix WebUI IVR アプリ (v15) (最小要件)
前提条件	• MSSQL 2019 または MSSQL 2022
オペレーティング・システム	• Microsoft Windows 2016 • Microsoft Windows 2019 • Microsoft Windows 2022
サポートされる BigFix のバージョン	• Windows ベースの BigFix Server v10 以降のバージョン  **Note:** BigFix IVR Retriever サービスは現在、Windows ベース以外の BigFix Server 環境をサポートしていません。
BigFix ライセンス要件	• BigFix 修復 • BigFix Lifecycle • BigFix Compliance • BigFix Workspace/Workspace • BigFix Enterprise/Enterprise+

<table>
<tr><th colspan="2">ソフトウェア要件</th></tr>
<tr><td>サポートされている脆弱性管理プラットフォーム</td><td>

Tenable 脆弱性管理 (以前の Tenable.IO)

Note:
IVR が Tenable とのインターフェースを維持するために使用する API キーの生成を有効にするには、Tenable で「管理者」ユーザー・ロールを使用する必要があります。

BigFix コンピューター ID と関連付けられる Tenable アセットは、次のいずれかの Tenable プラグイン ID に適用できる必要があります。

55817 - HCL BigFix クライアントがインストール済み (Windows)
159575 - HCL BigFix クライアントがインストール済み (Linux)
159628 - HCL BigFix クライアントがインストール済み (macOS)
</td></tr>
<tr><td>ネットワーク要件</td><td>
BES IVR Retriever サービス:

ポート 9011 で受信 (デフォルト)
ポート 8099 で受信 (セットアップ・プロセス中)
デフォルトでは、これらのポート 9012、9013、9014、9015 に対して localhost で内部的にリッスンします
Tenable Vulnerability Management API サーバー URL への接続 (デフォルトではポート 443 経由で送信)
SQL データベースへの接続 (デフォルトではポート 1433 経由で送信)
BigFix サーバー (デフォルトではポート 52311 経由で送信)
BigFix WebUI サーバー (デフォルトではポート 443 経由で送信)

Note:
注: すべてのネットワークポートは TCP であり、デフォルトの実装とは異なる場合があります。
</td></tr>
</table>

ソフトウェア要件	
システムの制限	• 取得するための脆弱性データ・ソースは 1 つだけです

ハードウェア要件

ハードウェア要件	
CPU	最小 2 コア (推奨 4 コア)
RAM	ホスト OS の要件に加えて、以下の要件があります。 • 20K エンドポイントあたり 2GB
ディスク・スペース	デフォルト設定では、以下のサイズ設定が想定されます。 • 20K エンドポイントあたり 4GB
実行時間	データの同期と処理の全体的な実行時間は、以下のような条件に応じて異なります。 • CPU 速度 • 検出結果の数 • アセットの数 • BFE 環境内にロードされたパッチ・サイトの数 • API レイテンシー • IVR マシンで競合するワークロード

Chapter 3. IVR4 Fixlet

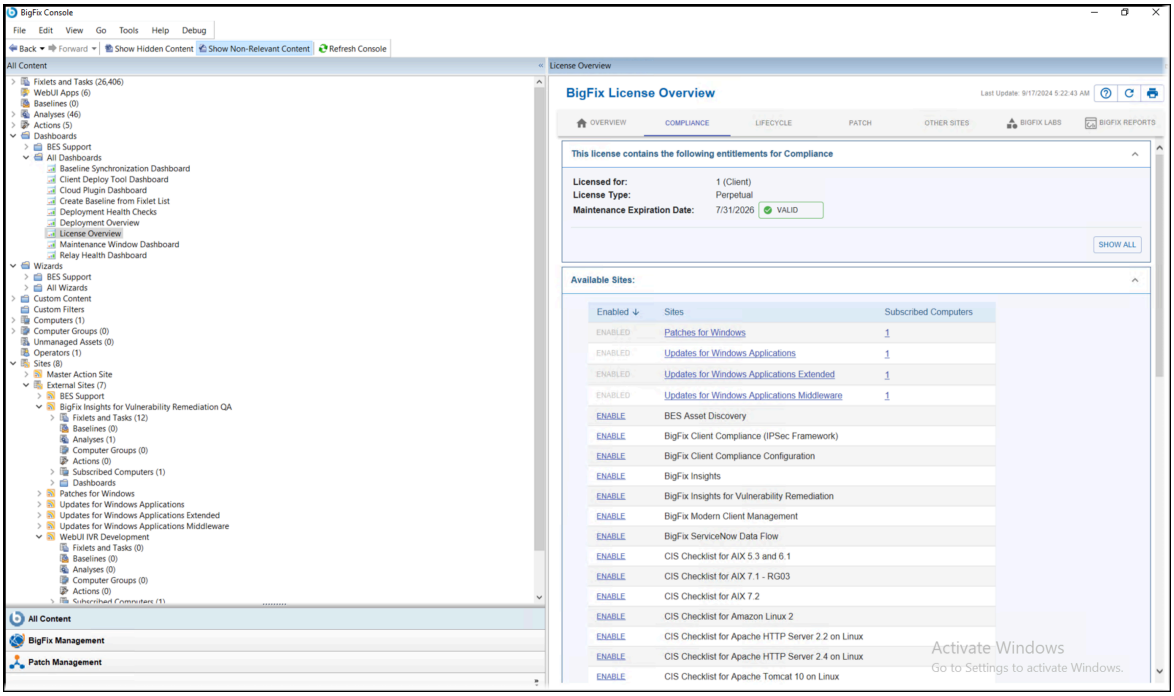
BigFix Insights for Vulnerability Remediation v.4.0.0 で使用可能な Fixlet とタスクについての詳細をご確認ください。

Fixlet を使用して IVR v.4.0.0 のセットアップを行うには、以下のステップに従います。

Note:
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。以前のバージョンのプロパティーを削除するには、BigFix Insights for Vulnerability Remediation サイトの「BigFix Insights for Vulnerability Remediation のアンインストール」タスクを参照してください。

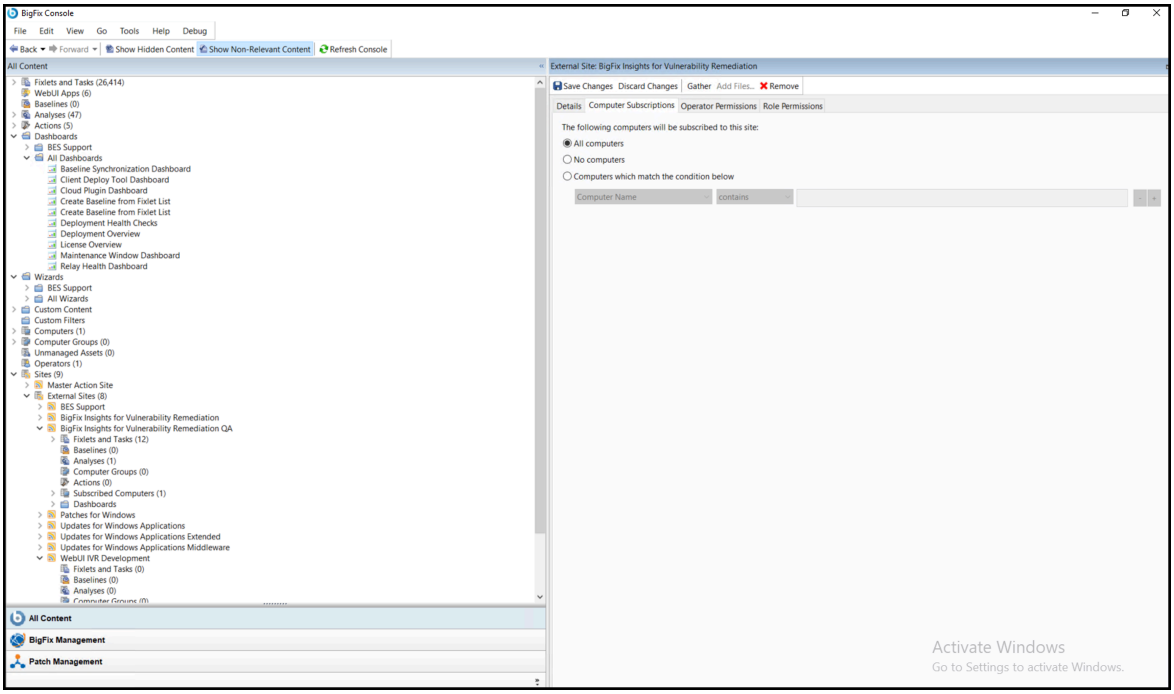
1. コンテンツ・サイトを有効にします

   「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** サイトを有効にする」をクリックして、必要なコンテンツを収集します。

