Fehler beim Navigations-Timeout für die SAML-Authentifizierung des Cisco Secure Client während der RAVPN-Verbindung

Inhalt

Problem

Bei der SAML-Authentifizierung von Benutzern treten unter Windows mithilfe des Cisco Secure Client zeitweilig RAVPN-Verbindungsfehler (Remote Access VPN) auf. Die Fehler treten unmittelbar nach der Installation des Cisco Secure Client auf und werden in Popup-Dialogfeldern als spezifische Fehlermeldungen angezeigt:

- "Fehler bei der Authentifizierung aufgrund eines Navigations-Timeouts."
- "Fehler bei der Authentifizierung aufgrund eines Problems beim Navigieren zur URL für die einmalige Anmeldung."

Der Fehler tritt nach der Identity Provider (IdP)-Authentifizierung auf, wenn der eingebettete WebView2-Browser versucht, die SAML-Antwort an die Cisco SSE SAML ACS-URL umzuleiten oder bereitzustellen. Dies führt zu einer Zeitüberschreitung, die den VPN-Zugriff für betroffene Benutzer verhindert. Es wurde festgestellt, dass das Problem mehrere Benutzer in derselben Organisation betrifft, wobei der Authentifizierungsprozess ca. 30 Sekunden nach dem Versuch, zum SAML-ACS-Endpunkt zu navigieren, abgelaufen ist.

Benutzer berichten, dass beim Drücken der Taste für die RAVPN-Verbindung zum Herstellen der VPN-Verbindung das Popup-Fenster "Timeout Error" (Zeitüberschreitung) angezeigt wird und der RAVPN-Aufbau fehlschlägt. Das Problem besteht auch nach dem Neustart des Betriebssystems weiter.

Umwelt

- Cisco Secure Client Version 5.1.13.177 unter Windows

- Konfiguration der SAML-Authentifizierung mit Cisco SSE
- RAVPN-Bereitstellung (Remote Access VPN)

Sofortige Lösung

Die folgenden temporären Problemumgehungen wurden bestätigt, um das Problem mit dem Navigations-Timeout zu beheben:

1: Netzwerkverbindungen zurücksetzen

Trennen Sie die Wi-Fi-Verbindung, und stellen Sie sie erneut her. Versuchen Sie dann mehrmals, eine RAVPN-Verbindung herzustellen. Nach dem erfolgreichen Start tritt das Problem in der Regel nicht mehr auf, auch nicht nach einem Neustart des Betriebssystems.

2: Neustart des RAVPN-Diensts

Beenden Sie den RAVPN-Dienst manuell, und starten Sie ihn neu, damit nachfolgende erfolgreiche Verbindungen möglich sind.

3: Systemneustart

Starten Sie das betroffene System neu, um den Authentifizierungsstatus zurückzusetzen.

Sammlung von Diagnoseinformationen

Für eine umfassende Fehlerbehebung müssen die folgenden Diagnoseinformationen bei einem aktiven Fehler erfasst werden:

- DART-Pakete bei Authentifizierungsfehlern erfasst
- Netzwerkpaketerfassung (Erfassung des Datenverkehrs mit Wireshark auf allen aktiven Adaptern (Öffnen von Wireshark - Klicken Sie auf Erfassung - Optionen, und wählen Sie mit Shift mehrere Schnittstellen aus) während des Authentifizierungsprozesses
- Netsh ETL-Spuren

Verfahren zur Erfassung von Netsh-Ablaufverfolgung

- Öffnen Sie auf dem Test-PC ein Eingabeaufforderungsfenster mit erhöhten Rechten (Als Administrator ausführen).
- Führen Sie den folgenden Befehl aus: "netsh trace start ario=InternetClient traceFile=C:\file_NetTrace.etl maxSize=1000 provider=Microsoft-Windows-TCPIP provider=Microsoft-Windows-WinHttp capture=yes level=5 overwrite=yes"
- Reproduzieren des Problems
- Sobald das Problem reproduziert wurde, stoppen Sie die Protokollierung mit folgendem Befehl: "netsh trace stop"

