SPA112: Problema de reconhecimento de certificado BE-SPA-SSL

Data de identificação

30 de janeiro de 2017

Data de resolução

N/A

Produtos afetados

SPA112	1.4.2

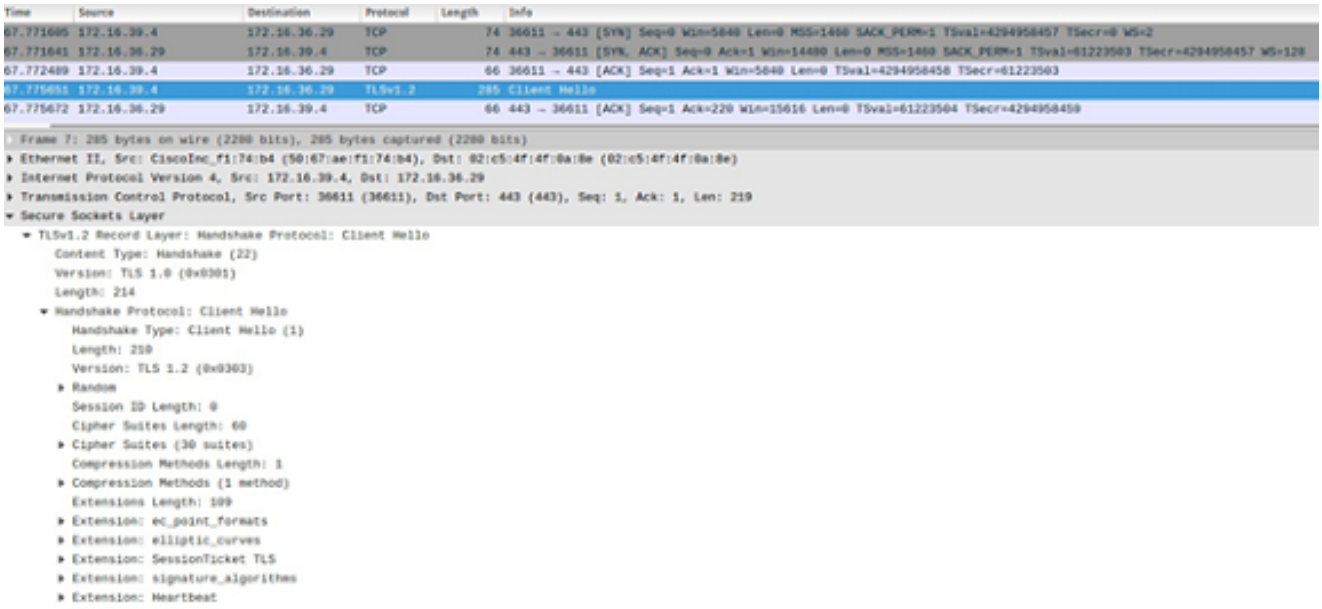
Descrição do problema

A solicitação recebida do SPA não suporta a indicação de nome do servidor (SNI). Sem o suporte SNI de indicação de nome na fase de segurança da camada de transporte, o Hello do cliente não contém as informações de nome do servidor.

Nas imagens a seguir, você tem a captura de tela da mensagem de saudação do CLIENTE TLS recebida pelo servidor quando:

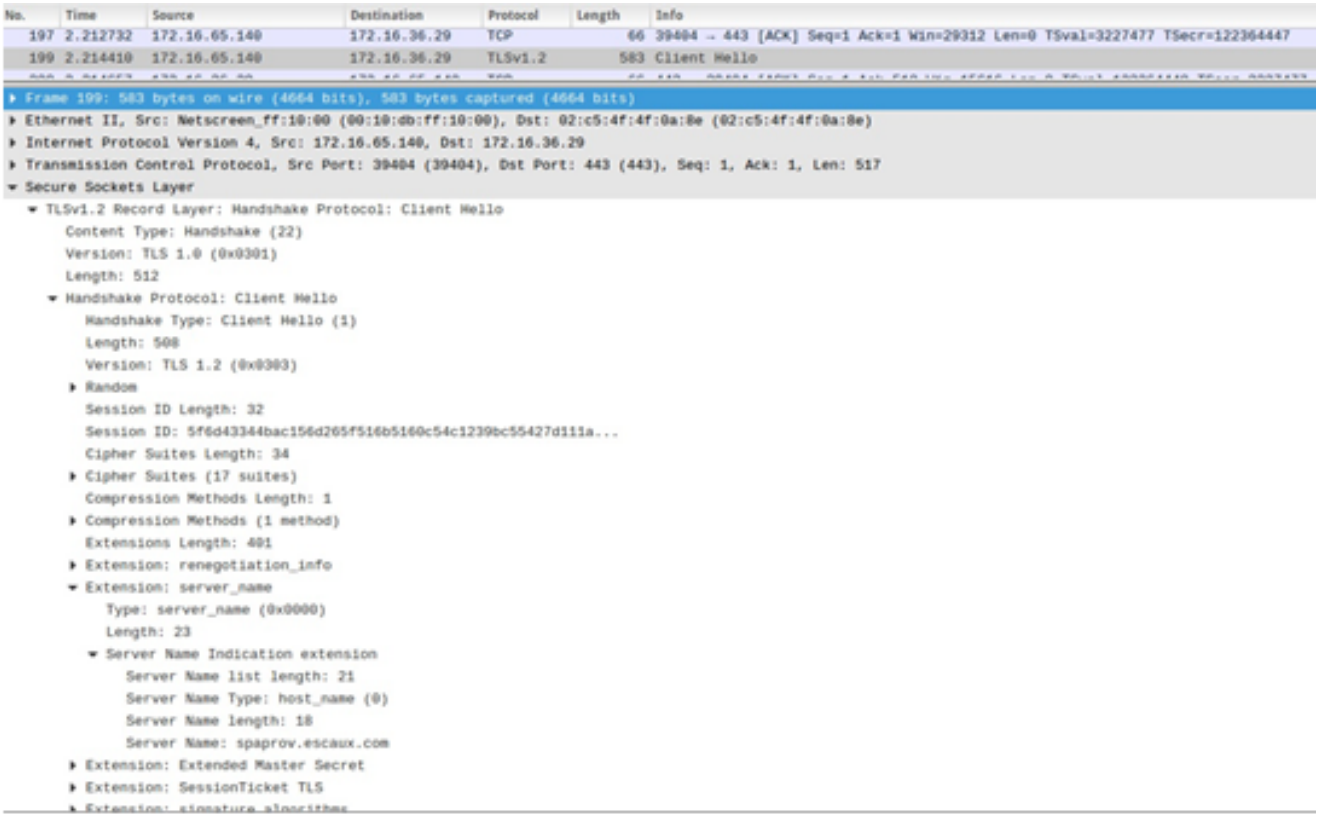
1. SNI não é suportado (solicitação recebida do SPA)

