Verifica pre-accesso CSD Hostscan non riuscita in client protetto

Sommario

Problema

Un utente rileva il messaggio di errore "Hostscan CSD: verifica pre-accesso non riuscita" quando tenta di connettersi a una VPN utilizzando Cisco Secure Client su un dispositivo Windows 11. L'errore si verifica prima della visualizzazione del prompt di accesso, impedendo all'utente di accedere alla connessione VPN. Lo stesso utente può connettersi correttamente alla VPN da un altro dispositivo utilizzando credenziali e profilo VPN identici, indicando che il problema è specifico del dispositivo anziché relativo alle credenziali.

Altre voci del log degli errori osservate includono:

- CONNECTIFC_ERROR_FILE_OPEN_FAILED (Codice restituito: -30015466 / 0xFE360016)
- Elaborazione di HostScan non riuscita
- Tentativo di connessione non riuscito a causa di un problema di rete o del PC

L'utente è riuscito a connettersi ad altri profili VPN in cui la postura non è abilitata, ma non è riuscito a connettersi ai profili in cui la postura è abilitata. L'installazione era già stata eseguita in precedenza senza apportare modifiche note alla configurazione.

Ambiente

- Cisco Secure Client versione 5.1.7.80
- Sistema operativo: Windows 11
- Profilo VPN con postura abilitata
- Il problema è specifico del dispositivo e interessa un solo utente su un determinato

dispositivo

- ID bug Cisco: CSCwk54713

Risoluzione

La risoluzione implica la disinstallazione completa e pulita di Cisco Secure Client e la reinstallazione del software. I metodi standard di disinstallazione e reinstallazione non sempre risolvono il problema a causa di voci del Registro di sistema danneggiate o file residui.

Passaggio 1: Disabilita servizi di terze parti

Disabilitare tutti i servizi di terze parti in Msconfig, inclusi i servizi proxy, se disponibili, e mantenere attivi solo i moduli Cisco Secure Client.

Passaggio 2: Pulisci disinstallazione con Microsoft Tool

Utilizzare lo strumento Risoluzione dei problemi di installazione e disinstallazione del programma Microsoft per rimuovere tutti i moduli Cisco dal dispositivo interessato. Questo strumento offre una disinstallazione più completa rispetto ai metodi di disinstallazione standard di Windows.

Risolvere i problemi che impediscono l'installazione o la rimozione di programmi.

Passaggio 3: Pulizia manuale file

Dopo la disinstallazione, controllare ed eliminare manualmente le cartelle, i file, gli eseguibili e i file DLL Cisco rimanenti dalle seguenti directory:

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

Rimuovere tutti i file e le cartelle che si trovano in questi percorsi, in quanto non rimangono sempre anche dopo la disinstallazione.

Passaggio 4: Pulizia Registro di sistema

Verificare in questo registro la presenza di eventuali voci Cisco Secure Client precedenti e rimuoverle, se presenti:

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

Passaggio 5: Abilita registrazione debug (facoltativo)

Se è necessario eseguire ulteriori operazioni di risoluzione dei problemi, abilitare la registrazione dei cursori copiando il file debuglogconfig.json:

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

in questa directory:

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

Passaggio 6: Riavvio del sistema

Riavviare l'endpoint per assicurarsi che tutte le modifiche abbiano effetto e cancellare eventuali processi o blocchi del Registro di sistema rimanenti.

Passaggio 7: Reinstalla Cisco Secure Client

Installare il pacchetto pre-distribuzione di Cisco Secure Client o consentire l'installazione automatica tramite strumenti di gestione come Intune. Verificare che l'installazione sia stata completata correttamente prima di procedere.

Passaggio 8: Test connessione VPN

Tentativo di connessione al profilo VPN precedentemente non riuscito. Se il problema persiste, generare un nuovo bundle DART per ulteriori analisi.

⚠ Attenzione: Possibile. I dettagli menzionati contengono procedure o comandi che potrebbero avere un impatto significativo se eseguiti. Assicurarsi che queste procedure o comandi siano stati valutati da uno SME o da una Business Unit prima di eseguire o consigliare.

Causa

Il problema è causato da voci del Registro di sistema danneggiate o da interferenze di software di terze parti che impediscono alle librerie Hostscan e alle esecuzioni di avviarsi o aggiornare correttamente. Questo danneggiamento influisce sul processo di verifica pre-accesso di CSD (Cisco Security Desktop), necessario per i profili VPN con postura abilitata. Il danneggiamento si verifica in genere a livello di dispositivo e spiega perché lo stesso utente può connettersi correttamente da altri dispositivi. I metodi di disinstallazione standard non sempre rimuovono tutti i componenti danneggiati, richiedendo la pulizia manuale dei file e delle voci del Registro di sistema.

Contenuto correlato

- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).