Erreurs de délai de navigation d'authentification SAML du client sécurisé Cisco pendant la connexion RAVPN

Table des matières

Problème

Les utilisateurs rencontrent des échecs de connexion RAVPN (Remote Access VPN) intermittents sous Windows à l'aide de Cisco Secure Client pendant l'authentification SAML. Les défaillances se produisent immédiatement après l'installation de Cisco Secure Client et se manifestent sous forme de messages d'erreur spécifiques affichés dans les boîtes de dialogue contextuelles :

- "L'authentification a échoué en raison du délai de navigation."
- "L'authentification a échoué en raison d'un problème de navigation vers l'URL d'authentification unique."

L'échec se produit après l'authentification du fournisseur d'identité (IdP) lorsque le navigateur WebView2 intégré tente de rediriger ou de publier la réponse SAML vers l'URL Cisco SSE SAML ACS. Il en résulte une condition de délai d'attente qui empêche l'accès VPN pour les utilisateurs affectés. Le problème a été observé affectant plusieurs utilisateurs dans la même organisation, avec un délai d'expiration du processus d'authentification d'environ 30 secondes après une tentative de navigation vers le point d'extrémité ACS SAML.

Les utilisateurs signalent que lorsque vous appuyez sur le bouton de connexion RAVPN pour établir la connexion VPN, la fenêtre contextuelle d'erreur de délai d'attente s'affiche et l'établissement RAVPN échoue. Le problème persiste même après le redémarrage du système d'exploitation.

Environnement

- Cisco Secure Client version 5.1.13.177 sous Windows

- authentification SAML configurée avec Cisco SSE ;
- Déploiement du VPN d'accès à distance (RAVPN)

Solution de contournement immédiate

Les solutions de contournement temporaires suivantes ont été confirmées pour résoudre le problème du délai de navigation :

1: Réinitialisation de la connectivité réseau

Déconnectez la connexion Wi-Fi et reconnectez-vous, puis essayez la connexion RAVPN plusieurs fois. Une fois le problème résolu, il ne se reproduit généralement pas même après le redémarrage du système d'exploitation.

2: Redémarrage du service RAVPN

Arrêtez et redémarrez manuellement le service RAVPN pour permettre les connexions suivantes.

3: Redémarrage du système

Redémarrez le système affecté pour réinitialiser l'état d'authentification.

Collecte des informations de diagnostic

Pour un dépannage complet, les informations de diagnostic suivantes doivent être collectées lors d'une défaillance active :

- Ensembles DART capturés lors d'un échec d'authentification
- Captures de paquets réseau (capture du trafic à l'aide de Wireshark sur toutes les cartes actives (ouverture de Wireshark - capture clic - options et utilisation de la touche Maj pour sélectionner plusieurs interfaces) pendant le processus d'authentification
- Suivis ETL Netsh

Procédure de collecte de la trace Netsh

- Ouvrez une fenêtre d'invite de commandes avec élévation de privilèges (Exécuter en tant qu'administrateur) sur le PC de test.
- Exécutez la commande : «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»
- Reproduisez le problème
- Une fois le problème reproduit, arrêtez la journalisation à l'aide de la commande : «netsh trace stop»

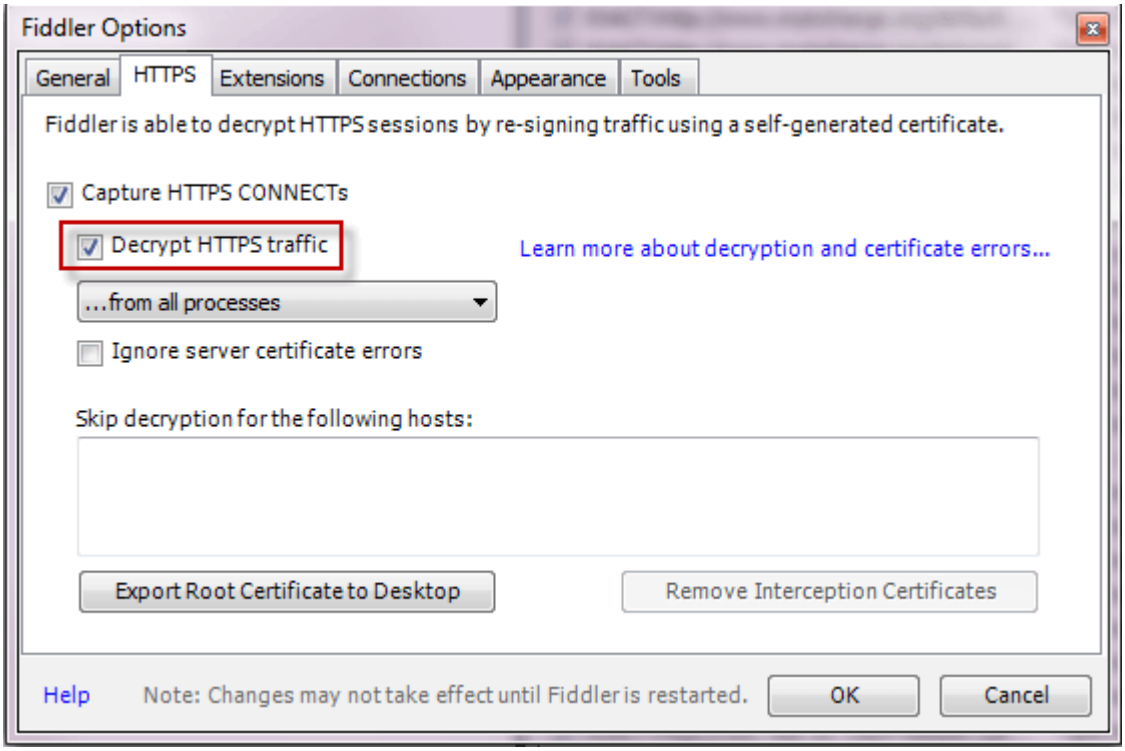
Collectez les journaux C:\file_NetTrace.etl