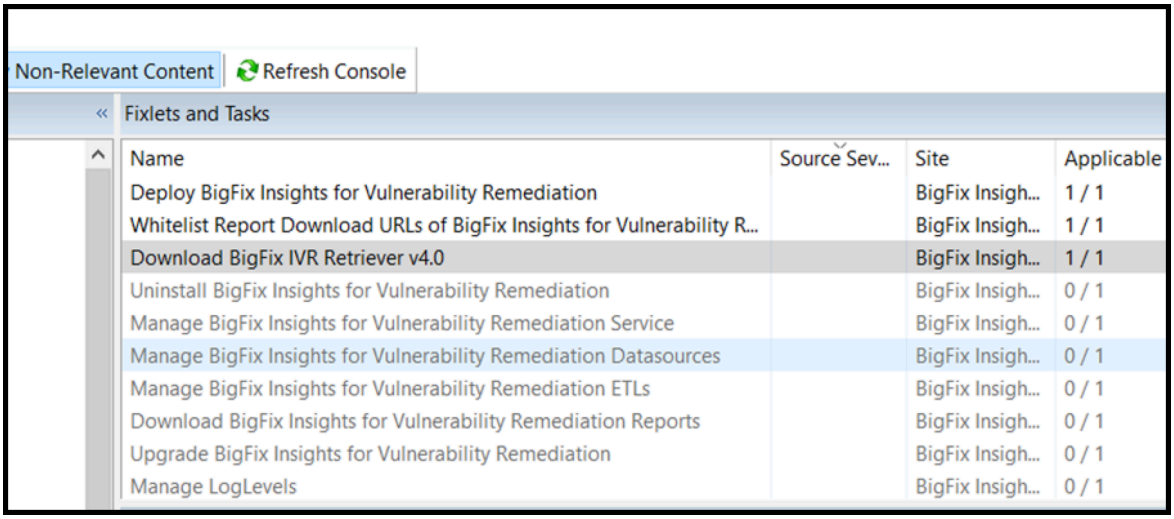


2. コンピューターをサイトにサブスクライブします。すべてのコンピューターにサブスクライブすることをお勧めします。

Note:
分析は、IVR2 のインストールでのみ有効にする必要があります。これは IVR4 インストールに属していません。



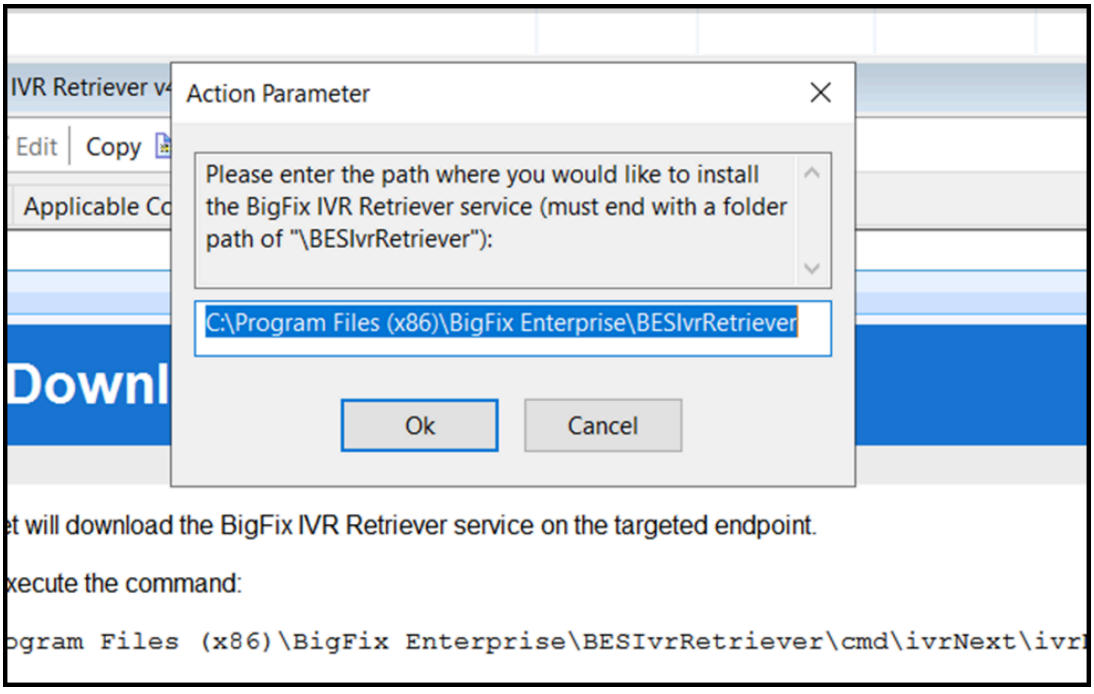
3. BESRetriever をターゲット・フォルダーにダウンロードします。



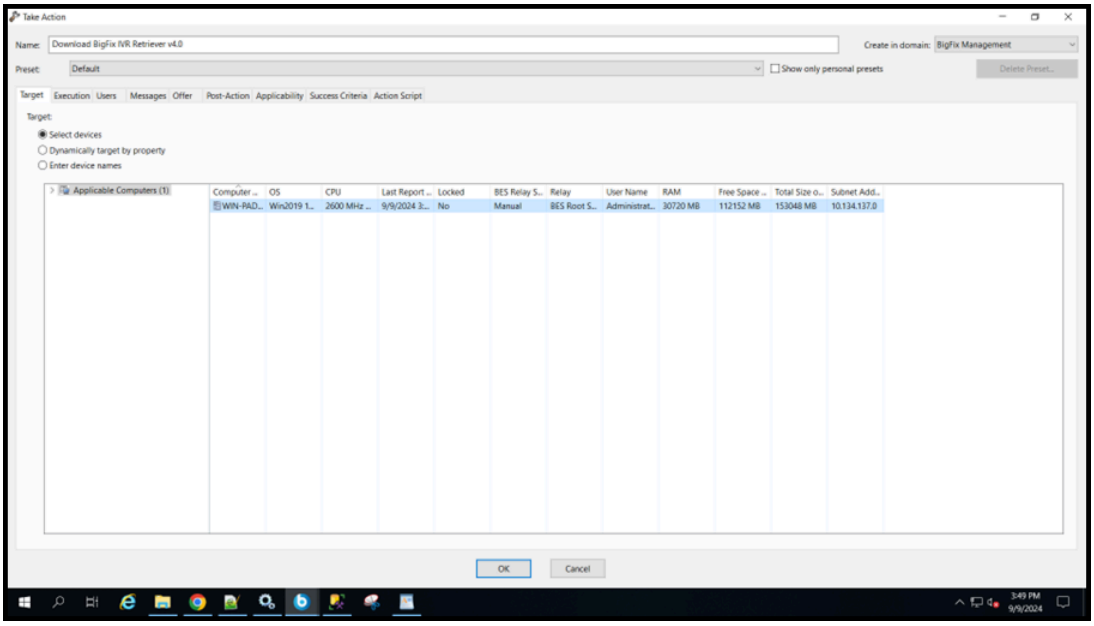
a. 「BigFix Insights for Vulnerability Remediation」外部サイトの「BigFix **IVR Retriever v4.0** のダウンロード」Fixlet をクリックします。
b. 「アクションの実行」をクリックし、必要なオプションを選択します。

Note:
デフォルトの場所は、C:\Program Files (x86)\BigFix Enterprise\BESIvrRetriever です。

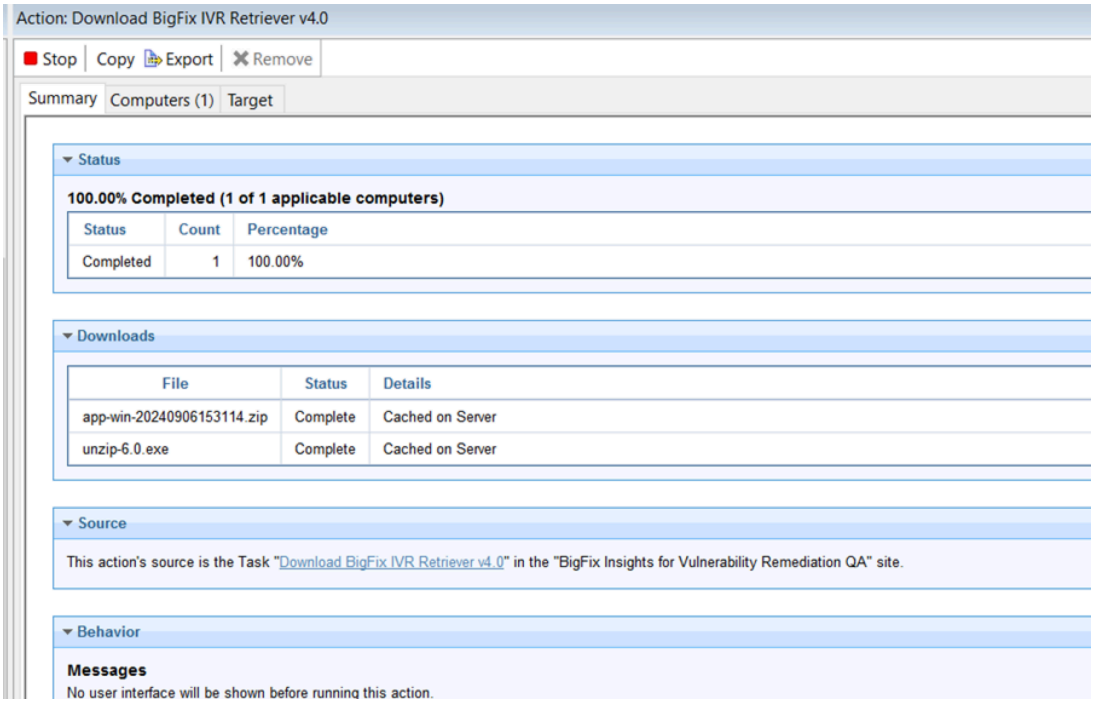
c. BigFix IVR Retriever サービスをデフォルトの場所以外のパスにダウンロードするには、2 番目のオプションを選択します。以下に示すように、ポップアップ・ウィンドウが表示され、パスを入力できます。



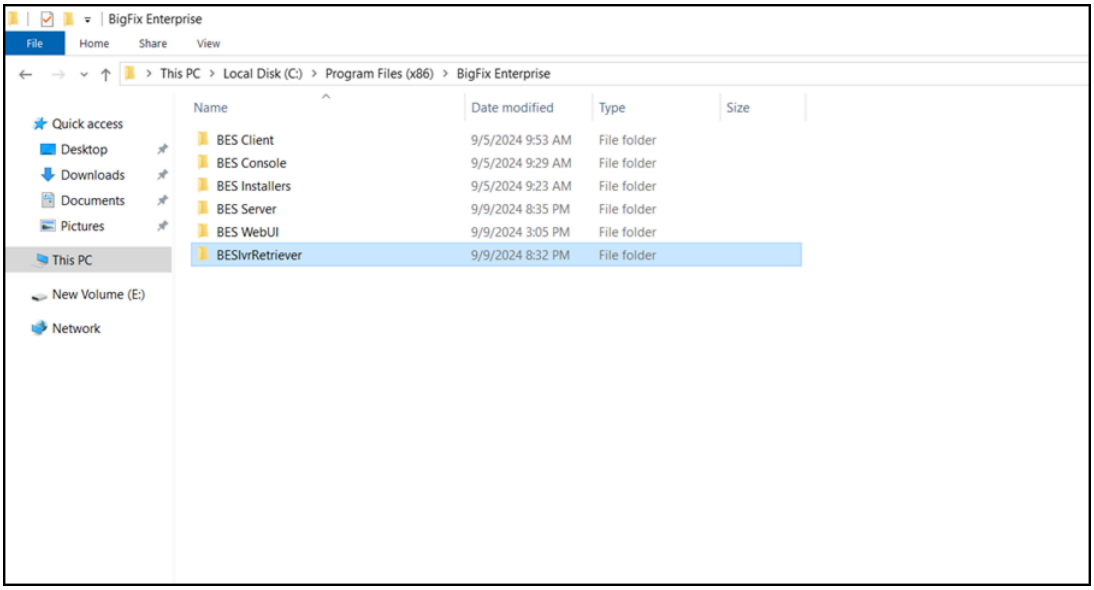
d. 「ターゲット」タブでターゲット・デバイスを選択し、「OK」をクリックします。



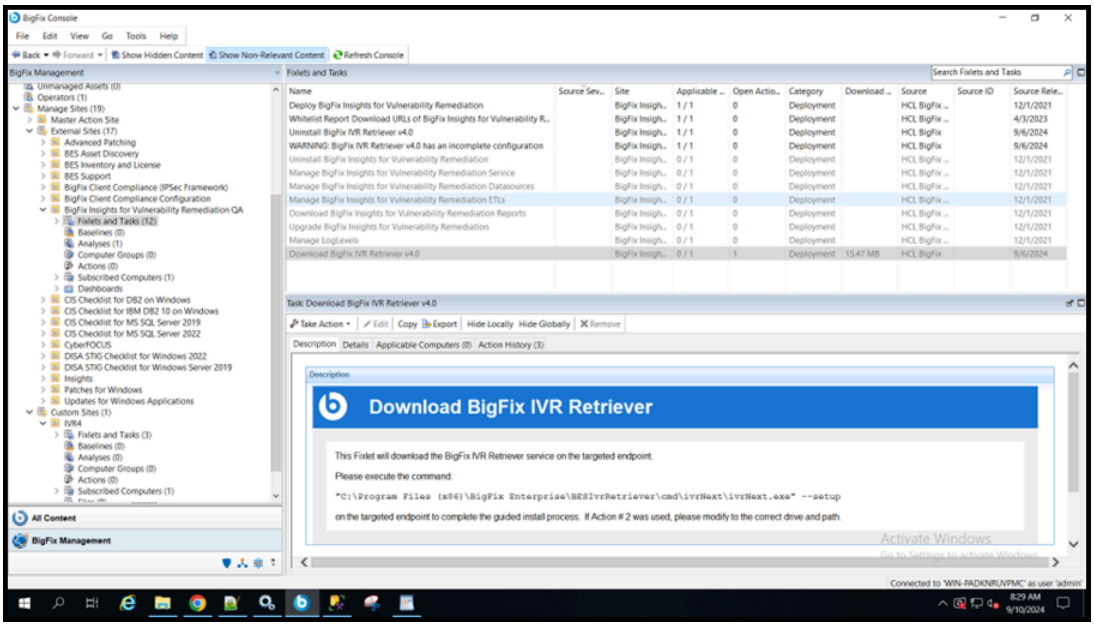
e. Fixlet の完了を待ちます。



f. 選択したオプションに従って、パスに移動し、「BigFix IVR Retriever v4.0 をダウンロード」Fixlet の完了ステータスで作成されている (アクションが実行されたマシンの) BESIvrRetriever フォルダーを確認します。

