Erro de falha na verificação de pré-login de CSD do Hostscan no cliente seguro

Contents

Problema

Um usuário encontra a mensagem de erro "Falha na verificação de pré-login do Hostscan CSD" ao tentar se conectar a uma VPN usando o Cisco Secure Client em um dispositivo Windows 11. O erro ocorre antes que o prompt de login seja exibido, impedindo que o usuário acesse a conexão VPN. O mesmo usuário pode se conectar com êxito à VPN de outro dispositivo usando credenciais e perfil de VPN idênticos, indicando que o problema é específico do dispositivo, em vez de relacionado à credencial.

Entradas adicionais de log de erros observadas incluem:

- CONNECTIFC_ERROR_FILE_OPEN_FAILED (Código de Retorno: -30015466 / 0xFE360016)
- Falha no processamento do HostScan
- Falha na tentativa de conexão devido a um problema na rede ou no PC

O usuário conseguiu se conectar a outros perfis VPN onde a postura não estava habilitada, mas não pôde se conectar a perfis onde a postura estava habilitada. A instalação estava funcionando anteriormente sem alterações conhecidas feitas na configuração.

Ambiente

- Cisco Secure Client versão 5.1.7.80
- Sistema operacional: Windows 11
- Perfil de VPN com postura habilitada

- O problema é específico ao dispositivo, afetando somente um usuário em um dispositivo específico
- Relacionado ao ID de bug da Cisco: CSCwk54713

Resolução

A resolução envolve a execução de uma desinstalação completa e limpa do Cisco Secure Client e a reinstalação do software. Os métodos padrão de desinstalação e reinstalação nem sempre resolvem o problema devido a entradas de registro corrompidas ou arquivos residuais.

Passo 1: Desabilitar Serviços de Terceiros

Desative todos os serviços de terceiros no Msconfig, incluindo serviços proxy, se disponíveis, e mantenha ativos apenas os módulos do Cisco Secure Client.

Passo 2: Limpar desinstalação usando a ferramenta da Microsoft

Use a ferramenta de solução de problemas Microsoft Program Install and Uninstall para remover todos os módulos Cisco do dispositivo afetado. Esta ferramenta oferece uma desinstalação mais completa do que os métodos de desinstalação padrão do Windows.

Corrija problemas que bloqueiem a instalação ou a remoção de programas.

Passo 3: Limpeza manual de arquivos

Após a desinstalação, verifique e exclua manualmente todas as pastas, arquivos, executáveis e arquivos DLL restantes dos seguintes diretórios:

```
C:\Program Files (x86)\Cisco
C:\ProgramData\Cisco\
C:\Users\<current user>\AppData\Local\Cisco
```

Remova todos os arquivos e pastas residuais encontrados nesses locais, pois eles nem sempre permanecem mesmo após o processo de desinstalação.

Passo 4: Limpeza do Registro

Verifique os caminhos do registro para qualquer entrada antiga do Cisco Secure Client e remova-as, se houver:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco
HKEY_LOCAL_MACHINE\Software\WOW6432node\Cisco
```

Passo 5: Ativar log de depuração (opcional)

Se for necessária uma solução de problemas adicional, habilite o log de Curl copiando o arquivo debuglogconfig.json:

```
{
"web_helper" : 3,
"vpn_ipsec_ikev2" : 3,
"vpn_curl" : 3,
"vpn_state" : 3
}
```

neste diretório:

```
C:\ProgramData\Cisco\Cisco Secure Client
```

Passo 6: Reinicialização do sistema

Reinicialize o endpoint para garantir que todas as alterações tenham efeito e limpe todos os processos restantes ou bloqueios de registro.

Passo 7: Reinstale o Cisco Secure Client

Instale o pacote de pré-implantação do Cisco Secure Client ou permita a instalação automática por meio de ferramentas de gerenciamento, como o Intune. Verifique se a instalação foi bem-sucedida antes de continuar.

Passo 8: Testar conexão VPN

Tente se conectar ao perfil VPN que estava falhando anteriormente. Se o problema persistir, gere um novo pacote DART para análise posterior.

⚠ Caution: Possível. Os detalhes mencionados aqui parecem conter procedimentos ou comandos que poderiam causar um impacto significativo se executados. Verifique se esses procedimentos ou comandos foram avaliados por um SME ou Unidade de negócios antes de executar ou recomendar.

Causa

O problema é causado por entradas de registro corrompidas ou interferência de software de terceiros que impede que as bibliotecas e execuções do Hostscan iniciem ou atualizem corretamente. Essa corrupção afeta o processo de verificação de pré-login do CSD (Cisco Security Desktop), que é necessário para perfis de VPN com postura habilitada. A corrupção geralmente ocorre no nível do dispositivo, explicando por que o mesmo usuário pode se conectar com êxito de outros dispositivos. Os métodos de desinstalação padrão nem sempre removem todos os componentes corrompidos, exigindo a limpeza manual de arquivos e entradas de registro.

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.