瞭解無線客戶端上的HTTPS Web身份驗證證書不信任行為並對其進行故障排除

目錄

簡介

本文描述無線客戶端在對Web瀏覽器處理安全套接字層(SSL)證書的方式進行更改後，連線到第3層身份驗證無線區域網(WLAN)時的行為。

必要條件

需求

思科建議您瞭解以下主題：

- 安全超文字傳輸通訊協定(HTTPS)。
- SSL證書。
- Cisco WLAN無線LAN控制器(WLC)。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Chrome Web瀏覽器74.x或更高版本。
- Firefox Web瀏覽器66.x或更高版本。
- Cisco無線LAN控制器8.5.140.0版或更高版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

超文字傳輸通訊協定 (HTTP)Internet上的網站流量不安全，可能會被無意中的個人攔截和處理。因此，敏感應用越來越多地使用HTTP，因此有必要實施其他安全措施，如SSL/TLS加密（構成HTTPS）。

HTTPS要求使用 SSL 用於驗證網站身份並允許在web伺服器和終端瀏覽器之間建立安全連線的證書。SSL證書必須由受信任的證書頒發機構(CA)頒發，該證書包含在瀏覽器和作業系統的受信任CA根證書清單中。

最初SSL證書使用安全雜湊演算法第1版(SHA-1)，它使用160位雜湊。但是，由於各種缺陷，SHA-1已逐漸被SHA-2所取代，後者是一組長度不同的雜湊演算法，其中最受歡迎的是256位。

問題

不受信任證書的常見方案

Web瀏覽器不信任SSL證書的原因有幾個，但最常見的原因是：

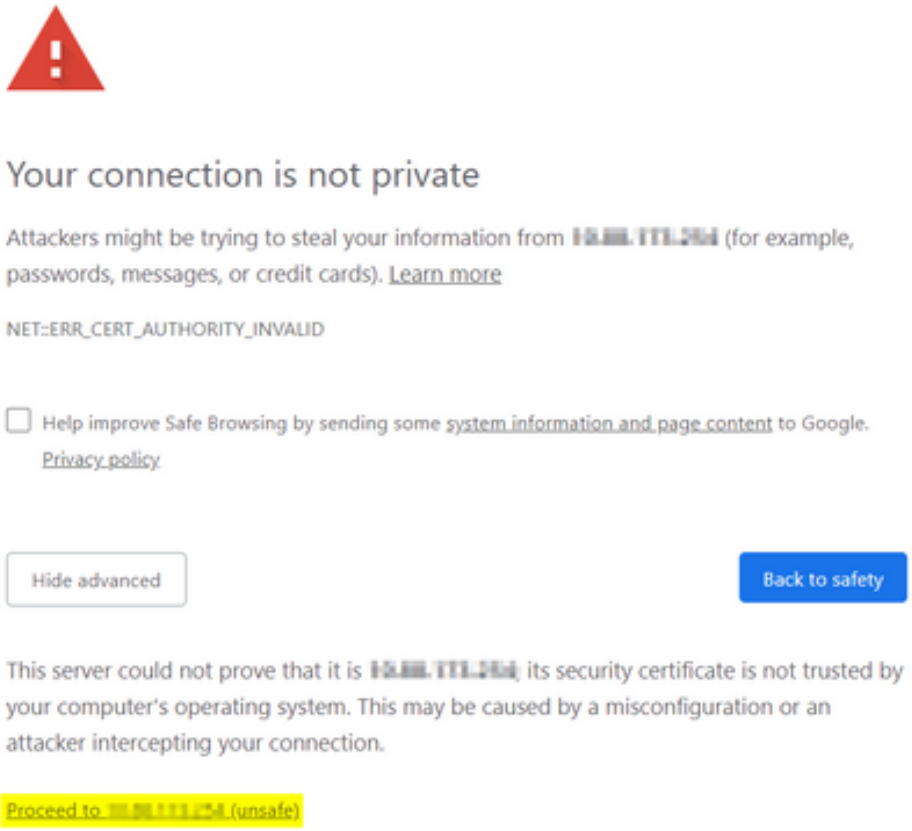
- 證書不是由受信任的證書頒發機構頒發(證書是自簽名的，或者客戶端未安裝根CA證書（如果是內部CA））。
- 證書的公用名(CN)或使用者替代名稱(SAN)欄位與為導航到此類站點而輸入的統一資源定位符(URL)不匹配。
- 憑證已到期或使用者端上的時鐘設定錯誤（在憑證有效期之外）。
- 中間CA或裝置憑證（如果沒有中間CA）正在使用SHA-1演演算法。