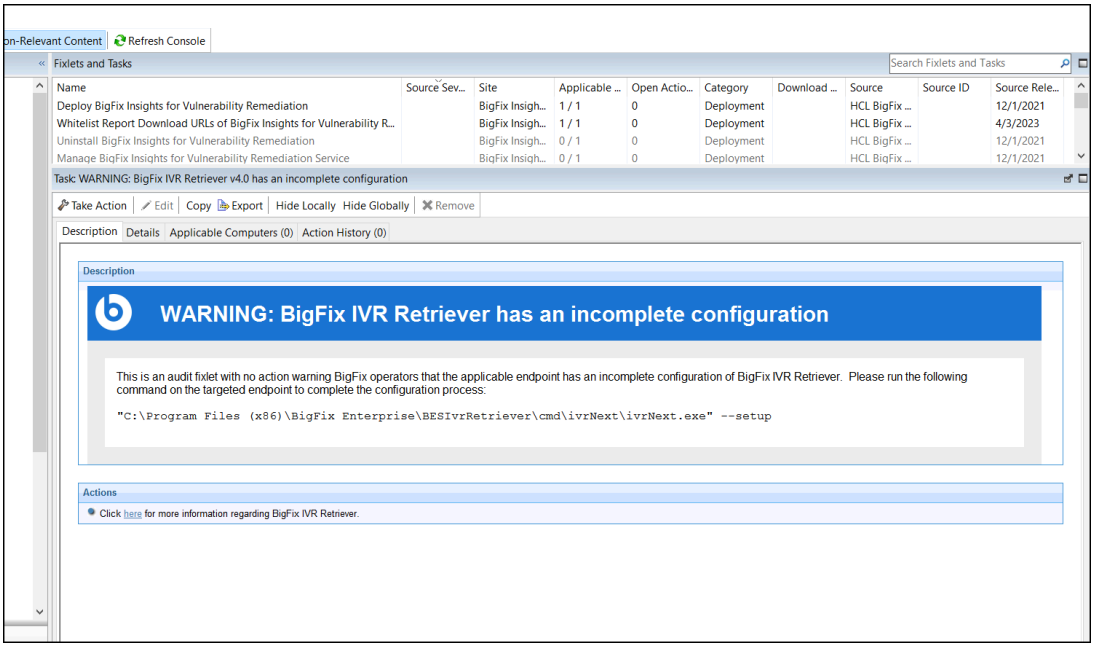


g. BigFix IVR Retriever v4.0 Fixlet のダウンロードが完了したら、「BigFix **IVR Retriever v4.0** のアンインストール」および「警告: **BigFix IVR Retriever v4.0** の構成が未完了です」Fixlet がアクティブになります。



h. 「警告: **BigFix IVR Retriever v4.0** の構成が未完了です」Fixlet に移動して、「アクションの実行」をクリックします。

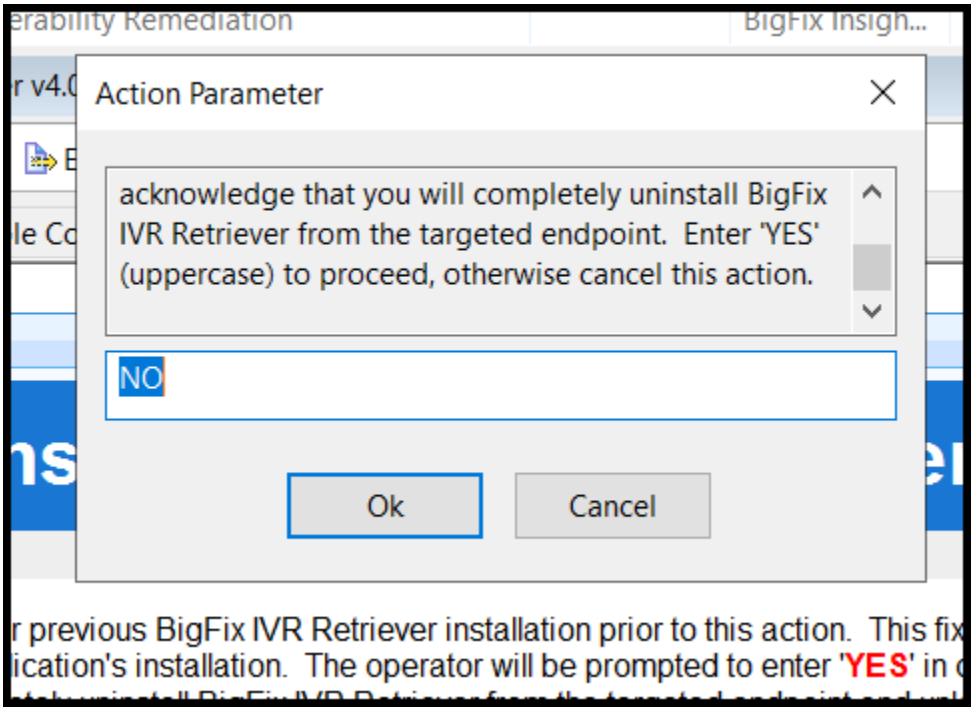
Fixlet を使用して、詳細情報を提供するガイド資料を表示できます。



i. **Note:**

「BigFix **IVR Retriever v4.0** のアンインストール」Fixlet を使用して、完全な IVRv4 セットアップをアンインストールできます。

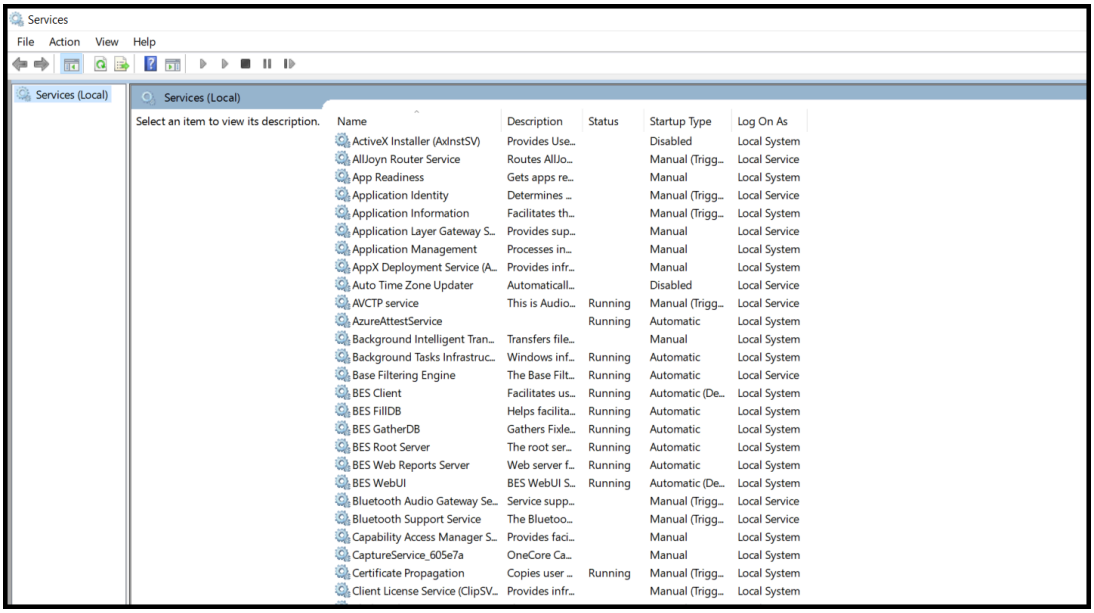
「BigFix **IVR Retriever v4.0** のアンインストール」に移動し、「アクションを実行」をクリックすると、以下のようなポップアップ・ウィンドウが表示されます。



「**YES**」と入力して、「OK」をクリックします。実行が完了ステータスになるまで待ちます。

j. `BESIvrRetriever` 「BigFix IVR Retriever v4.0 をダウンロード」Fixlet 時に指定されたパスからフォルダーを削除する必要があります。

k. Service BES IVR Retriever を Services App から削除する必要があります。



Note:

警告:「BigFix **IVR Retriever v4.0** の構成が未完了です」Fixlet を使用して、詳細情報を提供するガイド資料を表示できます。

Chapter 4. IVR4 セットアップ・プロセス

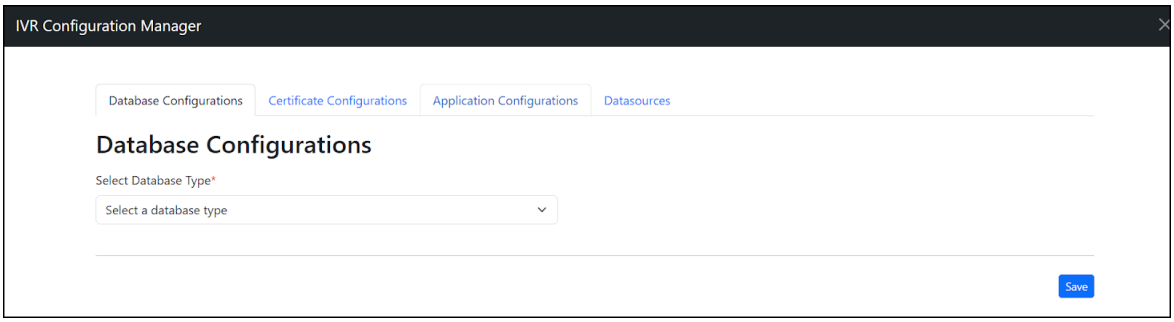
このセクションでは、IVR4 のセットアップについて説明します。

1. .exe ファイルが `C:\Program Files (x86)\BigFix Enterprise\BESIvrRetriever` の場所にダウンロードされたら、管理者としてコマンド・プロンプトを開き、実行可能ファイルがあるフォルダーに移動します。以下のように setup コマンドを実行します。

   ```
   ivrNext.exe --setup
   ```

   setup コマンドが実行されると、IVR 構成マネージャーのページにアクセスできるようになります。

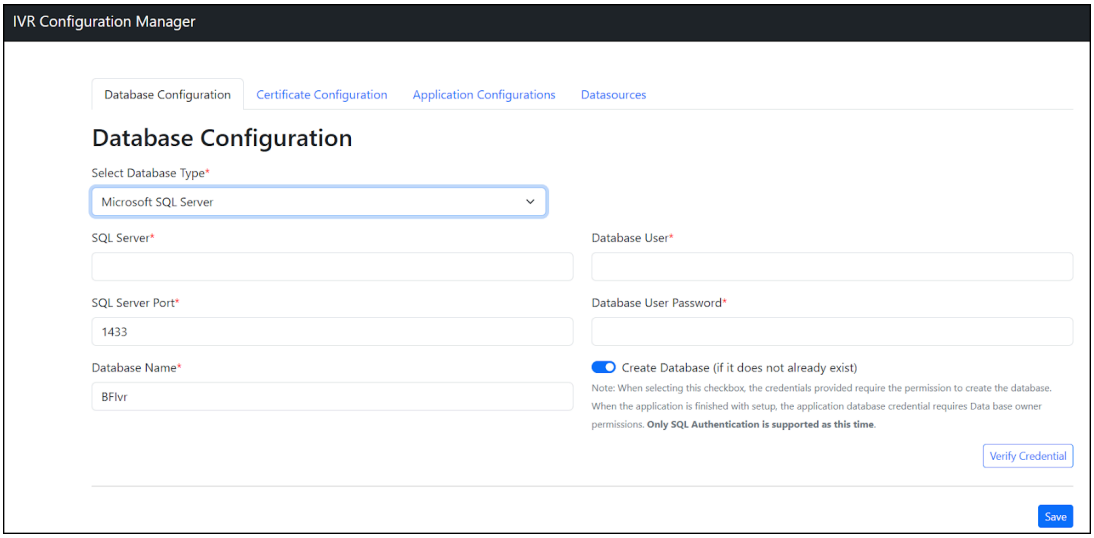
2. 「データベースの構成」タブ



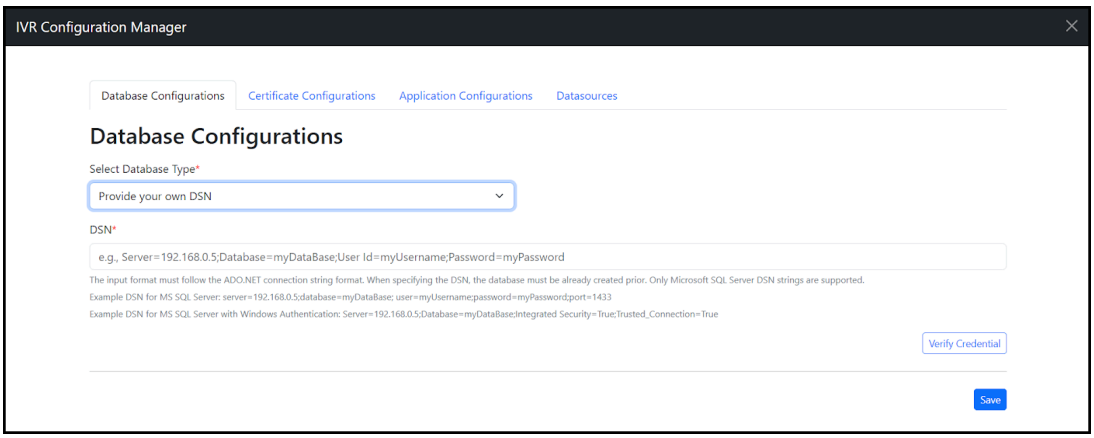
   - データベースの選択: データベースのタイプを選択するように求められます。以下のいずれかを実行できます。
     - Microsoft MS SQL Server を選択するか、
     - データ・ソース名が既に構成されている場合は、「自分の DSN を指定する」を選択します。
   - MS SQL Server を選択しながら、MS SQL Server の資格情報を使用して以下のフィールドを更新します。

