カスタムポリシー検出によりFTDのアップグレード中にSnortエンジンのアップグレードがブロックされる

内容

お問い合わせ内容

FMCによって管理されるHA FPR-4115でのバージョン7.2から7.4.4へのFTDアップグレード中に、Snort 3へのSnortエンジンのアップグレードがブロックされ、Snort 2カスタムルールの変換に失敗したこと、またはカスタム侵入ポリシーやネットワーク分析ポリシーの使用を示すエラーメッセージが表示されます。特定のエラーメッセージには、「Cannot upgrade to Snort 3.デバイスが少なくとも1つのカスタム侵入ポリシーまたはネットワーク分析ポリシーを使用している。」より詳細な失敗メッセージは、Snort 2カスタムルールを変換できない問題を参照し、詳細については/var/sf/htdocs/ips/snort.rejを参照してください。問題は、このエラーによってSnort 3への移行が妨げられ、インスペクション機能に影響が及ぶかどうかです。

環境

- Cisco Secure Firewall Firepowerバージョン7.3
- Firepower Management Center（FMC）バージョン 7.7.11
- ハイアベイラビリティ(HA)構成のFTDデバイス
- ハードウェア：FPR-4115
- アップグレードパス：FTD 7.2から7.4.4
- アップグレード前の最新バージョンのVDB
- Objects > Intrusion Rules > Snort 2 All Rules is emptyの下のLocal Rulesセクション

解決策

Snortエンジンのアップグレードをブロックするエラーメッセージは、Cisco Bug ID CSCwn46794に関連する動作として文書化されており、実際にカスタムのSnort 2ルールが存在しない場合のブロック機能を表すものではありません。

確認手順

ステップ1：カスタムSnort 2ルールのステータスを確認する

FMCインターフェイスに移動し、カスタムSnort 2ルールを確認します。

`Objects > Intrusion Rules > Snort 2 All Rules >ローカルルール`

ステップ2:VDBバージョンの確認

アップグレードを続行する前に、脆弱性データベース(VDB)が最新バージョンであることを確認してください。

ステップ3：エラーの詳細を確認します。

参照ファイルの詳細なエラー情報を確認します。

```
/var/sf/htdocs/ips/snort.rej
```

アップグレード プロセス

「ローカルルール」セクションが空であることが確認されると（カスタムSnort 2ルールが存在しない）、エラーメッセージが表示されてもアップグレードを続行できます。 このシナリオでは、ブロッキングエラーは誤検出であり、変換が必要な実際のカスタムルールを示すものではありません。

ステップ1:Snort 3のアップグレードに進む

Snort 3エンジンのアップグレードを含む、バージョン7.4.4へのFTDアップグレードプロセスを続行します。

ステップ2：アップグレード後の検証

アップグレードが正常に完了したら、トラフィックフローをテストして、Snort 3エンジンの予測動作を確認します。

ステップ3：システムパフォーマンスの監視

新しいSnort 3エンジンで、インスペクション機能が期待どおりに動作することを検証します。

原因

アップグレードブロッキングメッセージは、Cisco Bug ID CSCwn46794に関連する動作として文書化されています。 この不具合により、変換を必要とする実際のカスタムSnort 2ルールが存在しない場合でも、カスタム侵入ポリシーまたはネットワーク分析ポリシーに関するエラーメッセージが表示されます。 Local Rulesセクションが空の場合、エラーメッセージは誤検出として表示されますが、システムのアップグレード前検証でカスタムポリシーの存在が誤って識別されます。

関連コンテンツ

- Cisco Bug ID CSCwn46794
- Cisco Bug ID CSCwk07199
- 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。