ワイヤレスクライアントでのHTTPS Web認証証明書の信頼できない動作の理解とトラブルシューティング

内容

概要

このドキュメントでは、WebブラウザによるSecure Sockets Layer(SSL)証明書の処理方法の変更の後、レイヤ3認証Wireless Local Area Network(WLAN)に接続するワイヤレスクライアントの動作について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- HyperText Transfer Protocol Secure(HTTPS)。
- SSL 証明書.
- Cisco Wireless LAN Controller(WLC)。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Chrome Webブラウザバージョン74.x以降
- Firefox Webブラウザバージョン66.x以降
- Cisco Wireless LAN Controllerバージョン8.5.140.0以降

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

Hypertext Transfer Protocol (HTTP)インターネット上のWebサイトのトラフィックはセキュリティ保護されていないため、意図しないユーザによって傍受され、処理される可能性があります。したがって、HTTPSを構成するSSL/TLS暗号化として追加のセキュリティ対策を実装するために必要な機密アプリケーションに対するHTTPの使用が増えました。

HTTPSでは、 SSL 証明書を使用して、webサイトのidを検証し、webサーバとエンドポイントのブラウザ間のセキュアな接続を確立できます。SSL証明書は、ブラウザおよびオペレーティングシステムの信頼できるCAルート証明書のリストに含まれている信頼できる認証局(CA)によって発行される必要があります。

最初に、SSL証明書は160ビットハッシュを使用するセキュアハッシュアルゴリズムバージョン1(SHA-1)を使用しました。しかし、さまざまな弱点により、SHA-1は徐々にSHA-2に置き換えられています。SHA-2は、長さの異なるハッシュアルゴリズムのグループで、最も普及しているのは256ビットです。

問題

信頼できない証明書の一般的なシナリオ

WebブラウザがSSL証明書を信頼しない理由はいくつかありますが、最も一般的な理由は次のとおりです。

- 証明書が信頼できる認証局(CA)によって発行されていない（証明書が自己署名されているか、またはクライアントに内部CAの場合にルートCA証明書がインストールされていない）。
- 証明書の[Common Name (CN)]または[Subject Alternate Name (SAN)]フィールドが、そのサイトに移動するために入力したUniform Resource Locator (URL)と一致しません。
- 証明書の有効期限が切れているか、クライアントのクロックの設定に誤りがある（証明書の有効期間の範囲外）。
- SHA-1アルゴリズムは、中間CAまたはデバイス証明書（中間CAがない場合）によって使用されています。

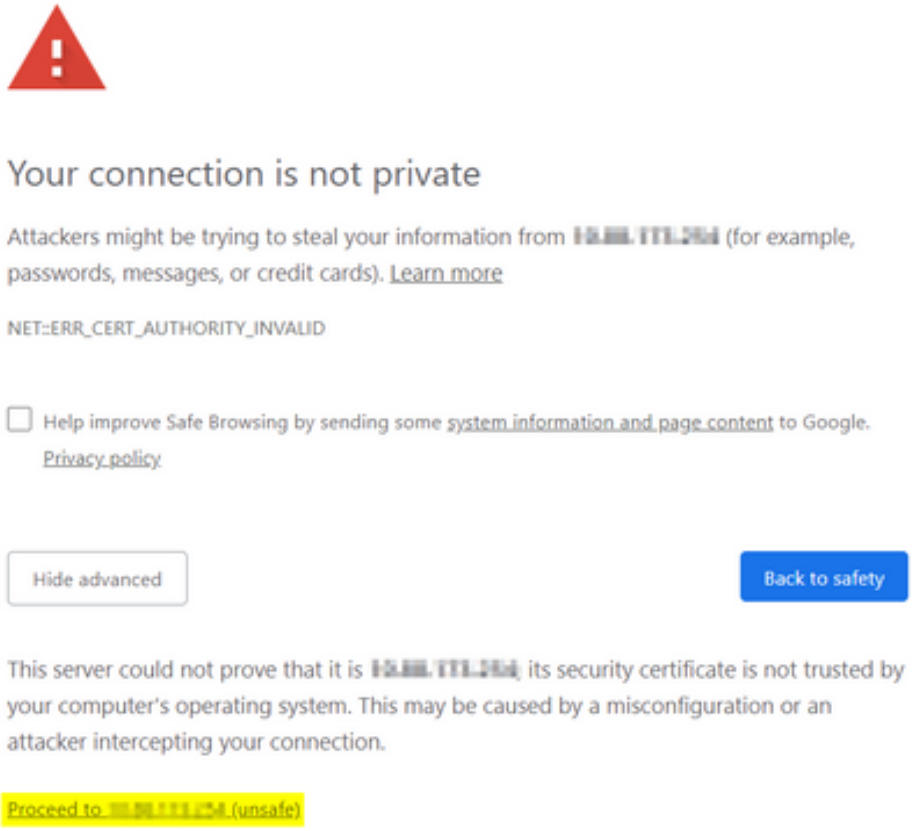
前の動作

以前のバージョンのWebブラウザがデバイス証明書を信頼できないと検出すると、セキュリティを要求します アラート（テキストと外観はブラウザによって異なります）。 [Security アラート セキュリティリスクを受け入れ、目的のwebサイトに継続するか、接続を拒否するようにユーザに依頼します。 ~の承認後 エンドユーザが意図されたキャプティブポータルにリダイレクト動作

