보안 액세스에서 WhatsApp의 DLP 정책 제한

목차

문제

Cisco Secure Access의 DLP 정책은 HTTPS 암호 해독이 활성화되어 있음에도 불구하고 WhatsApp(브라우저 또는 데스크톱 애플리케이션)을 통해 공유되는 경우 민감한 파일을 탐지하거나 차단하지 않습니다. DLP 엔진은 이러한 플랫폼을 통한 파일 업로드를 트리거하거나 탐지하지 못하는 반면, 동일한 DLP 정책이 다른 온라인 업로드 툴을 통해 업로드할 때 동일한 파일을 성공적으로 차단합니다. WhatsApp에 대한 기본 업로드 차단을 테스트할 때 이 기능은 브라우저와 데스크톱 버전 모두에서 올바르게 작동하지만, 이 문제는 DLP 정책 시행으로 특별히 격리됩니다.

환경

- Cisco 보안 액세스
- 구성된 DLP 정책
- HTTPS 암호 해독 사용
- WhatsApp 웹 및 WhatsApp 데스크톱 애플리케이션

해결

관찰된 동작은 WhatsApp 및 유사한 플랫폼의 E2EE(end-to-end encryption) 구현 및 비표준 트래픽 처리로 인해 예상되는 제한입니다. 다음 섹션에 설명된 문제 해결 단계 및 해결 방법을 구현할 수 있습니다.

문제 해결 확인 단계

해결 방법을 구현하기 전에 다음 컨피그레이션 항목을 확인하십시오.

- 올바른 SWG ID/출처 ID가 구성되었는지 확인합니다.
- 대상 플랫폼에 대해 HTTPS 검사/암호 해독이 활성화되고 선택적으로 우회되지 않는지 확인합니다.
- Isolation/RBI 및 Allow-Override 설정이 올바르게 구성되었는지 확인합니다.
- DLP 정책이 그룹 기반인 경우 AD 그룹 멤버십을 확인합니다.
- Traffic Steering Bypass 목록에서 제외를 확인합니다.
- 브라우저에서 QUIC 프로토콜이 비활성화되었는지 확인합니다.
- 검사를 우회할 수 있는 IPv6 트래픽 영향을 확인합니다.

권장 해결 방법

WhatsApp 웹 트래픽에 DLP 적용을 활성화하려면 WhatsApp 웹으로 향하는 트래픽에 대해 RBI(Remote Browser Isolation)를 구현합니다. 이 방법을 사용하면 브라우저 세션을 격리하고 격리된 환경 내에서 콘텐츠 검사를 활성화하여 DLP 정책을 적용할 수 있습니다.

웹 인터페이스를 통한 파일 업로드 및 콘텐츠 공유가 DLP 정책 평가의 대상이 되도록 WhatsApp 웹 도메인에 대해 특별히 RBI 적용을 구성합니다.

추가 정보

이 제한에 대한 제품 개선 요청(CSE-I-1249)이 문서화되었습니다.

원인

WhatsApp(WhatsApp Web 포함) 및 유사 협업 플랫폼은 메시지 텍스트 및 파일 업로드의 전체 콘텐츠 검사 및 검사를 방지하는 엔드 투 엔드 암호화(E2EE)를 구현합니다. 또한 WhatsApp 트래픽은 일반적인 웹 업로드와 같은 방식으로 표준 HTTP/HTTPS 포트를 사용하지 않습니다. 즉, SWG(Secure Web Gateway)가 일반적인 HTTPS 검사 경로를 통해 트래픽을 가로채서 검사할 수

없습니다. 이 암호화 및 트래픽 처리 방법은 설계에 따른 것이며 이러한 특정 플랫폼에 대한 현재 DLP 검사 기능의 예상 제한을 나타냅니다.

관련 콘텐츠

- 제품 개선 요청 CSE-I-1249
- 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.