Understand and Troubleshoot HTTPS WebAuthentication Certificate Mistrust Behavior on Wireless Clients

Contents

Introduction

This document describes the wireless clients behavior when they connect to a Layer 3 authentication Wireless Local Area Network (WLAN) after changes made on how web browsers handle Secure Sockets Layer (SSL) certificates.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- HyperText Transfer Protocol Secure (HTTPS).
- SSL certificates.
- CIsco WIreless LAN Controller (WLC).

Components Used

The information in this document is based on these software and hardware versions:

- Chrome web browser version 74.x or higher.
- Firefox web browser version 66.x or higher.
- Cisco Wireless LAN Controller version 8.5.140.0 or higher.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Hypertext Transfer Protocol **(**HTTP) traffic for websites on the Internet is not secure and can be intercepted and processed by unintended individuals. Therefore, increased use of HTTP for sensitive applications made necessary to implement additional security measures as SSL/TLS encryption, which constitutes HTTPS.

HTTPS requires the use of SSL certificates to validate the identity of a website and allows to establish a secure connection between the web server and the endpoint’s browser. SSL certificates must be issued by a trusted Certificate Authority (CA) that is included in the list of trusted CA root certificates of browsers and operating systems.

Initially, SSL certificates used Secure Hashing Algorithm version 1 (SHA-1), which uses a 160-bit hash. However, due to a variety of weaknesses, SHA-1 has been progressively replaced by SHA-2, a group of hashing algorithms with different lengths between which the most popular is 256-bit.

Problem

Common Scenarios for Untrusted Certificates

There are several reasons for a web browser to not trust an SSL certificate, but the most common reasons are:

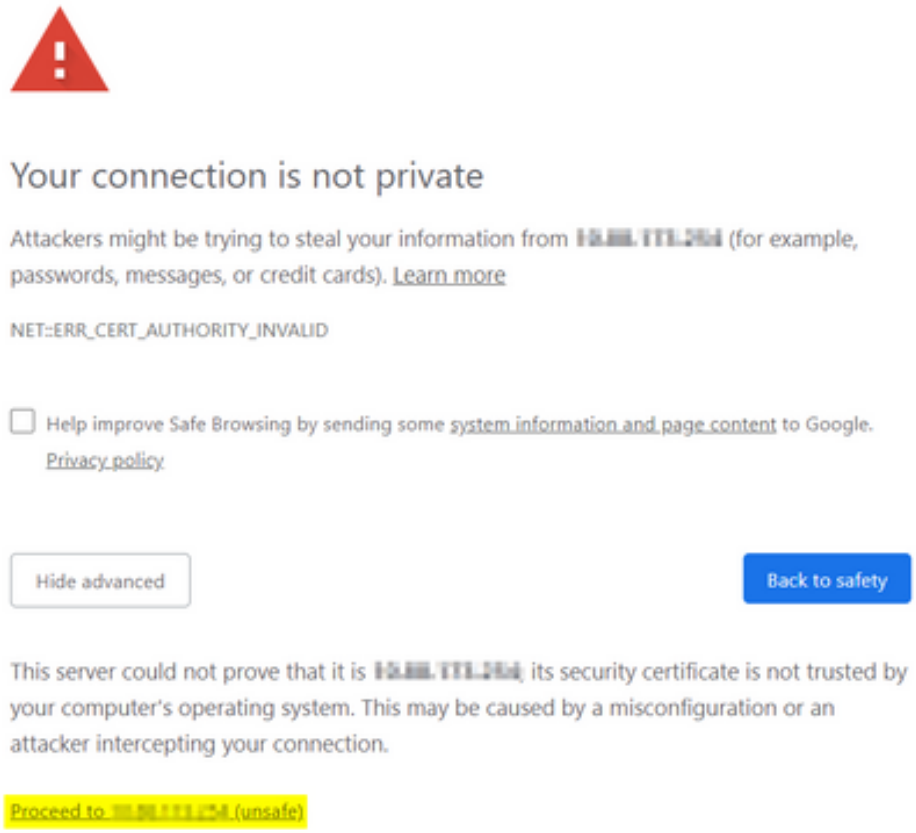
- The certificate is not issued by a trusted Certificate Authority (either the certificate is self-signed or the client doesn't have the root CA certificate installed in case of internal CA).
- The Common Name (CN) or Subject Alternate Name (SAN) fields of the certificate don’t match the Uniform Resource Locator (URL) entered to navigate to such site.
- The certificate has expired or the clock on the client is misconfigured (outside of the validity period of the certificate).
- SHA-1 algorithm is in use by the intermediate CA, or the device certificate (in case there are no intermediate CA).

