Comprendre et dépanner le comportement de méfiance des certificats d'authentification Web HTTPS sur les clients sans fil

Contenu

Introduction

Ce document décrit le comportement des clients sans fil lorsqu'ils se connectent à un réseau local sans fil (WLAN) d'authentification de couche 3 après des modifications apportées à la manière dont les navigateurs Web gèrent les certificats SSL (Secure Sockets Layer).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Protocole HTTPS (HyperText Transfer Protocol Secure).
- Certificats SSL.
- Contrôleur LAN sans fil Cisco (WLC).

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Chrome Web browser version 74.x ou ultérieure.
- Firefox version 66.x ou ultérieure.
- Contrôleur LAN sans fil Cisco version 8.5.140.0 ou ultérieure.

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 votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Protocole de transfert hypertexte (HTTP) le trafic des sites Web sur Internet n'est pas sécurisé et peut être intercepté et traité par des personnes involontaires. Par conséquent, une utilisation accrue du protocole HTTP pour les applications sensibles est rendue nécessaire pour mettre en oeuvre des mesures de sécurité supplémentaires comme le chiffrement SSL/TLS, qui constitue HTTPS.

HTTPS nécessite l'utilisation de SSL pour valider l'identité d'un site web et permettre d'établir une connexion sécurisée entre le serveur web et le navigateur du point d'extrémité. Les certificats SSL doivent être émis par une autorité de certification (CA) de confiance qui est incluse dans la liste des certificats racine CA de confiance des navigateurs et des systèmes d'exploitation.

Initialement, les certificats SSL utilisaient l'algorithme de hachage sécurisé version 1 (SHA-1), qui utilise un hachage de 160 bits. Cependant, en raison de diverses faiblesses, SHA-1 a été progressivement remplacé par SHA-2, un groupe d'algorithmes de hachage de différentes longueurs entre lesquelles le plus populaire est 256 bits.

Problème

Scénarios courants pour les certificats non approuvés

Il existe plusieurs raisons pour lesquelles un navigateur Web ne fait pas confiance à un certificat SSL, mais les raisons les plus courantes sont les suivantes :

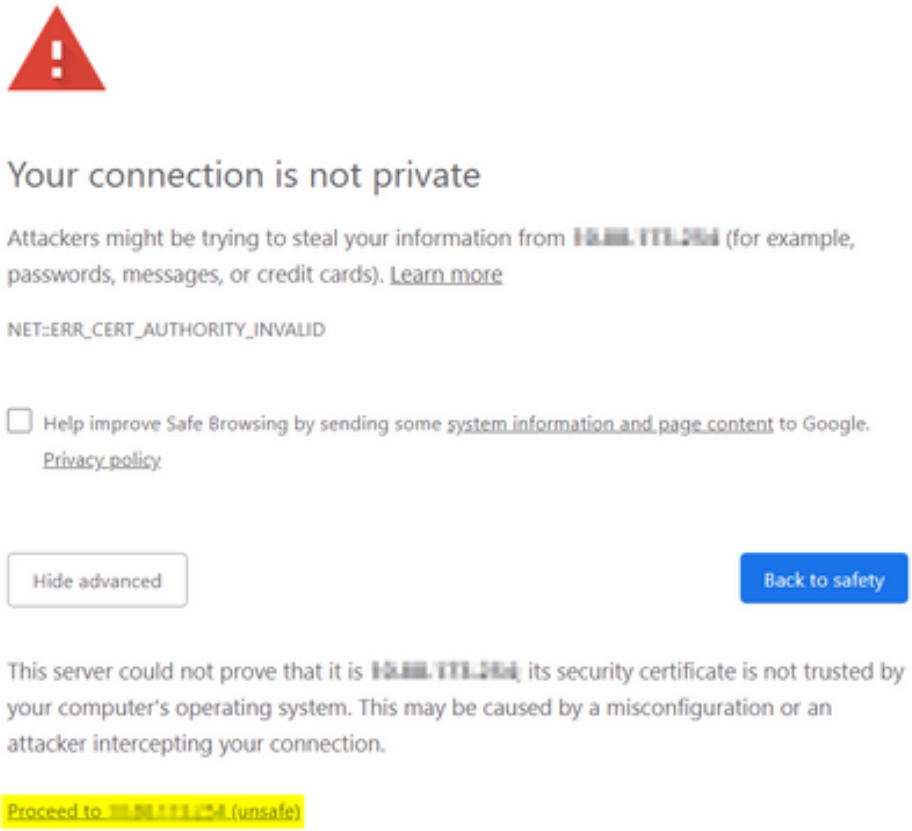
- Le certificat n'est pas émis par une autorité de certification de confiance (soit le certificat est autosigné, soit le certificat d'autorité de certification racine n'est pas installé sur le client en cas d'autorité de certification interne).
- Les champs Nom commun (CN) ou Nom secondaire de sujet (SAN) du certificat ne correspondent pas à l'URL Uniform Resource Locator (Uniform Resource Locator) entrée pour accéder à ce site.
- Le certificat a expiré ou l'horloge du client est mal configurée (en dehors de la période de validité du certificat).
- L'algorithme SHA-1 est utilisé par l'autorité de certification intermédiaire ou le certificat de périphérique (s'il n'y a pas d'autorité de certification intermédiaire).

