SPA112: Problema di riconoscimento del certificato BE-SPA-SSL

Data identificazione

30 gennaio 2017

Data risoluzione

N/D

Prodotti interessati

SPA112	1.4.2

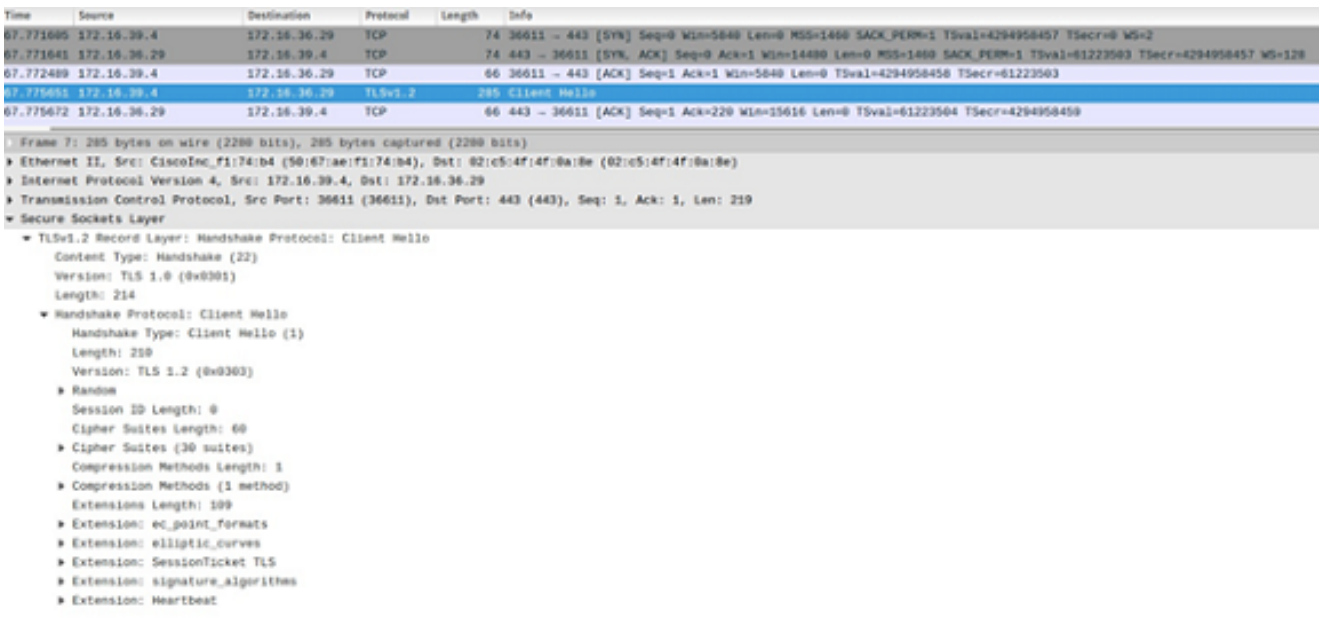
Descrizione del problema

La richiesta ricevuta dall'SP A non supporta l'indicazione del nome del server (SNI). Senza il supporto SNI per l'indicazione del nome nella fase Transport Layer Security, Client Hello non contiene le informazioni sul nome del server.

Nelle immagini seguenti viene visualizzata la schermata del messaggio Hello del CLIENT TLS ricevuto dal server quando:

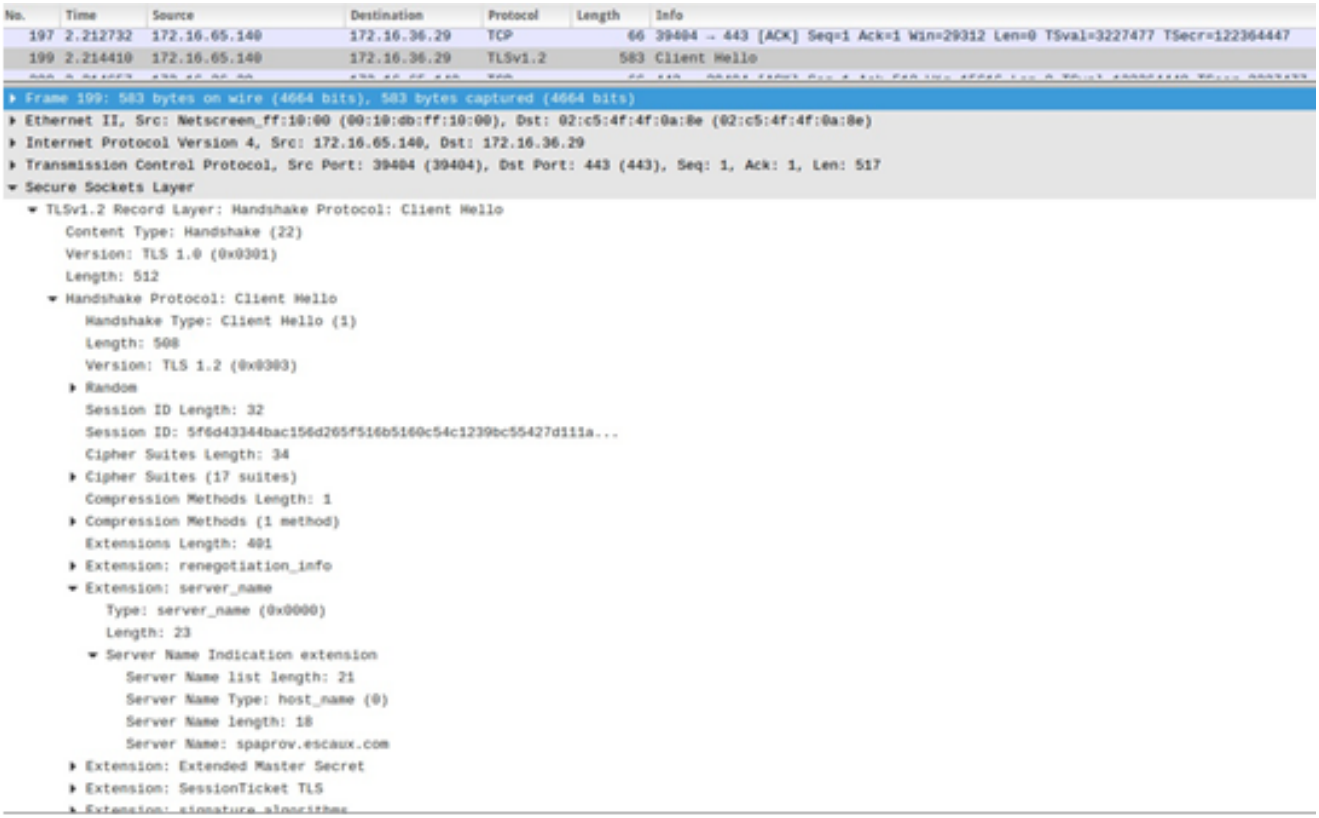
1. SNI non è supportato (richiesta ricevuta dall'SPA)