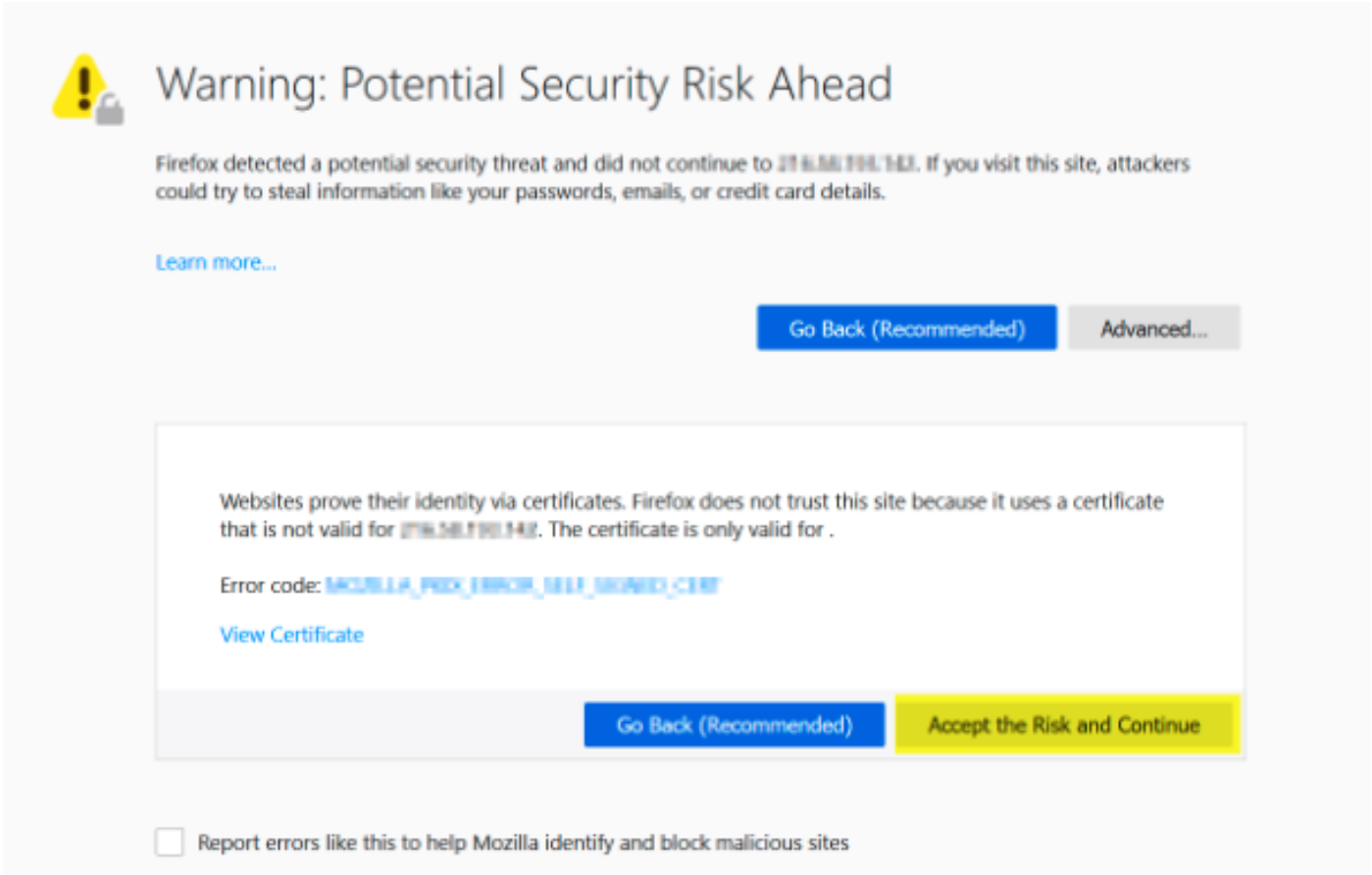
を実行するリスク：

注：続行するアクションは、特定のブラウザの[詳細オプション]で非表示にできます。

74より前のGoogle Chromeバージョンでは、図に示すようにアラートが表示されます。



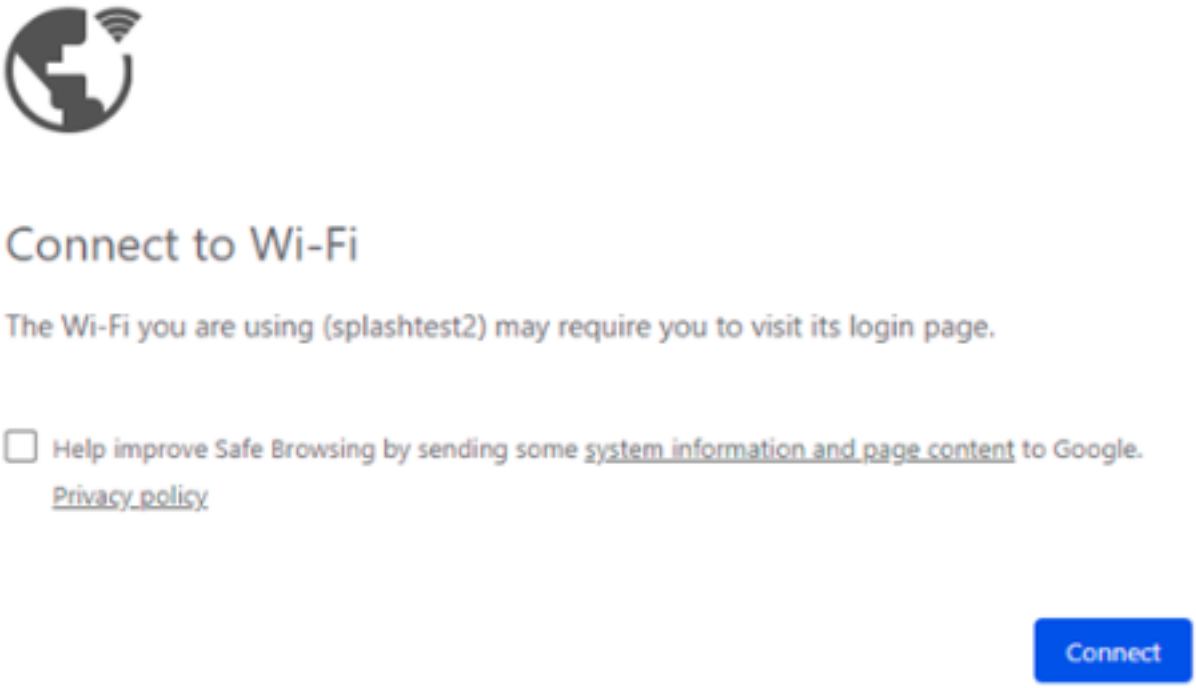
66より前のMozilla Firefoxバージョンでは、図に示すようにアラートが表示されます。