Comportement précédent

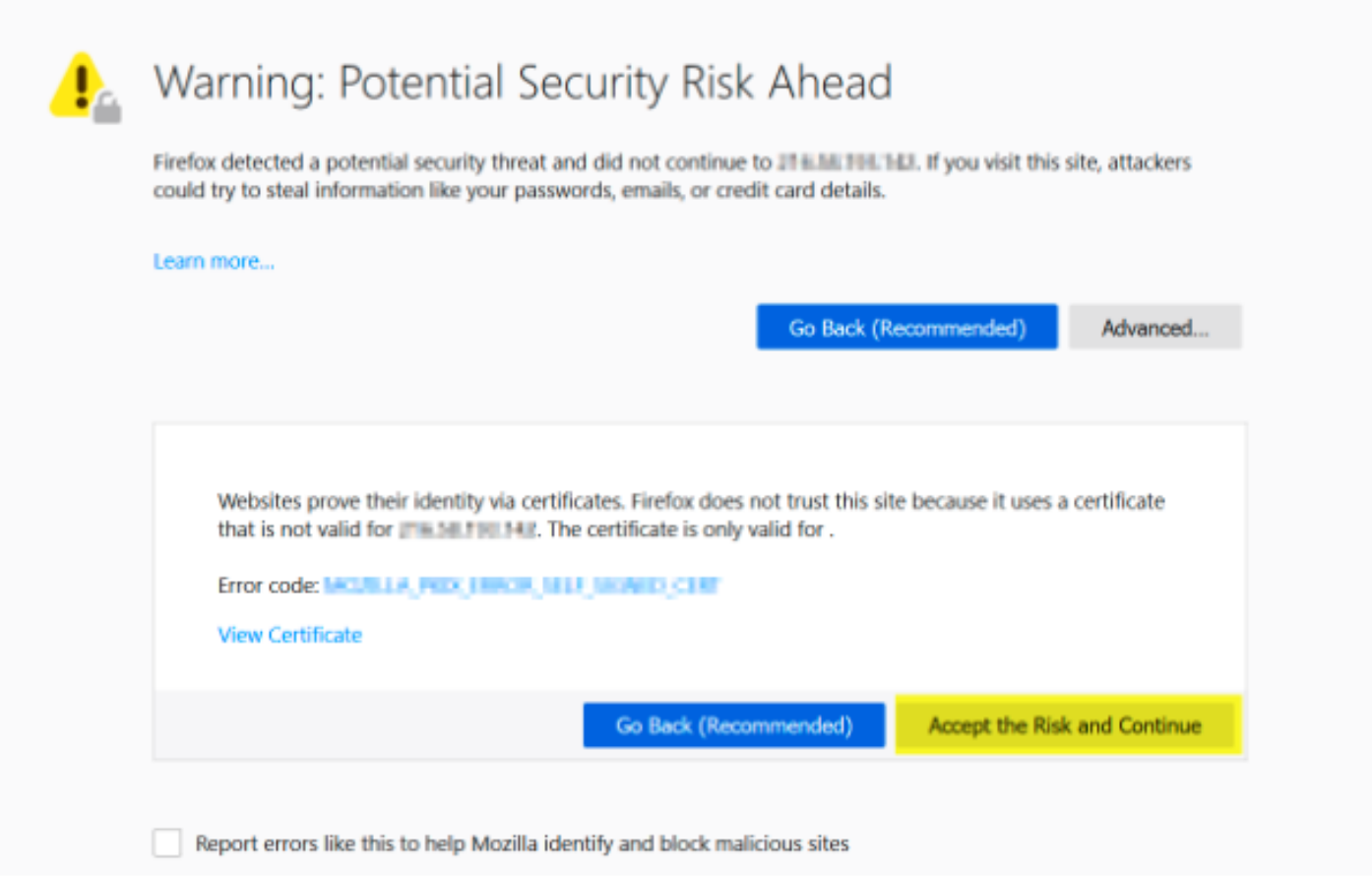
Lorsque des versions antérieures de navigateurs Web détectent un certificat de périphérique comme non fiable, elles invitent à une sécurité alerte (le texte et l'apparence varient sur chaque navigateur). La sécurité alerte demande à l'utilisateur d'accepter le risque de sécurité et de continuer à accéder au site Web prévu, ou de refuser la connexion. Après acceptation le risque que l'utilisateur obtienne un comportement de redirection pour l'utilisateur final vers le portail captif prévu :

