Beheben von Fehlverhalten bei HTTPS-Webauthentifizierungszertifikaten von Wireless-Clients und Beheben von Fehlern

Inhalt

Einführung

Dieses Dokument beschreibt das Verhalten von Wireless-Clients bei der Verbindung mit einem Wireless Local Area Network (WLAN) mit Layer-3-Authentifizierung, nachdem Änderungen an der Behandlung von SSL-Zertifikaten (Secure Sockets Layer) durch Webbrowser vorgenommen wurden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

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

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Chrome-Webbrowser Version 74.x oder höher
- Firefox Webbrowser Version 6.x oder höher.
- Cisco Wireless LAN Controller Version 8.5.140.0 oder höher

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Hypertext Transfer Protocol (HTTP) Datenverkehr für Websites im Internet ist nicht sicher und kann von unbeabsichtigten Personen abgefangen und verarbeitet werden. Aus diesem Grund machte die verstärkte Verwendung von HTTP für sensible Anwendungen die Implementierung zusätzlicher Sicherheitsmaßnahmen wie SSL/TLS-Verschlüsselung erforderlich, die HTTPS darstellt.

HTTPS erfordert die Verwendung von SSL Zertifikate zur Überprüfung der Identität einer Website und zum Herstellen einer sicheren Verbindung zwischen dem Webserver und dem Browser des Endpunkts. SSL-Zertifikate müssen von einer vertrauenswürdigen Zertifizierungsstelle (Certificate Authority, CA) ausgestellt werden, die in der Liste der vertrauenswürdigen CA-Stammzertifikate von Browsern und Betriebssystemen enthalten ist.

Zunächst verwendeten SSL-Zertifikate Secure Hashing Algorithm Version 1 (SHA-1), der einen 160-Bit-Hash verwendet. Aufgrund verschiedener Schwächen wurde SHA-1 jedoch schrittweise durch SHA-2 ersetzt, eine Gruppe von Hashing-Algorithmen mit unterschiedlichen Längen, zwischen denen die beliebteste 256-Bit-Gruppe liegt.

Problem

Allgemeine Szenarien für nicht vertrauenswürdige Zertifikate

Es gibt mehrere Gründe, warum ein Webbrowser einem SSL-Zertifikat nicht traut, aber die häufigsten Gründe sind:

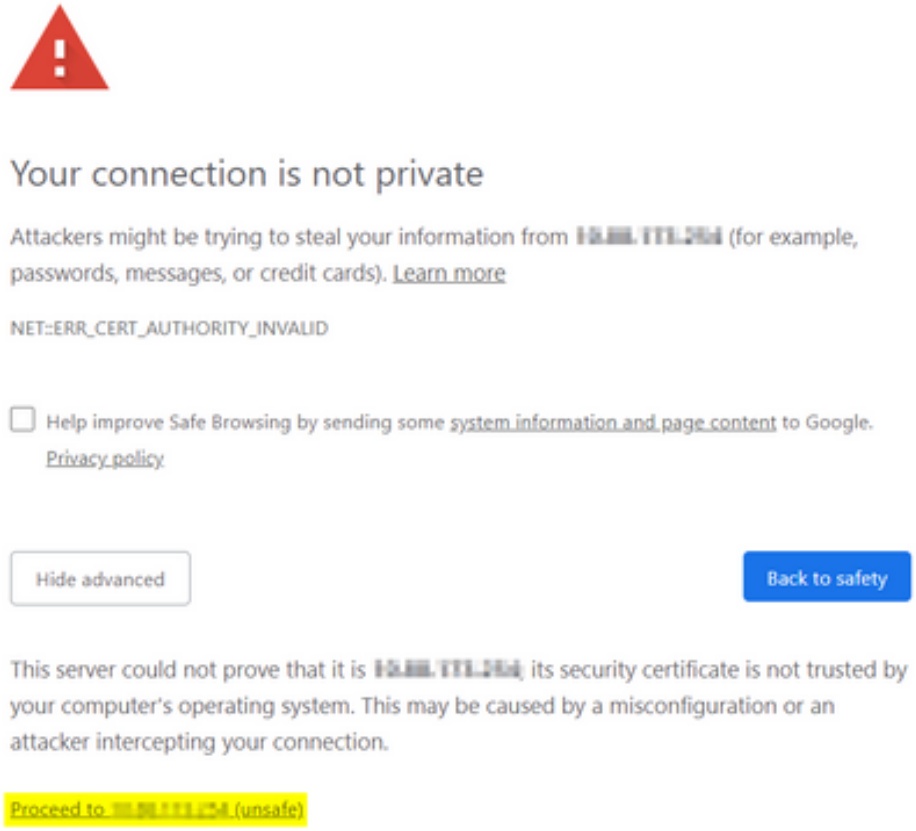
- Das Zertifikat wird nicht von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt (entweder das Zertifikat ist selbstsigniert oder der Client hat im Fall einer internen Zertifizierungsstelle kein Stammzertifikat der Zertifizierungsstelle installiert).
- Die Felder Common Name (CN) oder Subject Alternate Name (SAN) des Zertifikats stimmen nicht mit dem Uniform Resource Locator (URL) überein, der für die Navigation zu dieser Website eingegeben wurde.
- Das Zertifikat ist abgelaufen oder die Uhr auf dem Client ist falsch konfiguriert (außerhalb der Gültigkeitsdauer des Zertifikats).
- Der SHA-1-Algorithmus wird von der Zwischen-CA oder dem Gerätezertifikat verwendet (falls keine Zwischen-CA vorhanden ist).

