무선 클라이언트의 HTTPS WebAuthentication 인증서 불신행위 이해 및 문제 해결

목차

소개

이 문서에서는 웹 브라우저에서 SSL(Secure Sockets Layer) 인증서를 처리하는 방법을 변경한 후 레이어 3 인증 WLAN(Wireless Local Area Network)에 연결할 때 무선 클라이언트의 동작을 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- HTTPS(HyperText Transfer Protocol Secure).
- SSL 인증서.
- Cisco WLC(Wireless LAN Controller).

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Chrome 웹 브라우저 버전 74.x 이상
- Firefox 웹 브라우저 버전 66.x 이상
- Cisco Wireless LAN Controller 버전 8.5.140.0 이상

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

배경 정보

하이퍼텍스트 전송 프로토콜 ()인터넷 상의 웹 사이트에 대한 HTTP(Traffic)는 안전하지 않으며 의도하지 않은 개인이 가로채서 처리할 수 있습니다.따라서 HTTPS를 구성하는 SSL/TLS 암호화와 같은 추가 보안 조치를 구현하는 데 필요한 민감한 애플리케이션에 대해 HTTP의 사용이 증가했습니다.

HTTPS는 SSL 인증서는 웹 사이트의 ID를 확인하고 웹 서버와 엔드포인트 브라우저 간의 보안 연결을 설정할 수 있습니다.SSL 인증서는 브라우저 및 운영 체제의 신뢰할 수 있는 CA 루트 인증서 목록에 포함된 신뢰할 수 있는 CA(Certificate Authority)에서 발급해야 합니다.

처음에는 SSL 인증서가 160비트 해시를 사용하는 SHA-1(Secure Hashing Algorithm version 1)을 사용했습니다.그러나 여러 가지 약점으로 인해 SHA-1은 256비트라는 길이가 다른 해싱 알고리즘 그룹인 SHA-2로 점진적으로 대체되었습니다.

문제

신뢰할 수 없는 인증서에 대한 일반적인 시나리오

웹 브라우저에서 SSL 인증서를 신뢰하지 않는 이유는 여러 가지가 있지만 가장 일반적인 이유는 다음과 같습니다.

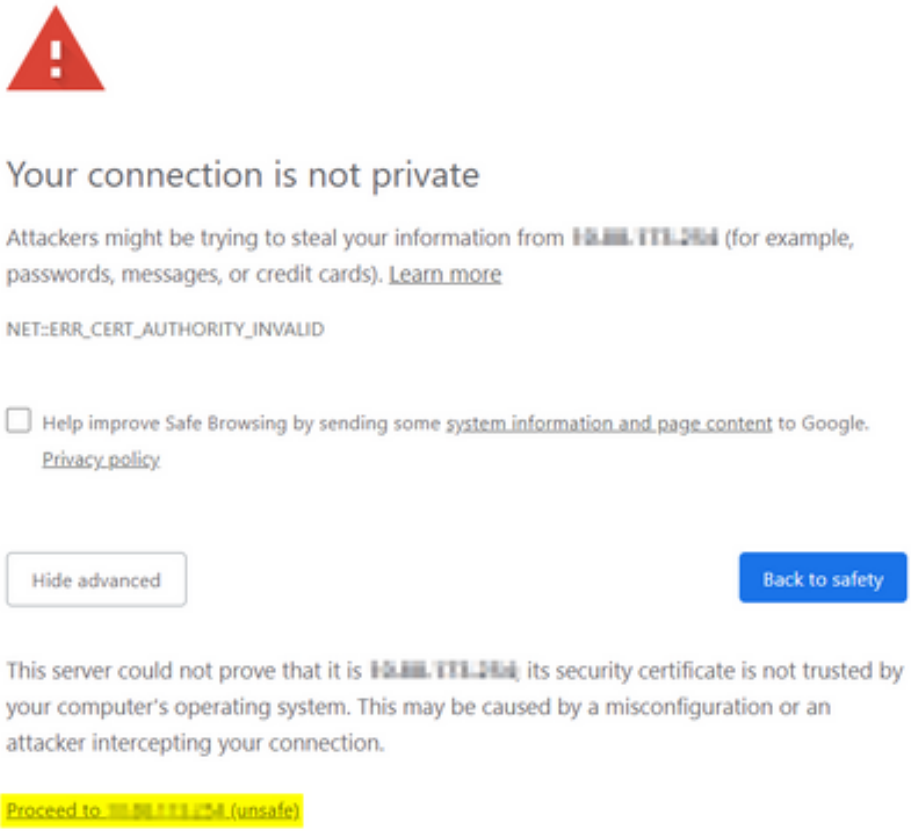
- 신뢰할 수 있는 인증 기관에서 인증서를 발급하지 않습니다(인증서가 자체 서명되어 있거나 클라이언트에 내부 CA의 경우 루트 CA 인증서가 설치되어 있지 않음).
- 인증서의 CN(Common Name) 또는 SAN(Subject Alternate Name) 필드가 해당 사이트로 이동하기 위해 입력한 Uniform Resource Locator(URL)와 일치하지 않습니다.
- 인증서가 만료되었거나 클라이언트의 시계가 잘못 구성되었습니다(인증서의 유효 기간 외).
- 중간 CA 또는 디바이스 인증서(중간 CA가 없는 경우)에서 SHA-1 알고리즘을 사용하고 있습니다.

