macOS에서 Firefox 및 Safari의 보안 액세스 맞춤형 CA 트러스트 문제

목차

문제

사용자는 Cisco Secure Access를 통해 암호 해독된 인터넷 트래픽에 액세스할 때 macOS 브라우저(Safari 및 Firefox)에서 인증서 신뢰 오류를 경험했습니다. 크롬 브라우저가 제대로 작동했지만 사파리와 파이어폭스는 '신뢰할 수 없는 인증서' 경고를 표시하고 웹사이트와 애플리케이션에 대한 접근을 차단했다.

전체 인증서 체인은 다음과 같이 표시되었습니다.

- 웹 사이트(예: cnn.com) > Cisco Secure Access Custom CA > Cisco Secure Access Custom R3 CA > Cisco Secure Access Custom CA > xxxx-SUBCA1 > xxxxROOT-CA

Firefox 및 Safari 브라우저는 Cisco 중간 인증서에서 인증서 검증을 중지했으며 루트 CA까지 체인을 시작하지 못했으며, Chrome은 전체 인증서 체인을 검증했습니다.

환경

- HTTPS 암호 해독을 위한 사용자 지정 인증 기관이 포함된 Cisco Secure Access 구축
- Safari 및 Firefox 브라우저가 있는 macOS 디바이스
- Microsoft Certificate Authority를 사용하는 맞춤형 CA 인증서 인프라
- 암호 해독 및 침입 방지 기능이 활성화된 인터넷 액세스 정책
- 조직 ID: xxxxx

해결

인증서 체인의 인코딩 불일치를 식별하고 암호 해독을 위해 Cisco Secure Access Root CA로 전환하여 문제를 해결했습니다.

근본 원인 분석

팀은 인쇄 가능한 문자열 인코딩을 사용하여 사용자 지정 인증 기관이 생성되었음을 식별했으며, 이로 인해 리프 인증서가 UTF8STRING으로 설정된 경우에도 비호환성 문제가 발생했습니다. Firefox 및 Safari에서는 체인의 모든 인증서가 동일한 형식이어야 하지만 Chrome에서는 이러한 엄격한 요구 사항이 없습니다.

해결 단계

Cisco Secure Access Root CA로 전환

대체 솔루션

사용자 지정 CA를 사용해야 하는 경우 다음 옵션이 식별되었습니다.

- UTF8 인코딩을 사용하여 전체 인증서 인프라를 재구축합니다(높은 영향, 권장하지 않음).
- UTF8 인코딩을 지원하는 다른 인증서 인프라 사용
- Firefox 및 Safari의 제한은 현재 맞춤형 CA 설정에서 작동하지 않습니다.

원인

근본 원인은 Microsoft Certificate Authority(기본적으로 printablestring 인코딩을 사용함)와 Cisco Secure Access에서 사용하는 UTF8 체인 간의 인코딩 불일치입니다. Firefox 및 Safari는 인증서 검증 요구 사항이 더 엄격하며 일관된 인코딩을 사용하기 위해 체인의 모든 인증서가 필요합니다. Chrome에서 더욱 관대한 검증을 통해 혼합 인코딩 체인과 연동할 수 있었고, Firefox 및 Safari는 일관되지 않은 인증서 형식을 거부했습니다.

Microsoft CA는 printablestring 인코딩을 사용하여 인증서를 생성했지만 Cisco Secure Access 중간 인증서는 UTF8STRING 인코딩을 사용했습니다. 이러한 불일치로 인해 Firefox와 Safari는 Cisco 중간 인증서 수준에서 인증서 체인 검증에 실패했습니다.

관련 콘텐츠

- SWG에서 Webex Meeting 액세스 구성
- 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.