Comprensión y resolución de problemas del comportamiento de desconfianza del certificado de autenticación web HTTPS en clientes inalámbricos

Contenido

Introducción

Este documento describe el comportamiento de los clientes inalámbricos cuando se conectan a una red de área local inalámbrica (WLAN) de autenticación de capa 3 después de realizar cambios en cómo los navegadores web manejan los certificados de capa de conexión segura (SSL).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Protocolo de transferencia de hipertexto seguro (HTTPS).

- Certificados SSL.
- Controlador de LAN inalámbrica de Cisco (WLC).

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Chrome web browser versión 74.x o posterior.
- Navegador web Firefox versión 66.x o superior.
- Controlador de LAN inalámbrica de Cisco versión 8.5.140.0 o superior.

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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Protocolo de transferencia de hipertexto (HTTP) el tráfico de sitios web en Internet no es seguro y puede ser interceptado y procesado por individuos no deseados. Por lo tanto, el mayor uso de HTTP para aplicaciones sensibles se hace necesario para implementar medidas de seguridad adicionales como cifrado SSL/TLS, que constituye HTTPS.

HTTPS requiere el uso de SSL certificados para validar la identidad de un sitio web y permite establecer una conexión segura entre el servidor web y el explorador del terminal. Los certificados SSL deben ser emitidos por una Autoridad de Certificación (CA) de confianza que se incluya en la lista de certificados raíz de CA de confianza de navegadores y sistemas operativos.

Inicialmente, los certificados SSL utilizaban Secure Hashing Algorithm versión 1 (SHA-1), que utiliza un hash de 160 bits. Sin embargo, debido a una variedad de debilidades, SHA-1 ha sido reemplazado progresivamente por SHA-2, un grupo de algoritmos de hash con diferentes longitudes entre las cuales la más popular es de 256 bits.

Problema

Escenarios comunes para certificados no fiables

Hay varias razones por las que un navegador web no confía en un certificado SSL, pero las razones más comunes son:

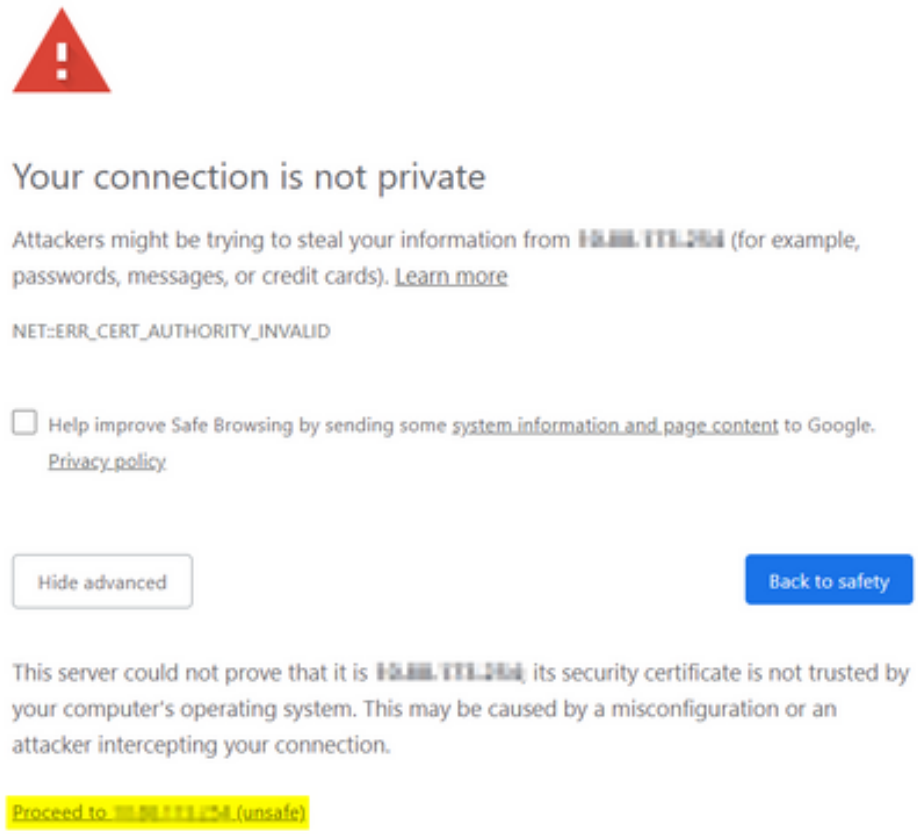
- El certificado no es emitido por una Autoridad de Certificación de Confianza (el certificado es autofirmado o el cliente no tiene instalado el certificado de CA raíz en caso de CA interna).
- Los campos Nombre común (CN) o Nombre alternativo del asunto (SAN) del certificado no coinciden con la URL (localizador uniforme de recursos) introducida para desplazarse a dicho sitio.
- El certificado ha caducado o el reloj del cliente está mal configurado (fuera del período de validez del certificado).
- El algoritmo SHA-1 está siendo utilizado por la CA intermedia o el certificado del dispositivo (en caso de que no haya una CA intermedia).