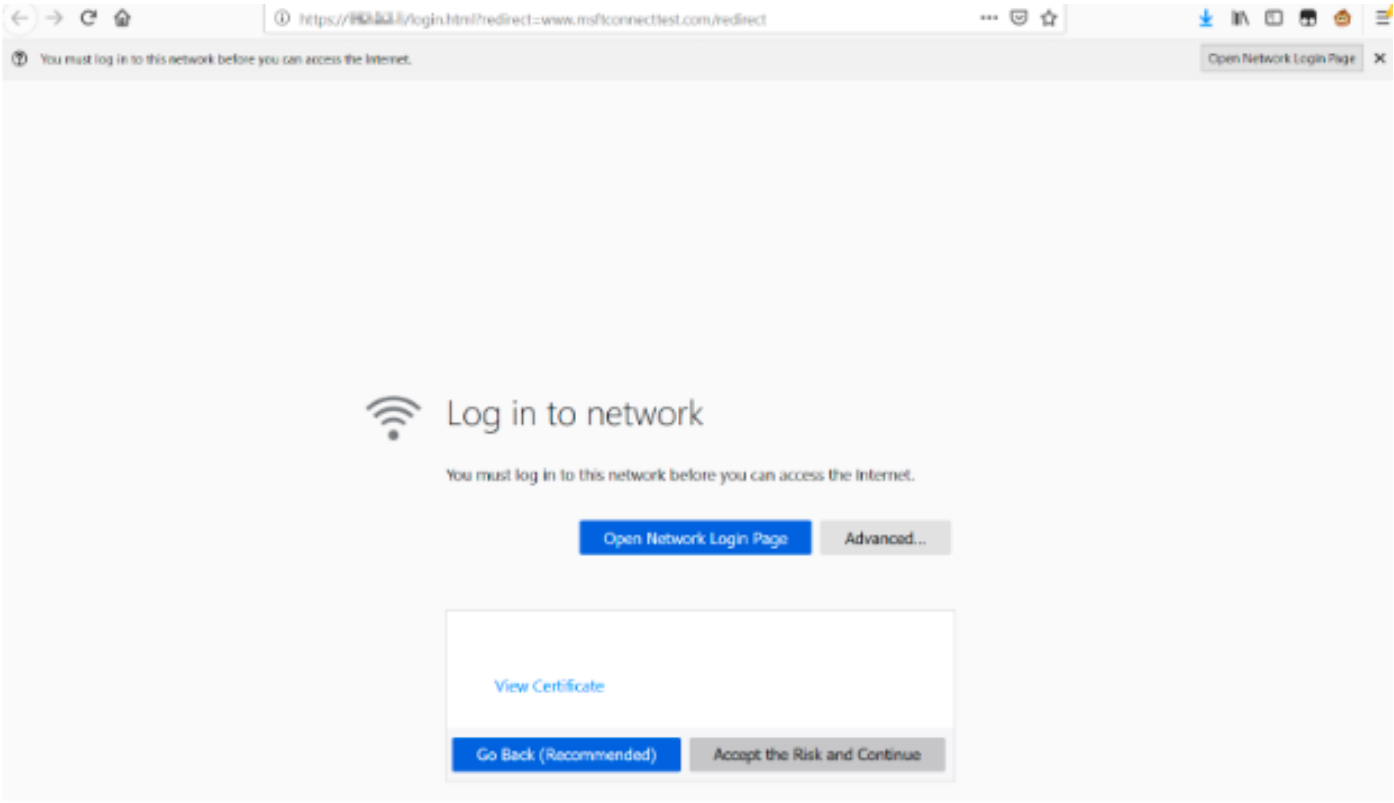
変更された動作

Google ChromeやMozilla Firefoxなどの一部のWebブラウザでは、証明書検証を通じてセキュアな接続を処理する方法が変更されました。Google Chrome（74.x以降）およびMozilla Firefox（66.x以降）では、ブラウザが外部URLにクックレス要求を送信してから ユーザは、キャプティブポータルを参照できます。ただし、この要求はワイヤレスコントローラによって代行受信されます。これは、すべてのトラフィックが最終的な接続状態に達する前にブロックされるためです。要求 then キャプティブポータルへの新しいリダイレクトを開始します 作成 ユーザからのリダイレクトループ 次のURLにアクセスできない ポータルを参照してください。

Google Chrome 74.x以降では、次のアラートが表示されます。**Connect to Wi-Fiお使いのWi-Fiでは、次の図に示すようにログインページにアクセスする必要がある場合があります。**



Mozilla Firefox 66.x以降では、次のアラートが表示されます： **Login To networkインターネットにアクセスする前に、このネットワークにログインする必要があります。**次の図を参照してください。



このページには、[リスクを受け入れて**続行する]オプションが**あります。ただし、このオプションを選択すると、同じ情報を持つ新しいタブが作成されます。

> **注：**このドキュメントのバグは、ISEチームがカスタマーの外部参照として送信したものです。CSCvj04703 - Chrome:ゲスト/BYODポータルのリダイレクトフローが、ISEポータルの信頼できない証明書で壊れている。

解決方法

内部Web認証（WLCの内部Webログインページ）の回避策

オプション 1

WLCでWebAuth SecureWebを無効にします。この問題は、HTTPSセキュリティメカニズムを作成するための証明書の検証によって発生するため、 使用 HTTPを使用して証明書の検証をスキップし、クライアントがキャプティブポータルをレンダリングできるようにします。

