Splunk 클라이언트 로그 업로드를 통한 보안 액세스 인증서 검증 오류

목차

문제

Cisco Secure Access에서 트래픽을 해독할 때 인증서 유효성 검사 오류로 인해 Splunk 클라이언트를 실행하는 Windows 클라이언트가 Splunk 클라우드에 로그를 업로드할 수 없습니다. 5,000개가 넘는 Windows 로그 소스에서 Splunk 클라우드에 데이터를 보내지 못해 로그 수집에 영향을 미쳤습니다. Splunk 클라이언트 로그에서 관찰된 특정 오류는 다음과 같습니다.

```
02-27-2026 16:51:54.830 +0530 ERROR X509Verify [15668 TcpOutEloop] - Server X509 certificate failed val
```

목적지로 가는 트래픽 *.splunkcloud.com이 방화벽을 통해 이동했지만 애플리케이션 수준 인증서 검증에 실패했습니다. SSL 해독이 활성화된 사이트에 대한 웹 브라우징이 계속 정상적으로 작동했습니다.

환경

- SSL/TLS 암호 해독이 활성화된 Cisco Secure Access
- Splunk Universal Forwarder가 설치된 Windows 클라이언트
- Splunk 클라우드 대상: *.splunkcloud.com
- 5,000개 이상의 Windows 로그 소스 영향
- Splunk 클라이언트는 Microsoft 시스템 인증서 저장소가 아닌 자체 인증서 저장소를 사용합니다

해결

Cisco Secure Access에서 Splunk 클라우드 트래픽에 대한 암호 해독 바이패스 정책을 구현하여 문제가 해결되었습니다.

몇 가지 조치가 취해졌다.

1단계: 문제 파악

WebEx 세션 중에 해당 동작이 확인되고 재현되었습니다. 테스트에 따르면 클라이언트에 대해 Secure Access 암호 해독이 비활성화되었거나 클라이언트에서 SWG 서비스가 비활성화되었을 때 Splunk 로그 업로드가 성공했습니다. 이로 인해 SSL/TLS 암호 해독 프로세스로 인해 인증서 유효성 검사 오류가 발생했음을 확인했습니다.

2단계: 대상 목록 만들기

Splunk 클라우드 서비스로 향하는 트래픽을 특별히 대상으로 하기 위해 Splunk 클라우드 FQDN 및 IP 주소를 포함하는 대상 목록이 생성되었습니다.

3단계: 암호 해독 우회 정책 구현

Splunk 클라우드 대상 목록과 일치하는 트래픽에 대해 SSL/TLS 암호 해독을 비활성화하는 Cisco Secure Access 정책이 구현되었습니다. 이 바이패스 정책은 Splunk 클라이언트가 Secure Access에 의한 인증서 가로채기 없이 Splunk 클라우드에 대한 직접 암호화된 연결을 설정할 수 있도록 허용했습니다.

4단계: 검증

암호 해독 바이패스 정책을 구현한 후 유효성 검사에서 다음을 확인했습니다.

- Splunk 클라이언트가 로그를 업로드할 수 있었습니다.
- Splunk 클라우드의 전체 보고 클라이언트 수가 크게 증가했습니다
- 추가 인증서 유효성 검사 오류가 관찰되지 않았습니다.

케이스 심각도를 1에서 3으로 낮추고 모니터링 상태로 두어 지속적으로 성공한 로그 수집을 관찰했습니다.

원인

근본 원인은 Splunk 클라이언트가 자체 인증서 저장소를 사용하며 SSL/TLS 암호 해독 중에 제공되던 Cisco Secure Access Primary SubCA 인증서를 신뢰하지 않기 때문입니다. Cisco Secure Access가 Splunk 클라우드에 대한 SSL 트래픽을 인터셉트하고 해독하면 자체 인증 기관을 사용하여 트래픽을 다시 암호화합니다. 자체 인증서 저장소의 신뢰할 수 있는 루트 인증 기관에 대한 인증서 체인을 다시 확인할 수 없기 때문에 Splunk 클라이언트 인증서 유효성 검사 프로세스에서 이 인증서를 거부했습니다.

특정 X.509 유효성 검사 오류 "로컬 발급자 인증서를 가져올 수 없음"(오류 코드 20)은 인증서 유효성 검사 프로세스에서 클라이언트 트러스트된 인증서 저장소에서 발급 인증 기관을 찾을 수 없어 연결이 실패했음을 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.