> **Note**: L'action à poursuivre peut être masquée sous Options avancées sur des navigateurs spécifiques.

Les versions de Google Chrome inférieures à 74 affichent l'alerte comme illustré sur l'image :



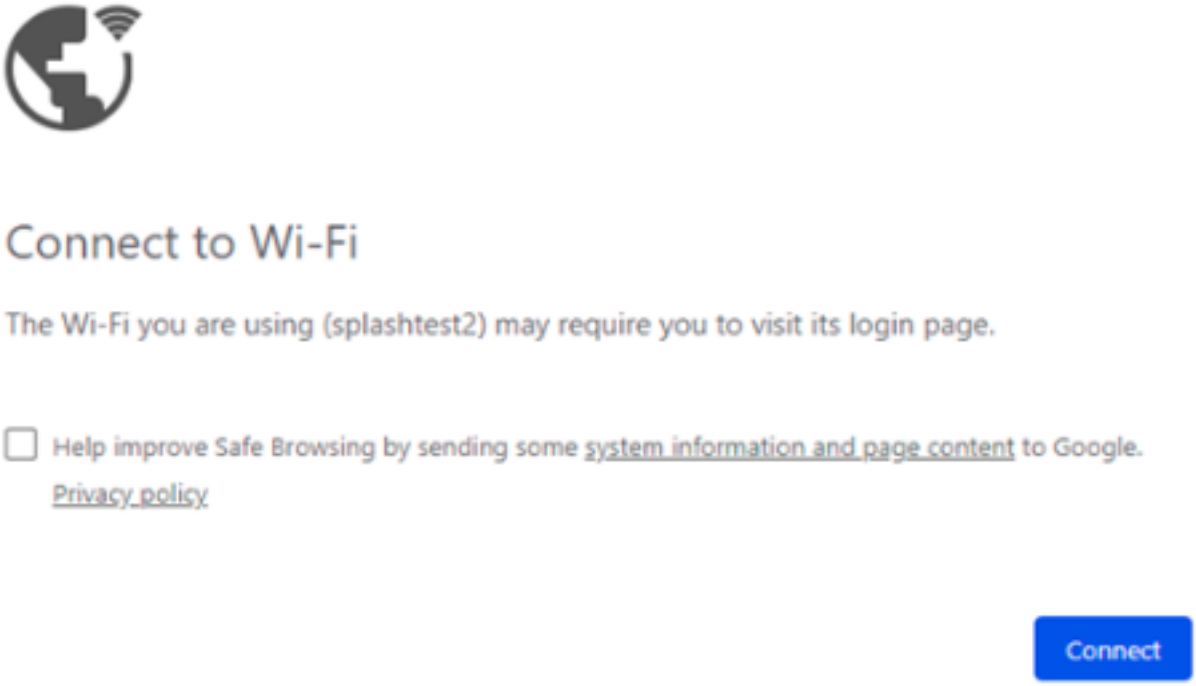
Les versions de Mozilla Firefox inférieures à 66 affichent l'alerte comme illustré dans l'image :