     セットアップ時に指定したデータベース・ユーザーがサーバーに新しいデータベースを作成するのに必要な権限を持っていることを確認します。

     セットアップ・プロセス中に新しいスキーマを作成するか、既存のスキーマを使用するかを選択できます。既存のスキーマがある場合は、そのスキーマを OnPrem データベースのセットアップに使用できます。スキーマが正しく設定されており、お使いのシステム要件に適合していることを確認します。



- IVR4 のセットアップ中に「自分の **DSN** を指定する」を選択する場合、DSN (データ・ソース名) 文字列を指定して、アプリケーションがデータベース・サーバーに接続できるようにする必要があります。以下のスクリーンショットにサンプル DSN 形式を示します。



MS SQL Server の DSN の例:

```
server=192.168.0.5;database=myDataBase;
user=myUsername;password=myPassword;port=1433
```

Windows 認証 (統合認証) を使用した MS SQL Server の DSN の例:

```
Server=192.168.0.5;Database=myDataBase;Integrated
Security=True;Trusted_Connection=True
```

- 使用する Windows ユーザー・アカウントには、SQL Server で十分な権限を持っている必要があります。具体的には、次のような権限が必要です。

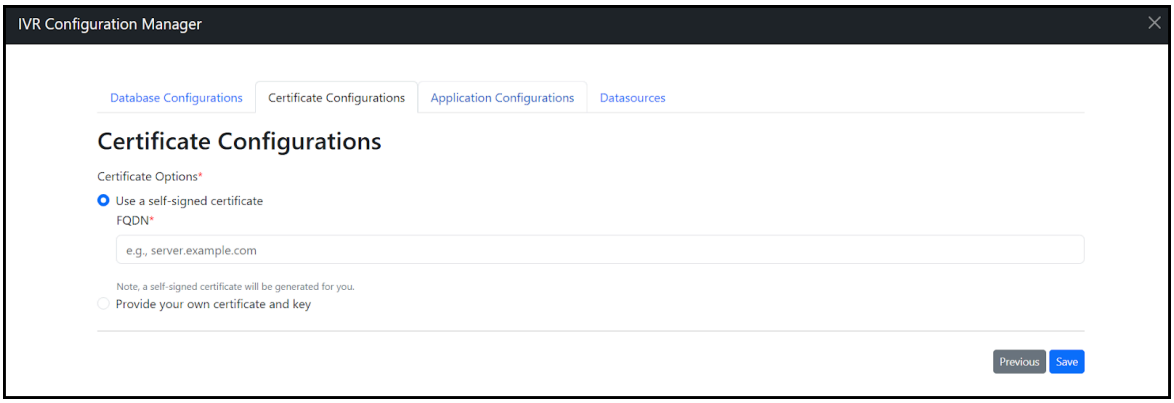
- ユーザーには、必要なデータベース作成権限が必要です。
- データベースの読み取り/書き込みおよび管理が可能である必要があります。

データベースの詳細を入力したら、資格情報を検証します。

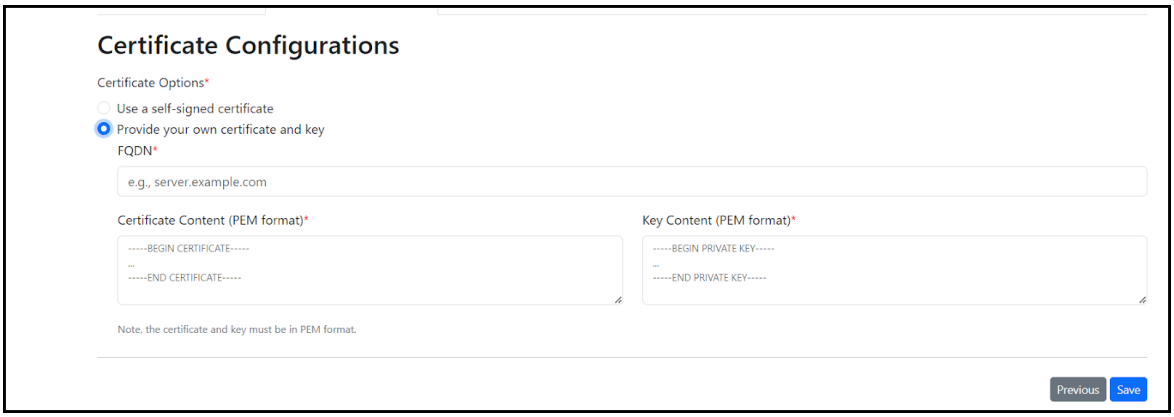
資格情報を確認したら、「保存」をクリックしてデータベース構成を保存します。

3. 「証明書の構成」タブ

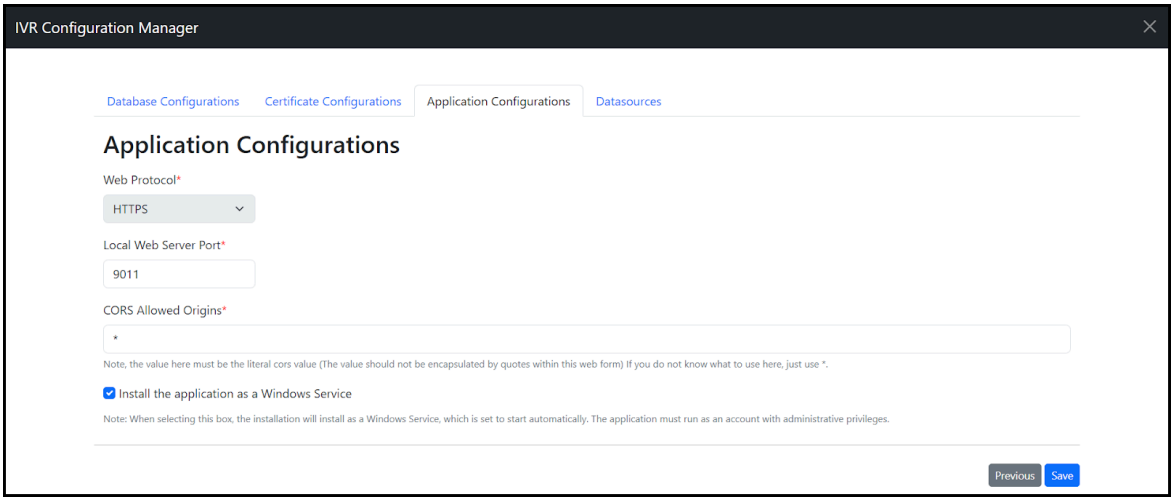
次のスクリーンショットは、自己署名証明書の使用に関するものです。



次のスクリーンショットは、2 番目のオプションを示しています。独自の証明書とキーを入力します。ここで、証明書と主要な内容は PEM 形式で指定する必要があります。



4. 「アプリケーション構成」タブ



このタブで、exe ファイルを実行する必要のあるポートを指定します。また、このタブには、アプリケーションを Windows サービスとしてインストールするオプションがあります。

アプリケーションを実行するポート番号を入力します。このポートは、IVR4 サービスが着信要求をリッスンするために使用されます。選択したポート番号がまだ別のサービスで使用されていないこと、およびファイアウォールで開いていることを確認します。デフォルト・ポートは 9011 です。このポートを使用する場合は、別の使用可能なポートを指定する必要があります。

アプリケーションを Windows サービスとしてインストールするオプションもあります。セットアップが完了すると、アプリケーションはバックグラウンドでサービスとして実行します。

インストール後、Windows の検索バーにサービスを入力するか、「ファイル名を指定して実行」ダイアログ (Win + R) で services.msc を実行して、Services.msc を開きます。「サービス」ウィンドウに、BES IVR Retriever サービスがリストされているはずです。必要に応じて、このページでサービスを開始、停止、または構成できます。

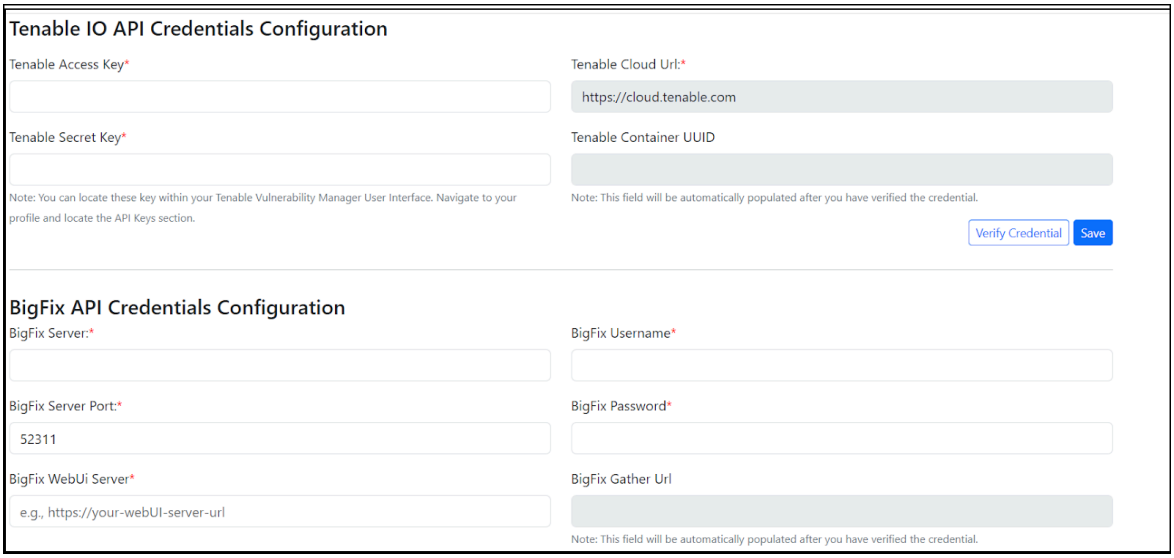
5. 「データ・ソース」タブ

Tenable API Credentials Configuration と BigFix API Credentials Configuration を入力できます。

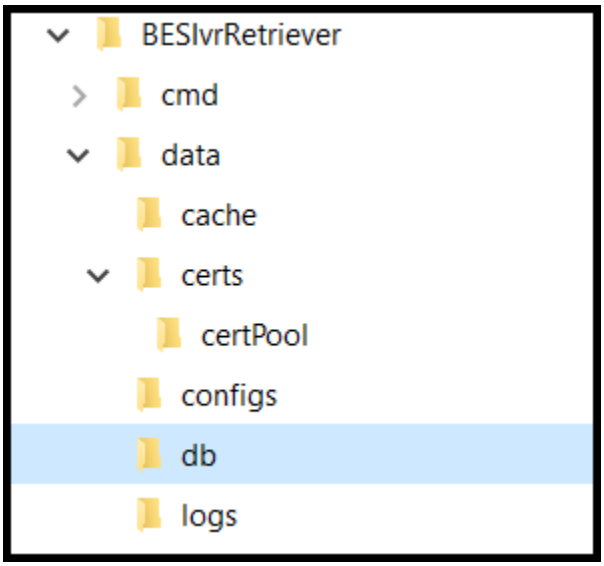
資格情報を確認し、「保存」をクリックします。

> **Note:**
> IVR が Tenable とのインターフェースを維持するために使用する API キーの生成を有効にするには、Tenable で管理者ユーザー・ロールを使用する必要があります。また、BigFix API 資格情報にはマスター・オペレーター権限が必要である点に注意してください。

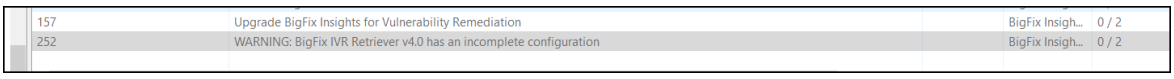
Note:
非マスターは、IVR 設定マネージャーの「データ・ソース」タブで Bes リソースを作成できません



セットアップが完了すると、証明書、構成、および lockbox db が作成されます。



セットアップ構成が未完了のままの場合、BigFix Insights for Vulnerability Remediation からの Fixlet「警告: **BigFix IVR Retriever** の構成が未完了です」は、マシンに関連します。



