SPA112: BE-SPA-SSL certificaatherkenning

Datum geïdentificeerd

30 januari 2017

Datum opgelost

N.v.t.

Producten getroffen

SPA112	1.4.2

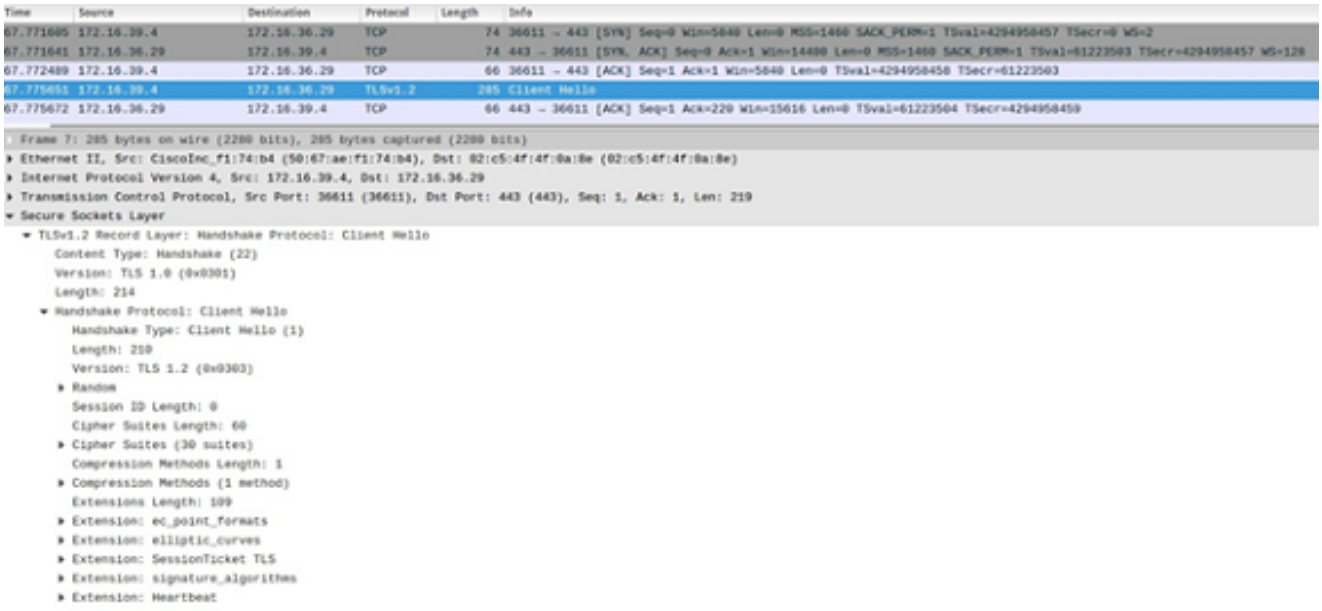
Beschrijving van probleem

Een verzoek dat van de SPA is ontvangen, ondersteunt de servernaamindicator (SNI) niet. Zonder de SNI-ondersteuning van de Naam in de Security fase van de Vervoerlaag bevat de Client Hallo niet de informatie over de servernaam.

In de volgende afbeeldingen hebt u het screenshot van het TLS CLIENT Hallo-bericht van de server ontvangen wanneer:

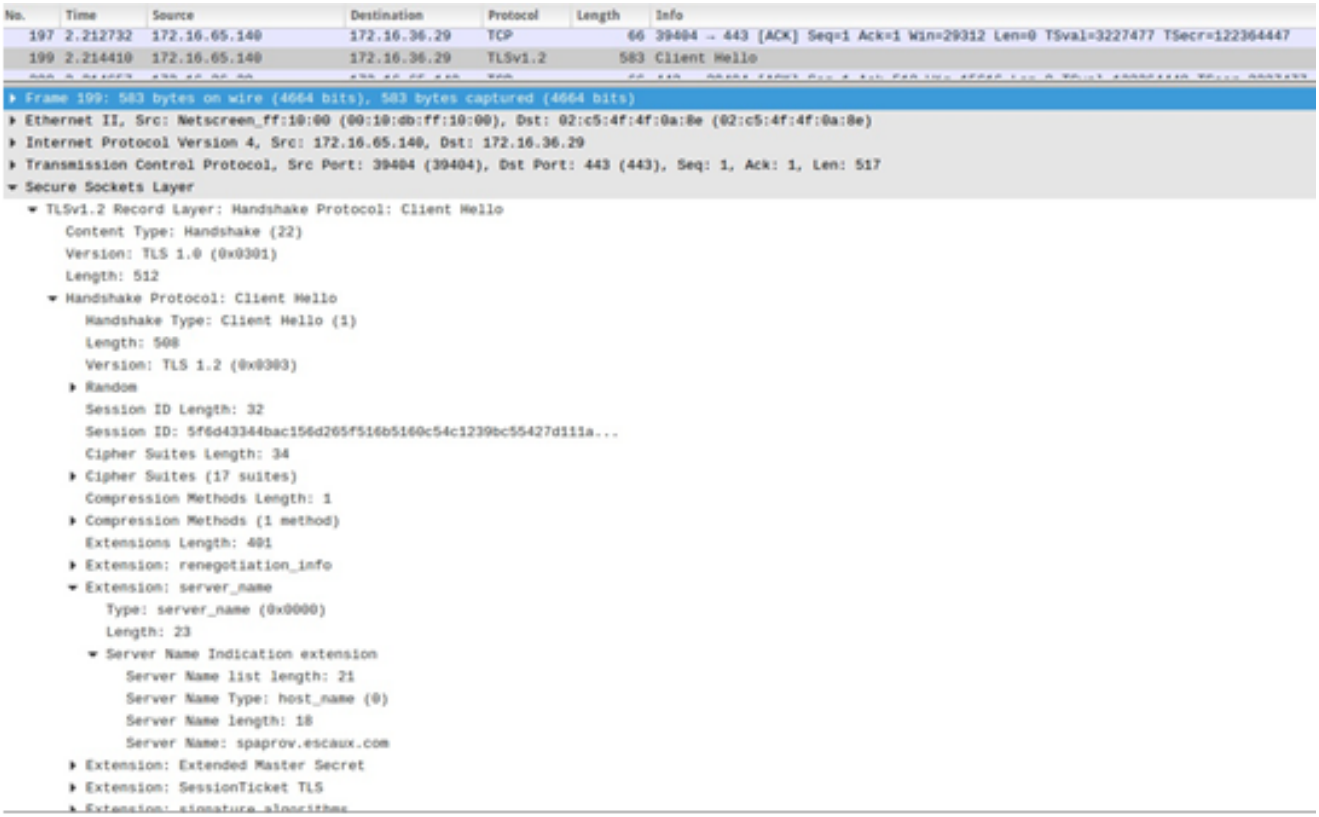
1. SNI wordt niet ondersteund (verzoek van de SPA ontvangen)