Traces violentes du trafic Web

1. Téléchargez la capture Fiddler à partir de ce lien https://www.telerik.com/download/fiddler-everywhere (utilisez la puce Intel (x86-64)
2. Installez-le sur une machine où le problème est reproductible.
3. Ouvrez l'application et activez le déchiffrement HTTPS

a. Cliquez sur Tools à Options à HTTPS.

b. Cochez la case Decrypt HTTPS Traffic.



image_en_ligne_0.png

4. Si vous obtenez le certificat à faire confiance, pls faites confiance à l'AC de fiddler et supprimez-le plus tard une fois que le problème est reproduit et

Deuxièmement, si vous rencontrez des problèmes avec la connectivité SSL lors du lancement, alors contournez le trafic de passerelle VPN (connect.ilemgroup.com) ou initiez la connectivité SAML basée sur IPsec (de préférence) de sorte qu'il n'est pas nécessaire de contourner le trafic de passerelle.

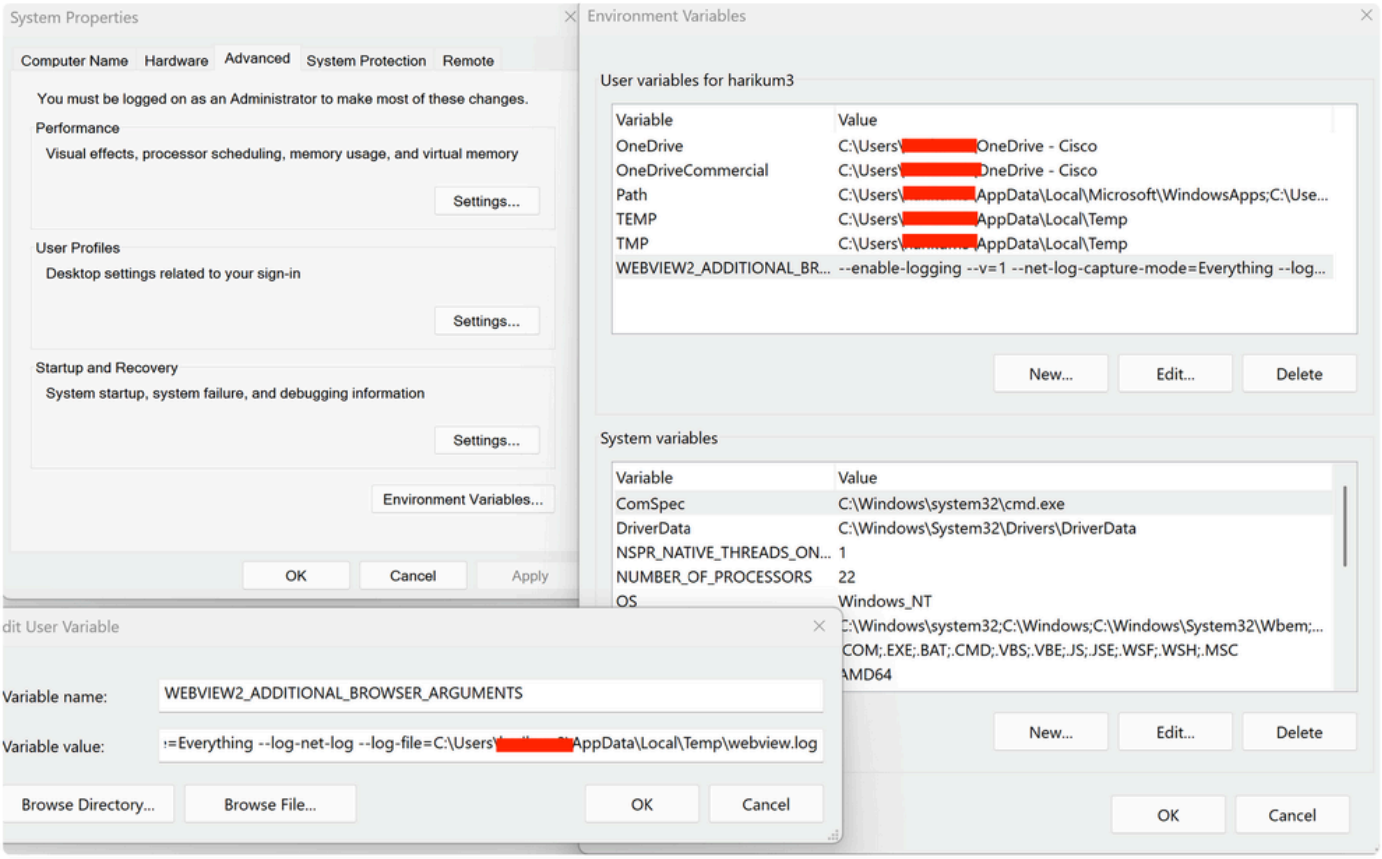
- Fermez toutes les applications inutiles et tous les processus en arrière-plan.
- Fermez et rouvrez l'outil, la collecte de données démarre automatiquement et de nouveaux enregistrements s'ajoutent au formulaire principal.
- Reproduisez le problème.
- Appuyez sur F12 pour arrêter le traçage.