Comportamiento anterior

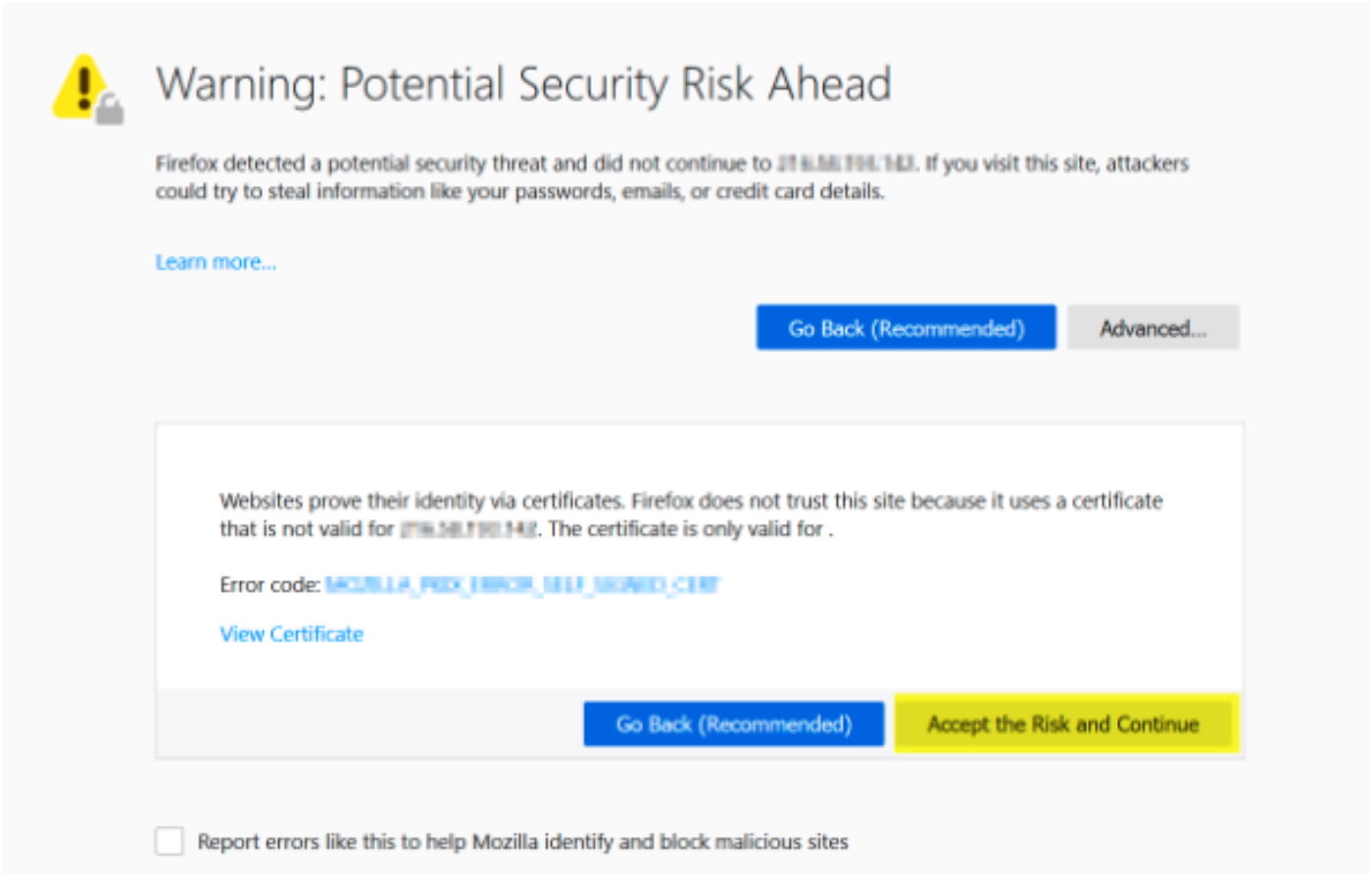
Cuando las versiones anteriores de los exploradores web detectan un certificado de dispositivo como no fiable, indican una seguridad alerta (el texto y la apariencia varían en cada navegador). La seguridad alerta pide al usuario que acepte el riesgo de seguridad y continúe en el sitio web previsto, o que rechace la conexión. Tras la aceptación de el riesgo de que el usuario obtenga un comportamiento de redirección para el usuario final al portal cautivo previsto:

