RAVPN接続中のCisco Secure Client SAML認証ナビゲーションタイムアウトエラー

内容

お問い合わせ内容

SAML認証中にCisco Secure Clientを使用するWindowsで、リモートアクセスVPN(RAVPN)の接続エラーが断続的に発生します。この障害は、Cisco Secure Clientをインストールした直後に発生し、ポップアップダイアログに表示される特定のエラーメッセージとして現れます。

- 「ナビゲーションタイムアウトが原因で認証に失敗しました。」
- 「シングルサインオンURLへの移動に問題があるため、認証に失敗しました。」

この障害は、アイデンティティプロバイダー(IdP)認証後に、組み込みのWebView2ブラウザがCisco SSE SAML ACS URLにSAML応答をリダイレクトまたは投稿しようとしたときに発生します。この結果、タイムアウト状態が発生し、影響を受けるユーザのVPNアクセスが妨げられます。この問題は、同じ組織内の複数のユーザに影響を与えており、SAML ACSエンドポイントに移動を試みた後、約30秒で認証プロセスがタイムアウトすることが確認されています。

ユーザから、RAVPN接続ボタンを押してVPN接続を確立すると、タイムアウトエラーのポップアップが表示され、RAVPNの確立が失敗するという報告がありました。OSを再起動しても問題が解決しない。

環境

- Windows上のCisco Secure Clientバージョン5.1.13.177
- Cisco SSEで設定されたSAML認証
- リモートアクセスVPN(RAVPN)の導入

当面の回避策

ナビゲーションのタイムアウトの問題を解決するために、次の一時的な回避策が確認されています。

1：ネットワーク接続のリセット

Wi-Fi接続を切断して再接続し、RAVPN接続を複数回試行します。正常に完了すると、通常はOSを再起動しても問題が再発しません。

2:RAVPNサービスの再起動

RAVPNサービスを手動で停止してから再起動し、以降の接続が成功するようにします。

3：システムの再起動

影響を受けるシステムを再起動して、認証状態をリセットします。

診断情報収集

包括的なトラブルシューティングを行うには、アクティブな障害発生時に次の診断情報を収集する必要があります。

- 認証失敗時にキャプチャされたDARTバンドル
- ネットワークパケットキャプチャ(認証プロセス中にすべてのアクティブアダプタでWiresharkを使用してトラフィックをキャプチャします（Wiresharkを開き、「capture - options」をクリックしてShiftキーを使用して複数のインターフェイスを選択します）
- Netsh ETLトレース

Netshトレースを収集する手順

- テストPCで、管理者特権での（管理者として実行）コマンドプロンプトウィンドウを開きます。
- 次のコマンドを実行します。「netsh trace start scenario=InternetClient

traceFile=C:\file_NetTrace.etl maxSize=1000 provider=Microsoft-Windows-TCPIP provider=Microsoft-Windows-WinHttp capture=yes level=5 overwrite=yes」