Previous Behavior

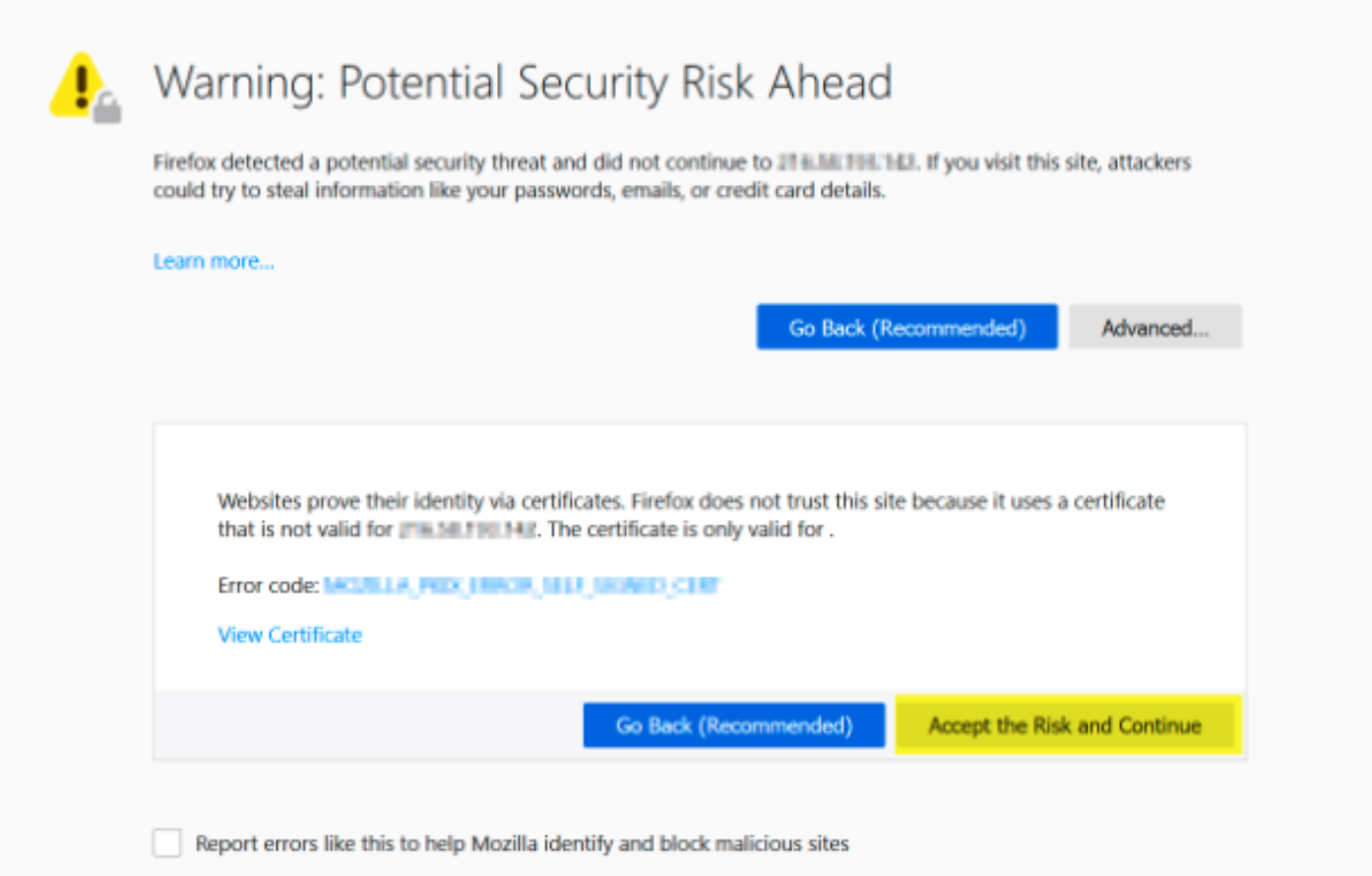
When earlier versions of web browsers detect a device certificate as untrusted, they prompt to a security alert (text and appearance vary on each browser). The security alert asks the user to accept the security risk and continue to the intended website, or refuse the connection. After acceptance of the risk the user gets redirection behavior for the end user to the intended captive portal:

Note: The action to proceed can be hidden under Advanced Options on specific browsers.

