SPA112 : Problème de reconnaissance de certificat BE-SPA-SSL

Date d'identification

30 janvier 2017

Date de résolution

S/O

Produits affectés

SPA112	1.4.2

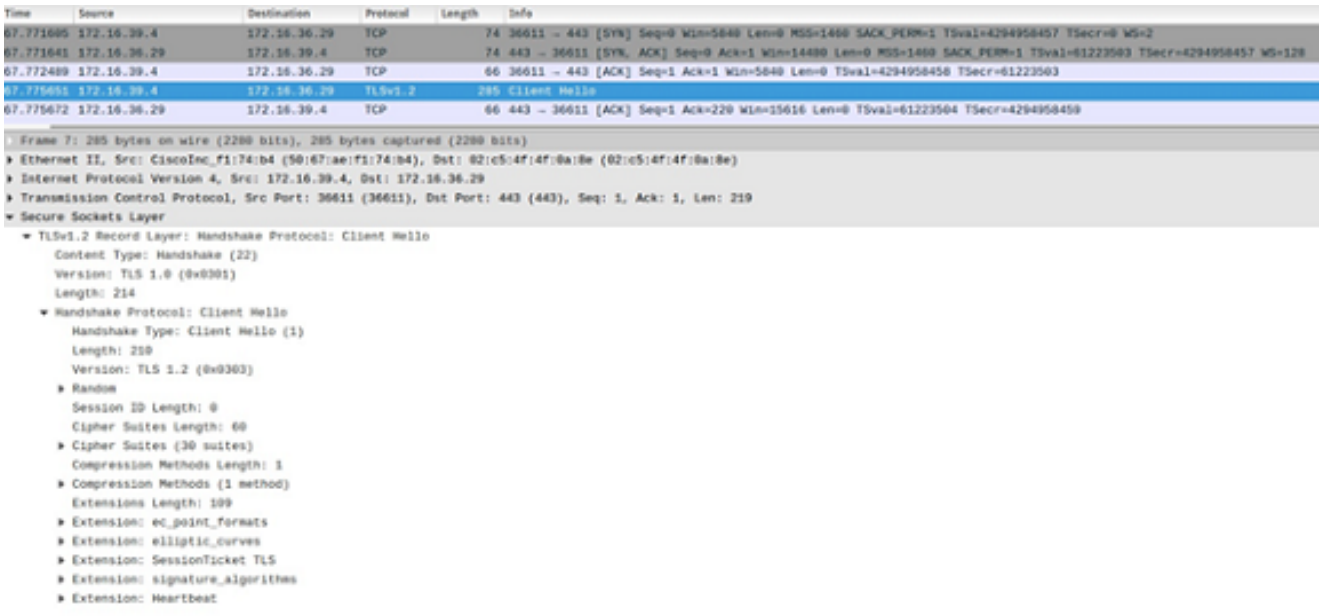
Description du problème

La demande reçue du SPA ne prend pas en charge l'indication de nom de serveur (SNI). Sans la prise en charge SNI de l'indication de nom dans la phase de sécurité de la couche transport, le client Hello ne contient pas les informations de nom de serveur.

Dans les images suivantes, vous avez la capture d'écran du message Hello du CLIENT TLS reçu par le serveur lorsque :

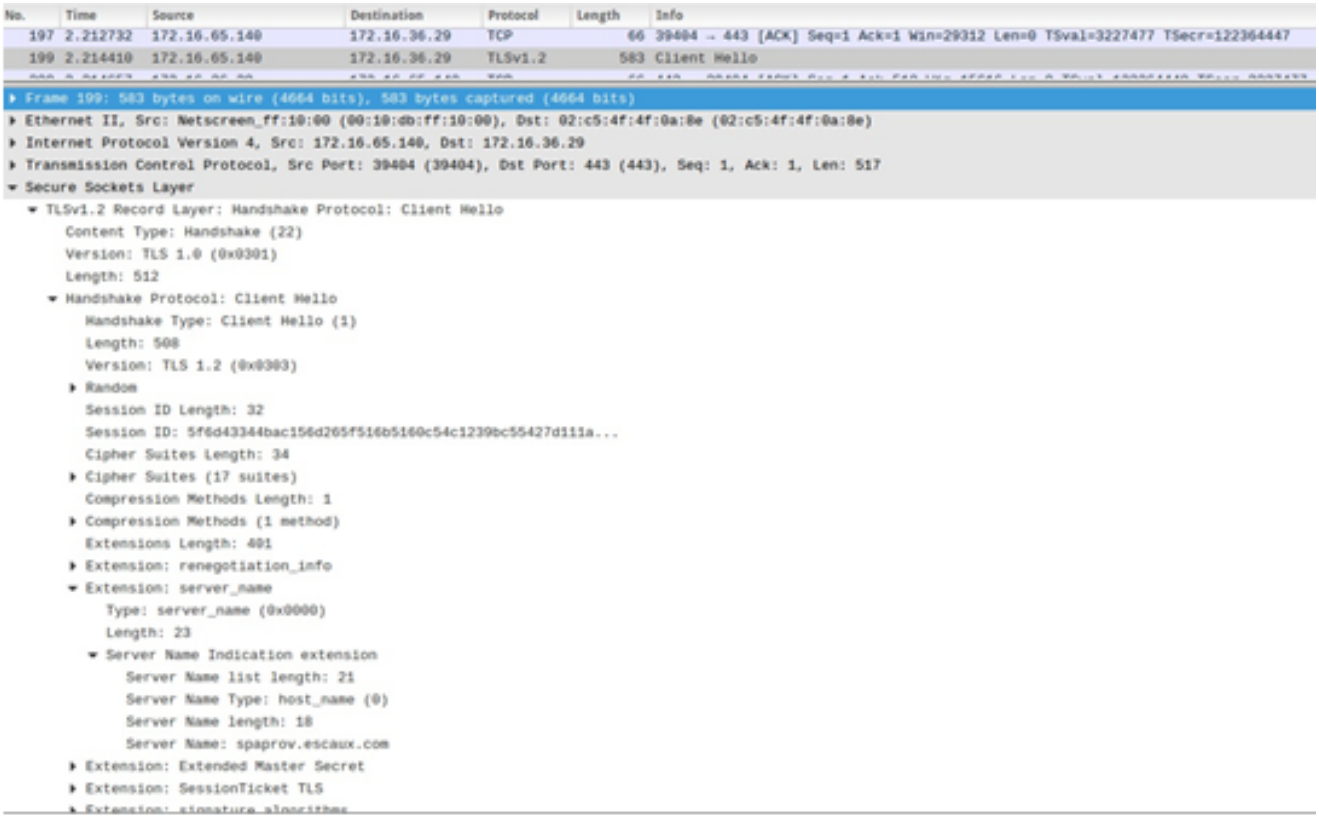
1. SNI n'est pas pris en charge (demande reçue du SPA)