Note: Nesse caso, não há extensão server_name no Handshake Protocol Client Hello.



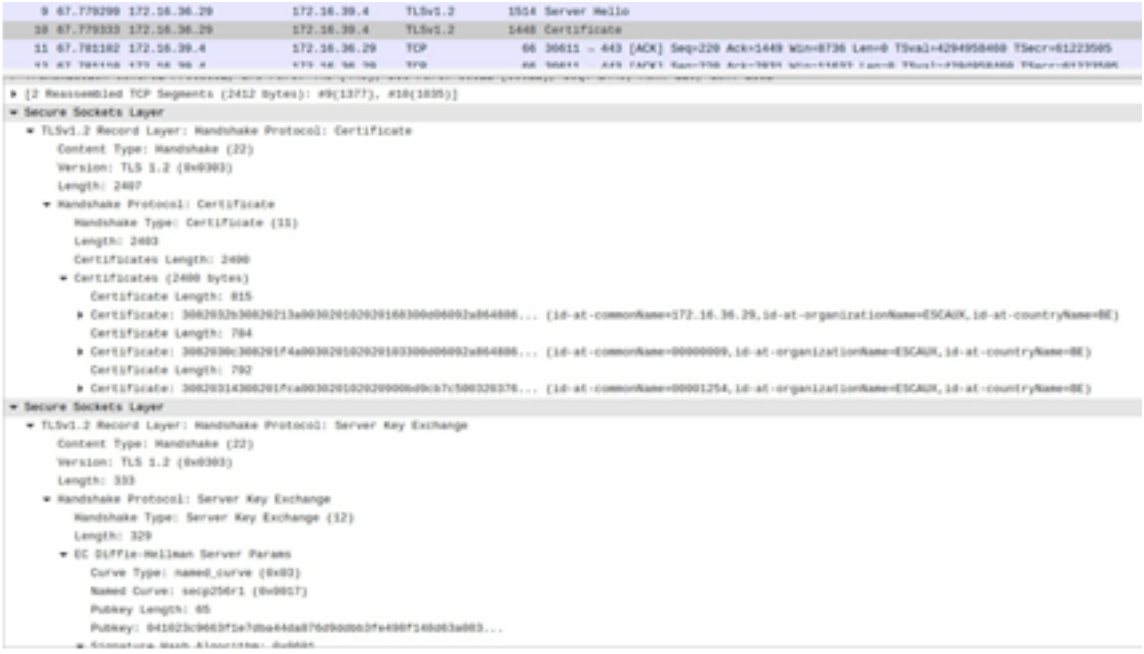
2. O SNI é suportado (solicitação feita através do navegador)

Note: Nesse caso, a extensão server_name está presente no Handshake Protocol Client Hello.



Após a resolução, a solicitação é encaminhada ao host virtual padrão, que tem um certificado diferente, assinado por uma CA diferente. É aqui que ocorre o erro de CA desconhecido na fase de negociação. Com um resultado diferente, dependendo se a solicitação estava contendo as informações de server_name ou não:

1. Sem SNI (solicitação recebida do SPA), o certificado contém o certificado errado.



2. Com o SNI suportado (solicitação recebida do navegador), o Server Hello, Certificate contém o certificado correto.

Status atual

A solicitação de aprimoramento para suportar SNI já foi inserida com a ID CDETS: CSCve12309.