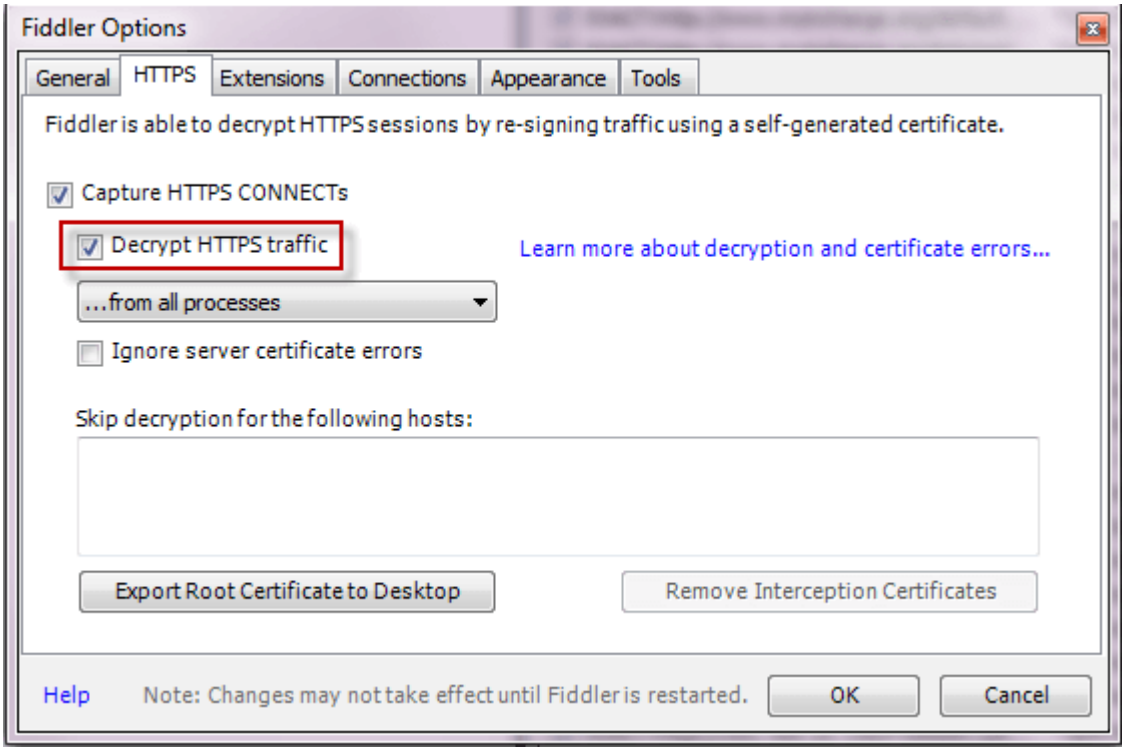
Sammeln Sie die Protokolle C:\file_NetTrace.etl

Fiddler-Spuren von Web-Datenverkehr

1. Laden Sie Fiddler Capture von diesem Link herunter https://www.telerik.com/download/fiddler-everywhere (verwenden Sie den Intel Chip (x86-64))
2. Installieren Sie es auf einem Computer, auf dem das Problem reproduzierbar ist.
3. Öffnen Sie die Anwendung, und aktivieren Sie die HTTPS-Entschlüsselung.

a. Klicken Sie auf Extras und Optionen und dann auf HTTPS.

b. Klicken Sie auf das Feld HTTPS-Datenverkehr entschlüsseln.



inline_image_0,png

4. Wenn Sie das Zertifikat als vertrauenswürdig einstufen, vertrauen Sie der CA aus dem Fiddler, und löschen Sie sie später, nachdem das Problem reproduziert wurde, und

Wenn beim Starten Probleme mit der SSL-Verbindung auftreten, umgehen Sie den VPN-Gateway-Datenverkehr (connect.ilemgroup.com) oder initiieren Sie eine IPsec-basierte SAML-Verbindung (am besten), sodass kein Gateway-Datenverkehr umgangen werden muss.