WLCでWebAuth SecureWebを無効にするには、次のコマンドを実行します。

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

注：変更を有効にするには、WLCをリブートする必要があります。

オプション 2

別のWebブラウザを使用します。これまでのところ、この問題はGoogle ChromeやMozilla Firefoxに分離されています。したがって、Internet Explorer、Edge、およびネイティブAndroidのWebブラウザなどのブラウザでは、この動作は表示されず、キャプティブポータルにアクセスするために使用できます。

外部Web認証の回避策

オプション 1

このWeb認証プロセスのバリエーションでは、事前認証アクセスリストを通じた通信制御が可能なため、ユーザがキャプティブポータルに継続できるように例外を追加できます。このような例外は、URLアクセスリストを使用して行います(集中型WLANではAireOSバージョン8.3.x、FlexConnectローカルスイッチングWLANでは8.7.xからサポートが開始されます)。 URLはWebブラウザによって異なる場合がありますが、次のように識別されています http://www.gstatic.com/ Google Chromeおよび http://detectportal.firefox.com/ Mozilla Firefox向け

パーマネント フィックス

この問題を解決するには、信頼できる認証局(CA)によって発行されたSHA-2アルゴリズムを使用するWebAuth SSL証明書をWLCにインストールすることを推奨します。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- サードパーティ証明書用 CSR の生成とチェーン証明書の WLC へのダウンロード
- Google Chromeプライバシーホワイトペーパー
- テクニカル サポートとドキュメント – Cisco Systems