Vorheriges Verhalten

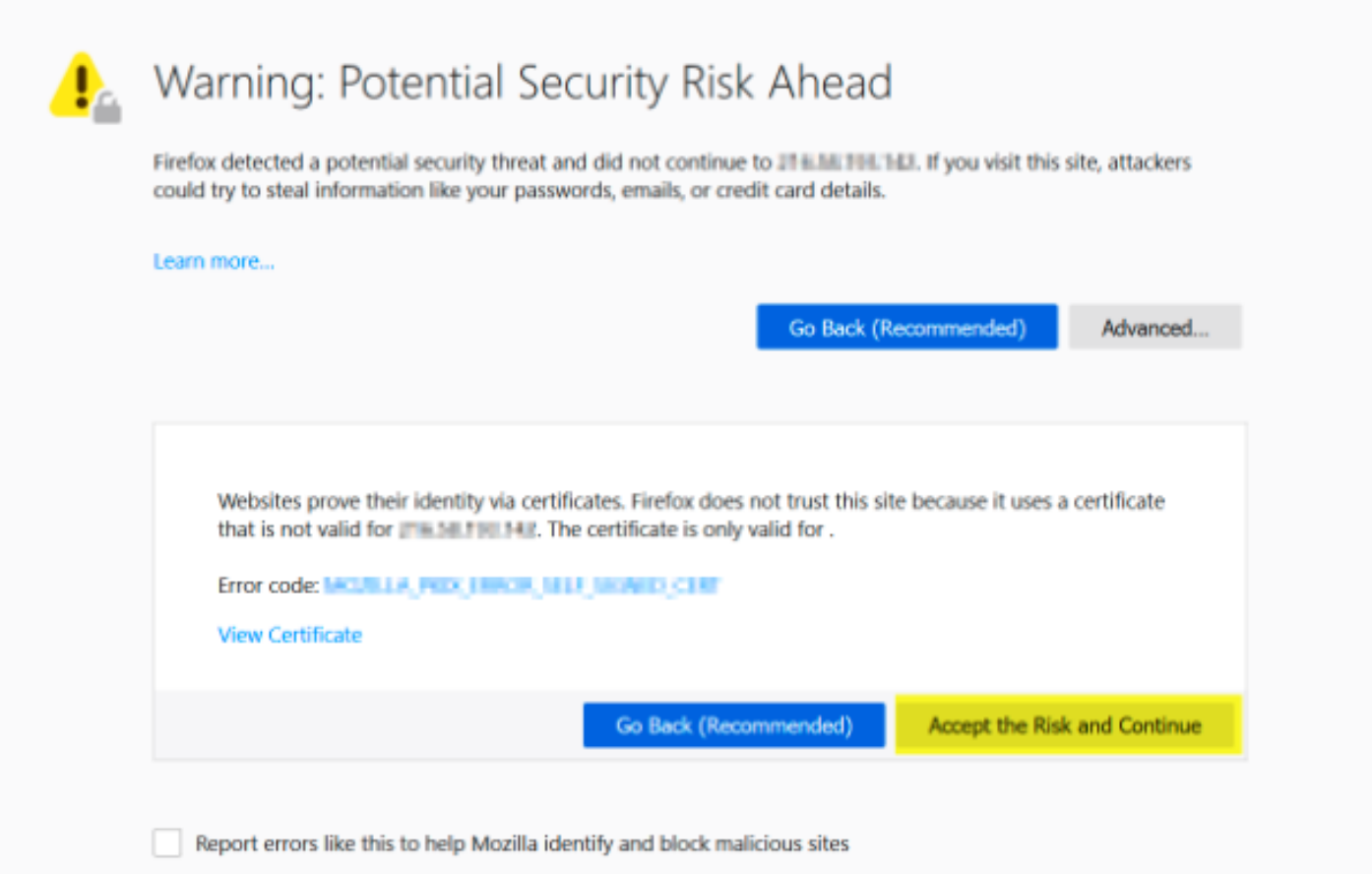
Wenn ältere Versionen eines Webbrowsers ein Gerätezertifikat als nicht vertrauenswürdig erkennen, werden sie aufgefordert, die Sicherheit zu gewährleisten. Warnung (Text und Darstellung variieren je nach Browser). Die Sicherheit Warnung fordert den Benutzer auf, das Sicherheitsrisiko zu akzeptieren und mit der beabsichtigten Website fortzufahren oder die Verbindung abzulehnen. Nach der Annahme das Risiko, dass der Benutzer das Umleitungsverhalten für den Endbenutzer zum beabsichtigten Captive Portal erhält:

> **Hinweis:** Die Aktion zum Fortfahren kann in bestimmten Browsern unter Erweiterte Optionen ausgeblendet werden.

In Versionen unter 74 von Google Chrome wird die Warnmeldung wie im Bild gezeigt angezeigt:



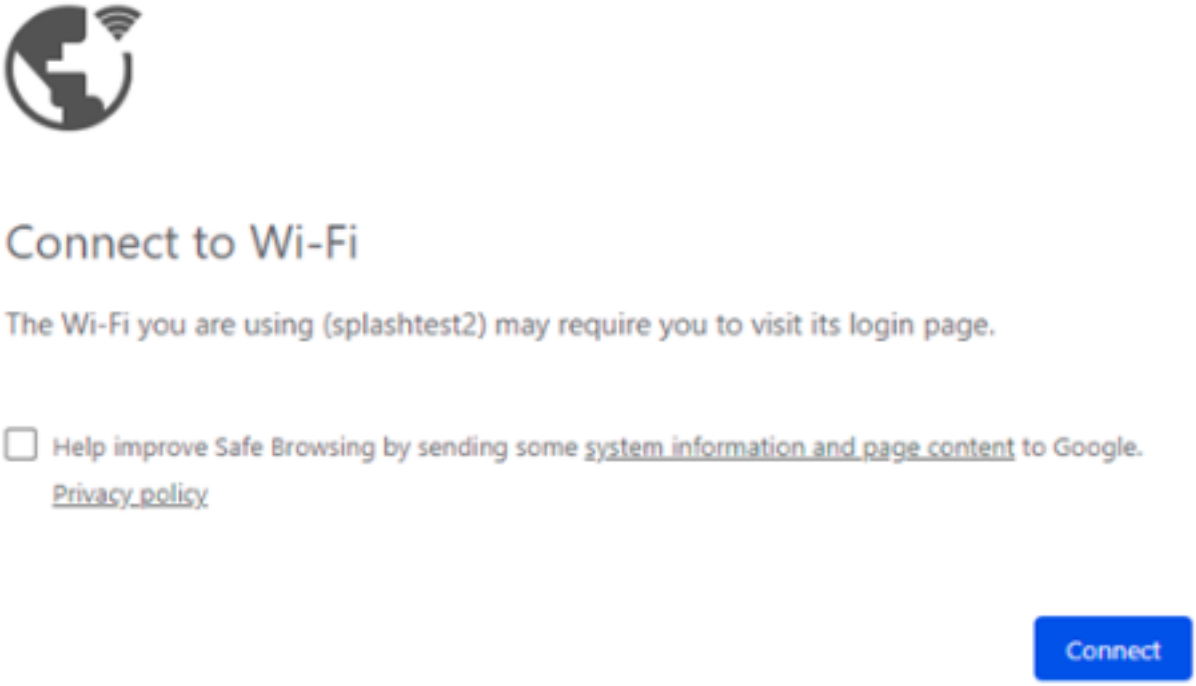
Mozilla Firefox-Versionen unter 66 zeigen die Warnmeldung wie im Bild gezeigt an:



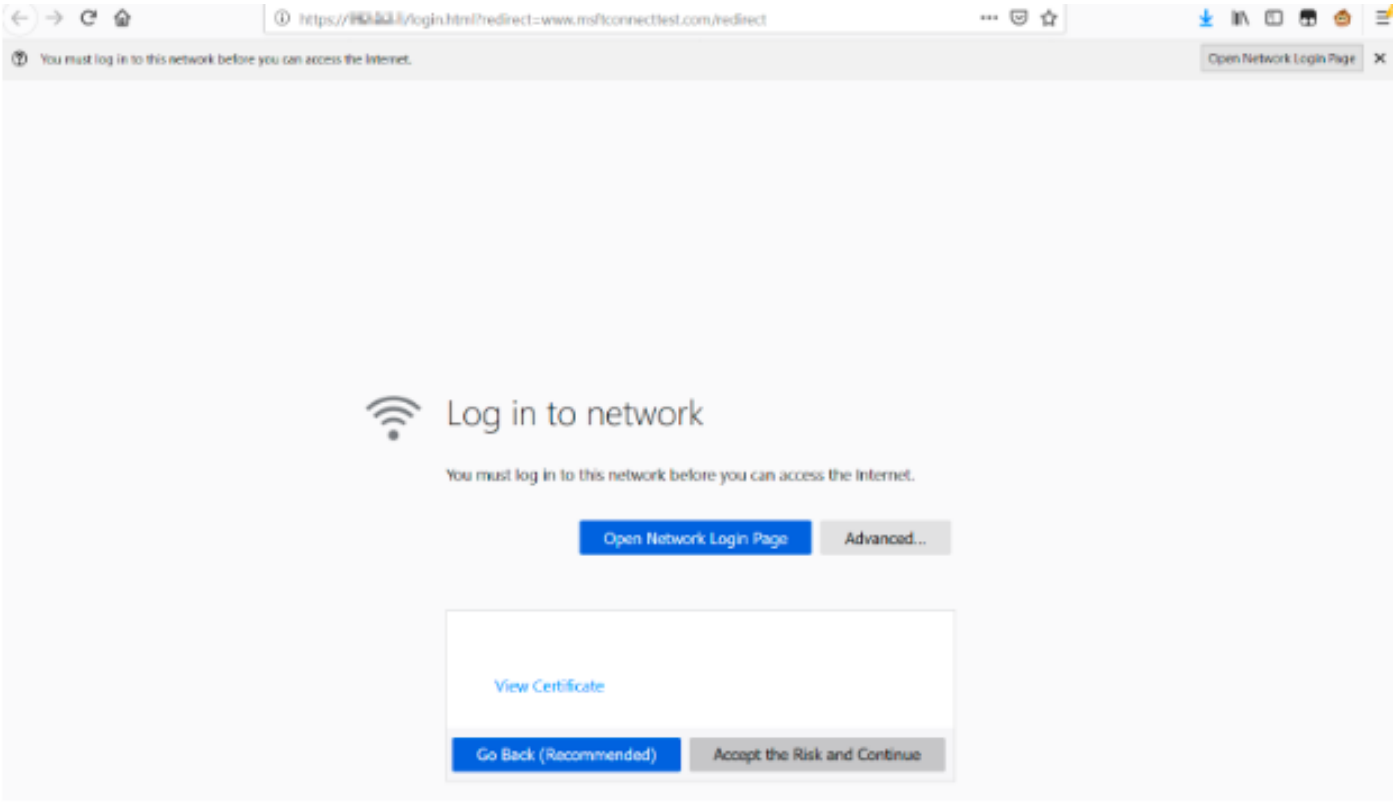
Geändertes Verhalten

Einige Webbrowser wie Google Chrome und Mozilla Firefox haben die Art und Weise, wie sie sichere Verbindungen durch Zertifikatsverifizierung handhaben, verändert. Bei Google Chrome (74.x und höher) und Mozilla Firefox (66.x und höher) muss der Browser zuvor eine Cookie-Anfrage an externe URLs senden. kann der Benutzer zum Captive Portal navigieren. Diese Anforderung wird jedoch vom Wireless Controller abgefangen, da der gesamte Datenverkehr blockiert wird, bevor er den endgültigen Verbindungsstatus erreicht. Die Anfrage dann eine neue Umleitung zum Captive Portal initiiert die eine Umleitungsschleife, da der Benutzer kann nicht im Portal.

Google Chrome 74.x und höher zeigt die Warnmeldung an: **Connect to Wi-Fi Die Wi-Fi-Verbindung, die Sie verwenden, kann es erfordern, dass Sie die Anmeldeseite besuchen**, wie im Bild gezeigt:



Mozilla Firefox 66.x und höher zeigt die Warnung an: **Anmelden** an **Netzwerk Sie müssen sich bei diesem Netzwerk anmelden, bevor Sie auf das Internet zugreifen können**, wie im folgenden Bild gezeigt:



Diese Seite enthält eine Option **Akzeptieren Sie die Risiken und Fortfahren**. Wenn diese Option aktiviert ist, wird jedoch eine neue Registerkarte mit den gleichen Informationen erstellt.

> **Hinweis:** Dieser Dokumentations-Bug wurde vom ISE-Team als externe Referenz für Kunden eingereicht:CSCvj04703 - Chrome: Der Umleitungsfluss im Gast-/BYOD-Portal wird im ISE-Portal mit nicht vertrauenswürdigen Zertifikaten unterbrochen.

Lösung

Problemumgehung für interne Web-Auth (interne Web-Anmeldeseite des WLC)

Option 1

Deaktivieren Sie WebAuth SecureWeb auf dem WLC. Da das Problem durch die Zertifikatsvalidierung zum Erstellen des HTTPS-Sicherheitsmechanismus verursacht wird, verwenden HTTP zum Überspringen der Zertifikatsvalidierung und zum Rendern des Captive Portals durch Clients.

