Hostscan CSD-verificatie vooraf is mislukt Fout in beveiligde client

Inhoud

uitgeven

Een gebruiker krijgt de foutmelding "Hostscan CSD prelogin verification failed" wanneer hij probeert verbinding te maken met een VPN met behulp van Cisco Secure Client op een Windows 11-apparaat. De fout treedt op voordat de aanmeldingsprompt wordt weergegeven, waardoor de gebruiker geen toegang heeft tot de VPN-verbinding. Dezelfde gebruiker kan met succes verbinding maken met de VPN vanaf een ander apparaat met behulp van identieke referenties en VPN-profiel, wat aangeeft dat het probleem apparaatspecifiek is in plaats van aanmeldingsgegevens.

Extra vermeldingen in het foutenlogboek die zijn waargenomen, zijn:

- CONNECT_ERROR_FILE_OPEN_FAILED (Retourcode: -30015466 / 0xFE360016)
- Verwerking HostScan mislukt
- Verbindingspoging is mislukt vanwege een netwerk- of pc-probleem

De gebruiker kon verbinding maken met andere VPN-profielen waarvoor posturing niet was ingeschakeld, maar kon geen verbinding maken met profielen waarvoor posturing was ingeschakeld. De installatie werkte eerder zonder bekende wijzigingen in de configuratie.

milieu

- Cisco Secure Client versie 5.1.7.80
- Besturingssysteem: Windows 11
- VPN-profiel met instelling ingeschakeld

- Probleem is apparaatspecifiek en treft slechts één gebruiker op één bepaald apparaat
- Gerelateerd aan Cisco Bug ID: CSCwk54713

resolutie

De oplossing houdt in dat de installatie van Cisco Secure Client volledig wordt gewist en dat de software opnieuw wordt geïnstalleerd. Standaard verwijderings- en herinstallatiemethoden lossen het probleem niet altijd op vanwege beschadigde registervermeldingen of resterende bestanden.

Stap 1: Services van derden uitschakelen

Schakel alle services van derden in Msconfig uit, inclusief proxyservices indien beschikbaar, en houd alleen Cisco Secure Client-modules actief.

Stap 2: Reinig de installatie met behulp van Microsoft Tool

Gebruik het hulpprogramma Microsoft Program Install and Uninstall Troubleshooter om alle Cisco-modules van het betreffende apparaat te verwijderen. Deze tool biedt een grondiger verwijdering dan standaard Windows-verwijderingsmethoden.

Problemen oplossen die voorkomen dat programma's worden geïnstalleerd of verwijderd.

Stap 3: Handmatig bestanden opschonen

Nadat u de installatie ongedaan hebt gemaakt, controleert en verwijdert u handmatig alle resterende Cisco-mappen, bestanden, uitvoerbare bestanden en DLL-bestanden uit deze mappen:

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

Verwijder alle resterende bestanden en mappen gevonden in deze locaties, omdat ze niet altijd blijven, zelfs na het verwijderingsproces.

Stap 4: Opschonen van het register

Controleer deze registerpaden voor oude Cisco Secure Client-vermeldingen en verwijder deze indien aanwezig:

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

Stap 5: Debug Logging inschakelen (optioneel)

Als er meer problemen moeten worden opgelost, schakelt u Curl-logboekregistratie in door het bestand debuglogconfig.json te kopiëren:

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

in deze directory:

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

Stap 6: Systeem opnieuw opstarten

Start het eindpunt opnieuw op om ervoor te zorgen dat alle wijzigingen van kracht worden en alle resterende processen of registervergrendelingen worden gewist.

Stap 7: Cisco Secure Client opnieuw installeren

Installeer het pre-implementatiepakket van Cisco Secure Client of sta automatische installatie toe via beheertools zoals Intune. Controleer of de installatie geslaagd is voordat u verdergaat.

Stap 8: VPN-verbinding testen

Probeer verbinding te maken met het VPN-profiel dat eerder niet werkte. Als het probleem zich blijft voordoen, genereert u een nieuwe DART-bundel voor verdere analyse.

⚠ Let op: mogelijk. De hier genoemde details lijken procedures of opdrachten te bevatten die aanzienlijke gevolgen kunnen hebben als ze worden uitgevoerd. Zorg ervoor dat deze procedures of opdrachten zijn geëvalueerd door een kmo of bedrijfseenheid voordat u deze uitvoert of aanbeveelt.

Oorzaak

Het probleem wordt veroorzaakt door beschadigde registervermeldingen of interferentie van software van derden die voorkomt dat Hostscan-bibliotheken en -uitvoeringen correct worden gestart of bijgewerkt. Deze beschadiging heeft invloed op het CSD-proces (Cisco Security Desktop) voor de verificatie van de aanmelding, dat vereist is voor VPN-profielen waarvoor posturing is ingeschakeld. De beschadiging treedt meestal op apparaatniveau op en verklaart waarom dezelfde gebruiker met succes verbinding kan maken vanaf andere apparaten. Standaard verwijderingsmethoden verwijderen niet altijd alle beschadigde componenten, waardoor het handmatig opschonen van bestanden en registervermeldingen vereist is.

Verwante inhoud

- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.