Hostscan CSD Prelogin Verification Failed Error in Secure Client

목차

문제

사용자가 Windows 11 디바이스에서 Cisco Secure Client를 사용하여 VPN에 연결을 시도할 때 "Hostscan CSD 사전 로그인 확인 실패" 오류 메시지가 나타납니다. 로그인 프롬프트가 표시되기 전에 오류가 발생하여 사용자가 VPN 연결에 액세스할 수 없습니다. 동일한 사용자가 동일한 자격 증명 및 VPN 프로파일을 사용하여 다른 디바이스에서 VPN에 성공적으로 연결할 수 있습니다. 이는 문제가 자격 증명과 관련이 아니라 디바이스별로 발생한다는 것을 의미합니다.

다음과 같은 오류 로그 항목이 추가로 발견됩니다.

- CONNECTIFC_ERROR_FILE_OPEN_FAILED(반환 코드: -30015466 / 0xFE360016)
- HostScan 처리 실패
- 네트워크 또는 PC 문제로 인해 연결 시도가 실패했습니다.

사용자는 Posture가 활성화되지 않은 다른 VPN 프로필에 연결할 수 있었지만 Posture가 활성화된 프로필에는 연결할 수 없었습니다. 이전에 컨피그레이션에 대해 알려진 변경 사항을 적용하지 않고 설치 프로그램이 작동했습니다.

환경

- Cisco Secure Client 버전 5.1.7.80
- 운영 체제: Windows 11
- VPN 프로파일(상태 설정 사용)
- 이 문제는 장치에 따라 다르며, 특정 장치에서 한 명의 사용자만 영향을 미칩니다.

- Cisco 버그 ID 관련: CSCw54713

해결

해결에는 Cisco Secure Client를 완전히 완전히 제거하고 소프트웨어를 다시 설치하는 작업이 포함됩니다. 표준 제거 및 재설치 방법으로는 손상된 레지스트리 항목 또는 잔여 파일로 인한 문제가 항상 해결되지 않습니다.

1단계: 서드파티 서비스 비활성화

사용 가능한 경우 프록시 서비스를 포함하여 Msconfig의 모든 타사 서비스를 비활성화하고 Cisco Secure Client 모듈만 활성 상태로 유지합니다.

2단계: Microsoft 도구를 사용하여 클린 제거

Microsoft Program Install and Uninstall Troubleshooter 툴을 사용하여 영향을 받는 디바이스에서 모든 Cisco 모듈을 제거합니다. 이 도구는 표준 Windows 제거 방법보다 더 철저한 제거를 제공합니다.

프로그램 설치 또는 제거를 차단하는 문제를 해결합니다.

3단계: 수동 파일 정리

제거한 후 다음 디렉터리에서 나머지 Cisco 폴더, 파일, 실행 파일 및 DLL 파일을 수동으로 확인하고 삭제합니다.

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

이러한 위치에서 발견된 나머지 파일과 폴더는 제거 프로세스 후에도 남아 있지 않으므로 제거합니다.

4단계: 레지스트리 정리

이 레지스트리 경로에서 이전 Cisco Secure Client 항목이 있는지 확인하고 있는 경우 제거합니다.

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

5단계: 디버그 로깅 사용(선택 사항)

추가 트러블슈팅이 필요한 경우 debuglogconfig.json 파일을 복사하여 Curl 로깅을 활성화합니다.

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

이 디렉터리로:

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

6단계: 시스템 재부팅

모든 변경 사항을 적용하고 나머지 프로세스 또는 레지스트리 잠금을 지우려면 엔드포인트를 재부

팅합니다.

7단계: Cisco Secure Client 재설치

Cisco Secure Client의 사전 구축 패키지를 설치하거나 Intune과 같은 관리 툴을 통해 자동 설치를 허용합니다. 계속하기 전에 성공적으로 설치되었는지 확인합니다.

8단계: VPN 연결 테스트

이전에 실패했던 VPN 프로필에 연결을 시도합니다. 문제가 계속되면 추가 분석을 위해 새 DART 번들을 생성하십시오.

⚠ 주의: 가능해요 여기에 언급된 세부사항에는 실행될 경우 중대한 영향을 미칠 수 있는 절차 또는 명령이 포함되어 있는 것으로 보입니다. 실행 또는 권장 전에 SME 또는 사업부에서 이러한 절차나 명령을 평가했는지 확인하십시오.

원인

이 문제는 손상된 레지스트리 항목 또는 Hostscan 라이브러리 및 실행이 제대로 시작되거나 업데이트되지 않도록 하는 타사 소프트웨어의 간섭으로 인해 발생합니다. 이러한 손상은 CSD(Cisco Security Desktop) 사전 로그인 확인 프로세스에 영향을 미치며, 이는 포스처가 활성화된 VPN 프로필에 필요합니다. 손상은 일반적으로 디바이스 레벨에서 발생하며, 동일한 사용자가 다른 디바이스에서 성공적으로 연결할 수 있는 이유를 설명합니다. 표준 제거 방법은 항상 모든 손상된 구성 요소를 제거하지 않으므로 파일 및 레지스트리 항목을 수동으로 정리해야 합니다.

관련 콘텐츠

- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.