Google Chrome versions lower than 74 display the alert as shown in the image:



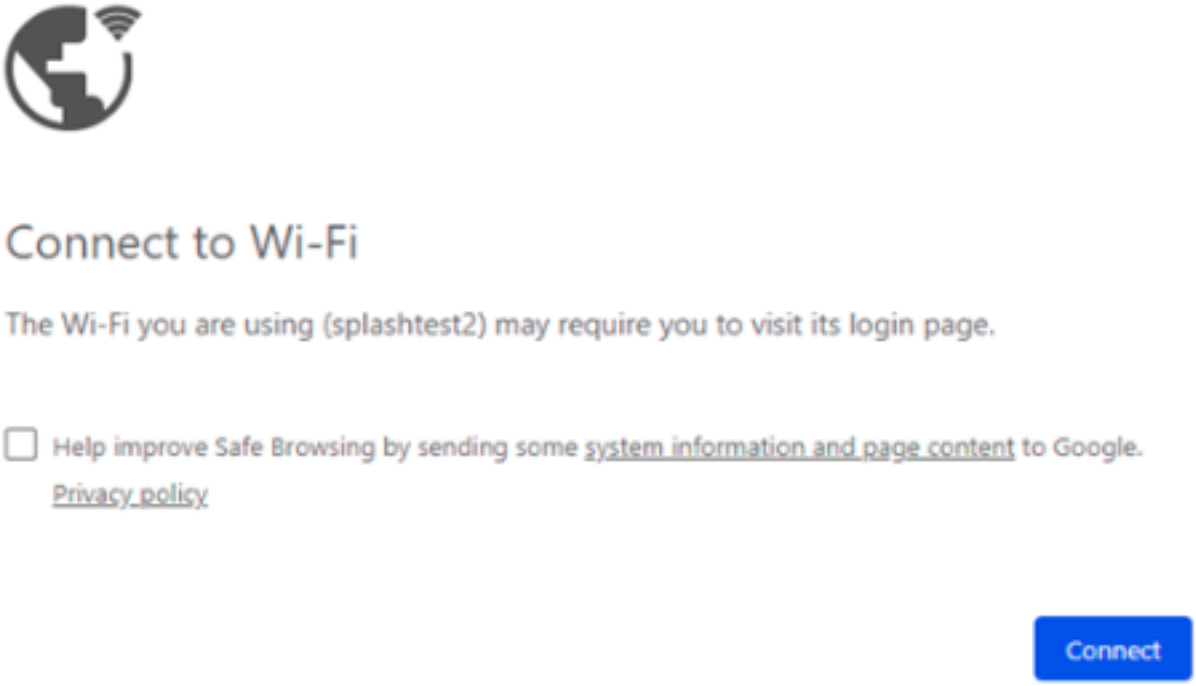
Mozilla Firefox versions lower than 66 display the alert as shown in the image:



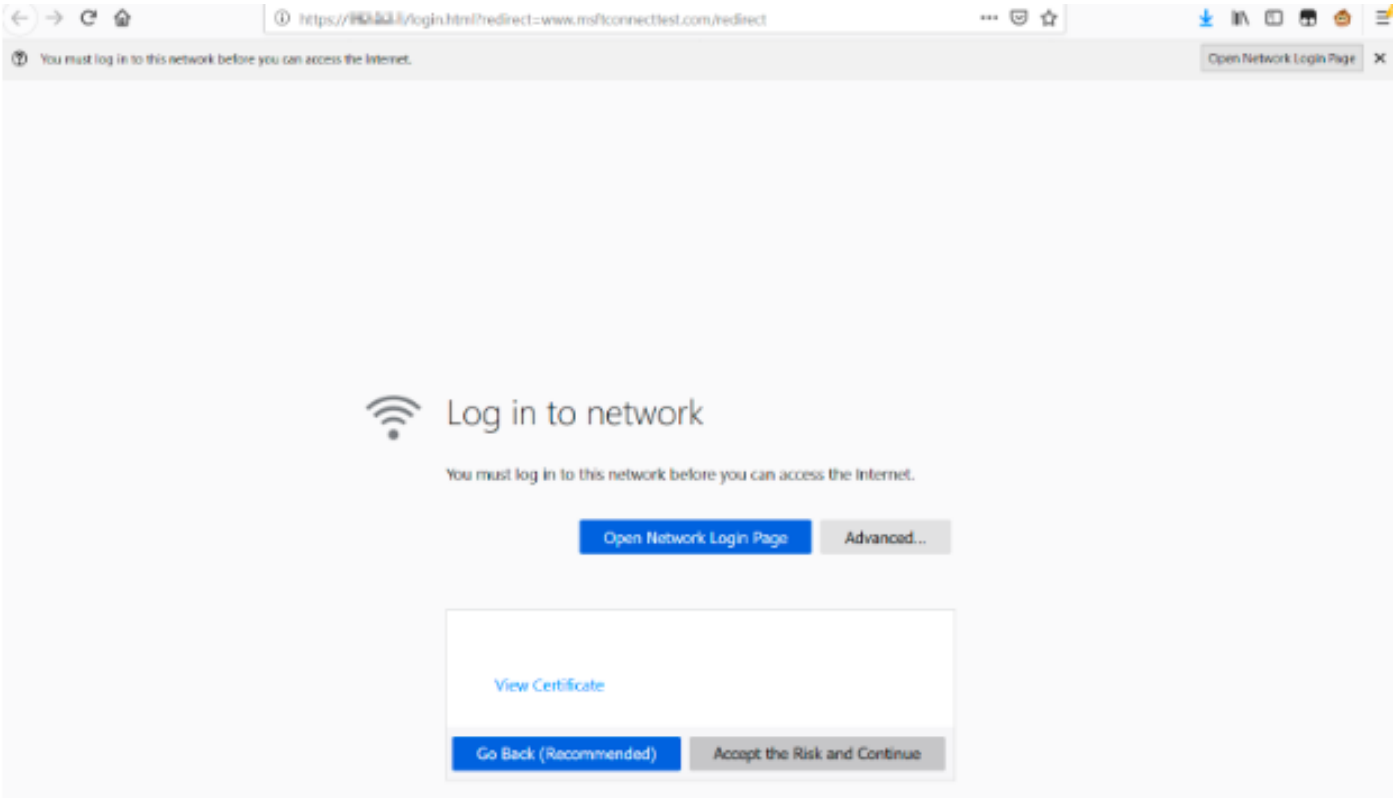
Changed Behavior

Some web browsers as Google Chrome and Mozilla Firefox changed the way they handle secure connections through certificate verification. Google Chrome (74.x and higher) and Mozilla Firefox (66.x and higher) require the browser to send a cookieless request to external URLs before the user can be allowed to browse to the captive portal. This request, however, is intercepted by the Wireless Controller since all traffic is blocked before it can reach the final connectivity state. The request then initiates a new redirection to the captive portal which creates a redirection loop since the user is unable to see the portal.

Google Chrome 74.x and above displays the alert: **Connect to Wi-Fi The Wi-Fi you are using may require you to visit its login page**, as shown in the image:



Mozilla Firefox 66.x and above displays the alert: **Login To network You must log in to this network before you can access the Internet**, as shown in the image:



This page includes an **Accept the Risk and Continue** option. However, when this option is selected, a new tab with the same information is created.

> **Note**: This documentation bug was submitted by the ISE team as an external reference for customers:CSCvj04703 - Chrome: Redirection flow on guest/BYOD portal is broken with untrusted certificate on ISE portal.

Solution

Workaround for Internal Web-Auth (WLC’s internal web login page)

Option 1

Disable WebAuth SecureWeb on the WLC. Since the issue is caused by the certificate validation to create the HTTPS security mechanism, use HTTP to skip the certificate validation and allow clients to render the captive portal.

In order to disable WebAuth SecureWeb on the WLC you can run the command:

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

> **Note**: You must reboot the WLC for the change to take effect.

Option 2

Use alternate web browsers. So far the issue has been isolated to Google Chrome, and Mozilla Firefox; therefore, browsers such as Internet Explorer, Edge, and native Android web browsers do not present this behavior and can be used to access the captive portal.

Workaround for External Web-Auth

Option 1

Since this variation of the web authentication process allows for communications control through the pre-authentication access list, an exception can be added so that the users can continue to the captive portal. Such exceptions are done through URL access lists (support starts on AireOS versions 8.3.x for centralized WLANs and 8.7.x for FlexConnect Local Switching WLANs). The URLs may be dependant on web browsers, but they have been identified as http://www.gstatic.com/ for Google Chrome and http://detectportal.firefox.com/ for Mozilla Firefox.

Permanent Fix

In order to solve this problem, it’s recommended to install a WebAuth SSL certificate with SHA-2 algorithm, issued by a trusted Certificate Authority, in the WLC.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- **Generate CSR for Third-Party Certificates and Download Chained Certificates to the WLC**
- **Google Chrome Privacy Whitepaper**
- **Technical Support & Documentation - Cisco Systems**