SPA112:BE-SPA-SSL憑證識別問題

識別日期

2017年1月30日

解決日期

不適用

受影響的產品

SPA112	1.4.2

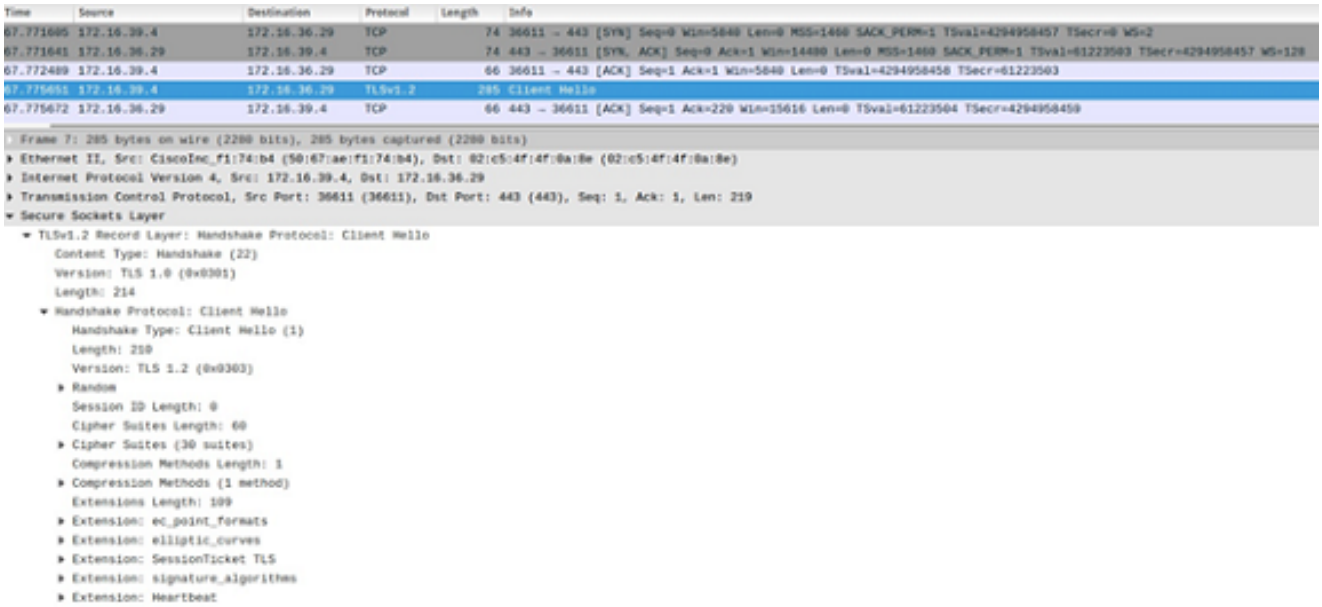
問題描述

從SPA收到的請求不支援伺服器名稱指示(SNI)。 如果傳輸層安全階段不支援名稱指示SNI，則客戶端Hello不包含伺服器名稱資訊。

在以下影象中，您會看到伺服器在以下情況下收到的TLS CLIENT Hello消息的螢幕快照：

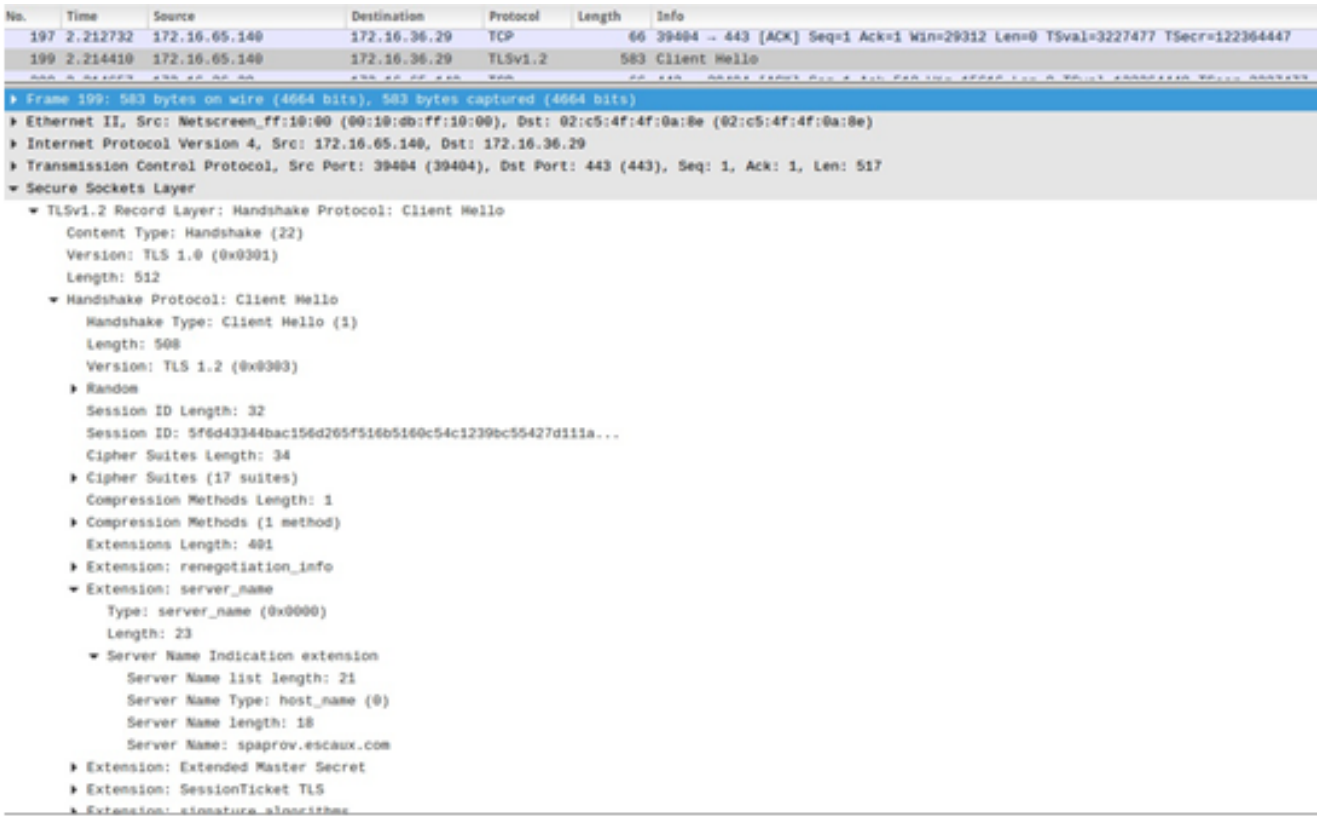
1.不支援SNI（收到來自SPA的請求）

附註：在這種情況下，握手協定客戶端Hello中沒有server_name擴展。



