

엔드포인트 보안 상태 규정 준수 문제로 인해 보안 클라이언트 AnyConnect VPN 액세스가 거부되었습니다.

목차

문제

여러 사용자가 AnyConnect VPN 및 ZTA(Zero Trust Access)에 연결할 수 없으며 "Login denied(로그인 거부됨)" 오류 메시지가 표시됩니다. 사용자 환경이 관리자가 정의한 액세스 기준을 충족하지 않습니다."

이 문제는 엔드포인트 보안 에이전트 요구 사항이 일치하지 않는 것으로 보고되는 엔드포인트 보안 상태 규정준수와 관련이 있습니다. 사용자는 Cisco Secure Client를 통해 연결을 시도할 때 VPN 및 ZTA 액세스 거부를 경험합니다.

상태 평가에서는 영향을 받는 엔드포인트에서 Trellix 엔드포인트 보안 상태가 실패하여 VPN 서비스에 대한 성공적인 인증이 불가능함을 보여 줍니다.

환경

- Cisco Secure Client(AnyConnect 및 제로 트러스트 액세스)
- Trellix Endpoint Security Agent 버전 5.8.4.505
- VPN Posture 프로파일: 엔드포인트 보안 에이전트 시행을 사용하는 KFIN_SECURE_VPN
- 상태 요구 사항: 지난 14일 이내에 업데이트와 함께 실행 중인 엔드포인트 보안 에이전트
- Trellix 에이전트 서비스가 실행 중인 Windows 엔드포인트
- 엔드포인트에서 탐지된 Umbrella 에이전트 프로세스

해결

Trellix Endpoint Security 에이전트 보안 상태 규정 준수 문제를 해결하여 문제가 해결되었습니다.
다음 섹션에서 설명하는 트러블슈팅 및 해결 단계가 구현되었습니다.

1단계: 상태 프로파일 구성 확인

VPN 포스터 프로필을 검토하여 엔드포인트 보안 에이전트 요구 사항을 확인합니다.
KFIN_SECURE_VPN 프로파일은 엔드포인트 보안 에이전트가 지난 14일 이내에 실행 및 업데이트되어야 함을 적용합니다.

2단계: Trellix 엔드포인트 보안 상태 확인

영향을 받는 엔드포인트에서 Trellix 엔드포인트 보안 에이전트의 현재 상태를 확인합니다.

```
Trellix Agent Service: masvc.exe  
Version: 5.8.4.505  
Install Location: C:\Program Files\McAfee\Agent\  
Display Name: Trellix Agent  
Publisher: Trellix
```

3단계: Trellix Endpoint Security 다시 설치

영향을 받는 엔드포인트에 Trellix Endpoint Security를 완전히 다시 설치합니다.

1. 기존 Trellix Endpoint Security 에이전트를 완전히 제거합니다.
2. 시스템을 재부팅합니다.
3. 조직 표준에 따라 승인된 최신 Trellix 에이전트 버전을 설치합니다.

4. 설치 후 에이전트가 제대로 실행되고 있는지 확인합니다.
5. 서명/콘텐츠 업데이트가 성공적으로 완료되었는지 확인합니다.

4단계: ZTA(Cisco Secure Client)에 대한 TRACE 로깅 활성화

상태 평가 세부사항을 캡처하기 위해 자세한 로깅을 활성화합니다.

다음 내용으로 logconfig.json 파일을 만듭니다.

```
{ "global": "DBG_TRACE" }
```

적절한 디렉토리에 파일을 배치합니다.

- 창: C:\ProgramData\Cisco\Cisco 보안 클라이언트\ZTA
- macOS: /opt/cisco/secureclient/zta

파일을 만든 후 Cisco Secure Client/ZTA 서비스를 다시 시작합니다.

5단계: 업데이트된 DART 번들 수집

변경 사항을 구현한 후 새 DART 번들을 수집하여 해상도를 검증하고 올바른 상태 규정 준수 탐지를 확인합니다.

원인

근본 원인은 Trellix Endpoint Security 에이전트 보안 상태 규정 준수 문제로 확인되었습니다. VPN 보안 상태 프로필에서는 지난 14일 이내에 엔드포인트 보안 에이전트를 업데이트로 실행해야 했지만 Trellix 엔드포인트 보안 에이전트가 이러한 규정 준수 기준을 충족하지 않았습니다. 상태 평가 모듈이 엔드포인트 보안 에이전트 상태를 제대로 탐지하거나 검증하지 못하여 VPN 및 ZTA 연결에 대한 액세스가 거부되었습니다. 이 문제는 특히 Trellix 에이전트 컨피그레이션과 관련된 것으로, 기본

에이전트 규정 준수 문제를 해결하기 위해 Trellix 지원 팀의 개입이 필요했습니다.

관련 콘텐츠

- [문제 해결을 위한 자세한 ZTNA 로그 수집](#)
- [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.