Entender e solucionar problemas do comportamento de desconfiança do certificado de autenticação da Web HTTPS em clientes sem fio

Contents

Introduction

Este documento descreve o comportamento dos clientes sem fio quando eles se conectam a uma autenticação de Camada 3 da rede local sem fio (WLAN) após alterações feitas em como os navegadores da Web lidam com certificados SSL (Secure Sockets Layer).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- protocolo HTTPS (HyperText Transfer Protocol Secure).
- Certificados SSL.
- Controlador de LAN sem fio (WLC) da Cisco.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Chrome web browser versão 74.x ou superior.
- O navegador Firefox versão 6.x ou superior.
- Cisco Wireless LAN Controller versão 8.5.140.0 ou 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Protocolo de Transferência de Hipertexto (HTTP) o tráfego de sites na Internet não é seguro e pode ser interceptado e processado por indivíduos não intencionais. Portanto, o maior uso de HTTP para aplicativos sensíveis tornou-se necessário para implementar medidas de segurança adicionais como criptografia SSL/TLS, que constitui HTTPS.

O HTTPS requer o uso de SSL certificados para validar a identidade de um site e permite estabelecer uma conexão segura entre o servidor da Web e o navegador do endpoint. Os certificados SSL devem ser emitidos por uma autoridade de certificação (AC) confiável incluída na lista de certificados raiz de CA confiáveis de navegadores e sistemas operacionais.

Inicialmente, os certificados SSL usavam o Secure Hashing Algorithm versão 1 (SHA-1), que usa um hash de 160 bits. No entanto, devido a uma variedade de fraquezas, o SHA-1 foi progressivamente substituído pelo SHA-2, um grupo de algoritmos hash com diferentes comprimentos entre os quais o mais popular é 256 bits.

Problema

Cenários comuns para certificados não confiáveis

Há vários motivos para um navegador da Web não confiar em um certificado SSL, mas os motivos mais comuns são:

- O certificado não é emitido por uma autoridade de certificação fidedigna (o certificado é autoassinado ou o cliente não tem o certificado de AC raiz instalado no caso de AC interna).
- Os campos Common Name (CN) ou Subject Alternate Name (SAN) do certificado não correspondem ao Uniform Resource Locator (URL) inserido para navegar para esse site.
- O certificado expirou ou o relógio do cliente está configurado incorretamente (fora do período de validade do certificado).
- O algoritmo SHA-1 está sendo usado pela CA intermediária ou pelo certificado do dispositivo (caso não haja CA intermediária).

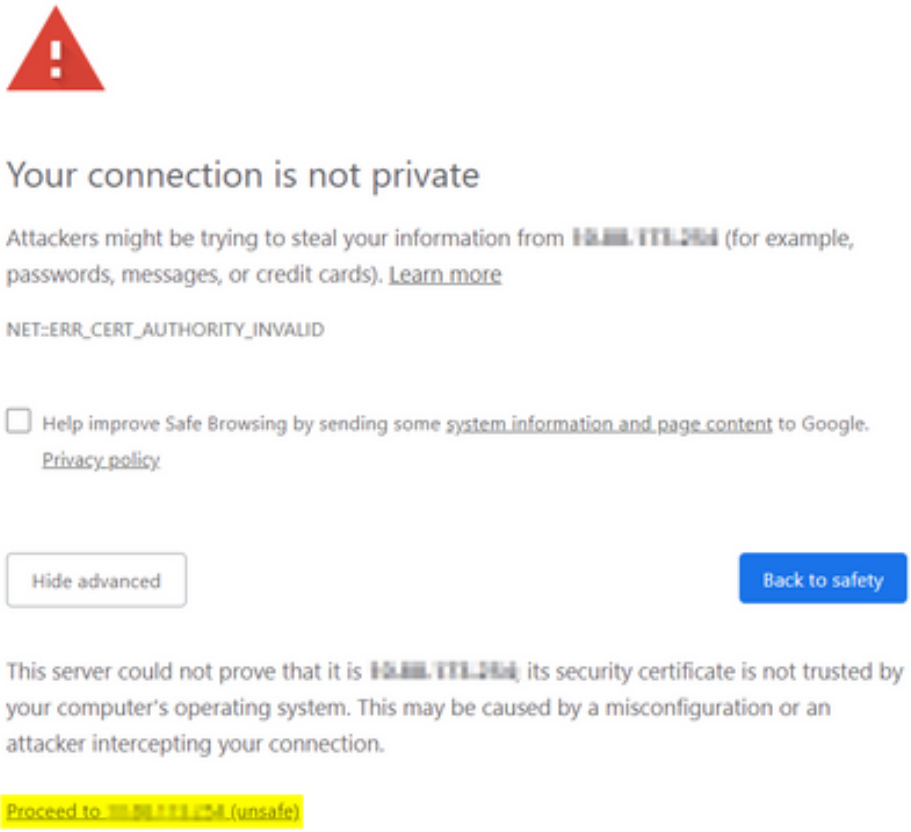
Comportamento anterior

Quando versões anteriores de navegadores da Web detectam um certificado de dispositivo como não confiável, eles solicitam uma segurança alerta (texto e aparência variam em cada