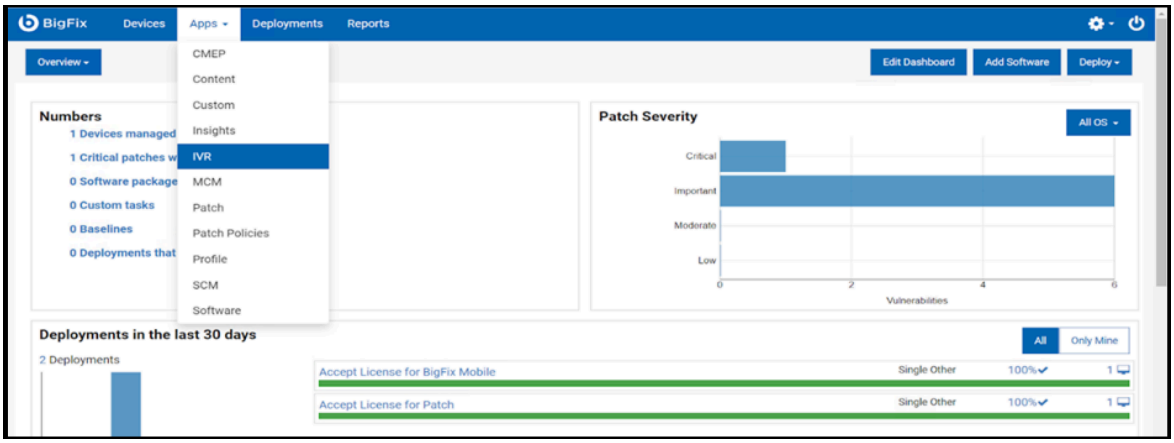
Chapter 5. IVR v.4.0.0 アプリのセットアップ

このセクションでは、IVR アプリケーションのセットアップ、メインの脆弱性リスト・ページからの修復、「脆弱性」ページからの修復、および脆弱性リストのエクスポートについて説明します。

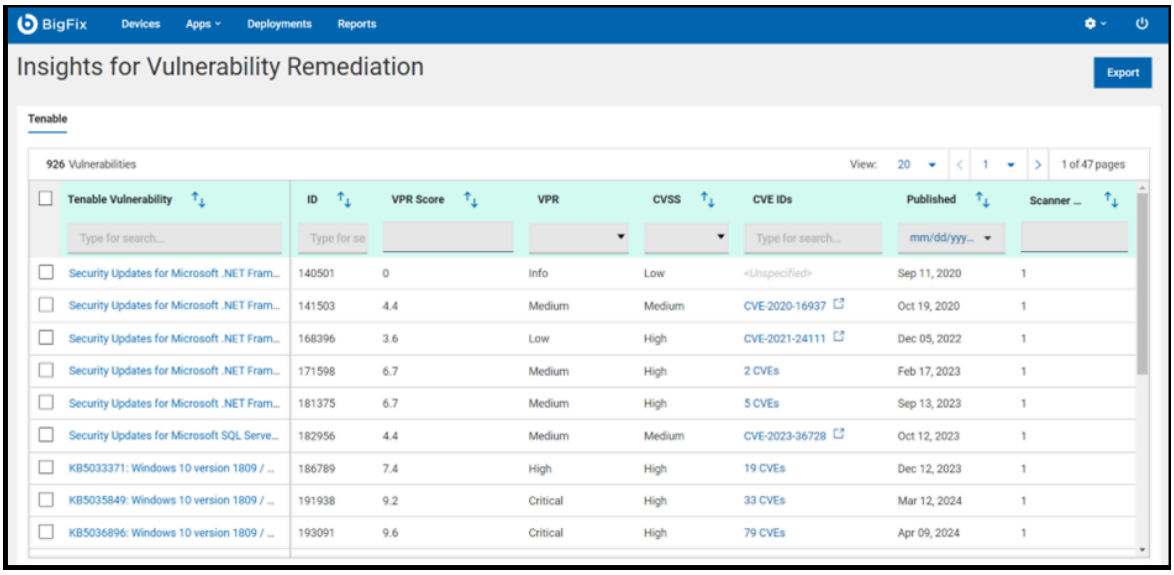
IVR v.4.0.0 アプリのセットアップ

IVR v.4.0.0 アプリをセットアップするには、以下のステップを実行します。

1. IVR を最新の WebUI バージョンにアップグレードします。
2. `ivrNext.exe` のオンプレミス・セットアップと起動が成功したら、自動化プロセスが完了するのを待ちます。プロセスは、「オートメーションが完了しました」というログ・エントリーで確認されます。
3. 有効な資格情報を使用して WebUI アプリにログインします。
4. デフォルト・ページに移動したら、ナビゲーション・バーの「アプリケーション」ドロップダウン・メニューから IVR アプリを選択して IVR アプリに移動します。

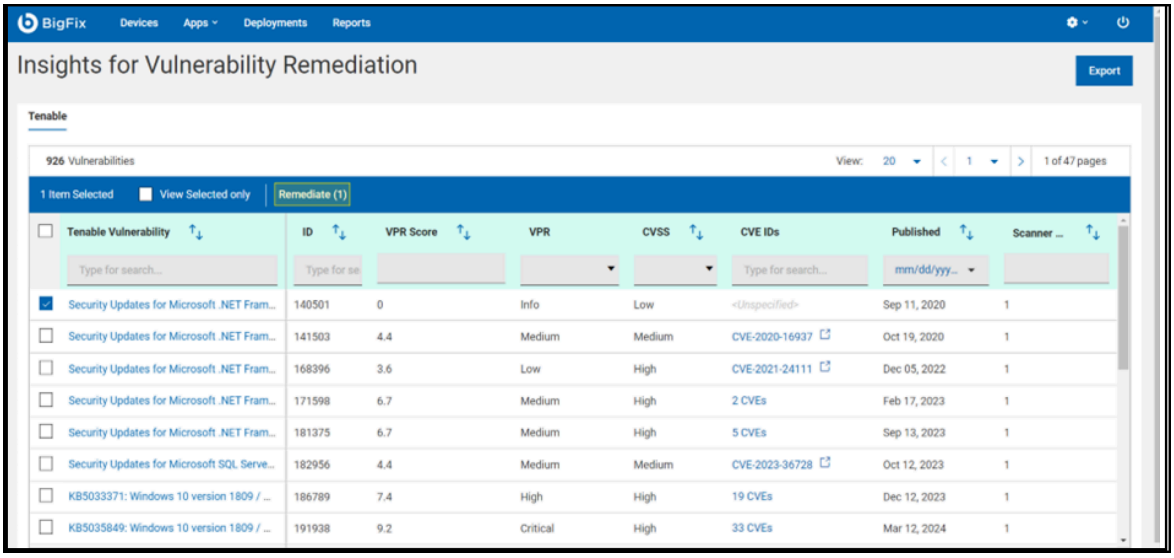


5. 自動化プロセスが正常に完了すると、下のスナップショットに示すように、データがグリッドに表示されます。

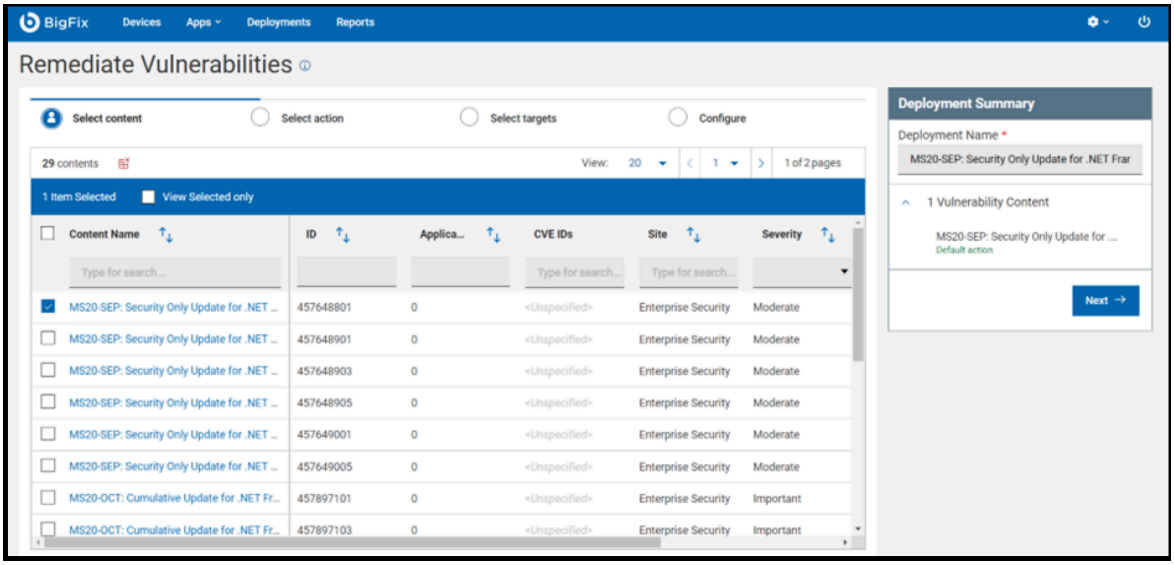


メインの脆弱性リスト・ページからの修復

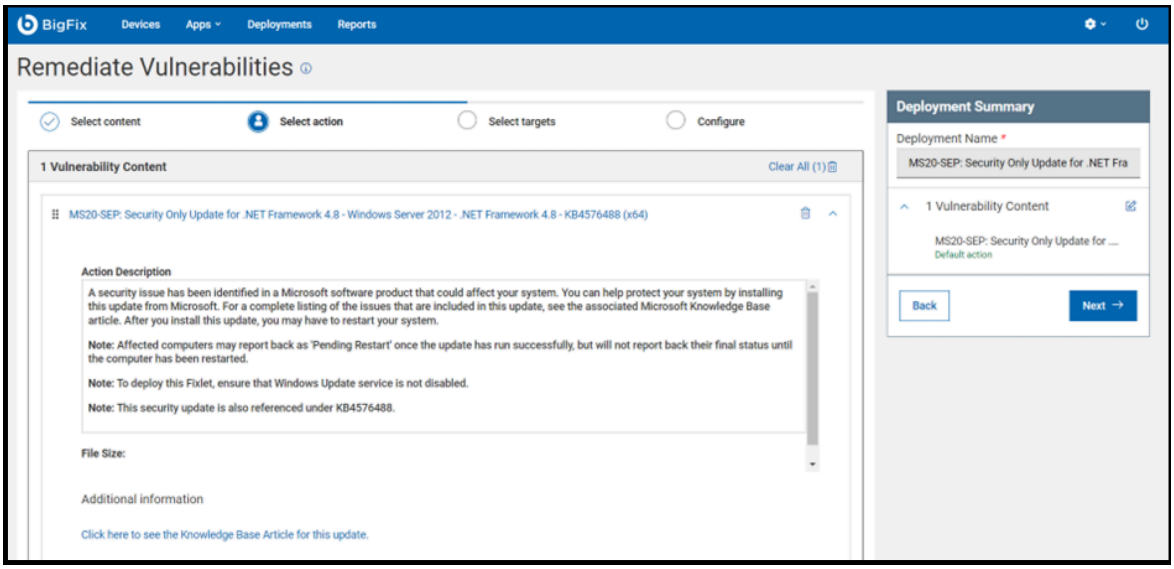
1. 修復する脆弱性を選択できるようになりました。脆弱性チェックボックスを選択すると、下の画像に示すように「修復」オプションが有効になります。



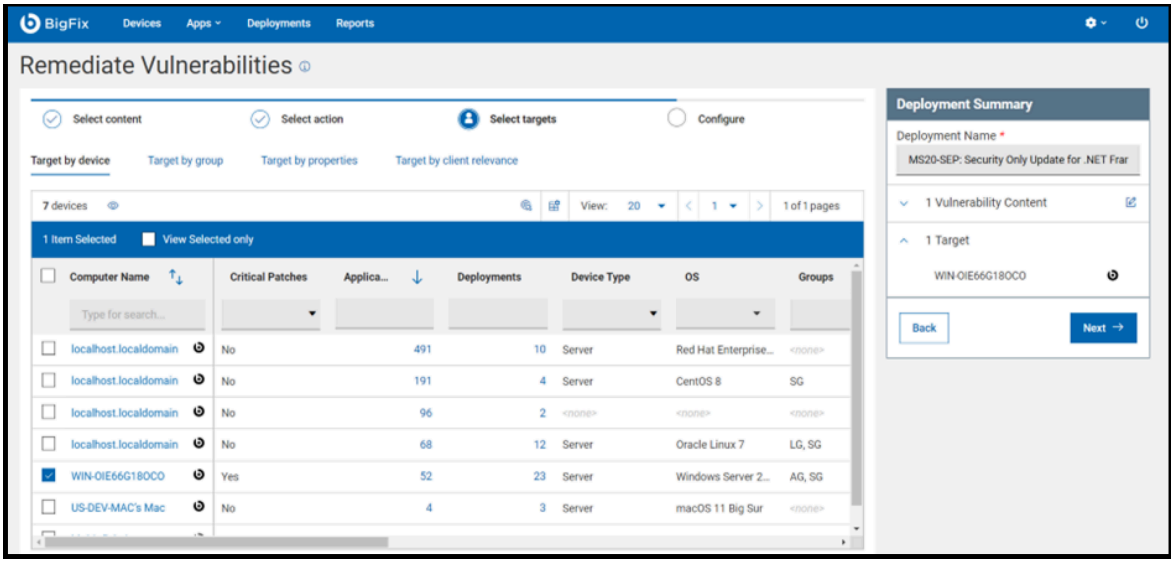
2. 「修復」をクリックして、「脆弱性の修復」ページにリダイレクトし、コンテンツを選択します。
3. 以下に示すページで、コンテンツを選択し、「次へ」をクリックできます。



