Umbrella가 활성화된 경우 Cowork(Frontier) 에이전트 연결 문제 해결

목차

문제

Cisco Umbrella가 사용하도록 설정된 경우 Cowork(Frontier) 에이전트가 노트북 컴퓨터에서 제대로 작동하지 않았습니다. Cisco Umbrella가 비활성 상태일 때 에이전트는 예상대로 작동했습니다. Umbrella가 활성 상태일 때는 사용자가 Cowork Agent 기능을 사용할 수 없었고, 사용자가 이 문제를 겪었을 때는 Cisco Umbrella에 블록 로그가 표시되지 않았습니다. Umbrella 작업 중 응용 프로그램 오류를 표시하는 오류 스크린샷이 제공되었습니다.

환경

- Cisco Umbrella는 엔터프라이즈 랩톱에 구축됨
- Cowork(Frontier) 에이전트 애플리케이션
- Cisco Umbrella에서 SSL/TLS 트래픽 검사 활성화
- Cowork 애플리케이션에서 인증서 피닝 구현

해결

Cisco Umbrella의 DND(Do Not Decrypt) 목록에 Cowork 애플리케이션을 추가하여 문제를 해결했습니다. 이 컨피그레이션 변경을 통해 Cowork 에이전트는 SSL/TLS 검사를 우회하고 Cowork 서버에 대한 직접 암호화 연결을 유지할 수 있습니다.

DND 목록 구성 단계

1단계: Cisco Umbrella 대시보드에 액세스하고 SSL 암호 해독 정책 컨피그레이션으로 이동합니다.

2단계: 이 애플리케이션에 대한 SSL 검사를 우회하려면 Do Not Decrypt 목록에 협업 관련 도메인 및 URL을 추가합니다.

3단계: 정책 변경 사항을 적용하고 컨피그레이션이 모든 엔드포인트에 전파되는 시간을 허용합니다.

4단계: Cisco Umbrella가 활성화된 상태에서 Cowork Agent 기능을 테스트하여 올바른 작동을 확인합니다.

검증

DND 목록 컨피그레이션을 구현한 후 Cisco Umbrella가 활성화된 상태에서 Cowork 애플리케이션이 정상적으로 작동했습니다. 내부 테스트를 통해 며칠 동안 모니터링해도 문제가 재발하지 않았으며 모든 사용자가 예상대로 Cowork 기능에 액세스할 수 있음이 확인되었습니다.

원인

Cowork(Frontier) 에이전트는 인증서 피닝을 보안 메커니즘으로 사용합니다. 인증서 피닝은 애플리케이션이 자체 특정 서버 인증서만 수락하고 신뢰하도록 하드코딩됨을 의미합니다. Cisco Umbrella가 트래픽을 인터셉트하고 원래 서버 인증서 대신 Cisco 인증서를 제공하면 Cowork 애플리케이션에서 이 변경을 탐지하고 연결이 안전하지 않다고 가정하고 의도적으로 연결을 삭제하여 데이터를 보호합니다. 이는 인증서 피닝 보안 측정을 구현하는 애플리케이션에 대한 예상 동작입니다.

관련 콘텐츠

- Microsoft 응용 프로그램에 대한 유효 암호 해독 안 함 목록 만들기
- 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.