先前行為

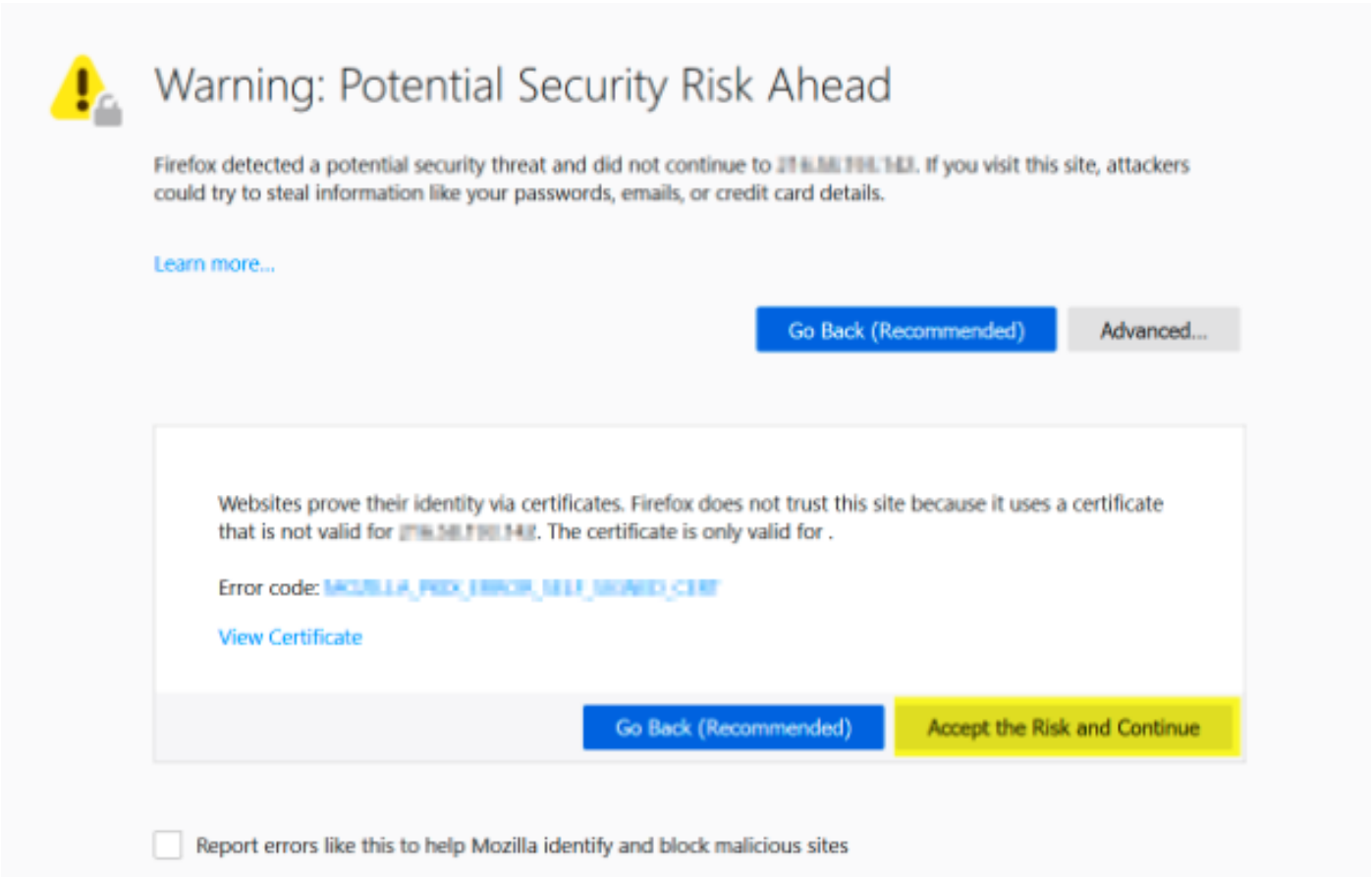
當早期版本的Web瀏覽器檢測到裝置證書不可信時，它們會提示安全 警報 （每個瀏覽器上的文本和外觀各不相同）。 安全性 警報 要求使用者接受安全風險並繼續訪問預期網站，或拒絕連線。 接受後 使用者將終端使用者重定向到預期強制網路門戶的風險：

