Comprendere e risolvere i problemi relativi al comportamento di diffidenza del certificato di autenticazione Web HTTPS sui client wireless

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Premesse](#)
[Problema](#)
[Scenari comuni per i certificati non attendibili](#)
[Comportamento precedente](#)
[Comportamento modificato](#)
[Soluzione](#)
[Soluzione per Internal Web-Auth (pagina di login sul Web interna del WLC)](#)
[Opzione 1](#)
[Opzione 2](#)
[Soluzione per Web-Auth esterno](#)
[Opzione 1](#)
[Correzione permanente](#)
[Verifica](#)
[Risoluzione dei problemi](#)
[Informazioni correlate](#)

Introduzione

In questo documento viene descritto il comportamento dei client wireless quando si connettono a un'autenticazione di layer 3 tramite una rete WLAN (Wireless Local Area Network) dopo le modifiche apportate alla modalità di gestione dei certificati SSL (Secure Sockets Layer) da parte dei browser Web.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Protocollo HTTPS (HyperText Transfer Protocol Secure).
- certificati SSL.
- Controller LAN wireless (WLC) Cisco.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Browser web Chrome versione 74.x o superiore.
- Web browser Firefox versione 6.x o successiva.
- Cisco Wireless LAN Controller versione 8.5.140.0 o superiore.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Hypertext Transfer Protocol (HTTP) il traffico dei siti Web su Internet non è sicuro e può essere intercettato ed elaborato da utenti non autorizzati. Pertanto, un maggiore uso del protocollo HTTP per le applicazioni sensibili è diventato necessario per implementare misure di sicurezza aggiuntive come la crittografia SSL/TLS, che costituisce HTTPS.

HTTPS richiede l'utilizzo di SSL certificati per convalidare l'identità di un sito web e consente di stabilire una connessione sicura tra il server web e il browser dell'endpoint. I certificati SSL devono essere emessi da un'Autorità di certificazione (CA) attendibile inclusa nell'elenco dei certificati radice CA attendibili dei browser e dei sistemi operativi.

Inizialmente, i certificati SSL utilizzavano l'algoritmo SHA-1 (Secure Hashing Algorithm versione 1), che utilizza un hash a 160 bit. Tuttavia, a causa di una varietà di debolezze, SHA-1 è stato progressivamente sostituito da SHA-2, un gruppo di algoritmi di hashing con diverse lunghezze tra cui il più popolare è 256 bit.

Problema

Scenari comuni per i certificati non attendibili

Un Web browser può non considerare attendibile un certificato SSL per diversi motivi, ma i motivi più comuni sono:

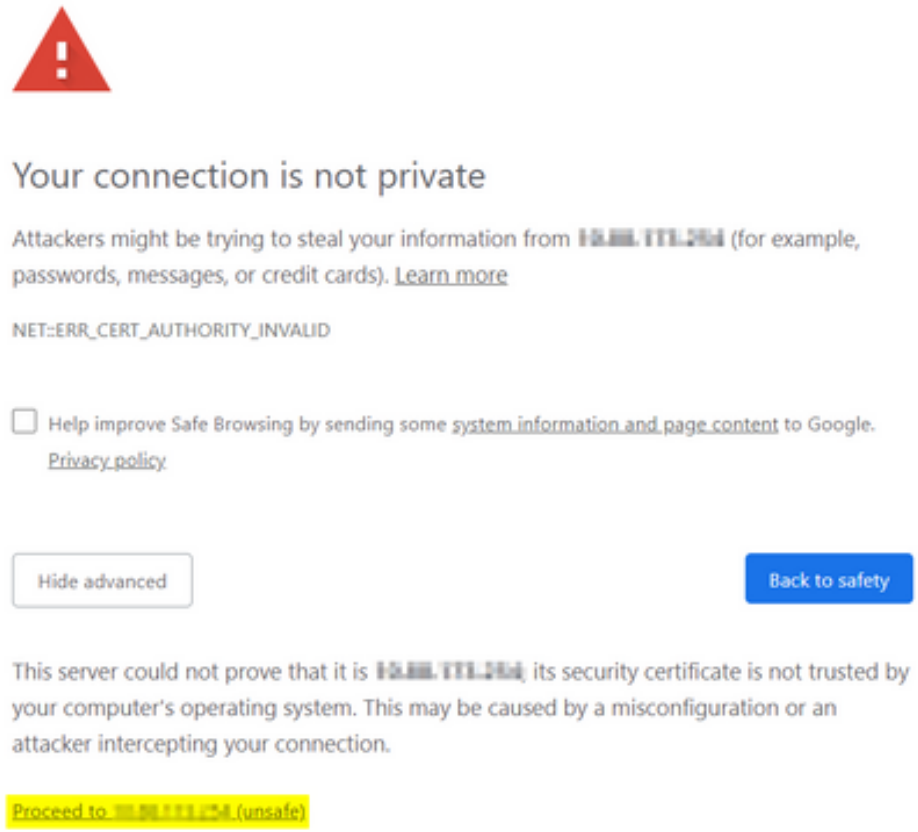
- Il certificato non è rilasciato da un'Autorità di certificazione attendibile (il certificato è autofirmato oppure nel client non è installato il certificato CA radice nel caso di una CA interna).
- I campi Nome comune (CN) o Nome alternativo soggetto (SAN) del certificato non corrispondono all'URL (Uniform Resource Locator) immesso per passare a tale sito.
- Il certificato è scaduto o l'orologio sul client non è configurato correttamente (oltre il periodo di validità del certificato).
- L'algoritmo SHA-1 è utilizzato dalla CA intermedia o dal certificato del dispositivo (nel caso non vi siano CA intermedie).