Um WebAuth SecureWeb auf dem WLC zu deaktivieren, können Sie den folgenden Befehl ausführen:

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

Hinweis: Sie müssen den WLC neu starten, damit die Änderung wirksam wird.

Option 2

Verwenden Sie alternative Webbrowser. Bisher wurde das Problem für Google Chrome und Mozilla Firefox isoliert; Browser wie Internet Explorer, Edge und native Android-Webbrowser zeigen dieses Verhalten daher nicht an und können für den Zugriff auf das Captive Portal verwendet werden.

Problemumgehung für externe Web-Auth

Option 1

Da diese Variante des Webauthentifizierungsprozesses die Steuerung der Kommunikation über die Zugriffsliste für die Pre-Authentication-Authentifizierung ermöglicht, kann eine Ausnahme hinzugefügt werden, sodass die Benutzer weiterhin auf das Captive Portal zugreifen können. Solche Ausnahmen werden über URL-Zugriffslisten (Unterstützung beginnt bei AireOS-Versionen 8.3.x für zentralisierte WLANs und 8.7.x für FlexConnect Local Switching WLANs) durchgeführt. Die URLs können von Webbrowsern abhängig sein, wurden jedoch als http://www.gstatic.com/ für Google Chrome und http://detectportal.firefox.com/ für Mozilla Firefox.

Permanente Behebung

Um dieses Problem zu beheben, wird empfohlen, ein WebAuth SSL-Zertifikat mit dem SHA-2-Algorithmus zu installieren, der von einer vertrauenswürdigen Zertifizierungsstelle im WLC ausgegeben wird.

Überprüfung

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- Generieren von CSR für Drittanbieterzertifikate und Herunterladen von verketteten Zertifikaten für den WLC
- Whitepaper zum Datenschutz zu Google Chrome
- Technischer Support und Dokumentation für Cisco Systeme