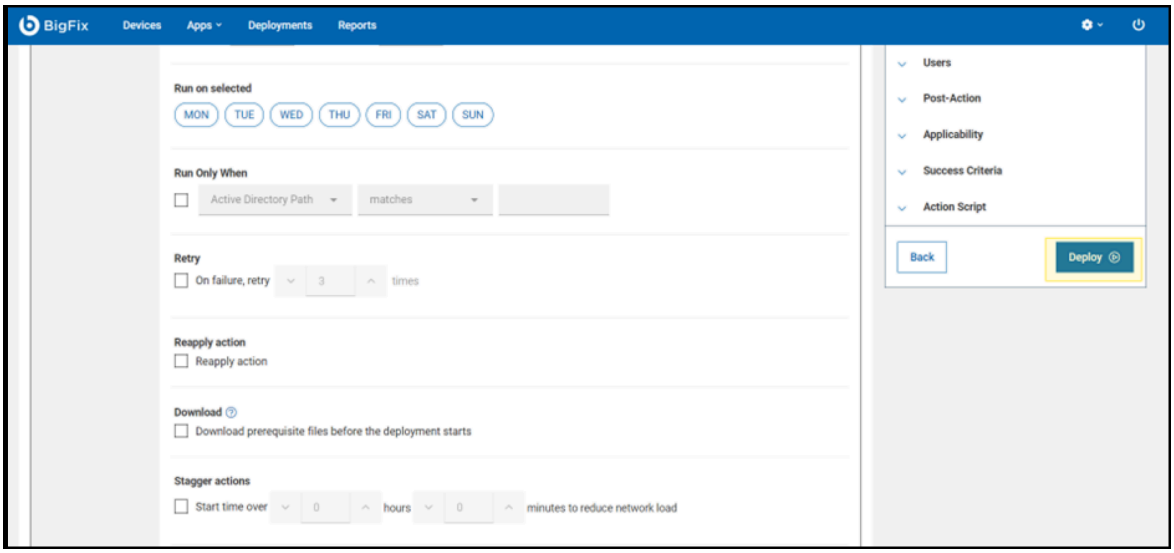
4. 適切なアクションを選択し、「次へ」をクリックして続行します。



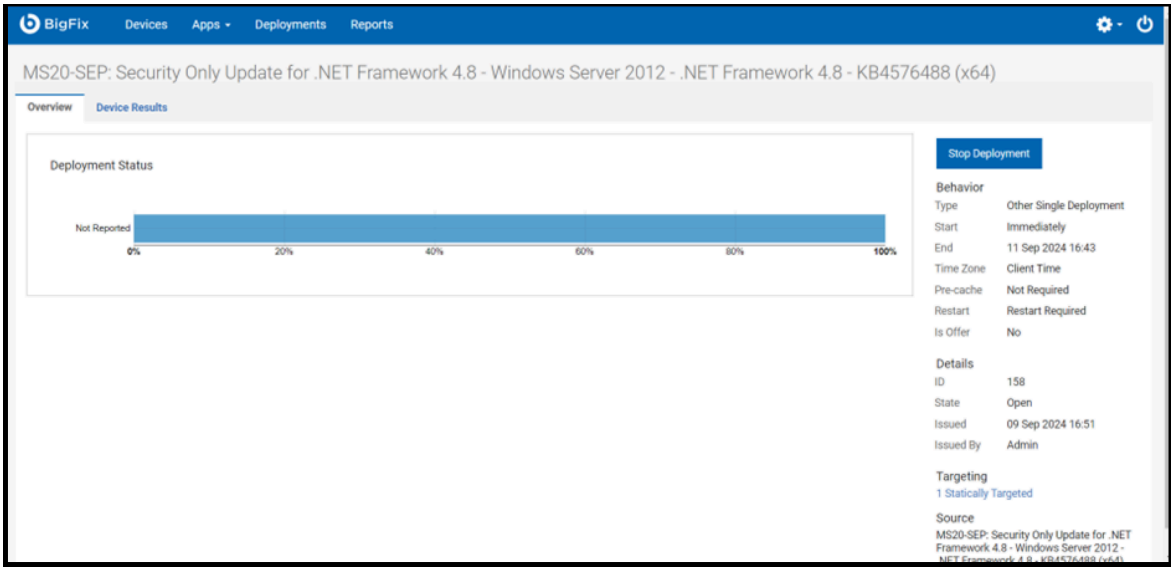
5. 脆弱性を修復するターゲット・マシンを選択し、「次へ」をクリックして続行します。