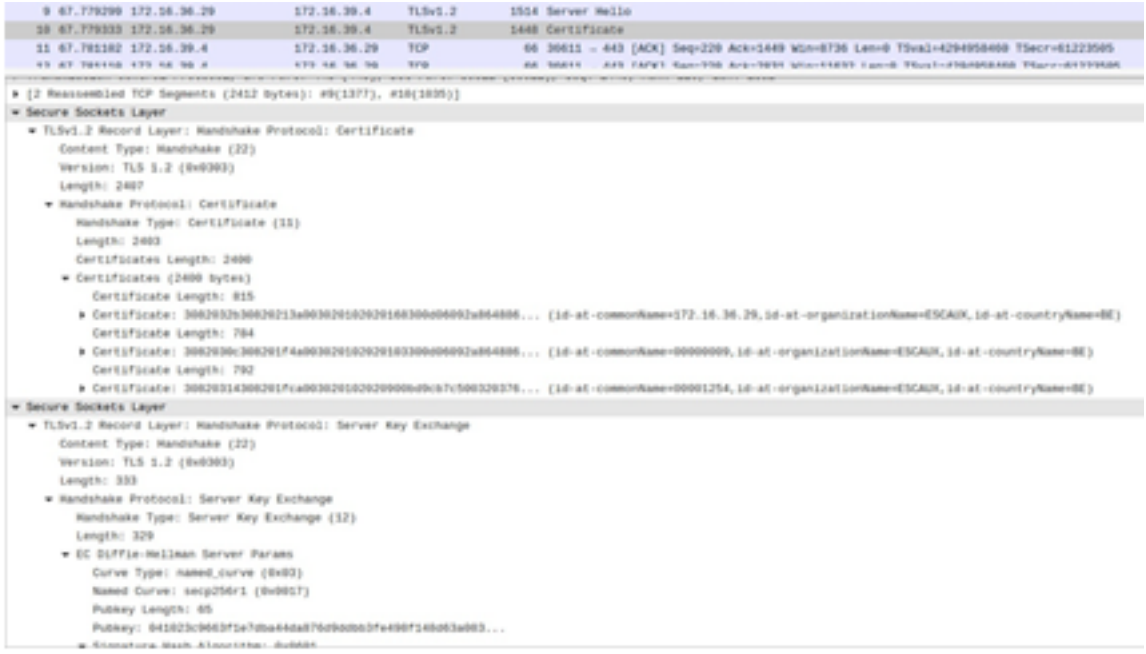
2.支援SNI（通過瀏覽器請求）

附註：在這種情況下，握手協定客戶端Hello中存在server_name擴展。



解析後，請求會被轉發到預設虛擬主機，該虛擬主機具有由其他CA簽名的不同證書。這是協商階段發生未知CA錯誤的地方。根據請求是否包含server_name資訊，結果不同：

1.如果沒有SNI（從SPA收到的請求），則證書包含錯誤的證書。



2.如果支援SNI（從瀏覽器接收請求），則伺服器Hello證書包含正確的證書。

當前狀態

支援SNI的增強請求已通過CDETS ID提交：CSCve12309。