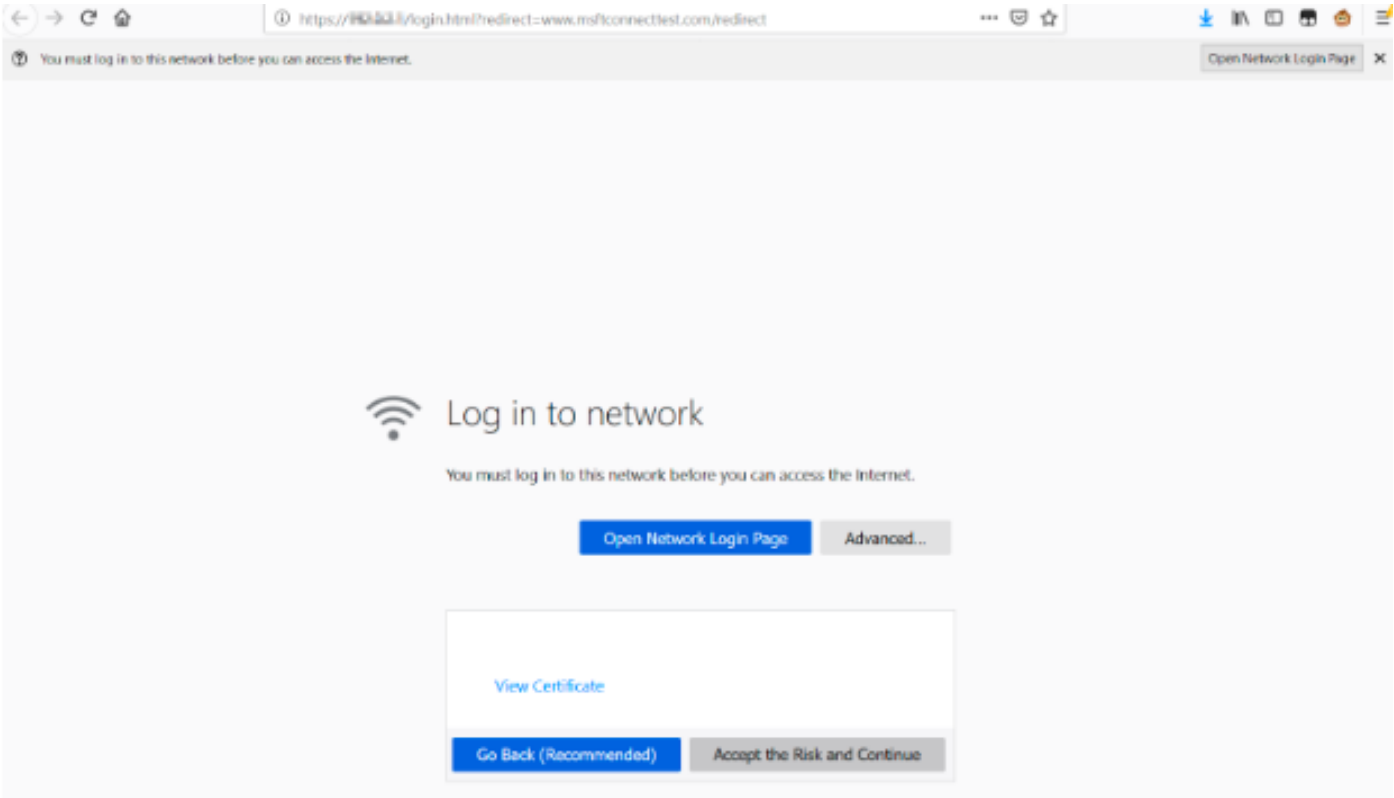
Comportement modifié

Certains navigateurs Web tels que Google Chrome et Mozilla Firefox ont changé la façon dont ils gèrent les connexions sécurisées par le biais de la vérification des certificats. Google Chrome (74.x et versions ultérieures) et Mozilla Firefox (66.x et versions ultérieures) nécessitent que le navigateur envoie une requête sans cookie aux URL externes avant l'utilisateur peut accéder au portail captif. Cependant, cette demande est interceptée par le contrôleur sans fil, car tout le trafic est bloqué avant de pouvoir atteindre l'état de connectivité final. La demande ensuite Lance une nouvelle redirection vers le portail captif qui crée Une boucle de redirection depuis l'utilisateur ne peut pas voir le portail.

Google Chrome 74.x et versions ultérieures affiche l'alerte : **Connexion au Wi-Fi Le Wi-Fi que vous utilisez peut vous demander de visiter sa page de connexion**, comme illustré sur l'image :



Mozilla Firefox 66.x et versions ultérieures affiche l'alerte : **Connexion au réseau Vous devez vous connecter à ce réseau avant de pouvoir accéder à Internet**, comme le montre l'image :



Cette page inclut une option **Accepter le risque et continuer**. Cependant, lorsque cette option est sélectionnée, un nouvel onglet contenant les mêmes informations est créé.

> **Note**: Ce bogue de documentation a été envoyé par l'équipe ISE comme référence externe pour les clients : CSCvj04703 - Chrome : Le flux de redirection sur le portail invité/BYOD est interrompu par un certificat non approuvé sur le portail ISE.

Solution

Solution pour l'authentification Web interne (page de connexion Web interne du WLC)

Option 1