> **Nota:** La acción para continuar se puede ocultar en Opciones avanzadas en exploradores específicos.

Las versiones de Google Chrome inferiores a 74 muestran la alerta como se muestra en la imagen:



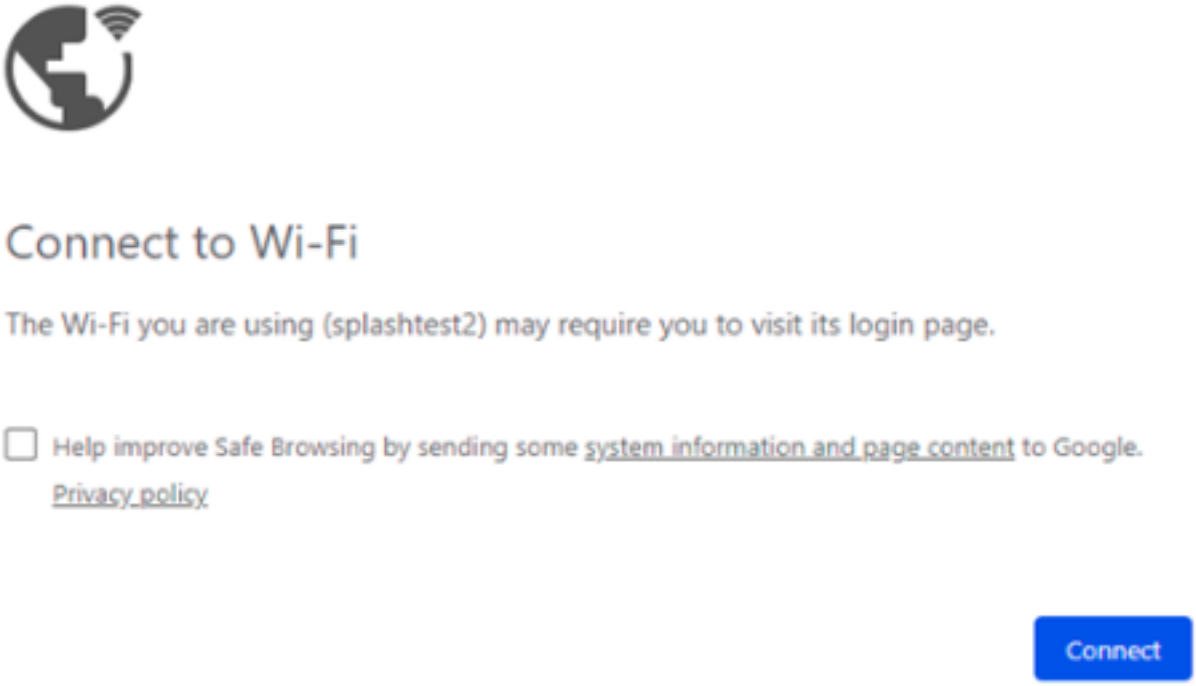
Las versiones de Mozilla Firefox inferiores a 66 muestran la alerta como se muestra en la imagen:



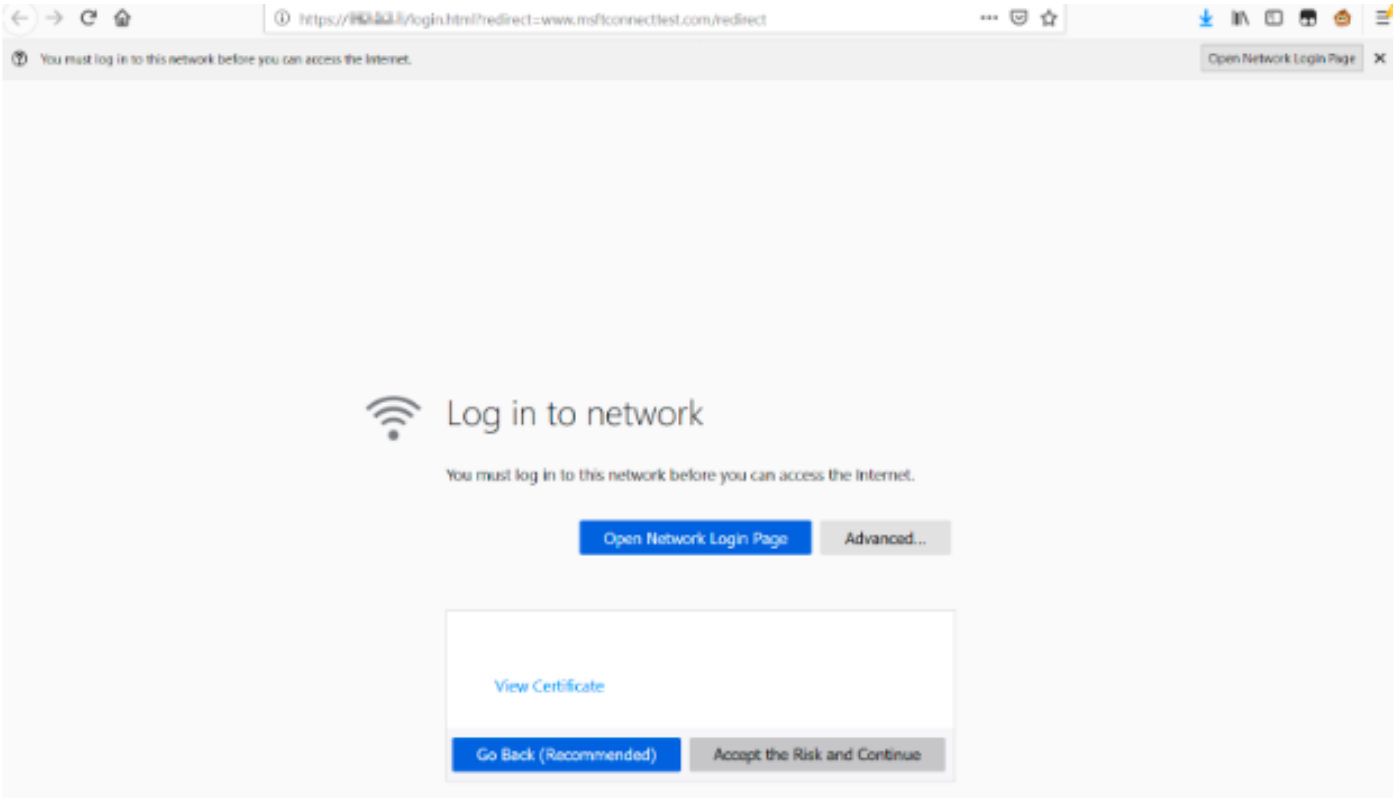
Comportamiento cambiado

Algunos navegadores web, como Google Chrome y Mozilla Firefox, cambiaron la forma en que manejan las conexiones seguras a través de la verificación de certificados. Google Chrome (74.x y superiores) y Mozilla Firefox (66.x y superiores) requieren que el navegador envíe una solicitud sin sentido a URL externas antes el usuario puede navegar al portal cautivo. Sin embargo, esta solicitud es interceptada por el controlador inalámbrico, ya que todo el tráfico está bloqueado antes de que pueda alcanzar el estado de conectividad final. La solicitud luego inicia una nueva redirección al portal cautivo que crea un bucle de redirección desde el usuario no puede consulte el portal.

Google Chrome 74.x y superiores muestra la alerta: **Connect to Wi-Fi (Conectarse a Wi-Fi) La Wi-Fi que está utilizando puede requerir que visite su página de inicio de sesión**, como se muestra en la imagen:



Mozilla Firefox 66.x y superiores muestra la alerta: **Login To Network (Iniciar sesión en la red) Debe iniciar sesión en esta red antes de poder acceder a Internet**, como se muestra en la imagen:



Esta página incluye una opción **Aceptar el riesgo y continuar**. Sin embargo, cuando se selecciona esta opción, se crea una nueva pestaña con la misma información.

> **Nota:** Este error de documentación fue enviado por el equipo de ISE como referencia externa para los clientes:CSCvj04703 - Chrome: El flujo de redirección en el portal de invitados/BYOD se rompe con un certificado no fiable en el portal de ISE.

Solución

Solución alternativa para autenticación web interna (página de inicio de sesión web interna del WLC)

Opción 1