Opmerking: In dit geval, is er geen server_name extensie in het Handshake Protocol Client Hallo.



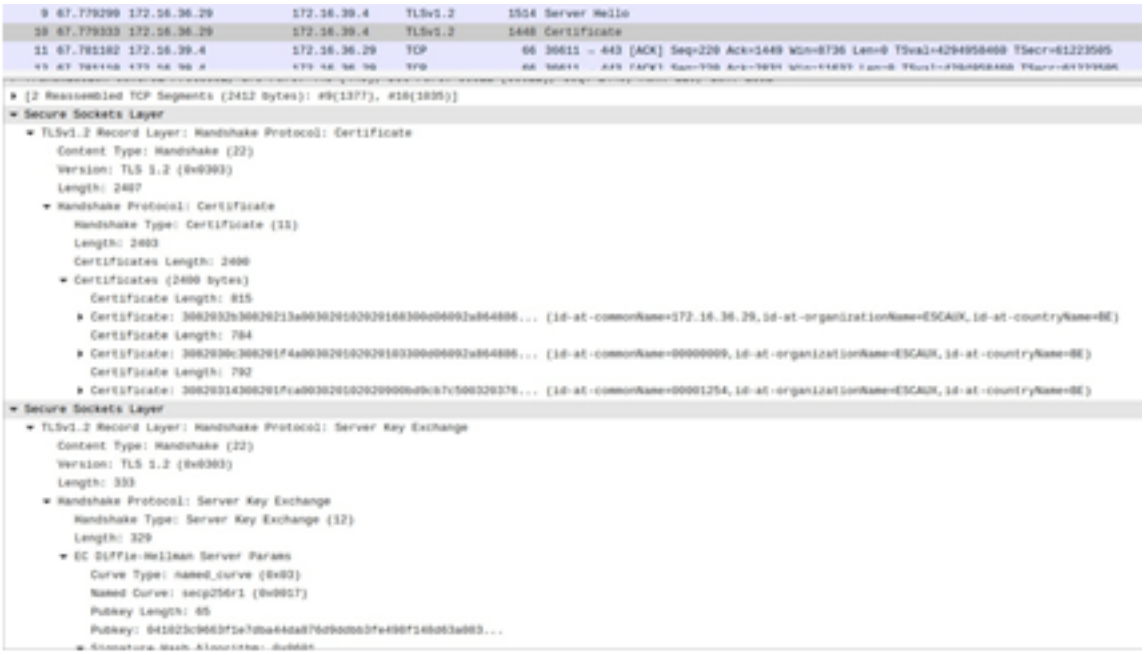
2. SNI wordt ondersteund (verzoek ingediend via de browser)

Opmerking: In dit geval, is de server_name extensie aanwezig in de Handshake Protocol Client Hallo.



Na de resolutie wordt het verzoek doorgestuurd naar de standaard virtuele host, die een ander certificaat heeft, ondertekend door een ander CA. Dit is waar de Onbekende CA-fout optreedt in de onderhandelingsfase. Met een ander resultaat afhankelijk van of het verzoek de server_name informatie bevatte of niet:

1. Zonder SNI (verzoek van de SPA ontvangen) bevat het certificaat het verkeerde certificaat.



2. Wanneer SNI wordt ondersteund (verzoek van de browser ontvangen), bevat het Server Hallo, Certificaat het juiste certificaat.

Huidige status

Een verzoek om ondersteuning van SNI is al bij CDETS-id ingediend: CSCve12309.