

エンドポイントセキュリティポスチャのコンプライアンス問題が原因で拒否されたセキュアクライアントAnyConnect VPNアクセス

内容

問題

複数のユーザがAnyConnect VPNおよびZero Trust Access(ZTA)に接続できず、「Login denied.ご使用の環境は、管理者が定義したアクセス基準を満たしていません。」

この問題は、Endpoint Security Agentの要件が一致しないと報告されるエンドポイントポスチャのコンプライアンスに関連しています。Cisco Secure Client経由で接続しようとする、VPNおよびZTAアクセス拒否が発生します。

ポスチャ評価は、Trellix Endpoint Securityポスチャが影響を受けるエンドポイントで失敗し、VPNサービスへの認証が成功しないことを示します。

環境

- Cisco Secure Client (AnyConnectおよびゼロトラストアクセス)
- Trellix Endpoint Security Agent/バージョン5.8.4.505
- VPNポスチャプロファイル：エンドポイントセキュリティエージェント適用のKFIN_SECURE_VPN
- ポスチャ要件：過去14日以内の更新で実行されるエンドポイントセキュリティエージェント
- Trellix Agent Serviceが実行されているWindowsエンドポイント
- エンドポイントで検出された包括エージェントプロセス

解決方法

この問題は、Trellix Endpoint Securityエージェントのポスチャコンプライアンスの問題に対処することで解決されました。次のセクションで説明するトラブルシューティング手順と解決手順が実装されました。

ステップ1: ポスチャプロファイル設定の検証

VPNポスチャプロファイルを確認し、エンドポイントセキュリティエージェントの要件を確認します。KFIN_SECURE_VPNプロファイルは、エンドポイントセキュリティエージェントが実行され、過去14日以内に更新される必要があることを強制します。

手順2:Trellixエンドポイントのセキュリティステータスを確認する

影響を受けるエンドポイントのTrellix Endpoint Securityエージェントの現在のステータスを確認します。

```
Trellix Agent Service: masvc.exe  
Version: 5.8.4.505  
Install Location: C:\Program Files\McAfee\Agent\  
Display Name: Trellix Agent  
Publisher: Trellix
```

ステップ3:Trellix Endpoint Securityを再インストールする

影響を受けるエンドポイントでTrellix Endpoint Securityの完全な再インストールを実行します。

1. 既存のTrellix Endpoint Securityエージェントを完全にアンインストールします。
2. システムを再起動します。
3. 組織の標準に従って、最新の承認済みTrellixエージェントバージョンをインストールします。

4. インストール後にエージェントが正常に動作していることを確認します。
5. 署名/コンテンツの更新が正常に完了したことを確認します。

ステップ4: Cisco Secure Client(ZTA)のトレースロギングの有効化

ポスチャ評価の詳細をキャプチャする詳細ロギングを有効にします。

次のコンテンツを使用してlogconfig.jsonファイルを作成します。

```
{ "global": "DBG_TRACE" }
```

適切なディレクトリにファイルを配置します。

- Windowsの場合 : C:\ProgramData\Cisco\Cisco Secure Client\ZTA
- macOS:/opt/cisco/secureclient/zta

ファイルの作成後に、Cisco Secure Client/ZTAサービスを再起動します。

ステップ5 : 更新されたDARTバンドルの収集

変更を実装したら、新しいDARTバンドルを収集して解決策を検証し、適切なポスチャコンプライアンス検出を確認します。

原因

根本原因は、Trellixエンドポイントセキュリティエージェントポスチャのコンプライアンスの問題として特定されました。VPNポスチャプロファイルでは、エンドポイントセキュリティエージェントが過去14日以内にアップデートで実行されている必要がありましたが、Trellix Endpoint Securityエージェントはこれらのコンプライアンス基準を満たしていませんでした。ポスチャ評価モジュールがエンドポイントセキュリティエージェントのステータスを正しく検出または検証

できなかったため、VPNおよびZTA接続が拒否されました。この問題は特にTrellixエージェントの設定に関連するもので、基盤となるエージェントコンプライアンスの問題を解決するためにTrellixサポートチームによる介入が必要でした。

関連コンテンツ

- [トラブルシューティングのための詳細なZTNAログの収集](#)
- [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。