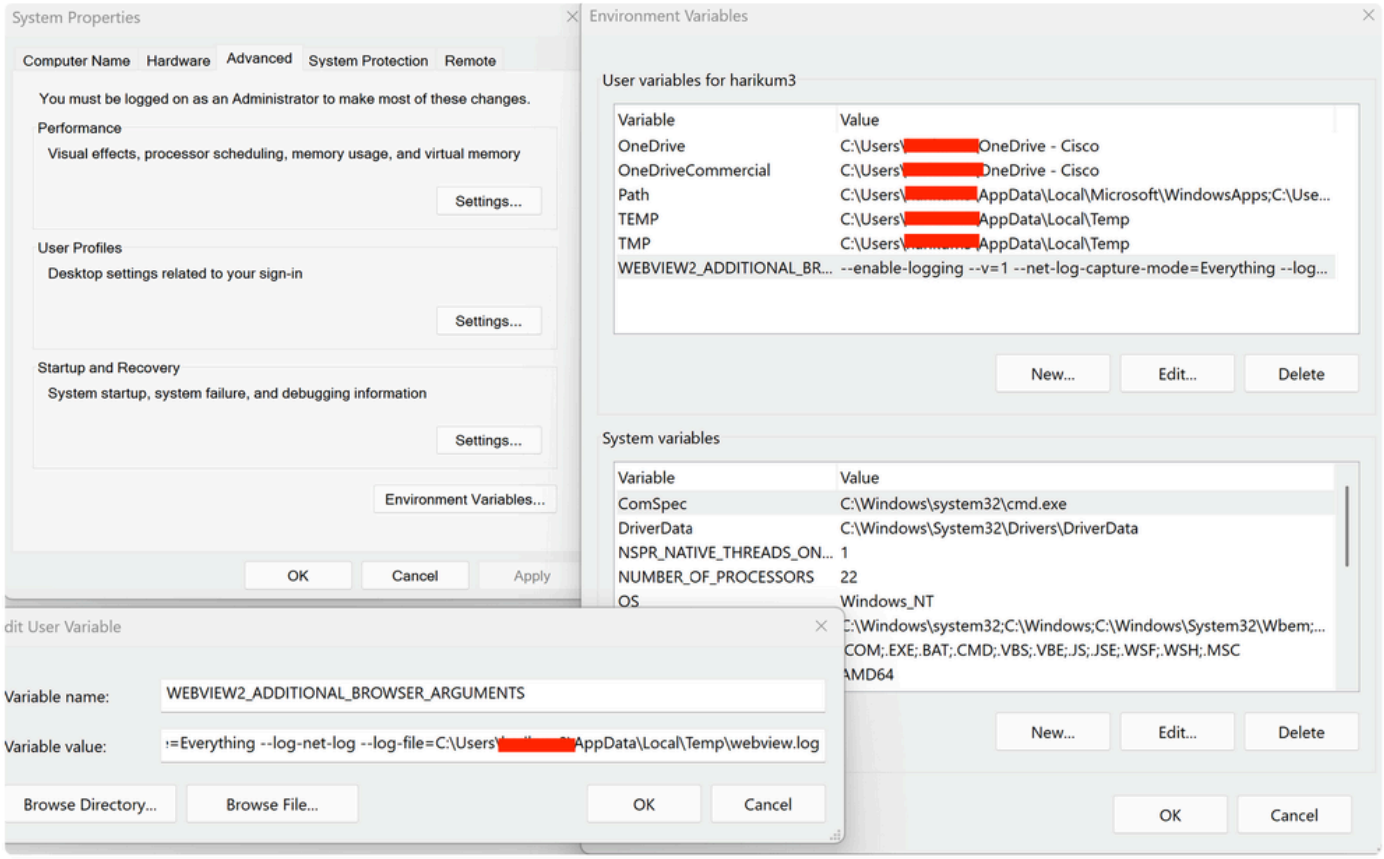
- Schließen Sie alle nicht benötigten Anwendungen und Hintergrundprozesse.
- Schließen und öffnen Sie das Tool erneut. Die Datenerfassung wird automatisch gestartet, und Sie sehen neue Datensätze, die zum Hauptformular hinzugefügt werden.
- Reproduzieren des Problems
- Drücken Sie F12, um die Ablaufverfolgung zu beenden.