Allez File à Save à All Sessions, puis enregistrez la trace dans un fichier .saz.

Journaux de Process Monitor - https://download.sysinternals.com/files/ProcessMonitor.zip

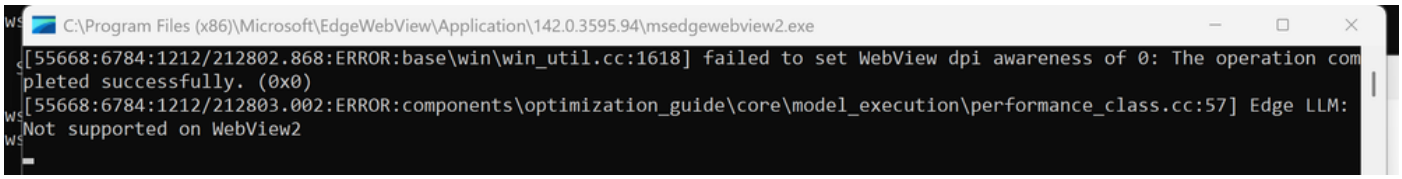
Journaux spécifiques à WebView2

Définition de la variable/valeur sur l'environnement utilisateur et système comme illustré ci-dessous



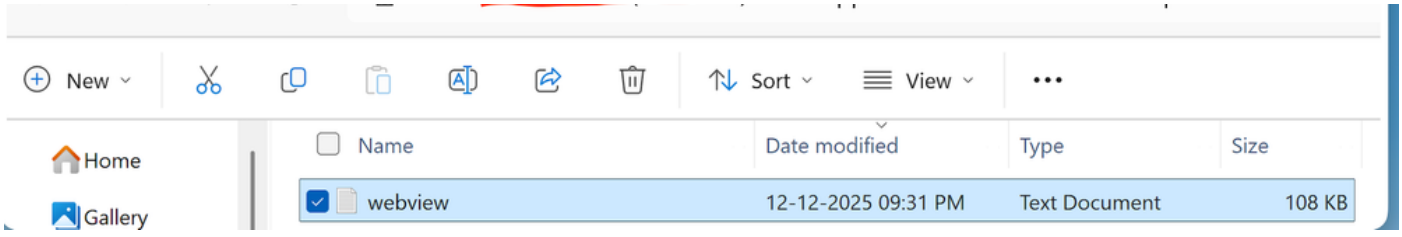
Capture d'écran_2026-05-12_at_9.43.19_AM.png

Lors du lancement du VPN, un niveau inférieur au terminal déclencherait



image_inline_1.png

C > Users > userid > Appdata > Local > Temp



image_en_ligne_2.png

Journaux de débogage SAML du fournisseur d'identité

Résolution

Motif

La cause principale est un dépassement du délai de navigation dans le composant de navigateur WebView2 intégré pendant le flux d'authentification SAML. Plus précisément, le délai d'attente se produit lorsque le navigateur WebView2 tente de publier la réponse SAML du fournisseur d'identité sur le point d'extrémité Cisco SSE SAML ACS (Assertion Consumer Service). La condition de délai d'attente est déclenchée après environ 30 secondes de tentative d'exécution de cette étape de navigation.

Le problème semble être lié à des conditions de temps ou de latence réseau qui retardent le traitement de la réponse SAML, entraînant le dépassement du seuil de délai d'attente interne du composant WebView2. Le problème se manifeste immédiatement après l'installation de Cisco Secure Client et affecte spécifiquement le workflow d'authentification SAML, tandis que les autres fonctionnalités VPN restent intactes une fois l'authentification terminée avec succès par les méthodes de contournement.

Autres informations utiles

- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.