- 問題を再現します。
- 問題が再現されたら、「netsh trace stop」コマンドを使用してロギングを停止します。

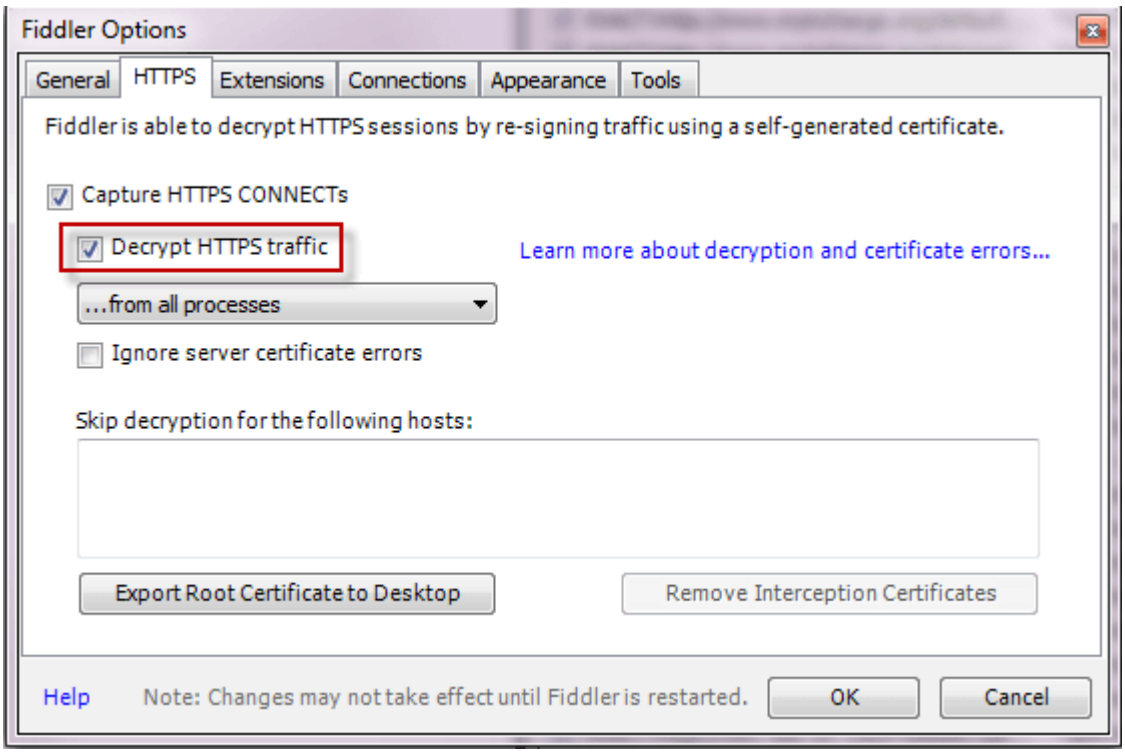
ログの収集：C:\file_NetTrace.etl

Webトラフィックの Fiddlerトレース

1. Fiddlerキャプチャは、次のリンクからダウンロードできます。
   https://www.telerik.com/download/fiddler-everywhere(Intelチップ(x86-64)を使用)
2. 問題を再現できるマシンにインストールします。
3. アプリケーションを開き、HTTPS復号化を有効にします

a. HTTPSの「ツール」 > 「オプション」の順にクリックします。

b. Decrypt HTTPS Trafficボックスをクリックします。



inline_image_0.png (インラインイメージ_0.png)

4. 証明書を信頼する場合は、fiddlerからCAを信頼し、問題が再現されたら後で削除してください。

次に、起動中にSSL接続の問題が発生した場合は、ゲートウェイトラフィックをバイパスする必要がないように、VPNゲートウェイトラフィックをバイパスする(connect.ilemgroup.com)か、IPsecベースのSAML接続を開始します（最も望ましい）。

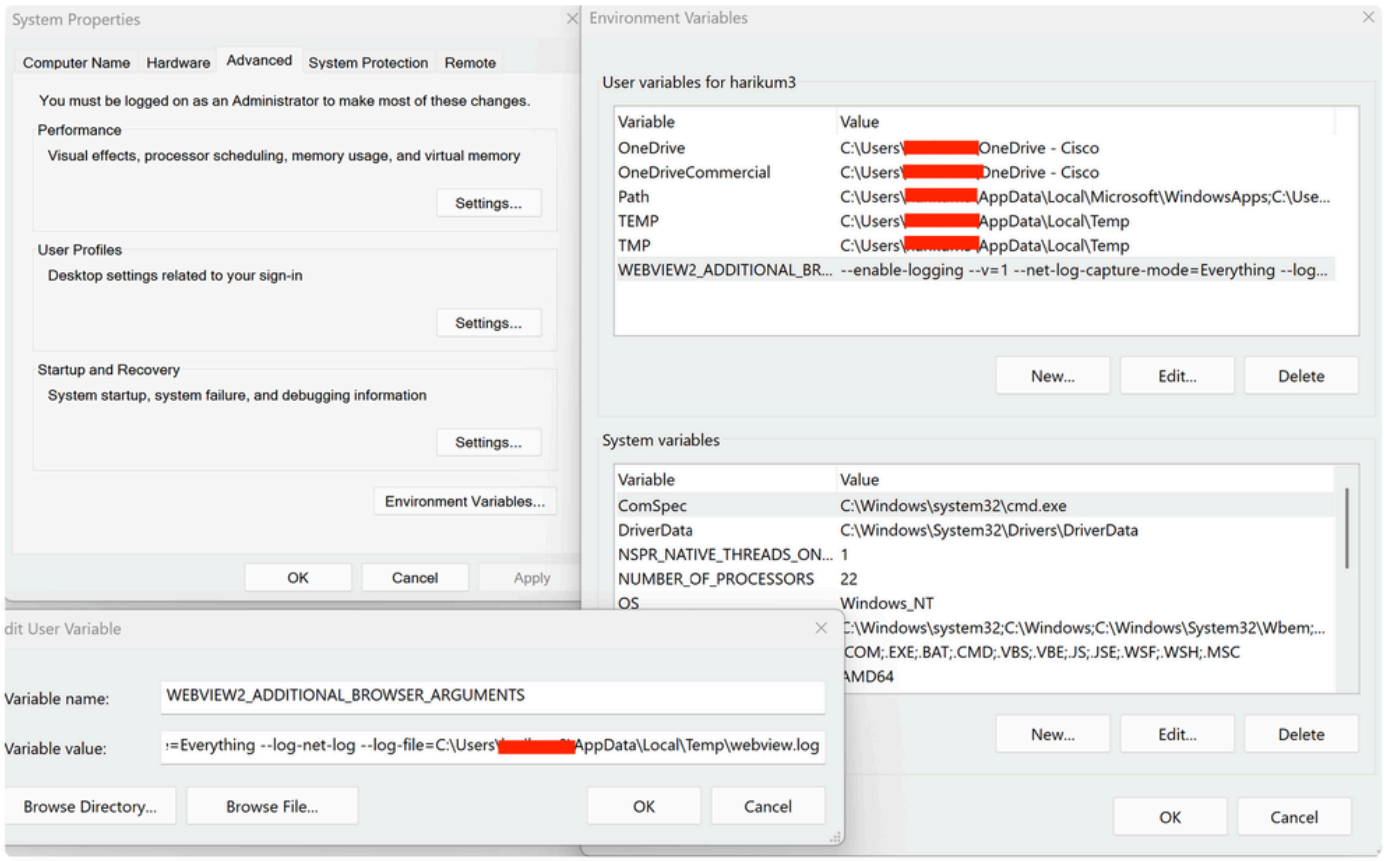
- 不要なアプリケーションとバックグラウンドプロセスをすべて閉じます。
- ツールを閉じて再度開くと、データ収集が自動的に開始され、メインフォームに新しいレコードが追加されます。
- 問題を再現します。
- トレースを停止するには、F12キーを押します。