> **附註**：可以在特定瀏覽器的「高級選項」下隱藏要執行的操作。

低於74的Google Chrome版本會顯示警報，如下圖所示：



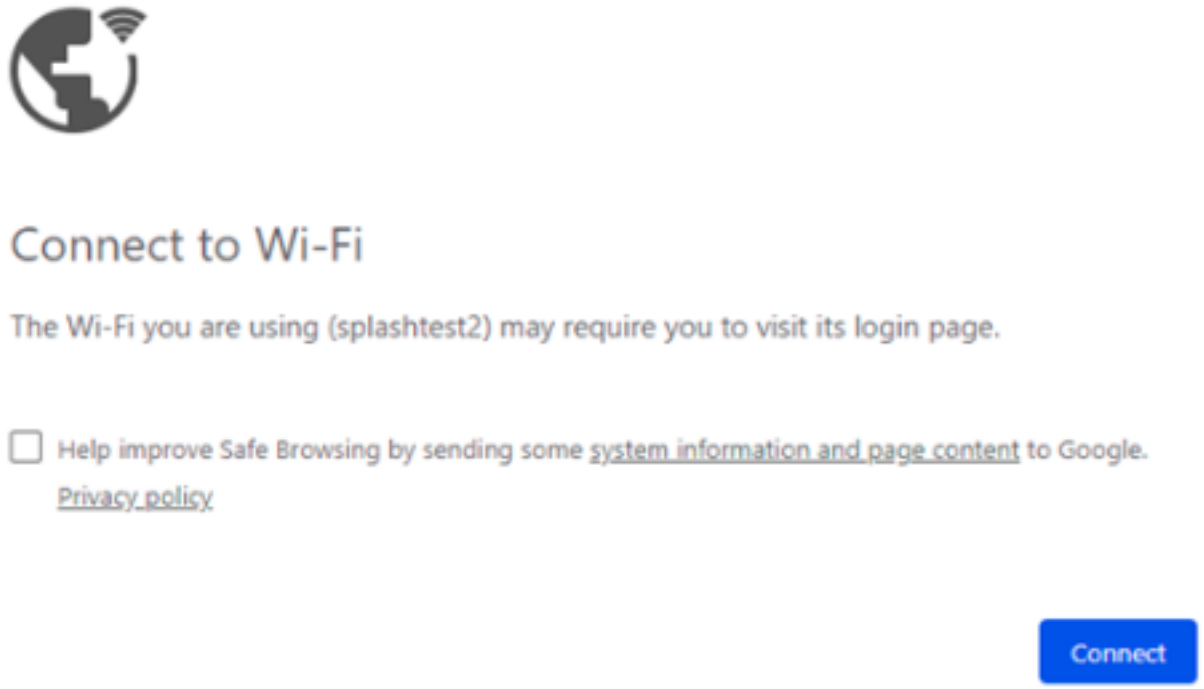
低於66的Mozilla Firefox版本將顯示警報，如下圖所示：



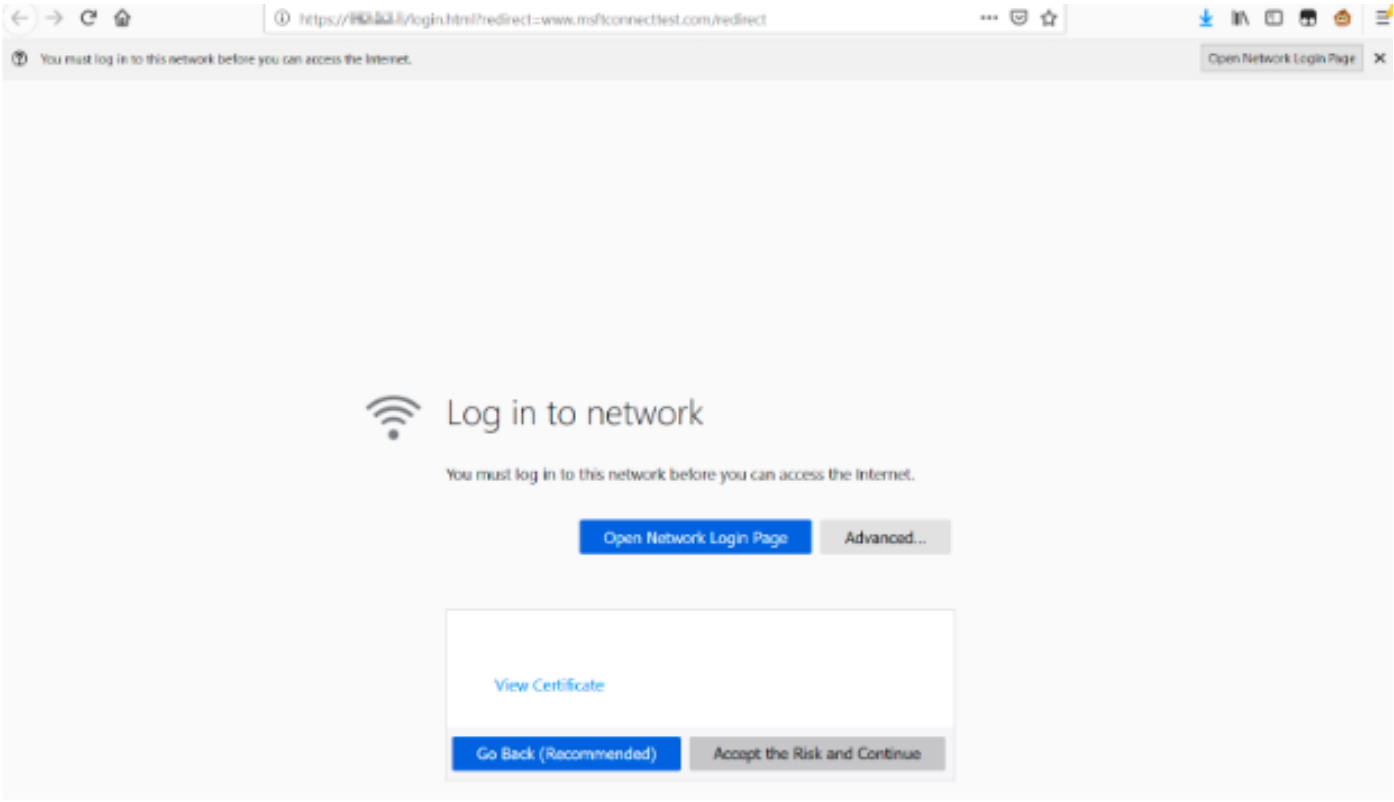
行為更改

Google Chrome和Mozilla Firefox等某些網路瀏覽器通過證書驗證改變了處理安全連線的方法。Google Chrome（74.x及更高版本）和Mozilla Firefox（66.x及更高版本）要求瀏覽器先向外部URL傳送無提示請求 允許使用者瀏覽強制網路門戶。但是，此請求會被無線控制器攔截，因為所有流量在到達最終連線狀態之前都會被阻止。請求 然後 啟動到強制網路門戶的新重定向 建立 由於使用者 無法 請參閱入口網站。

Google Chrome 74.x及更高版本顯示警報：**連線到Wi-Fi您使用的Wi-Fi可能需要您訪問其登入頁面**，如下圖所示：



Mozilla Firefox 66.x及更高版本顯示警報： **Login To network您必須先登入此網路才能訪問Internet**，如下圖所示：



此頁面包括**接受風險並繼續**選項。但是，選擇此選項後，會建立一個具有相同資訊的新頁籤。

> **附註**：此文檔錯誤由ISE團隊作為客戶的外部參考提交：CSCvj04703 - Chrome:訪客/BYOD門戶上的重定向流與ISE門戶上的不受信任證書斷開。

解決方案

內部Web-Auth的解決方法（WLC的內部Web登入頁面）

選項1