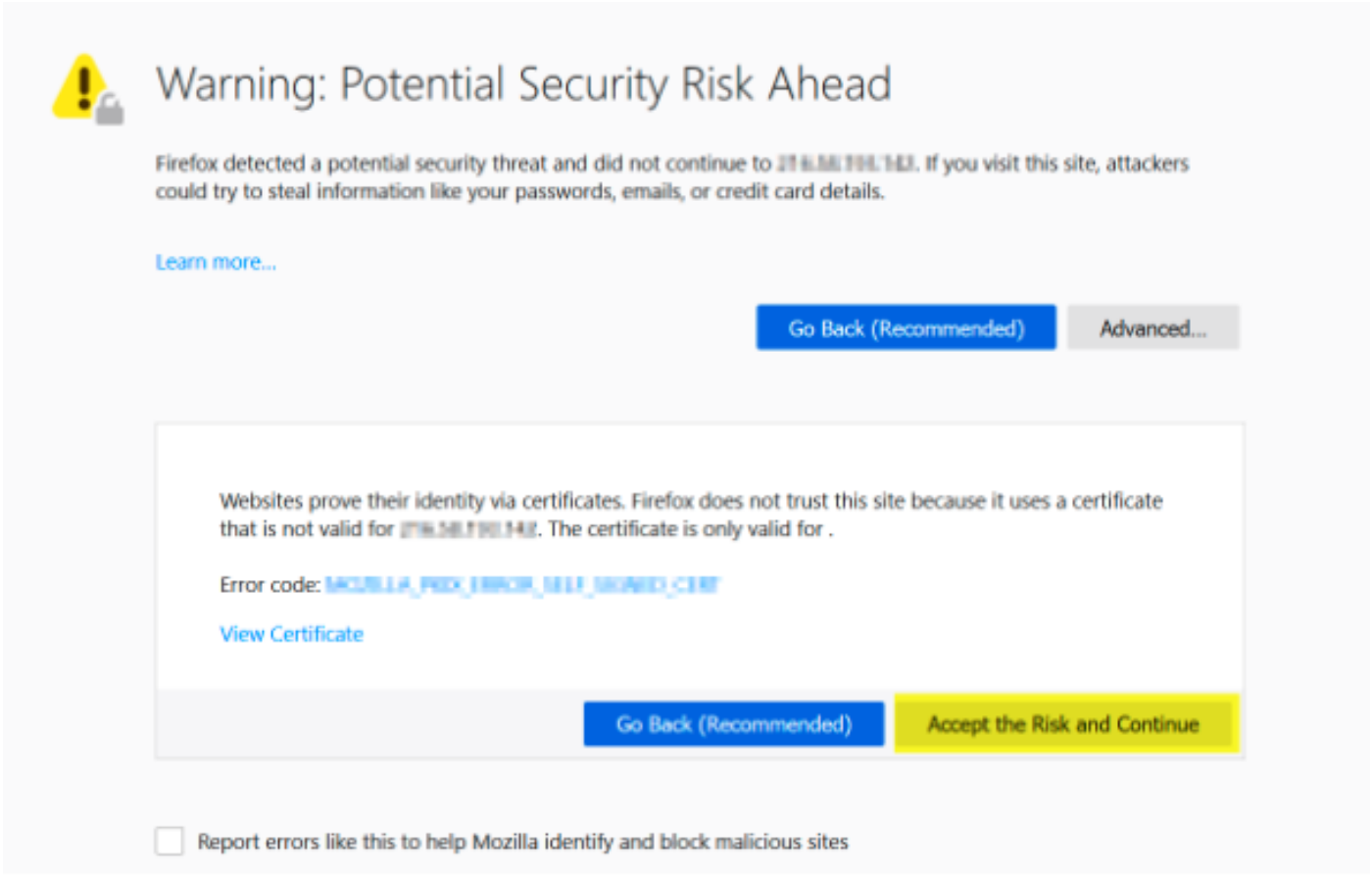
navegador). A segurança alerta solicita que o usuário aceite o risco de segurança e continue no site desejado, ou recuse a conexão. Após a aceitação do o risco de o usuário obter o comportamento de redirecionamento do usuário final para o portal cativo pretendido:

> **Note**: A ação a prosseguir pode ser oculta em Opções avançadas em navegadores específicos.