Note: Dans ce cas, il n'y a aucune extension server_name dans l'Hello du client de protocole de connexion.



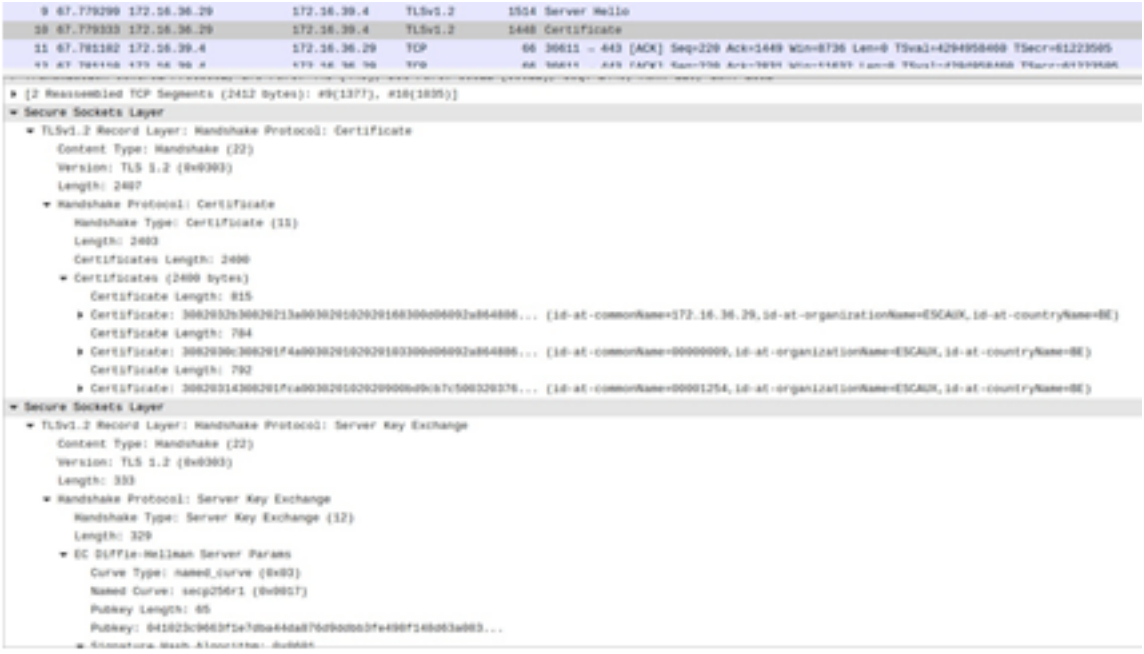
2. SNI est pris en charge (demande effectuée via le navigateur)

Note: Dans ce cas, l'extension server_name est présente dans l'Hello du client de protocole de connexion.



Après la résolution, la demande est transmise à l'hôte virtuel par défaut, qui a un certificat différent, signé par une autre autorité de certification. C'est là que l'erreur d'autorité de certification inconnue se produit dans la phase de négociation. Avec un résultat différent selon que la requête contenait ou non les informations nom_serveur :

1. Sans SNI (demande reçue du SPA), le certificat contient le mauvais certificat.



2. Avec SNI pris en charge (demande reçue du navigateur), le certificat Hello du serveur contient le certificat approprié.

État actuel

La demande d'amélioration de support SNI a déjà été déposée avec l'ID CDETS : CSCve12309.