セッション再認証後にトリガーされないISEエージェントレスポスチャのトラブルシューティング

内容

問題

Identity Services Engine(ISE)3.3のエージェントレスポスチャ機能は、セッション再認証イベントの後にトリガーに失敗します。初期認証では、エージェントレスポスチャが正しく機能し、エンドポイントが準拠するようになります。ただし、再認証が発生すると、エンドポイントはアカウンティング開始イベントではなくRADIUSアカウンティング中間更新イベントを受信するため、エージェントレスポスチャフローが呼び出されません。その結果、エンドポイントは未知のポスチャポリシーに一致し、未知のポスチャ状態のままになり、影響を受けるデバイスのネットワークアクセスに影響を与えます。

この問題は、再認証後にエンドポイントが「ポスチャ保留中」または「不明」のステータスのままになり、レポートされた環境では1200のエンドポイントのうち約800が影響を受けていることで発生します。ログ分析は、再認証中に、ISEがagentlessEnabled=trueのACCOUNTING_UPDATEイベントを受信するが、ポスチャフローが既存のセッションIDに対して再呼び出しされないことを示しています。

環境

- Identity Services Engine(ISE)バージョン3.3パッチ4
- MAC認証バイパス(MAB)による有線802.1X認証
- エージェントレスポスチャ設定の有効化
- 設定済みのセッション再認証タイマー（420秒タイムアウト）
- ネットワークアクセスデバイスとしてのCisco Catalystスイッチ
- 環境内に約1200のエンドポイント

解決方法

この動作は、ISEで想定されており、設計上は正常です。エージェントレスポスチャは、RADIUSアカウンティング開始イベントによってのみトリガーされ、フレーム化IPアドレスが変更されないときにセッション再認証中にアカウンティング中間更新イベントによって再呼び出しされません。

技術分析

ISE NetAccessEventHandlerコードパスは、新しいRADIUSアカウンティング開始パケットでエージェントレスポスチャフローを再調整するだけです。再認証中、ネットワークデバイスは通常、同じAcct-Session-Idを持つAccounting Interim-Update(ACI)パケットを送信します。これにより、shouldInvokePostureFlow()関数がfalseを返し、ポスチャ再評価が行われなくなります。

動作を示す証拠を口グに記録します。

初期認証（エージェントレスポスチャのトリガー）:

```
2026-04-01 11:28:20,466 DEBUG [PrRTEvents-Executor-2][[]] cisco.cpm.posture.events.NetAccessEventHandle

2026-04-01 11:28:20,466 DEBUG [PrRTEvents-Executor-2][[]] cisco.cpm.posture.events.NetAccessEventHandle
```

再認証（エージェントレスポスチャがトリガーされない）:

```
2026-04-01 11:35:37,669 DEBUG [PrRTEvents-Executor-2][[]] cisco.cpm.posture.events.NetAccessEventHandle
```

推奨される回避策

この動作の影響を緩和するには、ポスチャリース設定を設定して、再認証シナリオ中のエンドポイントコンプライアンスを維持します。

ステップ1:ISEポスチャポリシーで適切なポスチャリース期間を設定し、ポスチャ評価間でエンド

ポイントがネットワークアクセスを失わないようにします。

ステップ2:エンドポイントのポスチャステータスを監視し、組織のセキュリティ要件と再認証頻度に基づいてリースタイマーを調整します。

原因

この問題は、Cisco Bug ID CSCwu48086に記述されています。ISEのエージェントレスポスチャは、RADIUSアカウンティング開始イベントでのみトリガーされるように設計されており、暫定アカウンティング更新イベントではトリガーされません。セッション再認証中に、ネットワークアクセスデバイスは同じフレームIPアドレスとセッションIDを使用してアカウンティング暫定アップデートを送信します。この場合、エージェントレスポスチャ評価プロセスは再度呼び出されません。ISEコードは、エージェントレスポスチャフローを開始する前に、特に新しいセッション（ACCOUNTING_STARTイベント）を確認します。

関連コンテンツ

- Cisco Bug ID CSCwu48086
- 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。