Inhabilite WebAuth SecureWeb en el WLC. Dado que el problema es causado por la validación del certificado para crear el mecanismo de seguridad HTTPS, uso HTTP para omitir la validación del certificado y permitir a los clientes representar el portal cautivo.

Para inhabilitar WebAuth SecureWeb en el WLC puede ejecutar el comando:

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

> **Nota:** Debe reiniciar el WLC para que el cambio tenga efecto.

Opción 2

Utilice exploradores web alternativos. Hasta ahora, el problema se ha aislado de Google Chrome y Mozilla Firefox; por lo tanto, los exploradores como Internet Explorer, Edge y los exploradores web nativos de Android no presentan este comportamiento y se pueden utilizar para acceder al portal cautivo.

Solución alternativa para Web-Auth externa

Opción 1

Dado que esta variación del proceso de autenticación web permite el control de las comunicaciones a través de la lista de acceso de autenticación previa, se puede agregar una excepción para que los usuarios puedan continuar en el portal cautivo. Estas excepciones se realizan a través de listas de acceso de URL (la compatibilidad comienza en las versiones 8.3.x de AireOS para WLANs centralizadas y 8.7.x para WLANs de FlexConnect Local Switching). Las URL pueden depender de los exploradores web, pero se han identificado como http://www.gstatic.com/ para Google Chrome y http://detectportal.firefox.com/ para Mozilla Firefox.

Solución permanente

Para resolver este problema, se recomienda instalar un certificado SSL WebAuth con el algoritmo SHA-2, emitido por una Autoridad de Certificación de Confianza, en el WLC.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Generación de CSR para certificados de terceros y descarga de certificados encadenados al WLC
- Informe técnico sobre privacidad de Google Chrome
- Soporte Técnico y Documentación - Cisco Systems