影響=不明を示すFMC侵入イベントのトラブルシューティング

内容

お問い合わせ内容

新しいFirewall Management Center(FMC)を導入し、バージョン7.7.12にアップグレードした後で、すべての侵入イベントが、予測される影響値ではなく、「Impact=Unknown」と表示されます。これにより、アラートの設定に影響フィールドが必要になるため、適切なアラートメカニズムがトリガーされなくなります。

環境

- FMCバージョン7.7.12他のソフトウェアバージョンも影響を受ける可能性があります。
- 防御モードまたは検出モードの侵入ポリシー。

解決策

この問題の解決には、侵入イベントが生成されるすべての関連IPアドレスを含むようにディスカバリポリシースコープを確認して設定することが含まれます。

ステップ 1：影響を受けるIPアドレスの特定

「Impact=Unknown」と表示されている侵入イベントを確認し、これらのイベントに関係する特定のIPアドレスを特定します。現在のディスカバリポリシー設定と比較するために、これらのIPアドレスを文書化します。

ステップ 2現在のディスカバリポリシー設定の確認

FMCのPolicies > Network Discovery (新しいバージョンではPolicies > Advanced > Network Discovery)に移動し、現在の検出ポリシーの設定を調べて、どのIPアドレス範囲またはサブネットが現在検出スコープに含まれているかを確認します。

ステップ 3検出ポリシースコープの更新

侵入イベントが発生しているすべてのIPアドレスを含むように、ディスカバリポリシーの設定を変更します。適切なインパクトアセスメントとともに、侵入イベントの受信が予想されるすべてのネットワークセグメントが検出ポリシーの範囲に含まれていることを確認します。

ステップ 4設定の変更の導入

更新された検出ポリシー構成をすべての管理対象デバイスに展開し、セキュリティインフラストラクチャ全体に変更が適用されるようにします。

ステップ 5影響フィールドの母集団の確認

新しい侵入イベントを監視して、影響フィールドに「不明」ではなく適切な値が入力されていることを確認します。

原因

「Impact=Unknown」と表示される侵入イベントは、該当するIPアドレスがFMCのどのディスカバリポリシーにも含まれていない設定の問題が原因です。IPアドレスが、設定されたディスカバリポリシーの範囲外になると、FMCではそれらのアドレスに対する侵入イベントの影響を適切に評価できず、その結果、影響フィールドに「不明」の値が設定されます。これは、ソフトウェアやハードウェアの不具合ではなく、設定に関連する問題です。

関連コンテンツ

- 侵入イベントの影響レベル
- 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。