Fehler bei der Hostscan-CSD-Voranmeldungsprüfung im sicheren Client.

Inhalt

Problem

Ein Benutzer erhält die Fehlermeldung "Host Scan CSD Prelogin Verification failed" (Host-CSD-Vorabanmeldung fehlgeschlagen), wenn er versucht, über den Cisco Secure Client auf einem Windows 11-Gerät eine Verbindung zu einem VPN herzustellen. Der Fehler tritt auf, bevor die Anmeldeaufforderung angezeigt wird, sodass der Benutzer nicht auf die VPN-Verbindung zugreifen kann. Derselbe Benutzer kann sich mit identischen Anmeldeinformationen und VPN-Profilen erfolgreich von einem anderen Gerät aus mit dem VPN verbinden. Dies weist darauf hin, dass das Problem eher gerätespezifisch als anmeldeinformationsbezogen ist.

Zu den weiteren beobachteten Fehlerprotokolleinträgen gehören:

- CONNECTIFC_ERROR_FILE_OPEN_FAILED (Rückgabecode: -30015466/0xFE360016)
- HostScan-Verarbeitung fehlgeschlagen
- Verbindungsversuch schlug aufgrund eines Netzwerk- oder PC-Problems fehl

Der Benutzer konnte eine Verbindung zu anderen VPN-Profilen herstellen, bei denen das Posturing nicht aktiviert war, konnte jedoch keine Verbindung zu Profilen herstellen, bei denen das Posturing aktiviert war. Das Setup hat zuvor funktioniert, ohne dass Änderungen an der Konfiguration vorgenommen wurden.

Umwelt

- Cisco Secure Client Version 5.1.7.80
- Betriebssystem: Windows 11
- VPN-Profil mit aktiviertem Posturing

- Das Problem ist gerätespezifisch und betrifft nur einen Benutzer auf einem bestimmten Gerät
- Im Zusammenhang mit der Cisco Bug-ID: CSCwk54713

Auflösung

Die Lösung besteht darin, Cisco Secure Client vollständig zu deinstallieren und die Software neu zu installieren. Die Standarddeinstallations- und Neuinstallationsmethoden lösen das Problem nicht immer, da Registrierungseinträge oder Restdateien beschädigt sind.

Schritt 1: Deaktivieren von Drittanbieterdiensten

Deaktivieren Sie alle Drittanbieterdienste in Msconfig, einschließlich der Proxydienste, falls verfügbar, und aktivieren Sie nur die Cisco Secure Client-Module.

Phase 2: Deinstallation mit Microsoft-Tool löschen

Entfernen Sie alle Cisco Module vom betroffenen Gerät mithilfe des Troubleshooter-Tools zur Installation und Deinstallation des Microsoft-Programms. Dieses Tool bietet eine gründlichere Deinstallation als die üblichen Windows-Deinstallationsmethoden.

Beheben Sie Probleme, die verhindern, dass Programme installiert oder entfernt werden.

Schritt 3: Manuelle Dateibereinigung

Überprüfen und löschen Sie nach der Deinstallation manuell alle verbleibenden Cisco Ordner, Dateien, ausführbaren Dateien und DLL-Dateien aus den folgenden Verzeichnissen:

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

Entfernen Sie alle verbleibenden Dateien und Ordner, die an diesen Speicherorten gefunden wurden, da sie auch nach der Deinstallation nicht immer erhalten bleiben.

Schritt 4: Bereinigung der Registrierung

Überprüfen Sie diesen Registrierungspfad auf alle alten Cisco Secure Client-Einträge, und entfernen Sie ihn, sofern vorhanden:

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

Schritt 5: Debug-Protokollierung aktivieren (optional)

Wenn weitere Fehlerbehebungen erforderlich sind, aktivieren Sie die Curl-Protokollierung, indem Sie die Datei debuglogconfig.json kopieren:

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

in dieses Verzeichnis:

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

Schritt 6: Systemneustart

Starten Sie den Endpunkt neu, um sicherzustellen, dass alle Änderungen wirksam werden, und löschen Sie alle verbleibenden Prozesse oder Registrierungssperren.

Schritt 7: Neuinstallation von Cisco Secure Client

Installieren Sie das Cisco Secure Client-Paket vor der Bereitstellung, oder ermöglichen Sie eine automatische Installation über Verwaltungstools wie Intune. Überprüfen Sie die erfolgreiche Installation, bevor Sie fortfahren.

Schritt 8: VPN-Verbindung testen

Versuchen Sie, eine Verbindung mit dem VPN-Profil herzustellen, das zuvor fehlerhaft war. Wenn das Problem weiterhin besteht, erstellen Sie ein neues DART-Paket zur weiteren Analyse.

⚠ Vorsicht: Möglich. Die hier genannten Details enthalten offenbar Prozeduren oder Befehle, die bei ihrer Ausführung erhebliche Auswirkungen haben könnten. Stellen Sie sicher, dass diese Verfahren oder Befehle von einem SME oder einer Business Unit evaluiert wurden, bevor Sie sie ausführen oder empfehlen.

Ursache

Das Problem wird durch beschädigte Registrierungseinträge oder Störungen durch Software von Drittanbietern verursacht, die Hostscan-Bibliotheken und -ausführungen daran hindert, ordnungsgemäß zu starten oder zu aktualisieren. Diese Beschädigung betrifft den CSD (Cisco Security Desktop)-Verifizierungsprozess vor der Anmeldung, der für VPN-Profile mit aktiviertem Posturing erforderlich ist. Die Beschädigung erfolgt in der Regel auf Geräteebene, was erklärt, warum ein Benutzer erfolgreich eine Verbindung von anderen Geräten herstellen kann. Bei Standarddeinstallationsmethoden werden nicht immer alle beschädigten Komponenten entfernt, sodass Dateien und Registrierungseinträge manuell bereinigt werden müssen.

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.