

Norton Antivirusのアンインストール後に Windows Defenderシグニチャデータベースが空 になると、ISEポスチャが失敗する

内容

問題

VPN経由で接続しているWindows 11 25H2エンドポイントがISEポスチャチェックに失敗し、非準拠としてマークされるため、認証とネットワークリソースへのアクセスができなくなります。エンドポイントはISEルールの要件を満たしているが、VPN接続後に「user not meeting the requirement」が引き続き報告される。

Windows Defenderのウイルス対策定義バージョンの検証のポスチャチェックが次のエラーで失敗します。

```
[csc_iseposture]Function: CheckOpswat::CheckOpswatProd Thread Id: 0x277C File: CheckOpswat.cpp Line: 27
```

ポスチャエージェントは、Windows Defenderの定義バージョンが空で定義日が0であると報告し、AUC_WIN11_IT要件が失敗します。

環境

- Identity Services Engine(ISE)3.3
- Windows 11 25H2エンドポイント
- ISEポスチャモジュールを使用したCisco Secure Client
- ISEComplianceモジュールバージョン4.3.5626.8192
- Windows Defenderバージョン4.18.25080.5

- 以前はNorton 360 Antivirusをインストールおよびアンインストールしていた
- ISEポスチャ適用を有効にしたVPN接続

解決方法

この問題を解決するには、Nortonをアンインストールしてから、Windows Defenderの署名を手動で更新し、サードパーティ製のウイルス対策ソフトウェアとWindows Defenderの共存動作を理解する必要があります。

手順1: Windows Defenderの署名を更新する

- 1.- Windowsのセキュリティ設定に移動し、シグニチャデータベースを手動で更新します。
- 2.- Settings → Privacy & security → Windows Security → Virus & threat protection → Virus & threat protection updates → Check for updatesの順に選択します。
- 3.- Security intelligence versionに空ではない値と現在のタイムスタンプが表示されるまで待機してから、ポスチャ検証に進みます。

ステップ3：ポスチャ準拠の確認

シグニチャをアップデートした後、VPNに再接続し、ポスチャチェックに合格したことを確認します。セキュリティインテリジェンスバージョンは、空ではなく有効な値を表示する必要があります。

サードパーティ製アンチウイルスの重要な考慮事項

サードパーティ製のウイルス対策ソフトウェアがインストールされ、Windowsセキュリティセンターに正しく登録されている場合、Microsoft Windowsは意図的にWindows Defenderをパッシブモードにして競合を回避します。パッシブモードでは、DefenderはOPSWATが読み取るWindowsセキュリティセンター/WMI APIを介してシグニチャの鮮度データを公開しないため、ポ

スチャチェックが失敗します。

この問題を回避するには、Windowsがアクティブモードにするサードパーティアプリケーションをアンインストールします。Nortonまたはその他のサードパーティ製アンチウイルスソフトウェアを再インストールする必要がある場合は、エンドポイントが再び非準拠になる原因になることに注意してください。

原因

根本的な原因は、サードパーティのウイルス対策ソフトウェア(Norton)が主要なウイルス対策ソリューションである場合に、Windows Defenderシグニチャデータベースが古くなることです。Nortonがインストールされている間、パッシブモードのウイルス対策ソフトウェアがスケジュールされた更新を受信しないため、Windowsは意図的にDefender定義ストアを古い状態に保ちました。Nortonのアンインストール後、Windows Defenderが主要なウイルス対策ソフトウェアになりましたが、最初の署名のプルはWindows Updateの後ろにキューに入れられ、次のスケジュールされたトリガーで自動的に実行されるか、ユーザーによって手動で強制された場合にのみ実行されるため、署名データベースは空のままでした。

OPSWAT v4 SDKメソッド1001(GetDefinitionState)は、Defenderローカル定義ストアが空の場合に空のペイロードを返し、これによりISEポスチャエージェントは空の定義バージョンをISEに送信します。次に、ISEはこの空の値をポリシーのしきい値と比較し、エンドポイントを非準拠としてマークします。

関連コンテンツ

- [Cisco Secure Client管理者ガイド – サードパーティソフトウェアに関する考慮事項](#)
- [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。