FMCでのVDB更新プロセスの明確化

内容

お問い合わせ内容

脆弱性データベース(VDB)のアップデートを実行する際に、管理者はVDBのアップデートが累積されているかどうかを理解し、中継バージョンをスキップできるかどうかを理解する必要があります。

この例では、問題はVDBバージョン393からバージョン427にアップデートする場合です。特に、複数のアップグレード手順が必要かどうか、または直接的なアップグレードパスがサポートされているかどうかについては不明です。さらに、VDBのアップデートやその後のポリシー展開プロセス中にサービスが中断される可能性があるという懸念もあります。

環境

- セキュアファイアウォール管理センター(FMC)ソフトウェアバージョン7.4.2.4他のソフトウェアバージョンも該当します。
- FPR 2110のファイアウォール脅威対策(FTD)。他のハードウェアプラットフォームも影響を受けます。
- 現在のVDBバージョン：393。他のソフトウェアバージョンも該当します。
- ターゲットVDBバージョン：427。他のソフトウェアバージョンも該当します。

解決策

FMCでのVDBのアップデートは累積的であるため、途中で作業しなくても、古いバージョンから新しいバージョンに直接アップグレードできます。

VDBの更新プロセス

VDBの中間アップグレード手順を行わなくても、VDBバージョン393からVDBバージョン427に直接アップデートできます。VDBバージョン357以降、シスコはFMCプラットフォームのベースラインVDBまでのすべてのVDBバージョンのインストールをサポートしています。

最新のVDBバージョンをダウンロードするには、Cisco Software Download Center(https://software.cisco.com/download/home/286332319/type/286321931/release/VDB)に移動します。

サービスへの影響に関する考慮事項

主なリスクは、FMCでのVDBのインストール自体ではなく、VDBの更新後のFTDでの最初のポリシー展開に関連します。ほとんどの場合、VDB更新後の最初の展開ではSnortプロセスが再起動し、これによりトラフィック検査が一時的に中断されます。

この割り込み期間中：

- トラフィックは、それ以上の検査を行わずにドロップまたは通過できます。
- 具体的な動作は、プロセスの再起動時にトラフィックを処理するようにFTDがどのように設定されているかによって異なります。

ベストプラクティスの推奨事項：

- 計画されたメンテナンス時間中にポリシー導入部分をスケジュールします。
- ネットワーク運用と調整して、ユーザへの影響を最小限に抑える。
- 導入プロセス中および導入後のシステムステータスを監視します。

原因

- VDB 357以降では、VDBのアップデートをFMCのベースラインVDBまでインストールできます。

- このインストールでは、新しい脆弱性シグニチャをアクティブにするためにポリシーの再導入が必要です。これにより、管理対象FTDデバイスでSnortプロセスの再起動がトリガーされます。この再起動により、新しいデータベースがロードされ、インスペクションエンジンが再初期化される間、トラフィックインスペクション機能に短い中断が発生します。

関連コンテンツ

- Cisco Secure Firewall Management Centerアドミニストレーションガイド – システムアップデート
- Cisco Secure Firewall Management Centerデバイス設定ガイド – 導入
- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。