Errori di timeout di navigazione autenticazione SAML Cisco Secure Client durante la connessione RAVPN

Sommario

Problema

Gli utenti riscontrano errori di connessione della VPN ad accesso remoto intermittente (RAVPN) in Windows utilizzando Cisco Secure Client durante l'autenticazione SAML. Gli errori si verificano immediatamente dopo l'installazione di Cisco Secure Client e visualizzano messaggi di errore specifici visualizzati in finestre popup:

- "Autenticazione non riuscita a causa del timeout della navigazione."
- "Autenticazione non riuscita a causa di un problema durante l'esplorazione dell'URL Single Sign-On."

L'errore si verifica dopo l'autenticazione del provider di identità (IdP) quando il browser WebView2 incorporato tenta di reindirizzare o inviare la risposta SAML all'URL Cisco SSE SAML ACS. Il risultato è una condizione di timeout che impedisce l'accesso VPN agli utenti interessati. È stato rilevato un problema che interessa più utenti nella stessa organizzazione. Il processo di autenticazione scadrà circa 30 secondi dopo aver tentato di passare all'endpoint SAML ACS.

Gli utenti segnalano che quando si preme il pulsante di connessione RAVPN per stabilire la connessione VPN, viene visualizzato il popup dell'errore di timeout e la connessione RAVPN non riesce. Il problema persiste anche dopo il riavvio del sistema operativo.

Ambiente

- Cisco Secure Client versione 5.1.13.177 su Windows
- Autenticazione SAML configurata con Cisco SSE

- Distribuzione VPN ad accesso remoto

Soluzione immediata

Le seguenti soluzioni temporanee sono state confermate per risolvere il problema di timeout della navigazione:

1: Ripristino connettività di rete

Disconnettere la connessione Wi-Fi e riconnettersi, quindi tentare la connessione VPN più volte. Una volta risolto il problema, in genere non si ripresenta anche dopo il riavvio del sistema operativo.

2: Riavvio servizio RAVPN

Arrestare e riavviare manualmente il servizio RAVPN per consentire connessioni successive riuscite.

3: Riavvio del sistema

Riavviare il sistema interessato per reimpostare lo stato di autenticazione.

Raccolta informazioni di diagnostica

Per una risoluzione completa dei problemi, durante un guasto attivo devono essere raccolte le seguenti informazioni di diagnostica:

- Pacchetti DART acquisiti in caso di errore di autenticazione
- Acquisizione di pacchetti di rete (acquisizione del traffico tramite Wireshark su tutti gli adattatori attivi (apertura di Wireshark - clic su Capture - opzioni e uso di Shift per selezionare più interfacce) durante il processo di autenticazione
- Tracce ETL Netsh

Procedura per la raccolta della traccia Netsh

- Aprire una finestra del prompt dei comandi con privilegi elevati (Esegui come amministratore) nel PC di test.
- Eseguire il comando: "netsh trace start scenario=InternetClient traceFile=C:\file_NetTrace.etl maxSize=1000 provider=Microsoft-Windows-TCP provider=Microsoft-Windows-WinHttp capture=yes level=5 overwrite=yes"
- Riprodurre il problema
- Una volta riprodotto il problema, interrompere la registrazione utilizzando il comando: "netsh trace stop"

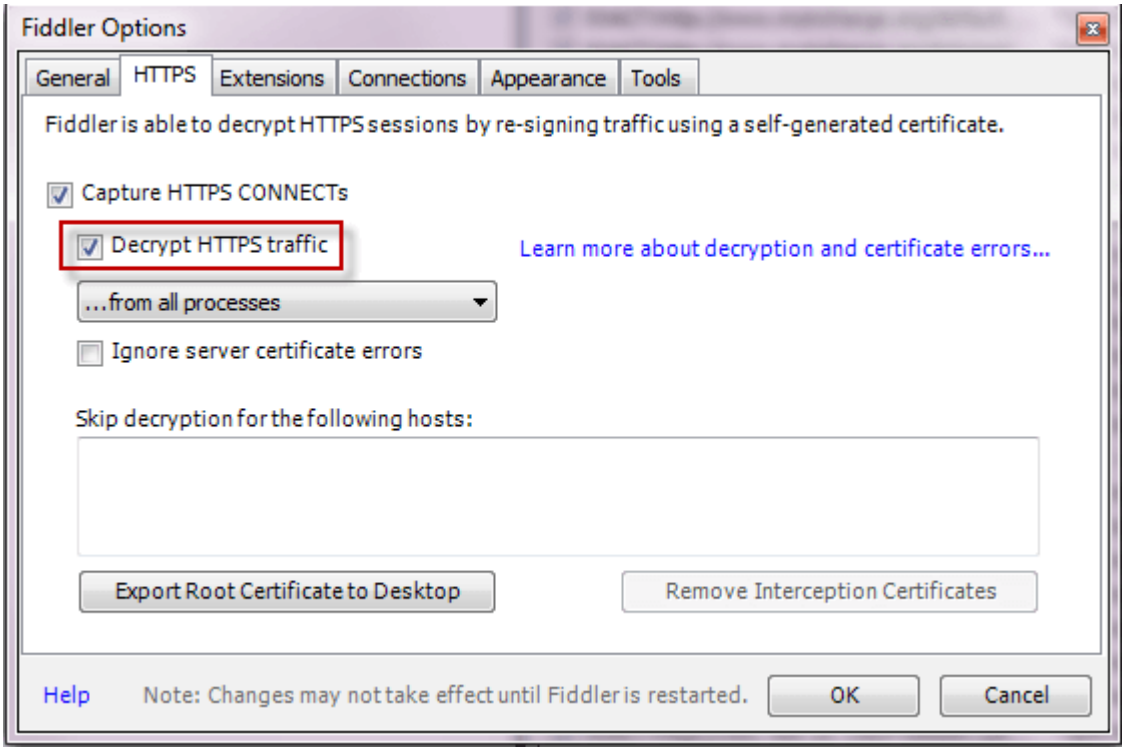
Raccogliere i registri C:\file_NetTrace.etl