Comportamento precedente

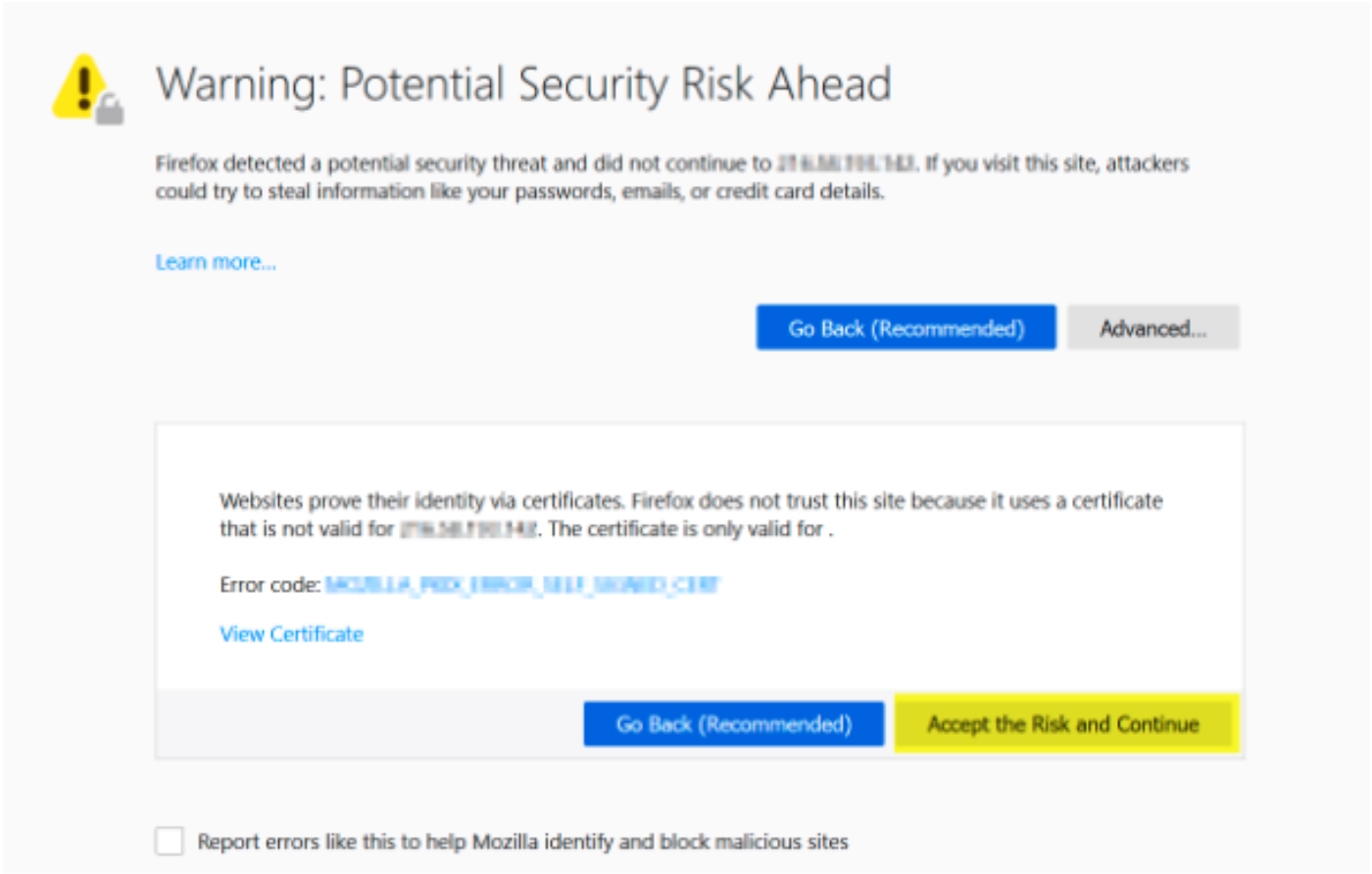
Quando le versioni precedenti dei browser Web rilevano un certificato di dispositivo come non attendibile, richiedono una protezione avviso (il testo e l'aspetto variano a seconda del browser). La sicurezza avviso chiede all'utente di accettare il rischio per la sicurezza e di continuare con il sito Web desiderato, oppure di rifiutare la connessione. Dopo l'accettazione il rischio che l'utente ottenga il comportamento di reindirizzamento per l'utente finale al portale vincolato previsto:

Nota: L'azione da eseguire può essere nascosta in Opzioni avanzate in browser specifici.

Le versioni di Google Chrome inferiori a 74 visualizzano l'avviso come mostrato nell'immagine:



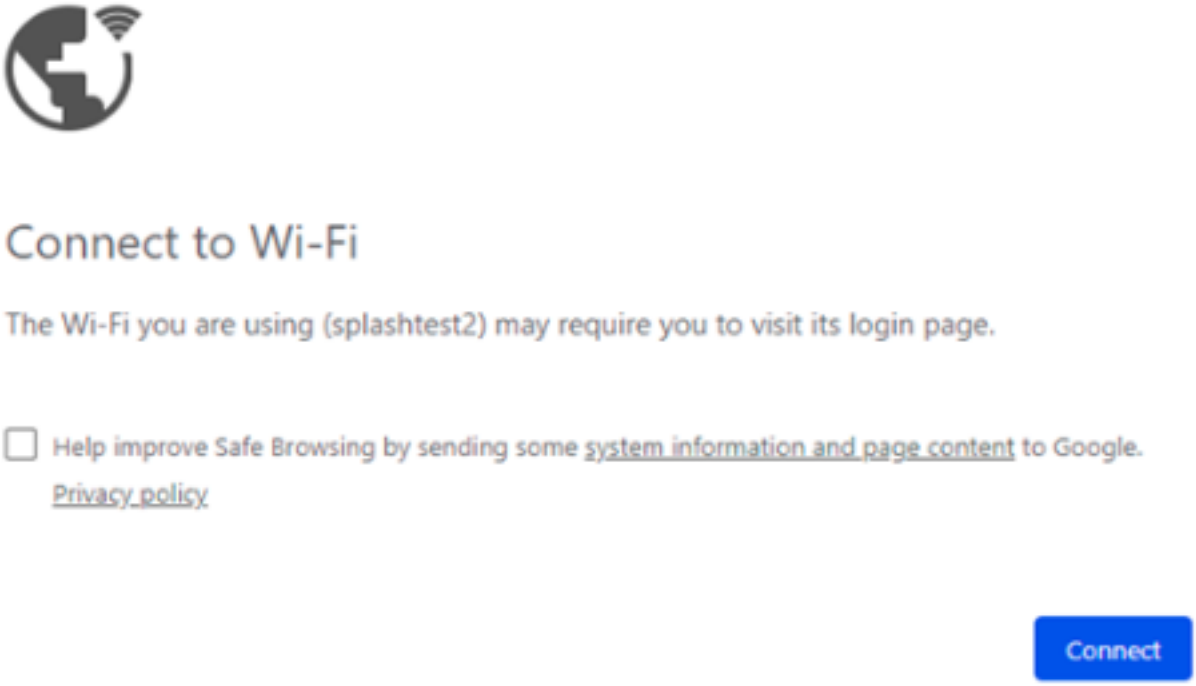
Le versioni di Mozilla Firefox inferiori a 66 visualizzano l'avviso come mostrato nell'immagine:



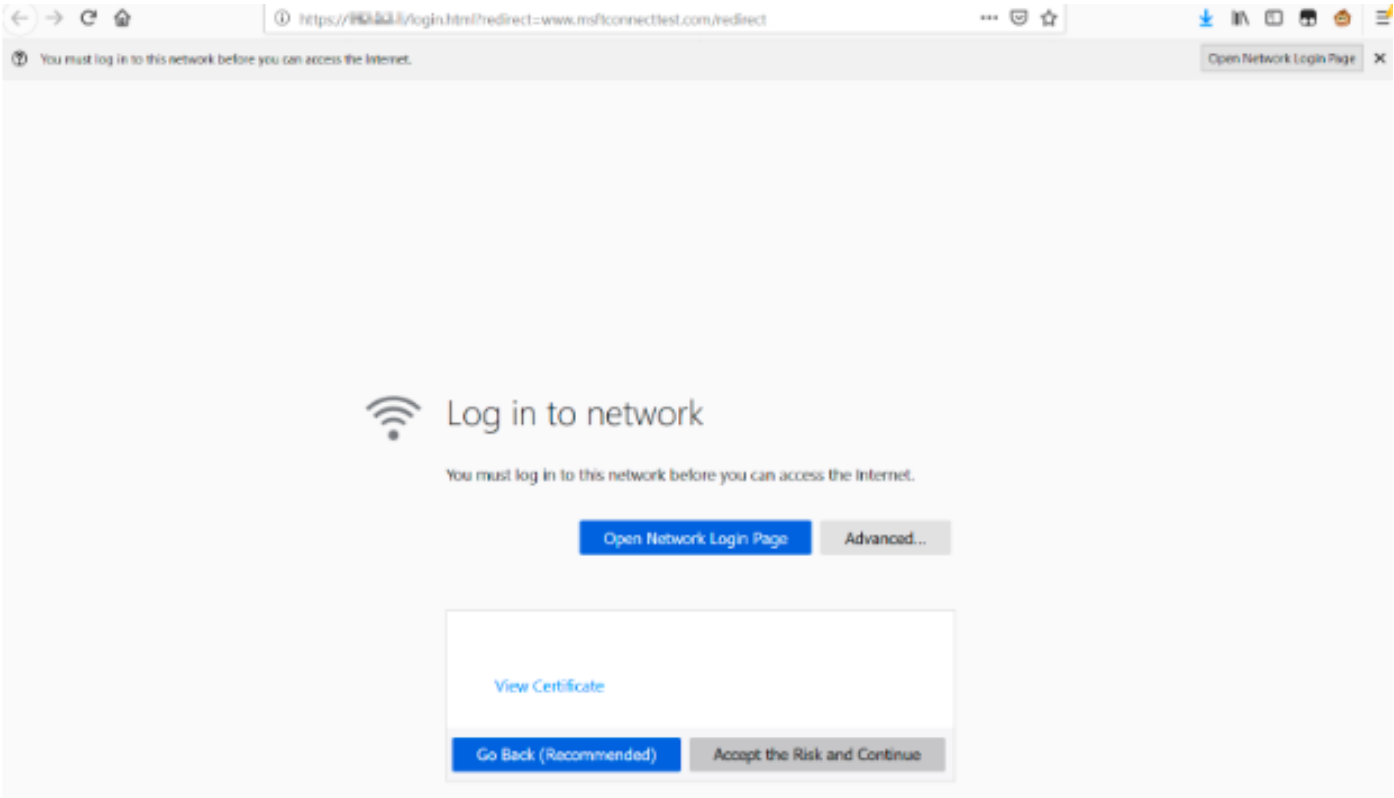
Comportamento modificato

Alcuni browser come Google Chrome e Mozilla Firefox hanno cambiato il modo in cui gestiscono le connessioni protette tramite la verifica dei certificati. Google Chrome (74.x e superiore) e Mozilla Firefox (6.x e superiore) richiedono al browser di inviare una richiesta senza cookie a URL esterni prima all'utente può essere consentito di passare al portale vincolato. Questa richiesta, tuttavia, viene intercettata dal controller wireless poiché tutto il traffico è bloccato prima che possa raggiungere lo stato di connettività finale. La richiesta quindi avvia un nuovo reindirizzamento al portale in modalità vincolata che crea un ciclo di reindirizzamento poiché l'utente non è in grado di vedere il portale.

Google Chrome 74.x e superiori visualizza l'avviso: **Connetti a Wi-Fi Il Wi-Fi che si sta usando potrebbe richiedere di visitare la sua pagina di accesso**, come mostrato nell'immagine:



Mozilla Firefox 6.x e versioni successive visualizza l'avviso: **Accedi alla rete Per accedere a Internet è necessario accedere a questa rete**, come mostrato nell'immagine:



Questa pagina include l'opzione **Accetta il rischio e continua**. Tuttavia, quando questa opzione è selezionata, viene creata una nuova scheda con le stesse informazioni.

> **Nota:** Questo bug è stato presentato dal team ISE come riferimento esterno per i clienti:CSCvj04703 - Chrome: Il flusso di reindirizzamento sul portale guest/BYOD è interrotto con un certificato non attendibile sul portale ISE.

Soluzione

Soluzione per Internal Web-Auth (pagina di login sul Web interna del WLC)

Opzione 1

Disabilitare WebAuth SecureWeb sul WLC. Poiché il problema è causato dalla convalida del certificato per creare il meccanismo di sicurezza HTTPS, utilizzo HTTP per ignorare la convalida del certificato e consentire ai client di eseguire il rendering del portale vincolato.

Per disabilitare WebAuth SecureWeb sul WLC, è possibile eseguire il comando:

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

Nota: Per rendere effettiva la modifica, è necessario riavviare il WLC.

Opzione 2

Utilizzare browser Web alternativi. Finora il problema è stato isolato a Google Chrome, e Mozilla Firefox; pertanto, i browser quali Internet Explorer, Edge e i browser Web nativi Android non presentano questo comportamento e possono essere utilizzati per accedere al portale captive.

Soluzione per Web-Auth esterno

Opzione 1

Poiché questa variante del processo di autenticazione Web consente il controllo delle comunicazioni tramite l'elenco degli accessi di preautenticazione, è possibile aggiungere un'eccezione in modo che gli utenti possano continuare a utilizzare il portale vincolato. Queste eccezioni vengono generate tramite gli elenchi degli accessi agli URL (il supporto inizia sulle versioni AireOS 8.3.x per le WLAN centralizzate e 8.7.x per le WLAN di switching locale FlexConnect). Gli URL possono dipendere dai browser, ma sono stati identificati come http://www.gstatic.com/ per Google Chrome e http://detectportal.firefox.com/ per Mozilla Firefox.

Correzione permanente

Per risolvere il problema, si consiglia di installare un certificato SSL WebAuth con algoritmo SHA-2, rilasciato da un'autorità di certificazione attendibile, nel WLC.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa

configurazione.

Informazioni correlate

- Generazione delle richieste CSR per certificati di terze parti e download di catene di certificati sul WLC
- White paper sulla privacy di Google Chrome
- Documentazione e supporto tecnico – Cisco Systems