Gehen Sie File à Save à All Sessions, und speichern Sie die Ablaufverfolgung in einer .saz-Datei.

Prozessüberwachungsprotokolle - https://download.sysinternals.com/files/ProcessMonitor.zip

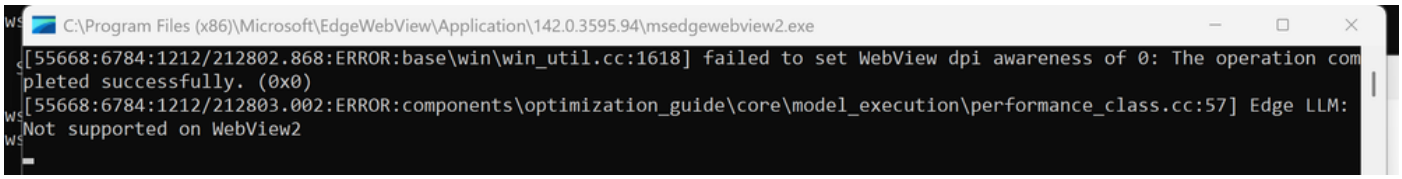
WebView2-spezifische Protokolle

Festlegen von Variablen/Werten für die Benutzer- und Systemumgebung wie unten beschrieben



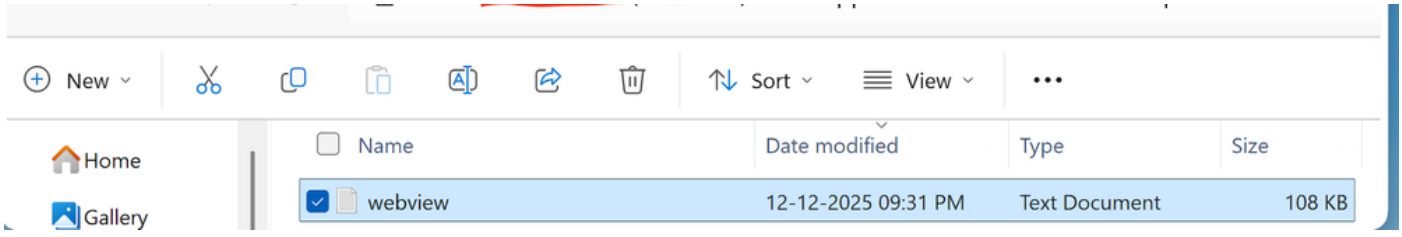
Screenshot_2026-05-12_at_9.43.19_AM.png

Beim Initiieren des VPN löst das folgende Terminal aus:



inline_image_1.png

C > Benutzer > Benutzer-ID > Anwendungsdaten > Lokal > Temp



inline_image_2.png

SAML-Debug-Protokolle vom Identitätsanbieter

Auflösung

Ursache

Die Hauptursache ist ein Navigations-Timeout, das in der eingebetteten WebView2-Browserkomponente während des SAML-Authentifizierungsflusses auftritt. Der Timeout tritt insbesondere auf, wenn der WebView2-Browser versucht, die SAML-Antwort vom Identitätsanbieter an den Endpunkt des Cisco SSE SAML ACS (Assertion Consumer Service) zu senden. Die Zeitüberschreitungsbedingung wird nach ca. 30 Sekunden des Versuchs ausgelöst, diesen Navigationsschritt abzuschließen.

Das Problem scheint mit dem Timing oder den Netzwerklatenzbedingungen zu zusammenhängen, die die SAML-Antwortverarbeitung verzögern, wodurch die WebView2-Komponente ihren internen Timeout-Grenzwert überschreitet. Das Problem tritt unmittelbar nach der Installation des Cisco Secure Client auf und betrifft speziell den SAML-Authentifizierungs-Workflow, während andere VPN-Funktionen intakt bleiben, sobald die Authentifizierung mithilfe der Workaround-Methoden erfolgreich abgeschlossen wurde.

Verwandte Inhalte

- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.