As versões do Google Chrome inferiores a 74 exibem o alerta como mostrado na imagem:



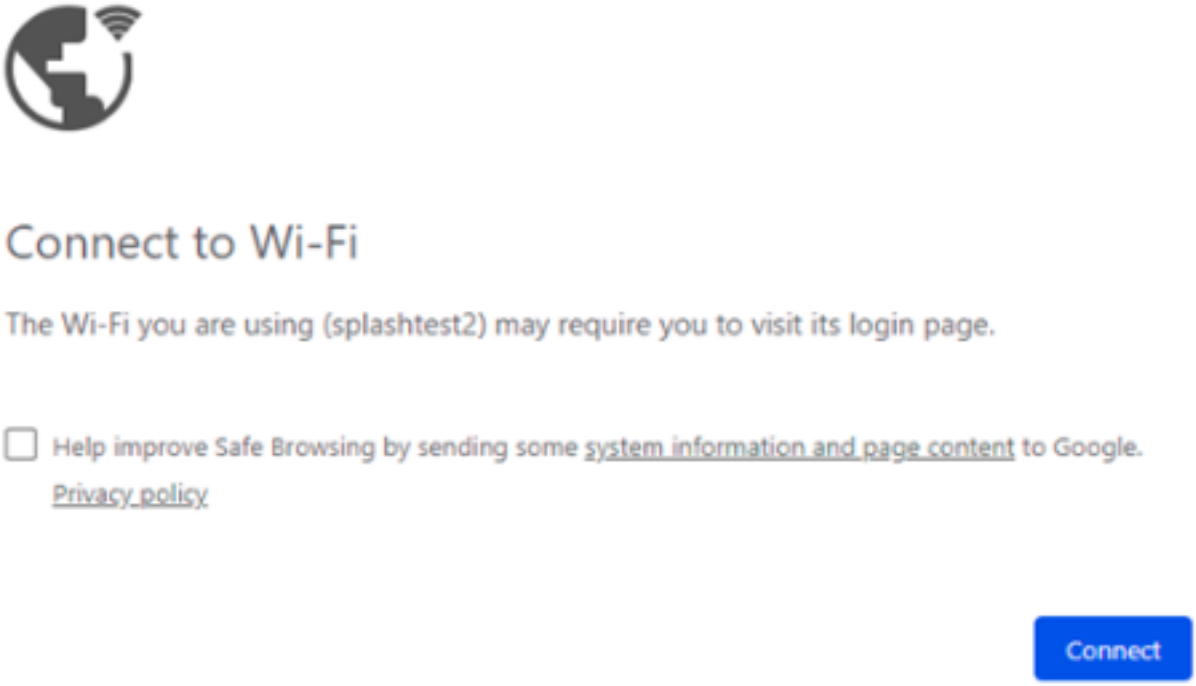
As versões inferiores a 66 do Mozilla Firefox exibem o alerta como mostrado na imagem:



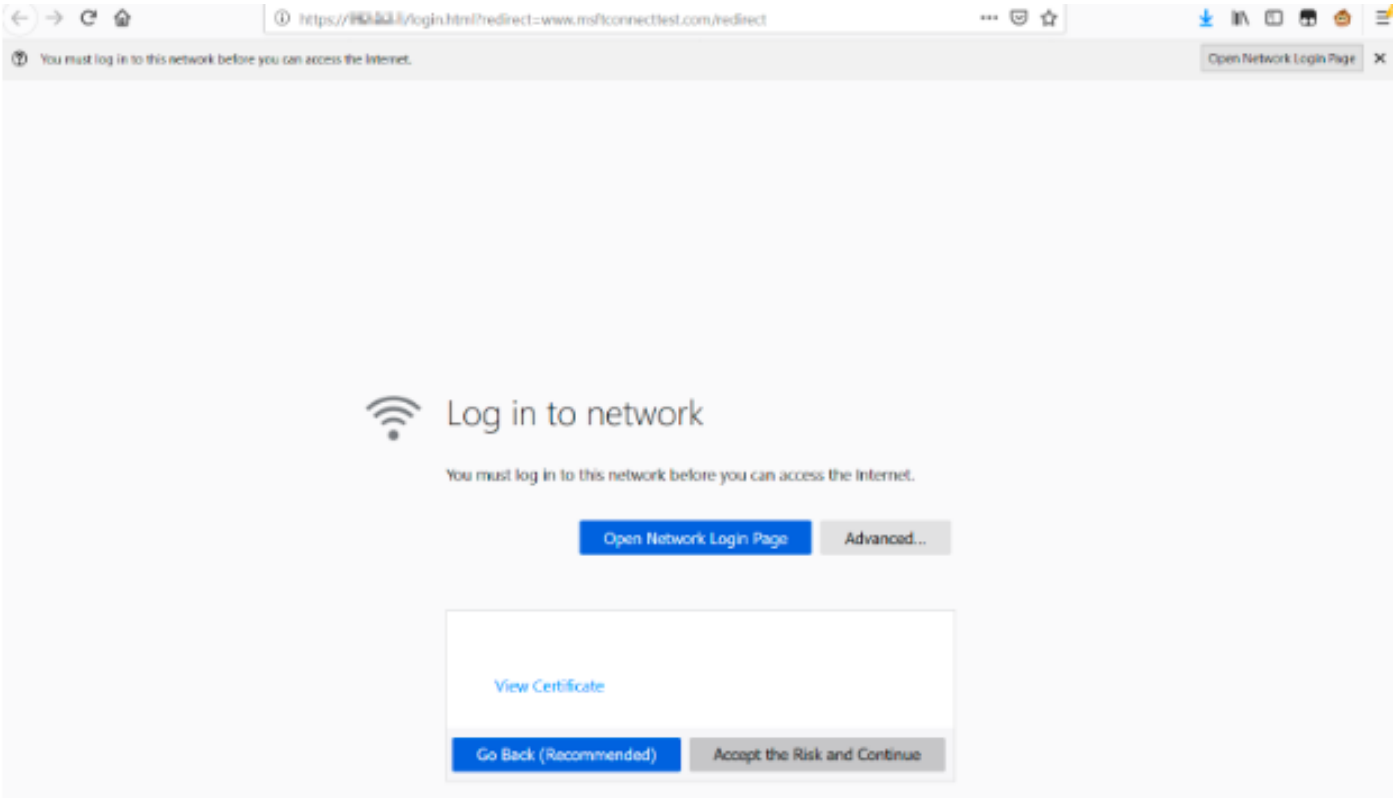
Comportamento alterado

Alguns navegadores da Web, como o Google Chrome e o Mozilla Firefox, mudaram a forma como lidam com conexões seguras através da verificação de certificados. O Google Chrome (74.x e superior) e o Mozilla Firefox (66.x e superior) exigem que o navegador envie uma solicitação sem cookies para URLs externas antes o usuário pode ter permissão para navegar até o portal cativo. Essa solicitação, no entanto, é interceptada pelo Wireless Controller, pois todo o tráfego é bloqueado antes de chegar ao estado de conectividade final. A solicitação em seguida inicia um novo redirecionamento para o portal cativo que cria um loop de redirecionamento desde o usuário não pode consulte o portal.

O Google Chrome 74.x e superior exibe o alerta: **Conectar-se ao Wi-Fi O Wi-Fi que você está usando pode exigir que você visite sua página de login**, como mostrado na imagem:



O Mozilla Firefox 66.x e superior exibe o alerta: **Fazer login na rede Você deve fazer login nessa rede antes de acessar a Internet**, como mostrado na imagem:



Esta página inclui uma opção **Aceitar o Risco e Continuar**. No entanto, quando essa opção é selecionada, uma nova guia com as mesmas informações é criada.

> **Note**: Este bug de documentação foi enviado pela equipe do ISE como referência externa para os clientes: CSCvj04703 - Chrome: O fluxo de redirecionamento no portal convidado/BYOD é interrompido com certificado não confiável no portal do ISE.

Solução

Solução alternativa para Web-Auth interno (página interna de login da Web do WLC)

Opção 1

Desative WebAuth SecureWeb na WLC. Como o problema é causado pela validação do certificado para criar o mecanismo de segurança HTTPS, use HTTP para ignorar a validação do certificado e permitir que os clientes processem o portal cativo.

Para desabilitar o WebAuth SecureWeb na WLC, você pode executar o comando:

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

> **Note**: Você deve reinicializar a WLC para que a alteração entre em vigor.

Opção 2

Usar navegadores da Web alternativos. Até o momento, o assunto foi isolado no Google Chrome e no Mozilla Firefox; portanto, navegadores como Internet Explorer, Edge e navegadores nativos da Web Android não apresentam esse comportamento e podem ser usados para acessar o portal cativo.

Solução alternativa para autenticação externa na Web

Opção 1

Como essa variação do processo de autenticação da Web permite o controle de comunicações através da lista de acesso de pré-autenticação, uma exceção pode ser adicionada para que os usuários possam continuar no portal cativo. Essas exceções são feitas através de listas de acesso de URL (o suporte começa nas versões 8.3.x do AireOS para WLANs centralizadas e 8.7.x para WLANs de switching local do FlexConnect). Os URLs podem depender de navegadores da Web, mas foram identificados como http://www.gstatic.com/ Google Chrome e http://detectportal.firefox.com/ para o Mozilla Firefox.

Correção permanente

Para resolver esse problema, é recomendável instalar um certificado SSL WebAuth com algoritmo SHA-2, emitido por uma autoridade de certificação confiável, na WLC.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Gerar o CSR para certificados de terceiros e baixar certificados em cadeia para o WLC
- White paper do Google Chrome Privacy
- Suporte Técnico e Documentação - Cisco Systems