Erros de Tempo Limite de Navegação de Autenticação SAML do Cisco Secure Client durante a Conexão RAVPN

Contents

Problema

Os usuários experimentam falhas intermitentes de conexão de VPN de Acesso Remoto (RAVPN - Remote Access VPN) no Windows usando o Cisco Secure Client durante a autenticação SAML. As falhas ocorrem imediatamente após a instalação do Cisco Secure Client e manifestam-se como mensagens de erro específicas exibidas em caixas de diálogo pop-up:

- "Falha na autenticação devido ao tempo limite de navegação."
- "Falha na autenticação devido a um problema na navegação para a URL de logon único."

A falha ocorre após a autenticação do Identity Provider (IdP) quando o navegador WebView2 incorporado tenta redirecionar ou postar a resposta SAML para o URL do ACS SAML do Cisco SSE. Isso resulta em uma condição de tempo limite que impede o acesso VPN para os usuários afetados. O problema foi observado afetando vários usuários na mesma organização, com o tempo limite do processo de autenticação aproximadamente 30 segundos após a tentativa de navegar para o ponto de extremidade ACS SAML.

Os usuários relatam que ao pressionar o botão de conexão RAVPN para estabelecer a conexão VPN, o pop-up de erro de timeout é exibido e o estabelecimento de RAVPN falha. O problema persiste mesmo após a reinicialização do sistema operacional.

Ambiente

- Cisco Secure Client versão 5.1.13.177 no Windows
- Autenticação SAML configurada com Cisco SSE

- Implantação de VPN de acesso remoto (RAVPN)

Solução imediata

As seguintes soluções temporárias foram confirmadas para resolver o problema de tempo limite de navegação:

1: Redefinição de Conectividade de Rede

Desconecte a conexão Wi-Fi, reconecte e depois tente a conexão RAVPN várias vezes. Uma vez bem-sucedido, o problema normalmente não se repete mesmo após a reinicialização do sistema operacional.

2: Reinicialização do Serviço RAVPN

Interrompa e reinicie manualmente o serviço RAVPN para permitir conexões bem-sucedidas subsequentes.

3: Reinicialização do sistema

Reinicie o sistema afetado para redefinir o estado de autenticação.

Coleta de Informações de Diagnóstico

Para uma solução de problemas abrangente, as seguintes informações de diagnóstico devem ser coletadas durante uma falha ativa:

- Pacotes DART capturados durante falha de autenticação
- Capturas de pacotes de rede (capture o tráfego usando o Wireshark em todos os Adaptadores Ativos (abra o Wireshark - clique em capture - opções e use Shift para selecionar várias interfaces) durante o processo de autenticação
- Rastreamentos ETL Netsh

Procedimento para coletar rastreamento Netsh

- Abra uma janela do prompt de comando elevado (Executar como administrador) no PC de teste.
- Execute o comando: "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"
- Reproduza o problema
- Quando o problema for reproduzido, pare o registro usando o comando: "netsh trace stop"

