SPA112: BE-SPA-SSL Certificate Recognition Issue

Date Identified

January 30, 2017

Date Resolved

N/A

Products Affected

SPA112	1.4.2

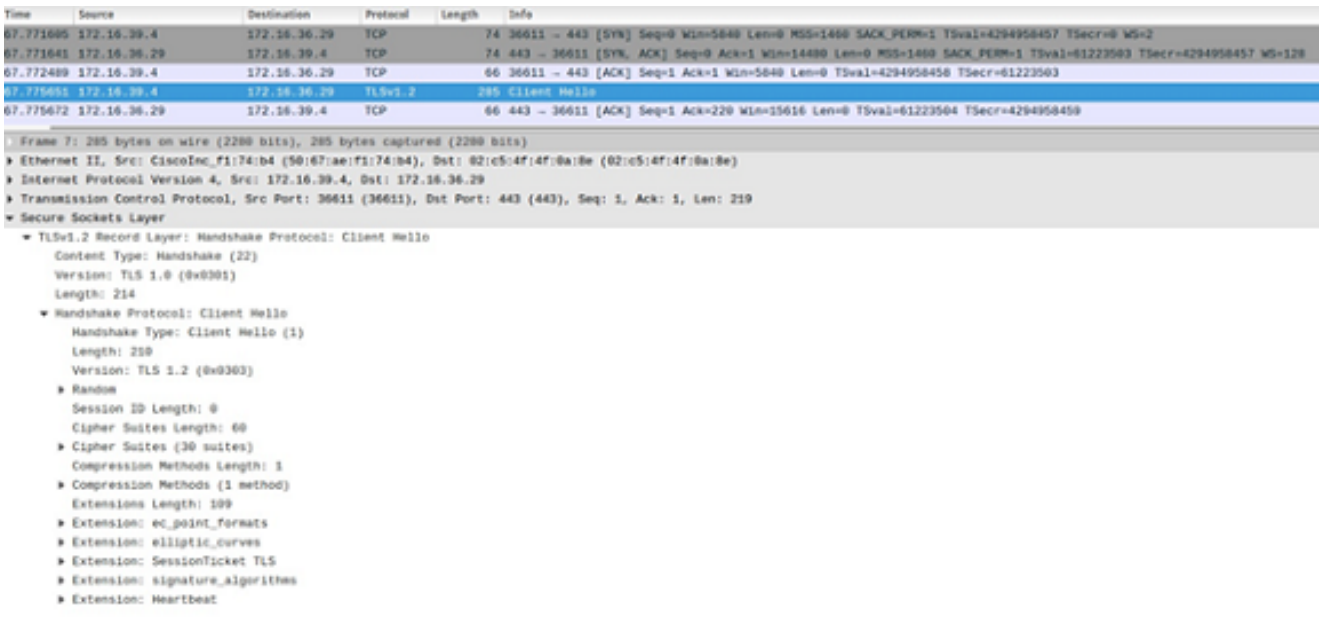
Problem Description

Request received from the SPA does not support the Server Name Indication (SNI). Without the Name Indication SNI support on the Transport Layer Security phase, the Client Hello does not contain the server name information.

In the following images, you have the screenshot of the TLS CLIENT Hello message received by the server when:

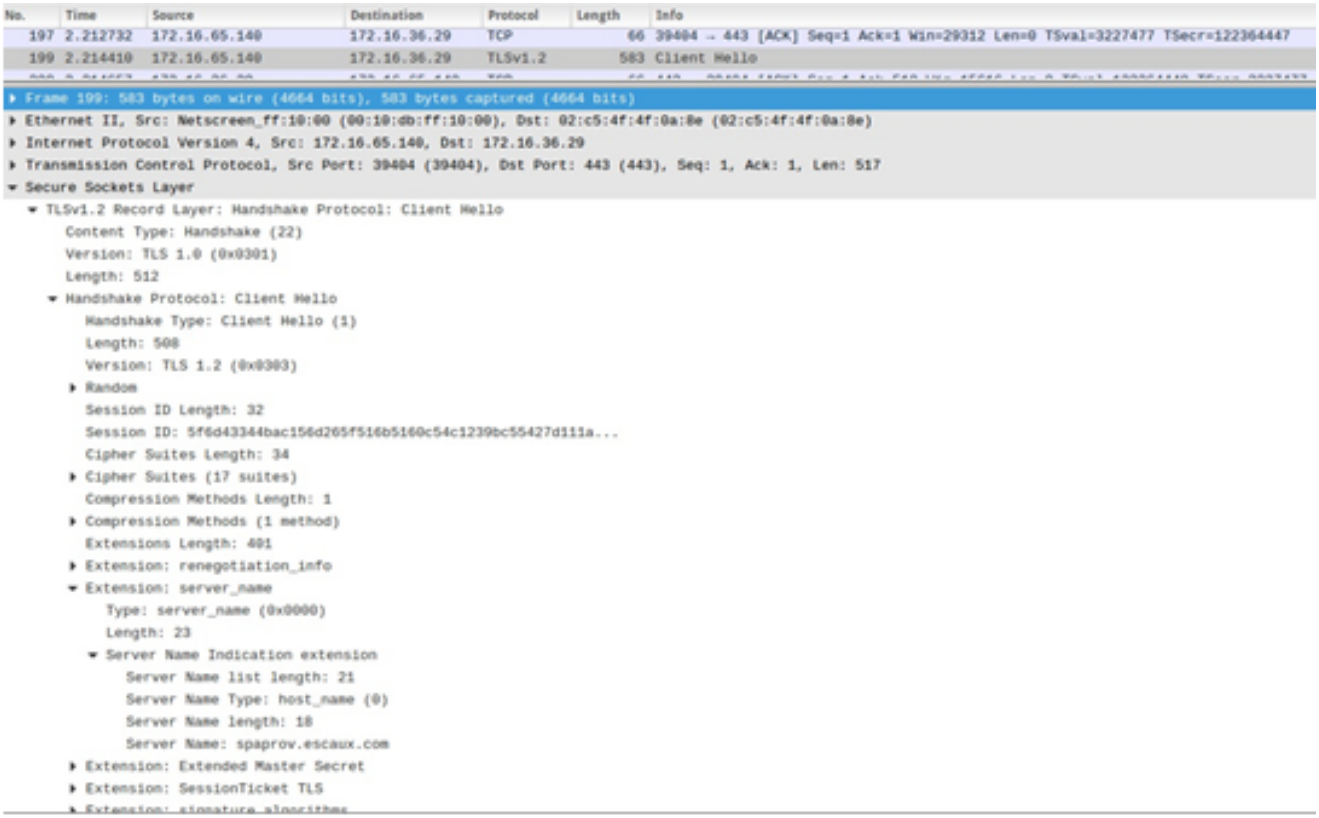
1. SNI is not supported (Request received from the SPA)

Note: In this case, there is no server_name extension in the Handshake Protocol Client Hello.



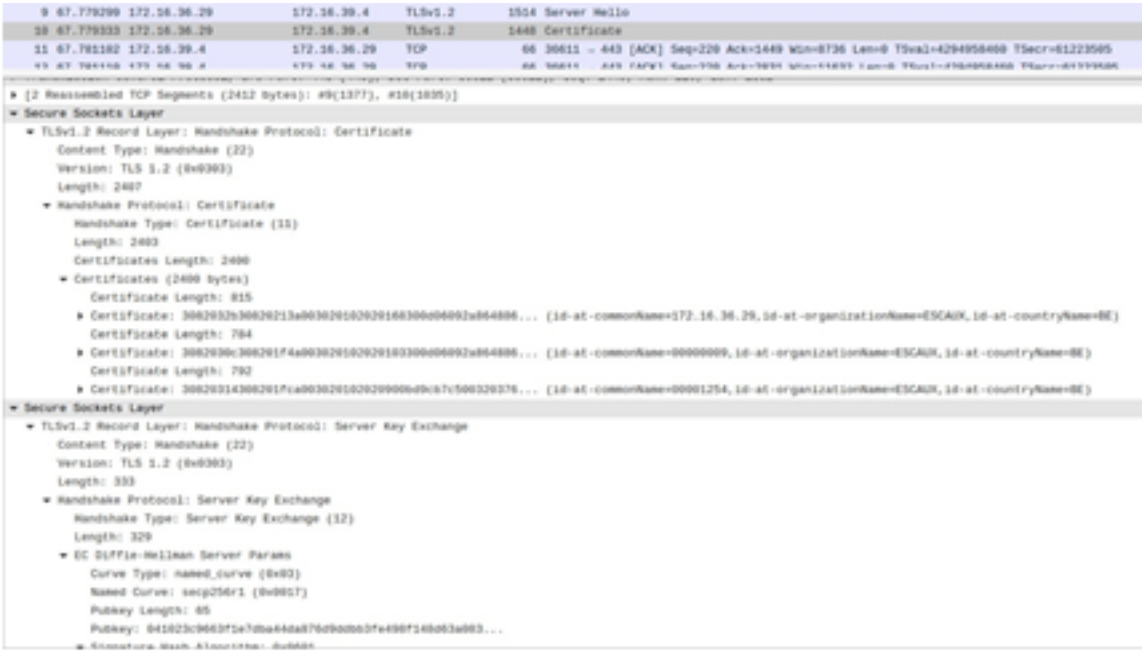
2. SNI is supported (request made via the browser)

Note: In this case, the server_name extension is present in the Handshake Protocol Client Hello.



After the resolution, the request is forwarded to the default virtual host, which has a different Certificate, signed by a different CA. This is where the Unknown CA error occurs in the negotiation phase. With a different result depending on if the request was containing the server_name information or not:

1. Without SNI (request received from the SPA), the Certificate contains the wrong certificate.



2. With SNI supported (request received from the browser), the Server Hello, Certificate

contains the right certificate.

Current Status

Enhancement request to support SNI has already been filed with CDETS ID: CSCve12309.