6. デプロイメント・スケジュールを構成し、「デプロイ」ボタンをクリックしてプロセスを開始する前に、優先オプションを選択します。

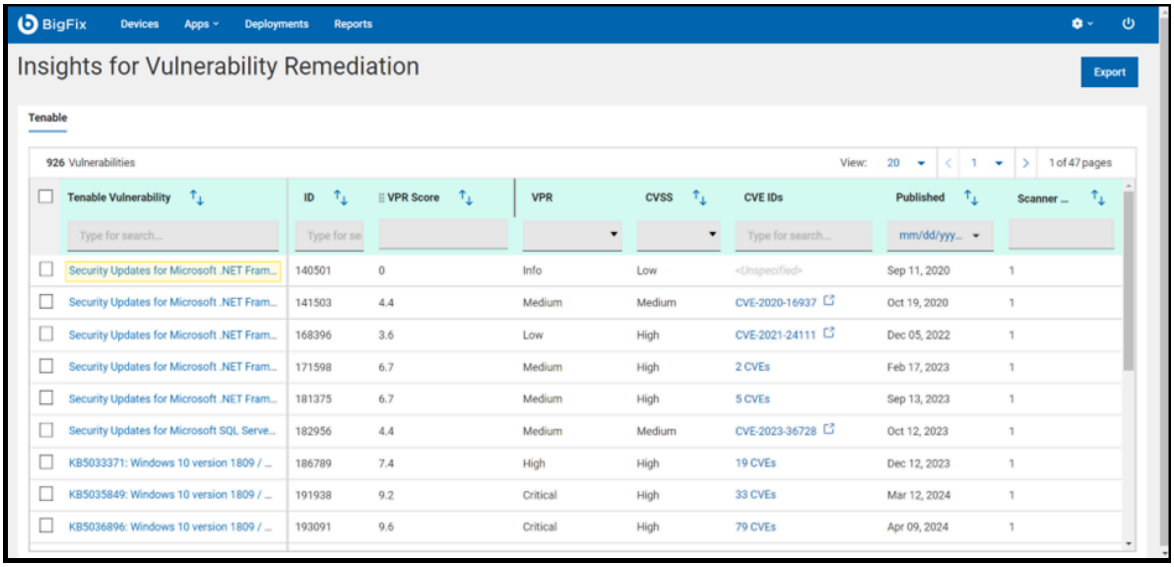


7. 最後の画面では、デプロイメント・プロセスを監視できます。

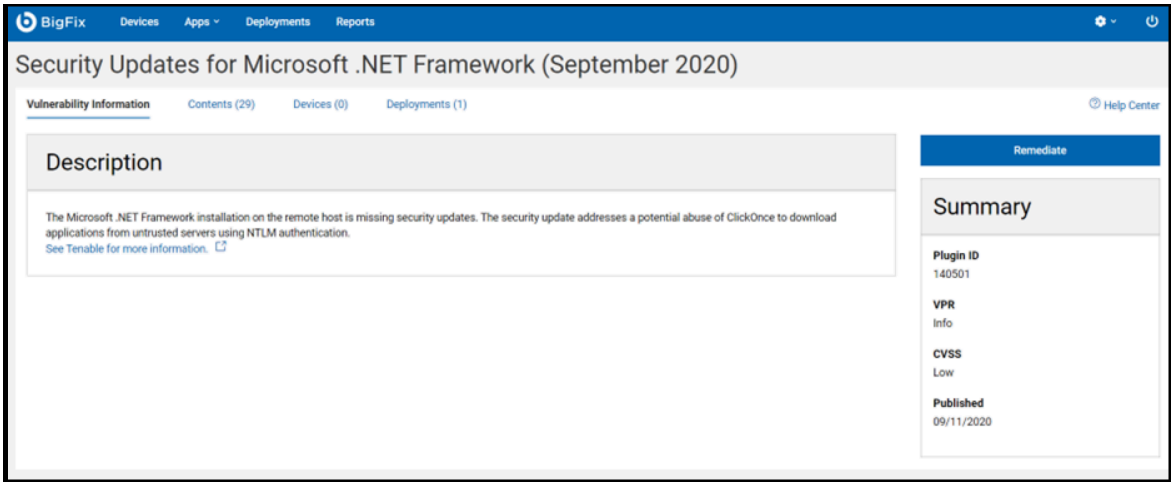


「脆弱性」ページからの修復

1. 脆弱性リスト・ページで脆弱性をクリックします。

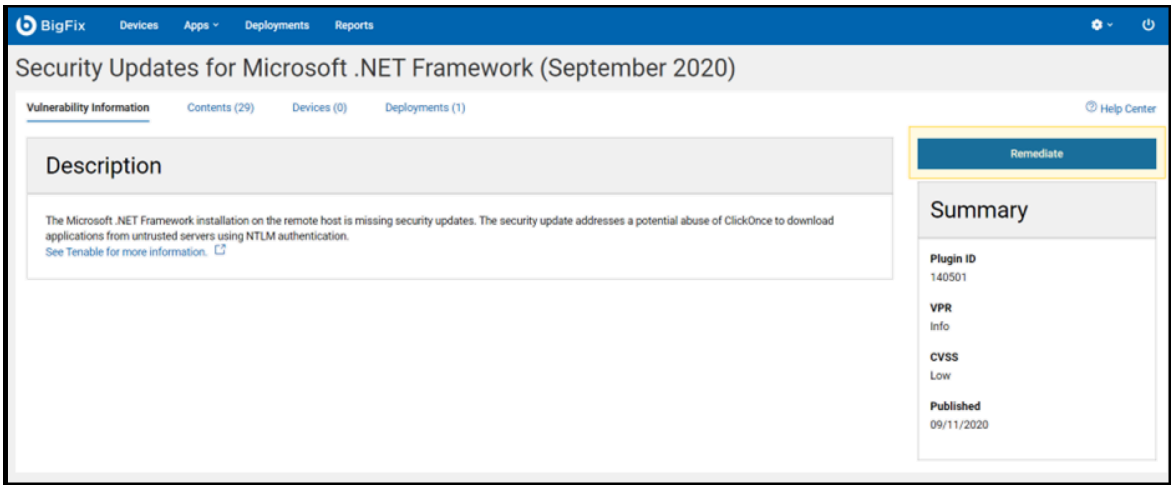


2. 以下のスナップショットに示されている脆弱性情報ページにリダイレクトされます。

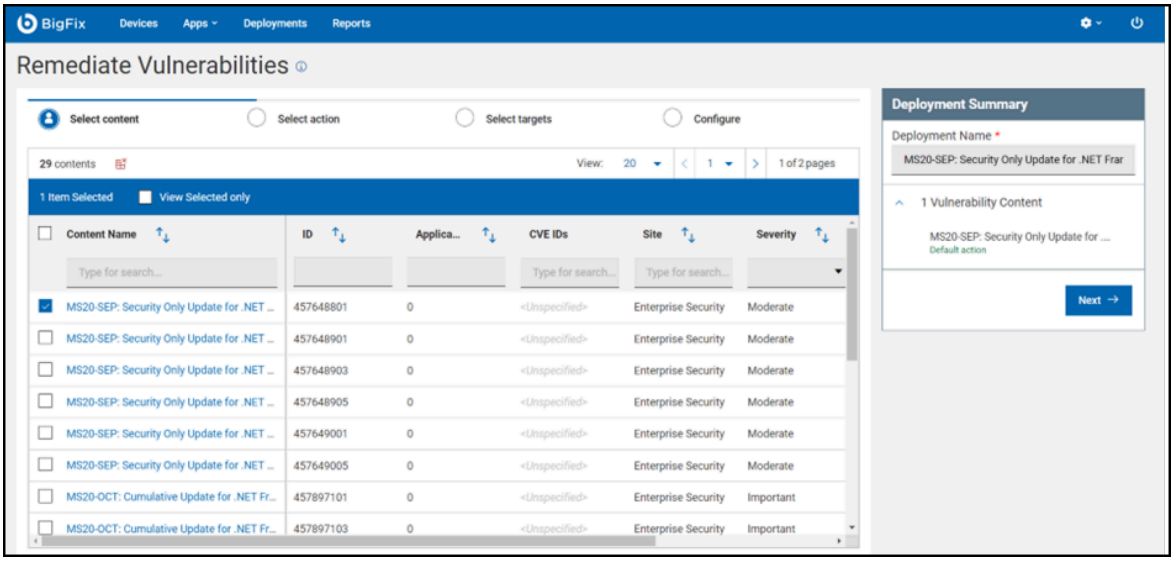


このページで、選択した脆弱性のコンテンツ、デバイス、およびデプロイメントを表示できます。

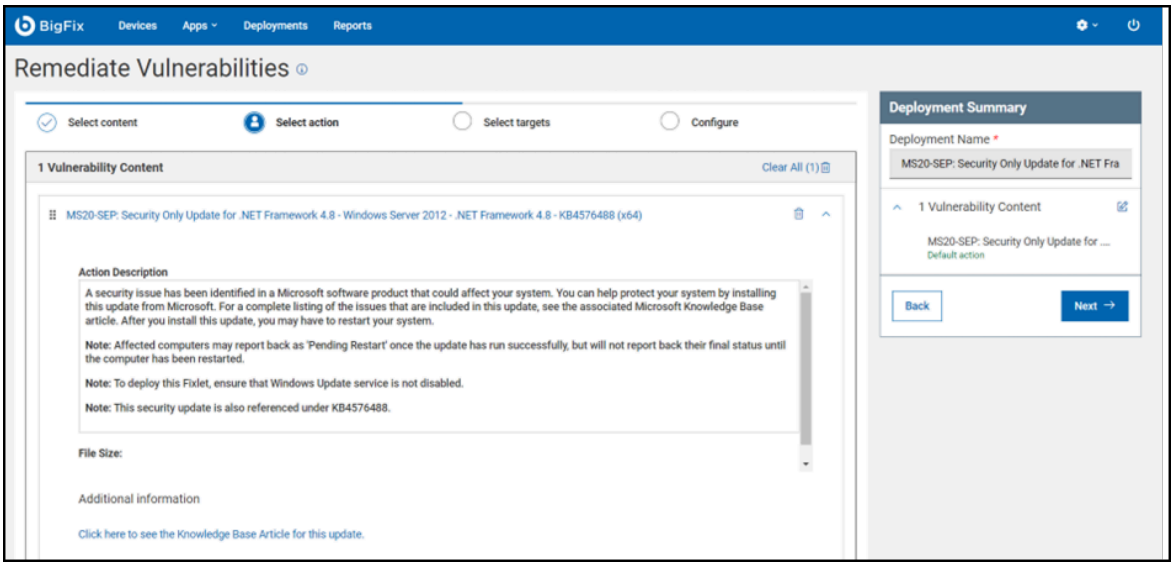
3. 下のスナップショットに示すように、「修復」ボタンをクリックします。



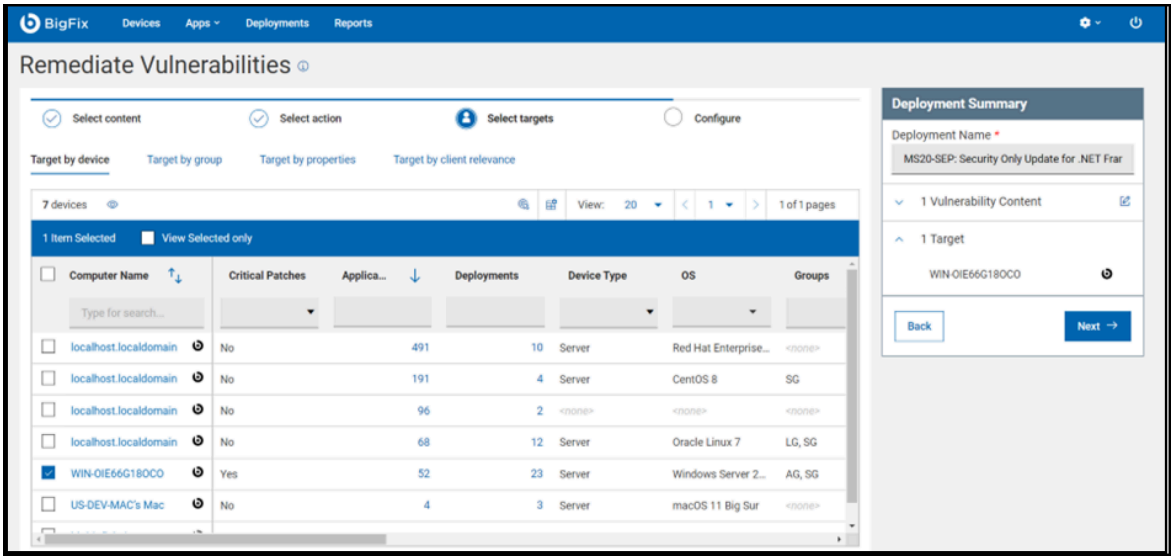
4. 「脆弱性の修復」ページにリダイレクトされ、コンテンツを選択します。コンテンツを選択して、「次へ」をクリックします。



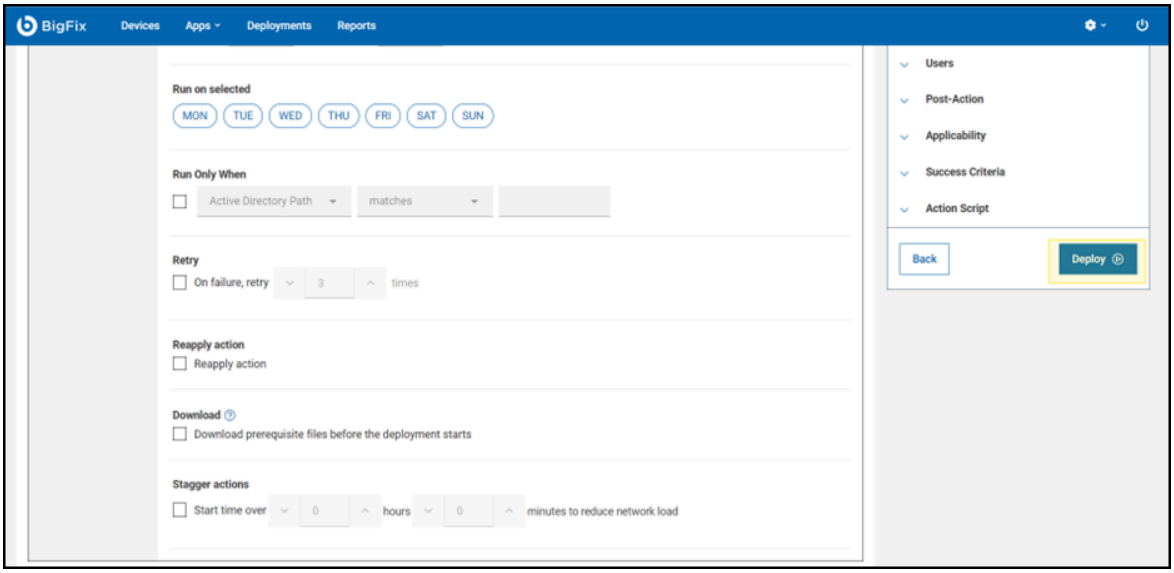
5. 適切なアクションを選択し、「次へ」をクリックして続行します。



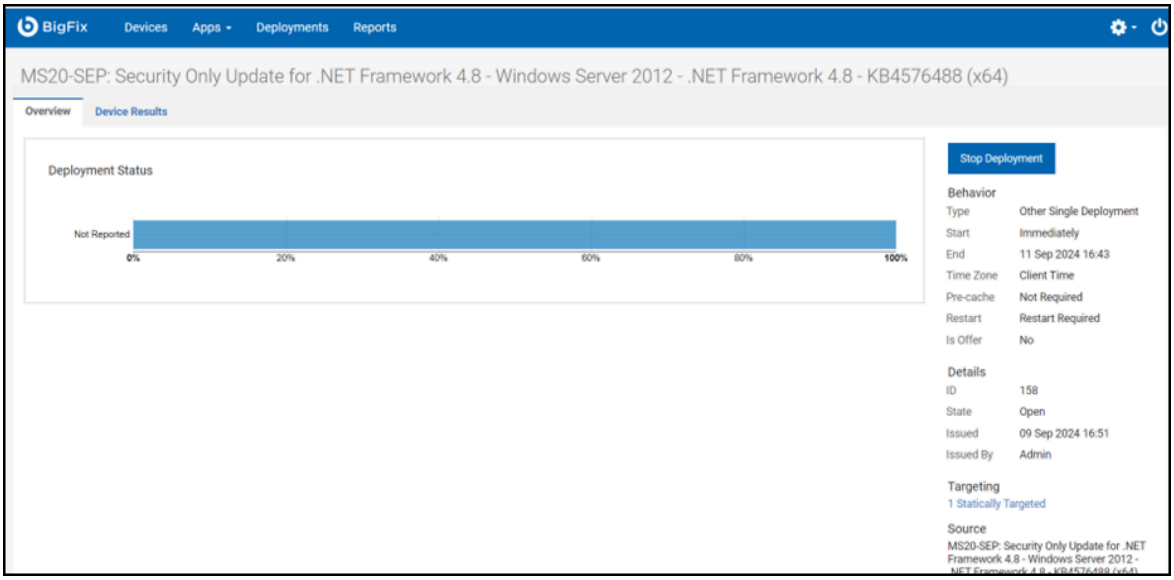
6. 脆弱性を修復するターゲット・マシンを選択し、「次へ」をクリックして続行します。