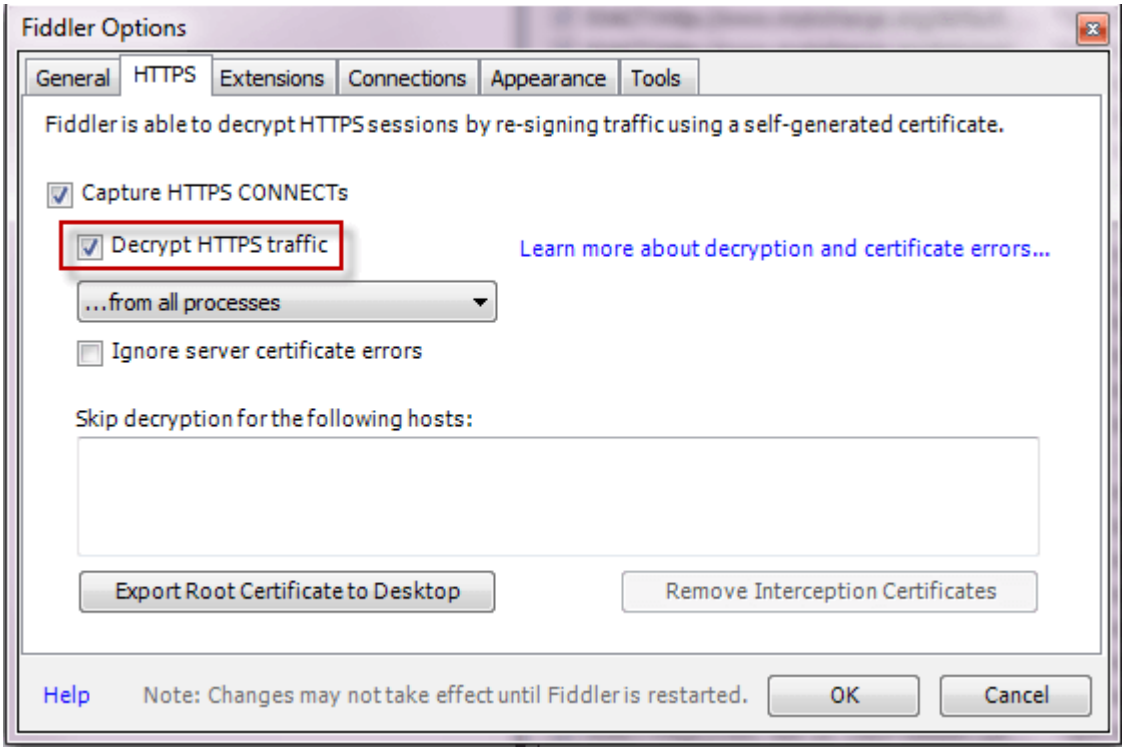
Coletar os logs C:\file_NetTrace.etl

Rastreamentos de fiddler do tráfego da Web

1. Descarregue a captura do alimentador deste link https://www.telerik.com/download/fiddler-everywhere (use o chip Intel (x86-64)
2. Instale-o em uma máquina onde o problema possa ser reproduzido.
3. Abrir o aplicativo e habilitar a descriptografia HTTPS

a. Clique em Ferramentas à Opções à HTTPS.

b. Clique na caixa Decrypt HTTPS Traffic.



inline_image_0.png

4. Se o certificado for confiável, confie no CA do violador e exclua-o depois que o problema for reproduzido e

Em segundo lugar, se você encontrar qualquer problema com a conectividade SSL durante a inicialização, ignore o tráfego do gateway VPN (connect.ilemgroup.com) ou inicie a conectividade SAML baseada em IPsec (mais preferível) para que não haja necessidade de ignorar nenhum tráfego de gateway.

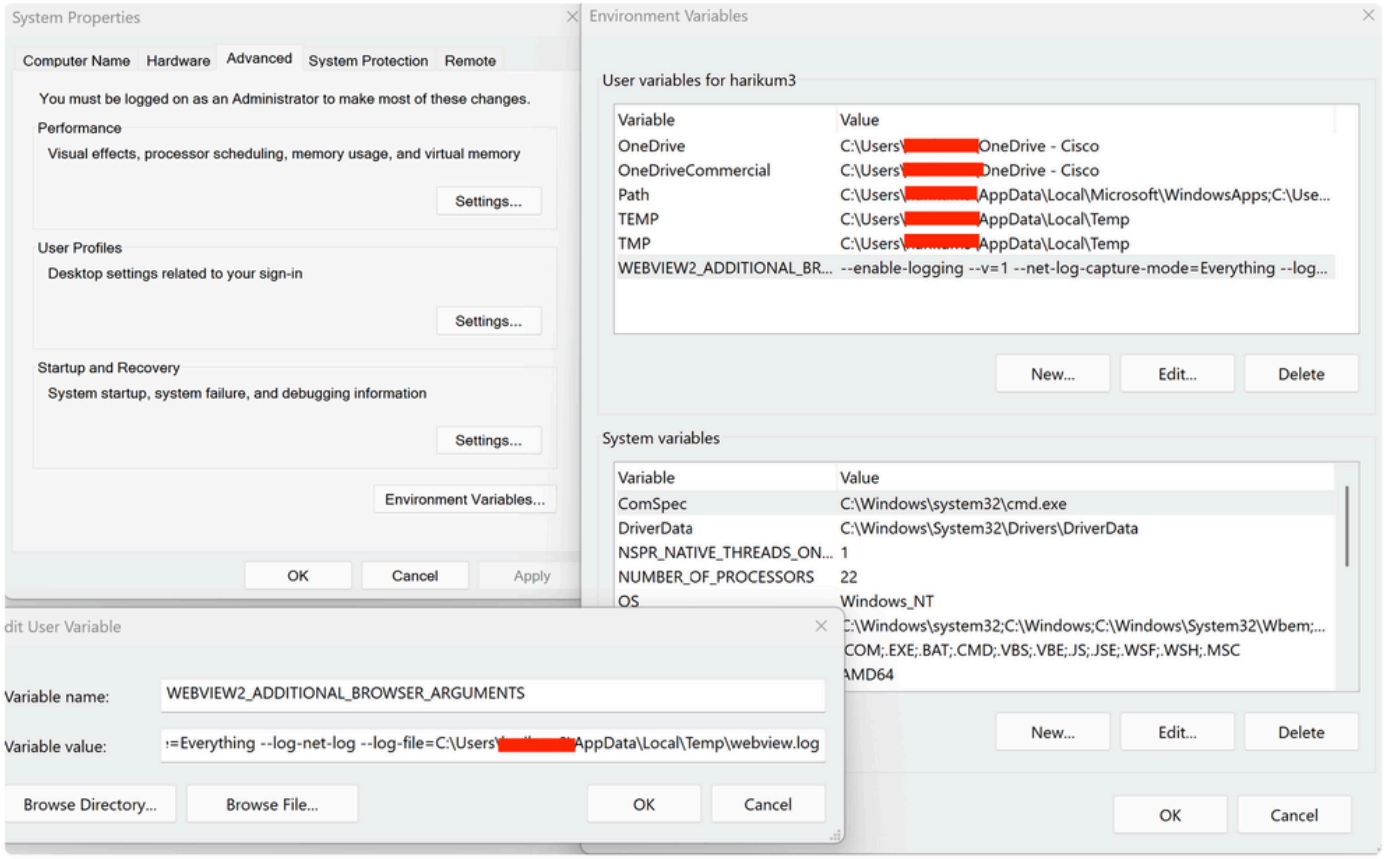
- Feche todos os aplicativos desnecessários e processos em segundo plano.
- Feche e reabra a ferramenta, a coleta de dados é iniciada automaticamente e você verá novos registros sendo adicionados ao formulário principal.
- Reproduza o problema.
- Pressione F12 para parar o rastreamento.

