Google 드라이브 보안 다운로드 중 CRYPTO_INTERNAL_ERROR

목차

문제

트래픽 암호 해독이 활성화된 상태에서 Cisco Secure Access를 통해 액세스하면 암호화된 Google Sheets 파일이 열리지 않습니다. Google Drive 보안 다운로드 중에 사용자에게 CRYPTO_INTERNAL_ERROR가 발생했습니다. 이 문제는 특히 SWG(Secure Web Gateway) 검사가 활성 상태일 때 발생합니다. 암호 해독 및 검사 프로세스 중에 범위 헤더가 무시되므로 Google 보안 다운로드 메커니즘에 간섭이 발생합니다.

이 문제는 RAVPN+ZTA 구현을 사용하는 환경에 영향을 미치며, 대규모 사용자 집단에 대해 암호화된 Google 시트에 액세스하는 데 영향을 미칩니다.

환경

- 기술: Cisco Secure Access(솔루션 지원)
- 하위 기술: 보안 액세스
- 구현: RAVPN+ZTA(원격 액세스 VPN + 제로 트러스트 액세스)
- 영향을 받는 구성 요소: ZTA 프로필
- 영향을 받는 도메인: clients6.google.com 및 기타 Google 드라이브 관련 도메인

해결

해결 방법에는 영구 공급업체 측 수정을 모니터링하면서 임시 해결 방법을 구현하는 작업이 포함됩니다.

다음 섹션에 설명된 접근 방식은 암호화된 Google 시트에 대한 액세스를 복원하도록 검증되었습니다.

임시 해결 옵션

옵션 1: 트래픽 암호 해독 사용 안 함

영향을 받는 사용자 그룹 또는 정책에 대한 트래픽 해독을 완전히 비활성화합니다. 이렇게 하면 Google Sheets 액세스를 복원하지만 모든 암호 해독 기반 보안 검사 기능은 제거됩니다.

옵션 2: 암호 해독에서 Google 드라이브 도메인 제외

보안 액세스 정책 컨피그레이션의 do-not-decrypt 목록에 Google 드라이브 관련 도메인을 추가합니다.

- clients6.google.com
- 트래픽 분석에서 확인된 기타 Google 드라이브 관련 도메인

이 접근 방식은 다른 트래픽에 대한 암호 해독을 유지하면서 Google Sheets가 정상적으로 작동하도록 합니다. 그러나 이 방법을 사용하면 제외된 도메인에 대해 CASB Google Drive 업로드 블록 기능을 비활성화할 수 있습니다.

기술 분석 및 모니터링

Cisco 분석 결과, Secure Web Gateway 검사에서 Range 헤더를 무시하여 파일 콘텐츠에 대한 포괄적인 보안 검사가 가능함을 확인했습니다. 이 동작은 Google Drive 보안 다운로드 프로세스를 방해하며, 이는 올바른 암호 해독 흐름을 위해 범위 헤더에 의존합니다.

Google은 이 문제를 인정하고 프록시 동작(Cisco Umbrella/네트워크 프록시 포함)이 Range 헤더를 제거하거나 다시 작성하여 Google Drive 보안 다운로드 요청을 방해하는 것으로 확인했습니다. 이렇게 하면 Google 암호 해독 메커니즘을 깨는 전체 파일 다운로드가 강제로 수행됩니다. Google은

도착 예정 시간이 제공되지 않았지만 클라이언트 측 픽스를 개발하고 있습니다.

구현 고려 사항

이 해결 방법을 구현하는 조직은 보안과 관련된 문제를 고려해야 합니다.

- Google 드라이브 도메인을 암호 해독 검사에서 제외할 위험을 평가합니다.
- 도메인 제외의 영향을 받을 수 있는 CASB 정책을 검토합니다.
- 향후 정책 검토를 위해 해결 방법의 임시 특성을 문서화합니다.
- Google에서 클라이언트 측 수정 개발과 관련된 업데이트를 모니터링합니다.

원인

근본 원인은 Cisco Secure Access SWG 검사 동작과 Google Drive 보안 다운로드 메커니즘 간의 호환성 문제입니다.

구체적으로,

Cisco Secure Web Gateway 검사는 암호 해독 및 보안 검사 프로세스 중에 범위 헤더를 무시하여 완벽한 파일 분석을 보장합니다. 그러나 Google Drive 암호화 파일 액세스는 보안 다운로드를 위한 암호 해독 흐름을 제대로 처리하기 위해 범위 헤더를 사용합니다. 프록시 검사 프로세스 중에 이러한 헤더가 제거되거나 수정되면 Google 클라이언트 측 해독이 실패하여 CRYPTO_INTERNAL_ERROR가 발생합니다.

이는 보안 검사 요구 사항(전체 파일 검사)과 Google 암호화 파일 전송 메커니즘(범위 기반 보안 다운로드) 간의 근본적인 비호환성을 나타냅니다.

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.