7. デプロイメント・スケジュールを構成し、「デプロイ」ボタンをクリックしてプロセスを開始する前に、優先オプションを選択します。

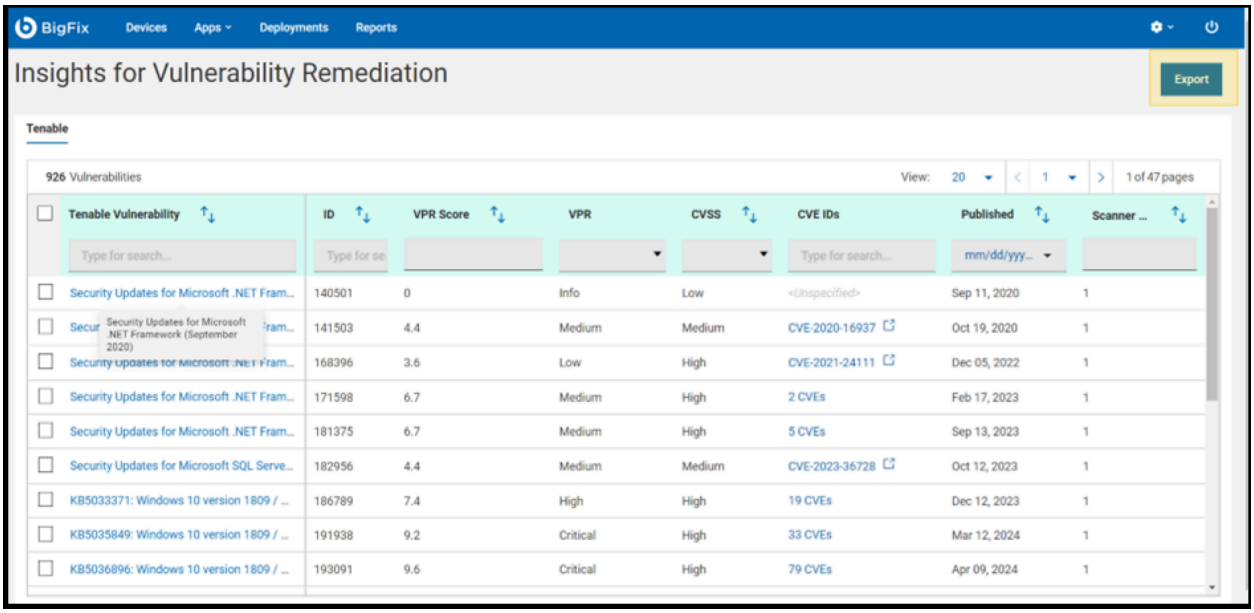


8. 最後の画面では、デプロイメント・プロセスの概要が表示されます。

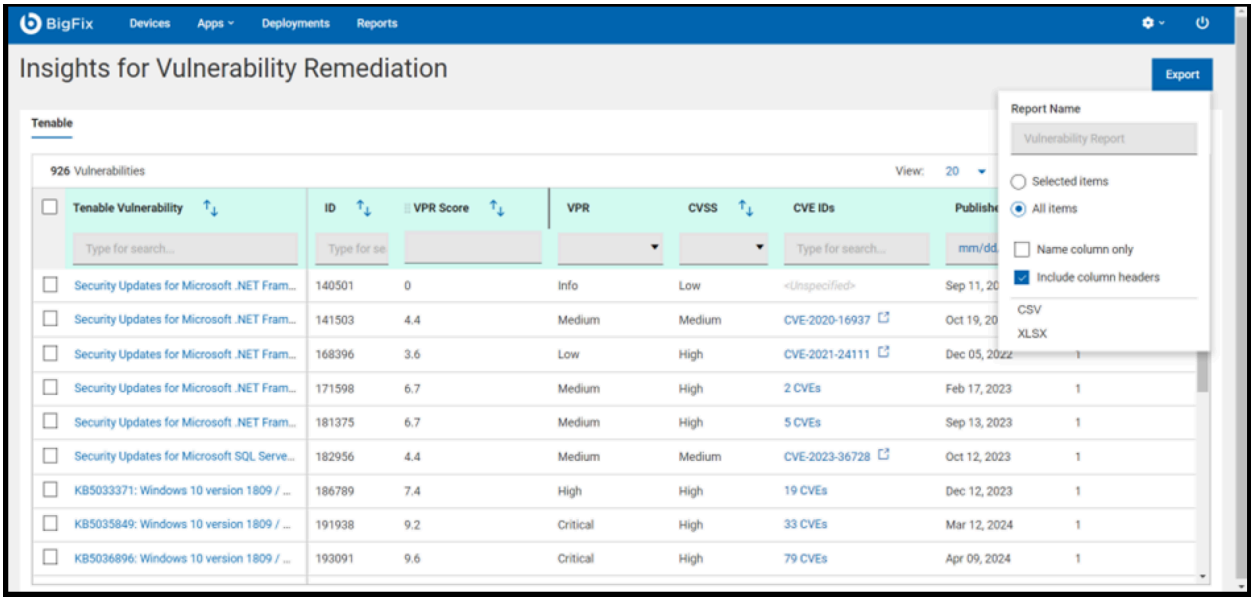


脆弱性リストのエクスポート

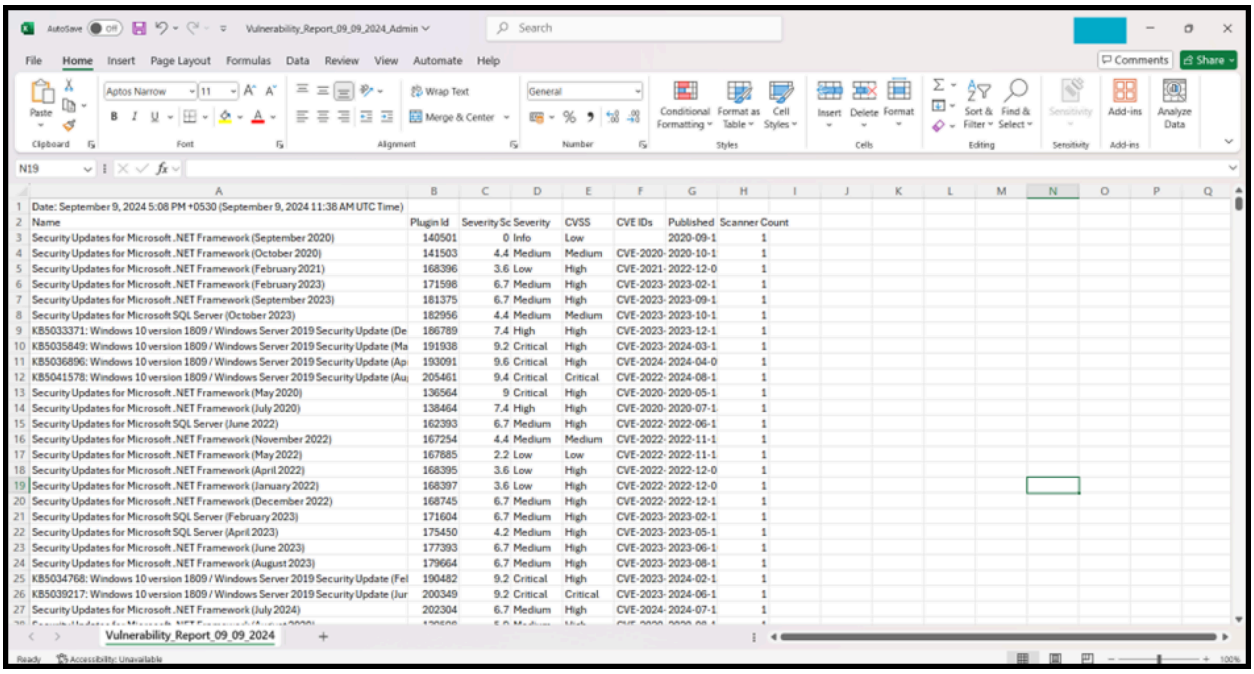
脆弱性リストをエクスポートするには、脆弱性情報ページの「エクスポート」ボタンをクリックします。



「エクスポート」ドロップダウンで、入力領域に名前を入力し、目的のオプションを選択してから、ファイル形式を選択します。ファイルが選択された形式でエクスポートされます。



以下に、エクスポートされた CSV ファイルの例を示します。



Chapter 6. IVR オンプレミス・ リセット

構成セットアップを最初から再起動する必要がある場合は、reset オプションを使用します。

管理者としてコマンド・プロンプトを開き、実行ファイルが保存されているフォルダーに移動します。次のように入力して、reset コマンドを実行します。

```
\$ ivrNext.exe --reset
```

reset コマンドが実行されると、以下の確認内容がチェックされます。

```
Are you sure that you want to reset your configuration ? (y/n):
```

「**y**」と入力すると、db 関連フォルダー以外のデータ・ フォルダーが削除されます。

Chapter 7. IVR オンプレミスの構成設定

IVR v.4.0.0 オンプレミス・アプリケーションの構成を次に示します。これらのいずれかの構成を変更する場合、アプリケーションを停止し、構成設定を変更してからアプリケーションを起動してください。

`AppConfig.yaml`

この YAML ファイルには、アプリケーションの構成設定が含まれています。

設定名	データ型	デフォルト値	説明	指定可能な値	注釈
構成					
ByPass-Certificat-eVerifica-tion	ブール値	TRUE	証明書検証をバイパスするかどうかを示すブール値	• TRUE • FALSE	
CorsAl-lowedOri-gins	ストリング	'*'	CORS に許可されているオリジンを示すストリング値		
LogCom-pression	ブール値	TRUE	ログ圧縮を有効にするかどうかを示すブール値。		圧縮形式は .gz になります (このファイル形式を開くには 7zip などの外部ツールが必要です)。
LogMax-AgeDays	Int	15	ログ・ファイルの最大保存期間 (日数)		
LogMax-Backups	Int	100	保持するログ・バックアップの最大数。		
LogMax-SizeMb	Int	10	ログ・ファイルの最大サイズ (MB 単位)。		
ポート	Int	9011	アプリケーションのポート番号。		
BesReConfigs					
ポート	Int	9013	BesRetriever サービスのポート番号。		

設定名	データ型	デフォルト値	説明	指定可能な値	注釈
構成					
Web サーバー		127.0.0.1	このサービスがホストされているサーバー。		
EngConfigs					
ポート		9014	EngConfigs サービスのポート番号。		
Web サーバー		127.0.0.1	このサービスがホストされているサーバー。		
AutomationIntervalHours	Int	12	自動化の間隔 (時間)。		
LBConfigs					
ポート		9012	LBConfigs サービスのポート番号。		
Web サーバー		127.0.0.1	このサービスがホストされているサーバー。		

Chapter 8. IVR v.4.0.0 ログ

このセクションでは、IVR v.4.0.0 のログについて説明します。

このログは、`C:\Program Files (x86)\BigFix Enterprise\BESIvrRetriever\data\logs` の場所にあります。

`AppConfig.log`

この口グには、最後の実行時にランタイムで使用されたアプリケーションの構成と設定に関する情報が含まれています。また、このファイルはアプリケーションの実行中にユーザーが AppConfig.yaml ファイル設定を変更するたびに更新されます。

`ivrn.log`

これは、アプリケーションで起こっていることを示すメインの口グ・ファイルです。初期状態では、デバッグ (冗長) 口ギングはオフの状態になります。ユーザーが AppConfig.yaml ファイルの「設定」セクションで LogVerbose を true に設定すると、デバッグ・口グが有効になります。

この場合、ファイルが (AppConfig.yaml ファイルで指定されている) 最大サイズ制限に達すると、口グ・ローテーションが発生します。つまり、日付と時刻が ivrn.log ファイルに添付され、新しい ivrn.log ファイルが記録され始めることを意味します。

Chapter 9. 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 v.4.0.0 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。

主な機能:

- インフラストラクチャー要件 (計算リソース、サーバー構成、またはデータ処理時間) を削減する、IVR 4.0 向けのまったく新しいフレームワーク
- BigFix IVR v.4.0.0 は、Tenable VM との統合をサポートしています
- Tenable の検出結果と BigFix 修復コンテンツの相関関係に関するより信頼性が高く、より正確な改善済みロジック。CVE だけでなく、Tenable データ・ フローで利用可能な追加メタデータに基づいています
- 修復の識別の最適化。BigFix は、Tenable の検出結果と BigFix コンテンツ間の事前相関マッピングを提供します。これは、BigFix によって維持および更新されます
- より正確で効果的で高速なデバイス相関ロジック。ID に基づいており、最終的な相関結果の信頼性が大幅に向上します。

IVR の目的はこれまでと同様です。つまり、セキュリティーおよび運用チームが連携できるようにインテリジェントなパッチ適用の優先順位付けと自動修復機能を提供し、脆弱性の発見から修復までの時間を短縮し、攻撃に脆弱な領域を減らすことでリスクを大幅に削減することです。

機能および機能拡張

- IVR 向けの全く新しいアーキテクチャーと設計
- Tenable.vm の IVR サポート
- インフラストラクチャー要件の削減
- アセットの相関関係の向上
- 合理化されたデプロイメント
- 修復相関関係に対する脆弱性の最適化

リソース

- 資料

サイトのバージョン:

サイト・タイプ	名前	バージョン
Fixlet サイト	BigFix Insights for Vulnerability Remediation	14
WebUI サイト	WebUI IVR	15
WebUI サイト	WebUI 共通	90

Chapter 10. 既知の制限

IVR v.4.0.0 の制限については、次のリストを参照してください。

- セットアップ時に選択したポート番号がまだ使用されていないことを確認します。
- 証明書は、構成に関する問題を回避するために有効である必要があります。
- SQL DB 資格情報は、セットアップ・プロセスが中断されると失敗します。
- IVR OnPrem セットアップ・プロセス中に、「アプリケーション構成」ページで、選択したポート番号が別のサービスで使用されていないこと、およびファイアウォールで開いていることを確認します。
- 「証明書の構成」ページで、無効な問題を回避するための適切な証明書を追加します
- IVR 構成マネージャーの「データベースの構成」タブでは、cmd から setup コマンドを停止すると、SQL DB 資格情報が失敗します。セットアップ・プロセスが停止しているため、以下のエラーが表示される場合があります。取り出しに失敗しました。このため、setup コマンドを開始し、修正を行います。
- IVR データベースと Insights DB との依存関係はありません。
- 非マスターは、IVR 設定マネージャーの「データ・ソース」タブで Bes リソースを作成できません
- IVR2 または IVR3 に戻すには、BFEnterprise データベースの dbo.WEBUI_DATA テーブルの「名前」列からトークンを削除します。