Tracce del filtro del traffico Web

1. Scaricare Fiddler capture da questo collegamento https://www.telerik.com/download/fiddler-everywhere (utilizzare il chip Intel (x86-64)
2. Installarlo su un computer in cui il problema è riproducibile.
3. Apri l'applicazione e abilita la decrittografia HTTPS

a. Fare clic su Strumenti à Opzioni à HTTPS.

b. Fare clic sulla casella Decrittografa traffico HTTPS.



inline_image_0.png

4. Se si ottiene il certificato da considerare attendibile, pls trust the CA from fiddler ed eliminarlo in seguito una volta che il problema è stato riprodotto e

In secondo luogo, in caso di problemi di connettività SSL durante l'avvio, ignorare il traffico del gateway VPN (connect.ilemgroup.com) o avviare la connettività SAML basata su IPsec (preferibilmente) in modo che non sia necessario ignorare il traffico del gateway.

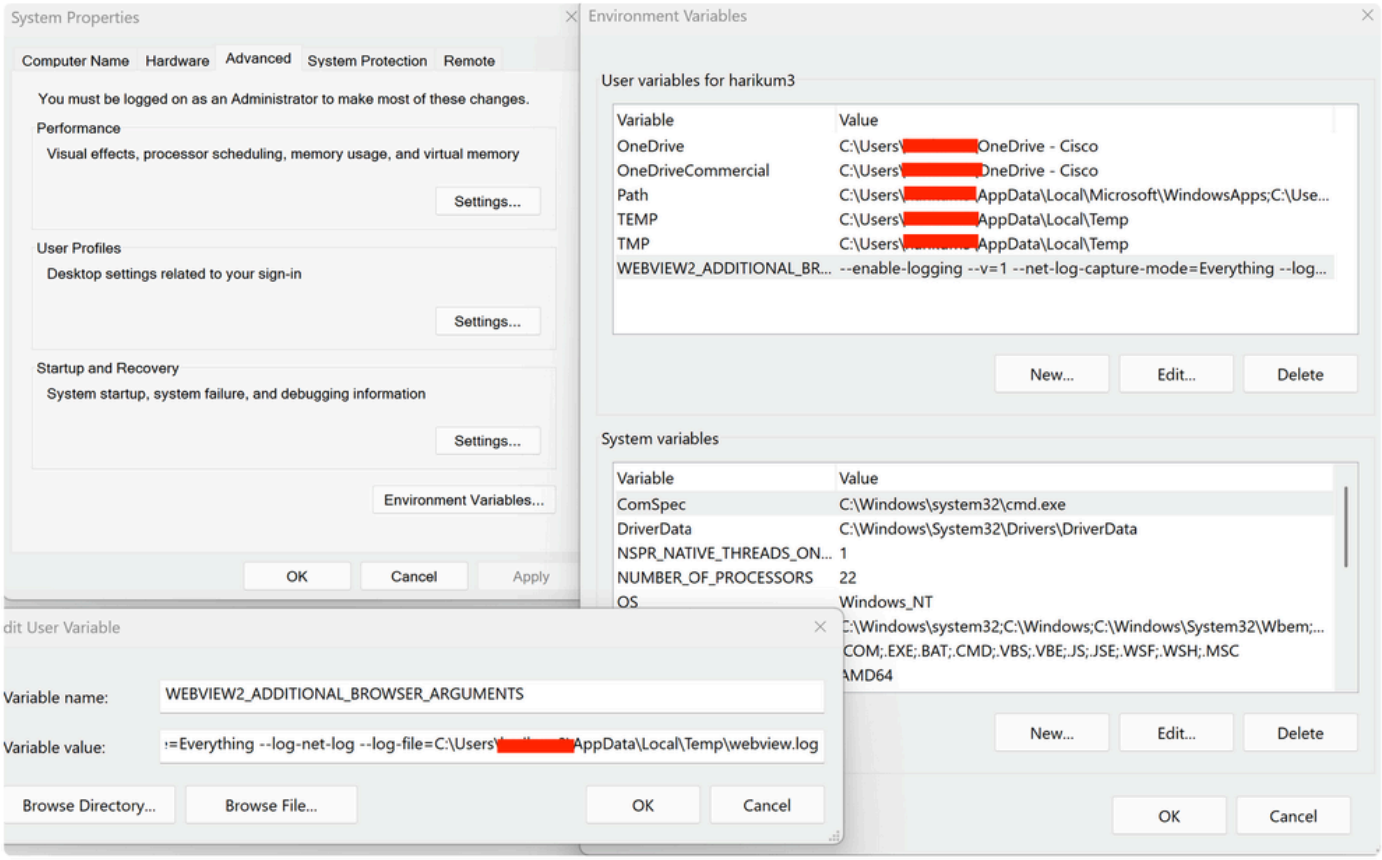
- Chiudere tutte le applicazioni e i processi in background non necessari.
- Chiudere e riaprire lo strumento. La raccolta dei dati verrà avviata automaticamente e i nuovi record verranno aggiunti alla maschera principale.
- Riprodurre il problema.
- Premere F12 per interrompere la traccia.