Désactivez WebAuth SecureWeb sur le WLC. Puisque le problème est causé par la validation du certificat pour créer le mécanisme de sécurité HTTPS, utilisation HTTP pour ignorer la validation du certificat et permettre aux clients de rendre le portail captif.

Afin de désactiver WebAuth SecureWeb sur le WLC, vous pouvez exécuter la commande :

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

Note: Vous devez redémarrer le WLC pour que la modification prenne effet.

Option 2

Utilisez d'autres navigateurs Web. Jusqu'à présent, le problème a été isolé sur Google Chrome, et Mozilla Firefox ; par conséquent, les navigateurs Internet Explorer, Edge et Android natifs ne présentent pas ce comportement et peuvent être utilisés pour accéder au portail captif.

Solution pour l'authentification Web externe

Option 1

Comme cette variante du processus d'authentification Web permet le contrôle des communications via la liste d'accès pré-authentification, une exception peut être ajoutée afin que les utilisateurs puissent continuer à accéder au portail captif. Ces exceptions sont effectuées par le biais de listes d'accès URL (la prise en charge commence sur AireOS versions 8.3.x pour les WLAN centralisés et 8.7.x pour les WLAN de commutation locale FlexConnect). Les URL peuvent dépendre des navigateurs Web, mais elles ont été identifiées comme http://www.gstatic.com/ pour Google Chrome et http://detectportal.firefox.com/ pour Mozilla Firefox.

Correction permanente

Afin de résoudre ce problème, il est recommandé d'installer un certificat SSL WebAuth avec un algorithme SHA-2, émis par une autorité de certification de confiance, dans le WLC.

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Génération d'une demande CSR pour des certificats tiers et téléchargement des certificats chaînés sur le contrôleur de réseau local sans fil
- Livre blanc sur la confidentialité Google Chrome
- Support et documentation techniques - Cisco Systems