이전 동작

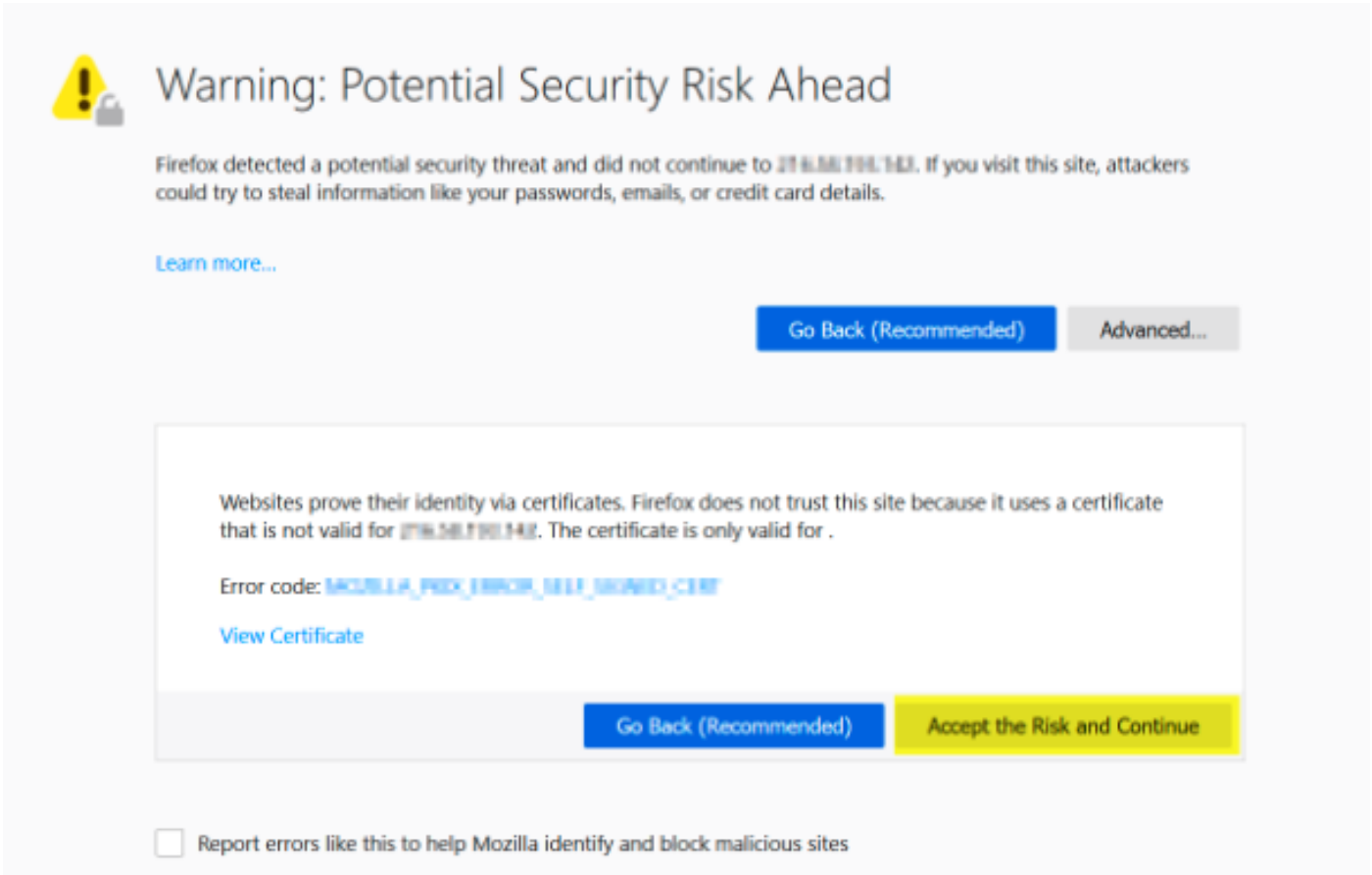
이전 버전의 웹 브라우저에서는 디바이스 인증서를 신뢰할 수 없는 것으로 탐지하면 보안 확인 경고 텍스트 및 모양은 각 브라우저에 따라 다릅니다. 보안 경고 사용자에게 보안 위험을 수락하고 의도한 웹 사이트를 계속 방문하도록 요청하거나 연결을 거부하도록 요청합니다. 수락 후 최종 사용자에 대한 리디렉션 동작을 의도된 종속 포털에 가져올 위험:

참고:진행 작업은 특정 브라우저의 고급 옵션 아래에 숨길 수 있습니다.

Google Chrome 버전 74 이하: 이미지에 표시된 것처럼 알림이 표시됩니다.



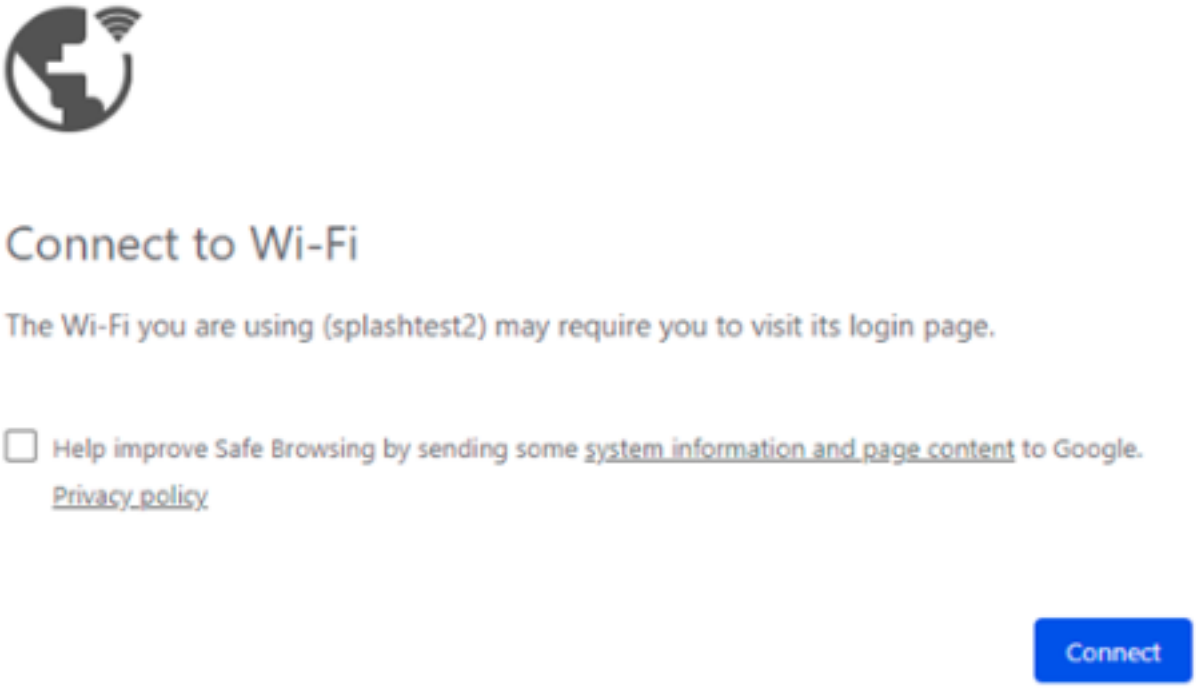
66보다 낮은 Mozilla Firefox 버전은 이미지에 표시된 대로 알림을 표시합니다.