「File > Save > All Sessions」に移動し、トレースを.sazファイルに保存します。

プロセスモニタログ:https://download.sysinternals.com/files/ProcessMonitor.zip

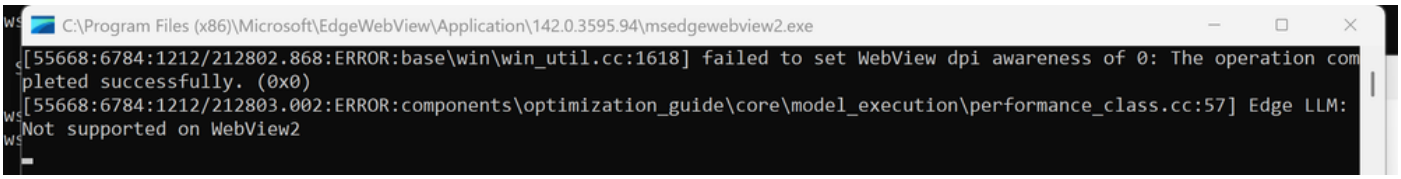
WebView2固有のログ

以下にスナップされたユーザーおよびシステム環境の変数/値を設定しています



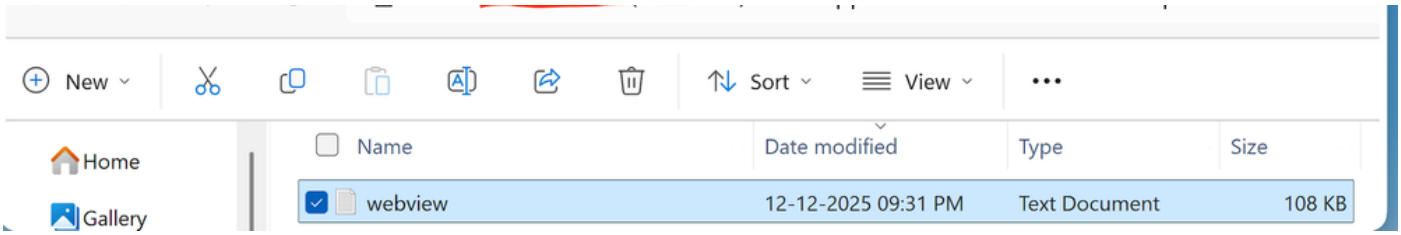
スクリーンショット_2026-05-12_at_9.43.19_AM.png

VPNの起動中に、次の端末が



inline_image_1.pngファイル

C > Users > userid > Appdata > Local > Temp



inline_image_2.pngファイル

アイデンティティプロバイダーからのSAMLデバッグログ

解決策

原因

根本的な原因は、SAML認証フロー中に組み込みのWebView2ブラウザコンポーネントで発生するナビゲーションタイムアウトです。具体的には、タイムアウトは、WebView2ブラウザがアイデンティティプロバイダーからCisco SSE SAML ACS(Assertion Consumer Service)エンドポイントにSAML応答を送信しようとしたときに発生します。タイムアウト条件は、このナビゲーション手順を完了しようとして約30秒後にトリガーされます。

この問題は、SAML応答処理の遅延によるWebView2コンポーネントの内部タイムアウトしきい値の超過を引き起こすタイミングまたはネットワーク遅延の条件に関連していると考えられます。この問題はCisco Secure Clientのインストール直後に発生し、特にSAML認証ワークフローに影響しますが、回避策を使用して認証が正常に完了した後も、他のVPN機能はそのまま残ります。

関連コンテンツ

- 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。