在WLC上停用WebAuth SecureWeb。由於此問題是由用於建立HTTPS安全機制的證書驗證引起的，使用 HTTP跳過證書驗證並允許客戶端呈現強制網路門戶。

若要在WLC上停用WebAuth SecureWeb，您可以執行命令：

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

> **附註**：您必須重新啟動WLC以使變更生效。

選項2

使用其他Web瀏覽器。迄今為止，這個問題被孤立於谷歌Chrome和Mozilla Firefox;因此，Internet Explorer、Edge和本機Android Web瀏覽器等瀏覽器不會出現此行為，可用於訪問強制網路門戶。

外部Web-Auth的解決方法

選項1

由於Web身份驗證過程的這種變體允許通過預身份驗證訪問清單進行通訊控制，因此可以新增異常，以便使用者可以繼續訪問強制網路門戶。此類例外通過URL訪問清單來完成(集中式WLAN的AireOS版本8.3.x和FlexConnect本地交換WLAN的8.7.x版開始支援)。 URL可能取決於Web瀏覽器，但它們被標識為 http://www.gstatic.com/ 適用於Google Chrome和 http://detectportal.firefox.com/ 用於Mozilla Firefox。

永久修復

為了解決此問題，建議在WLC中安裝具有由受信任憑證授權機構頒發的SHA-2演算法的WebAuth SSL憑證。

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- **產生第三方憑證的 CSR，並將鏈結的憑證下載到 WLC**
- **Google Chrome隱私白皮書**
- **技術支援與文件 - Cisco Systems**