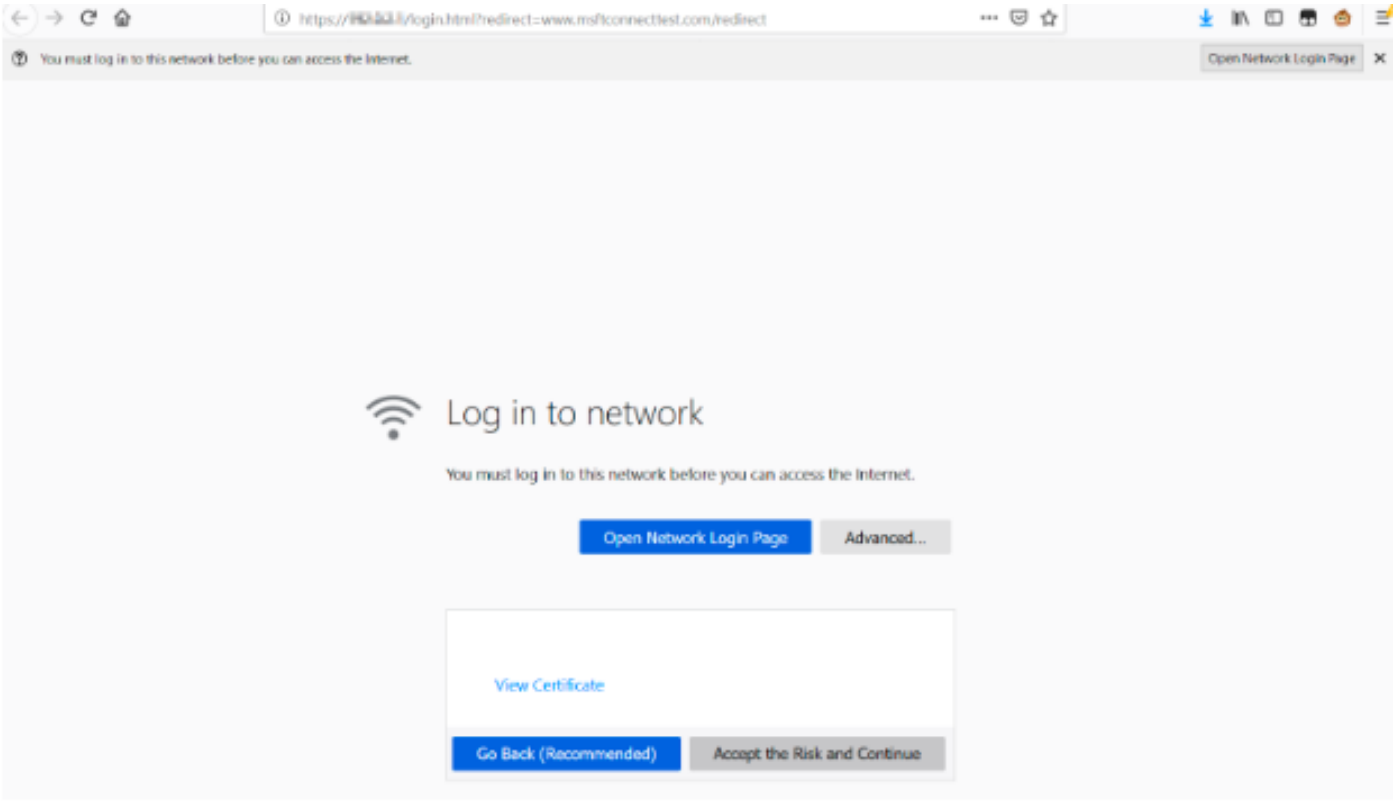
변경된 동작

Google Chrome 및 Mozilla Firefox와 같은 일부 웹 브라우저는 인증서 확인을 통해 보안 연결을 처리하는 방식을 변경했습니다.Google Chrome(74.x 이상) 및 Mozilla Firefox(66.x 이상)는 브라우저에서 이전에 외부 URL에 쿠키 없는 요청을 보내야 합니다. 사용자는 종속 포털을 탐색할 수 있습니다.그러나 이 요청은 모든 트래픽이 최종 연결 상태에 도달하기 전에 차단되므로 Wireless Controller에 의해 가로채집니다.요청 그런 다음 종속 포털에 대한 새 리디렉션 시작 Cisco의 사용자 이후의 리디렉션 루프 이(가) 포털을 참조하십시오.

Google Chrome 74.x 이상에는 다음과 같은 경고**가 표시됩니다. Connect to Wi-Fi 사용 중인 Wi-Fi에는** 다음과 같이 **로그인 페이지**를 방문해야 **할 수 있습니다**.



Mozilla Firefox 66.x 이상에는 다음과 같은 경고**가 표시됩니다. Login To Network** 이미지에 표시된 것처럼 **인터넷에 액세스하려면 먼저 이 네트워크에 로그인해야 합니다**.



이 페이지에는 Accept **the Risk and Continue** 옵션이 포함됩니다.그러나 이 옵션을 선택하면 동일한 정보가 있는 새 탭이 만들어집니다.

> **참고:**이 문서 버그는 고객을 위한 외부 참조로 ISE 팀에서 제출했습니다.CSCvj04703 - Chrome:게스트/BYOD 포털의 리디렉션 흐름은 ISE 포털에서 신뢰할 수 없는 인증서로 끊어집니다.

솔루션

내부 웹 인증(WLC의 내부 웹 로그인 페이지)에 대한 해결 방법

옵션 1

WLC에서 WebAuth SecureWeb을 비활성화합니다.인증서 유효성 검사에서 HTTPS 보안 메커니즘을 생성하므로 사용 인증서 검증을 건너뛰고 클라이언트가 종속 포털을 렌더링하도록 허용하려면 HTTP를 선택합니다.