Nota: In questo caso, il client Hello del protocollo Handshake non include alcuna estensione nome_server.



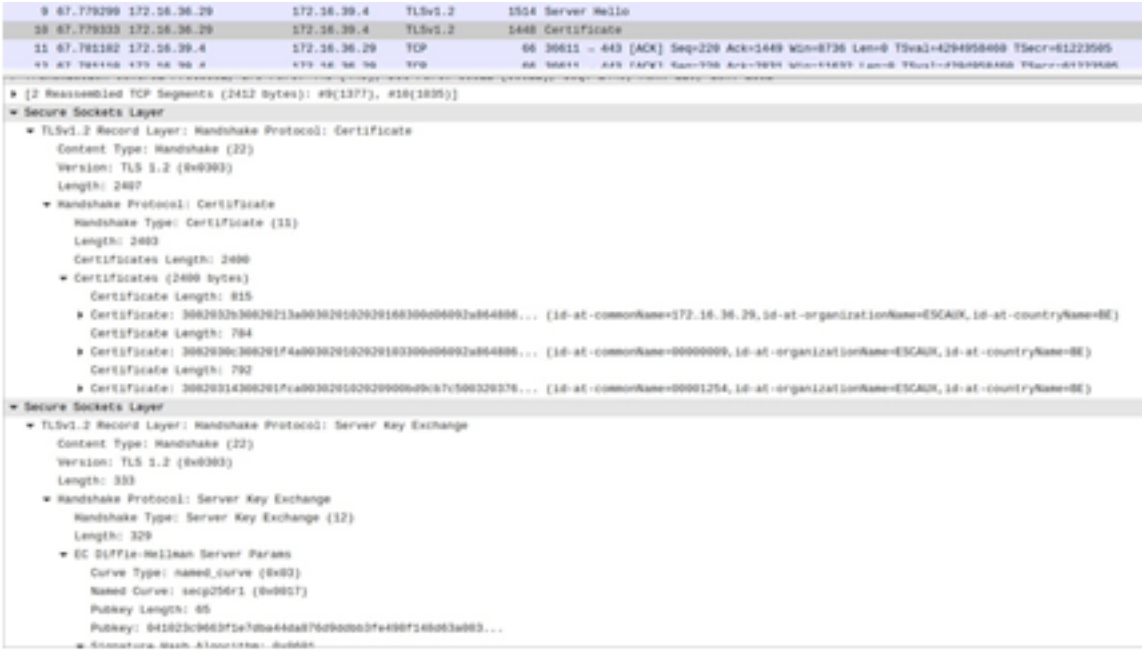
2. È supportato l'SNI (richiesta effettuata tramite browser)

Nota: In questo caso, l'estensione server_name è presente nel client Hello del protocollo Handshake.



Dopo la risoluzione, la richiesta viene inoltrata all'host virtuale predefinito, che dispone di un certificato diverso, firmato da un'altra CA. In questo caso, l'errore CA sconosciuta si verifica nella fase di negoziazione. Con un risultato diverso a seconda che la richiesta contenesse o meno le informazioni server_name:

1. Senza SNI (richiesta ricevuta dall'SPA), il certificato contiene un certificato errato.



2. Con il supporto SNI (richiesta ricevuta dal browser), Server Hello, Certificato contiene il certificato corretto.

Stato corrente

La richiesta di miglioramento per il supporto di SNI è già stata archiviata con ID CDETS: CSCve12309