Scegliere Salva à Tutte le sessioni dal menu File, quindi salvare la traccia in un file saz.

Registri di Process Monitor - https://download.sysinternals.com/files/ProcessMonitor.zip

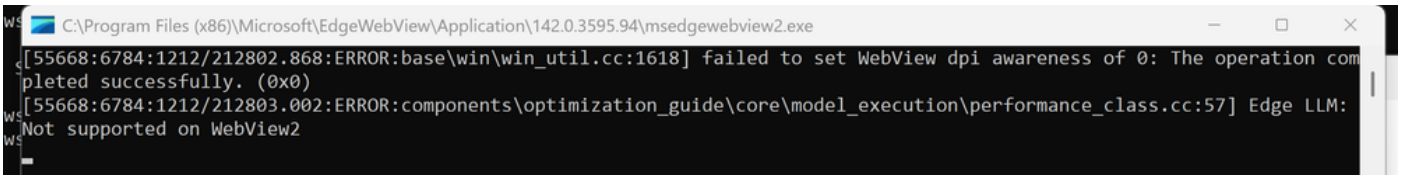
Registri specifici di WebView2

Impostazione della variabile/valore sull'ambiente utente e di sistema come ancorato di seguito



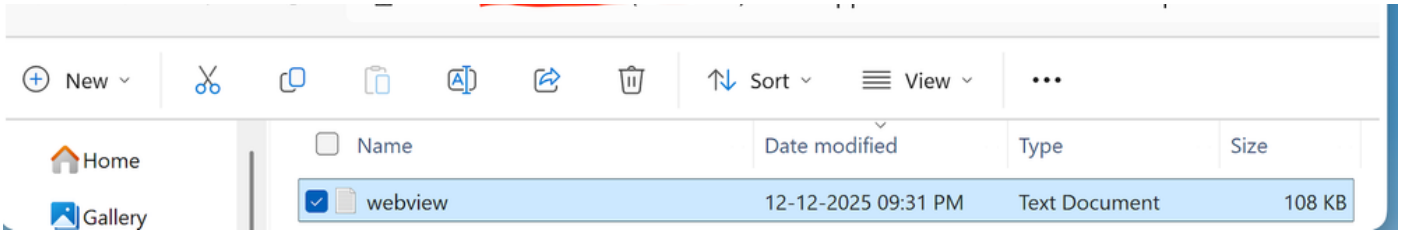
Screenshot_2026-05-12_at_9.43.19_AM.png

Durante l'avvio della VPN, il terminale sottostante attiverebbe



inline_image_1.png

C > Utenti > id utente > Appdata > Locale > Temp



inline_image_2.png

Registri di debug SAML dal provider di identità

Risoluzione

Causa

La causa principale è un timeout di navigazione che si verifica nel componente browser WebView2 incorporato durante il flusso di autenticazione SAML. In particolare, il timeout si verifica quando il browser WebView2 tenta di inviare la risposta SAML dal provider di identità all'endpoint Cisco SSE SAML ACS (Assertion Consumer Service). La condizione di timeout viene attivata dopo circa 30 secondi dal tentativo di completare questo passaggio della navigazione.

Il problema sembra essere correlato a condizioni di tempo o latenza di rete che ritardano l'elaborazione della risposta SAML, causando il superamento della soglia di timeout interna del componente WebView2. Il problema si verifica immediatamente dopo l'installazione di Cisco Secure Client e influisce sul flusso di lavoro dell'autenticazione SAML in modo specifico, mentre le altre funzionalità VPN rimangono invariate una volta completata l'autenticazione tramite i metodi di

soluzione.

Contenuto correlato

- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).