WLC에서 WebAuth SecureWeb을 비활성화하려면 다음 명령을 실행할 수 있습니다.

```
config network web-auth secureweb disable
```

> **참고:**변경 사항을 적용하려면 WLC를 재부팅해야 합니다.

옵션 2

대체 웹 브라우저를 사용합니다.지금까지 이 문제는 Google Chrome 및 Mozilla Firefox로 격리되었습니다.따라서 Internet Explorer, Edge 및 네이티브 Android 웹 브라우저와 같은 브라우저는 이러한

동작을 나타내지 않으며 종속 포털에 액세스하는 데 사용할 수 있습니다.

외부 웹 인증에 대한 해결 방법

옵션 1

이러한 웹 인증 프로세스 변형은 사전 인증 액세스 목록을 통한 통신 제어를 허용하므로, 사용자가 종속 포털을 계속 사용할 수 있도록 예외를 추가할 수 있습니다.이러한 예외는 URL 액세스 목록을 통해 수행됩니다(중앙 집중식 WLAN의 경우 AireOS 버전 8.3.x에서 지원 시작 및 FlexConnect 로컬 스위칭 WLAN의 경우 8.7.x). URL은 웹 브라우저에 종속될 수 있지만, URL은 http://www.gstatic.com/ Google Chrome 및 http://detectportal.firefox.com/ 있습니다.

영구 수정

이 문제를 해결하려면 WLC에 신뢰할 수 있는 인증 기관에서 발급한 SHA-2 알고리즘으로 WebAuth SSL 인증서를 설치하는 것이 좋습니다.

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- 서드파티 인증서용 CSR 생성 및 WLC에 체인 인증서 다운로드
- Google Chrome 개인 정보 보호 백서
- 기술 지원 및 문서 – Cisco Systems