Vá para File à Save à All Sessions e salve o rastreamento em um arquivo .saz.

Registros do monitor de processos - https://download.sysinternals.com/files/ProcessMonitor.zip

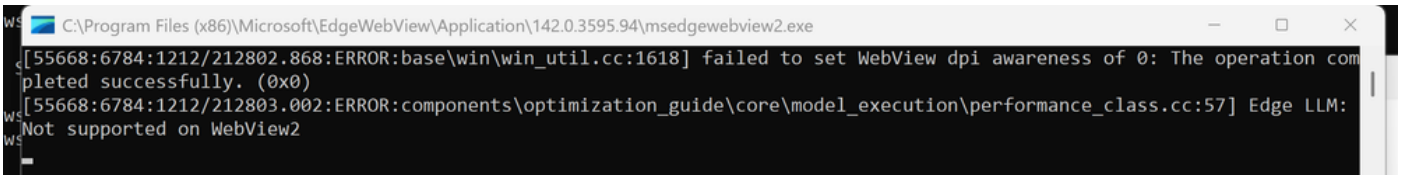
Logs específicos do WebView2

Definindo variável/valor no ambiente do usuário e do sistema conforme definido abaixo



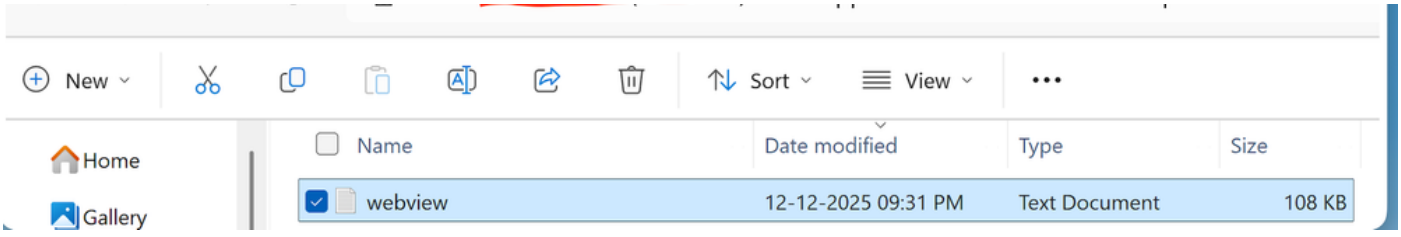
Screenshot_2026-05-12_at_9.43.19_AM.png

Ao iniciar a VPN, o terminal abaixo dispararia



inline_image_1.png

C > Usuários > ID do usuário > Appdata > Local > Temp



inline_image_2.png

Logs de depuração SAML do provedor de identidade

Resolução

Causa

A causa raiz é um tempo limite de navegação que ocorre no componente do navegador WebView2 incorporado durante o fluxo de autenticação SAML. Especificamente, o tempo limite ocorre quando o navegador WebView2 tenta publicar a resposta SAML do provedor de identidade no ponto final ACS (Assertion Consumer Service) do Cisco SSE SAML. A condição de tempo limite é acionada após aproximadamente 30 segundos da tentativa de concluir essa etapa de navegação.

O problema parece estar relacionado à temporização ou às condições de latência da rede que atrasam o processamento da resposta SAML, fazendo com que o componente WebView2 exceda seu limite de tempo interno. O problema se manifesta imediatamente após a instalação do Cisco Secure Client e afeta especificamente o fluxo de trabalho de autenticação SAML, enquanto outra funcionalidade de VPN permanece intacta quando a autenticação é concluída com sucesso através dos métodos de solução.

Conteúdo relacionado

- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.