SPA112:BE-SPA-SSL証明書認識の問題

指定日

2017年1月30日

解決日

N/A

影響を受ける製品

SPA112	1.4.2

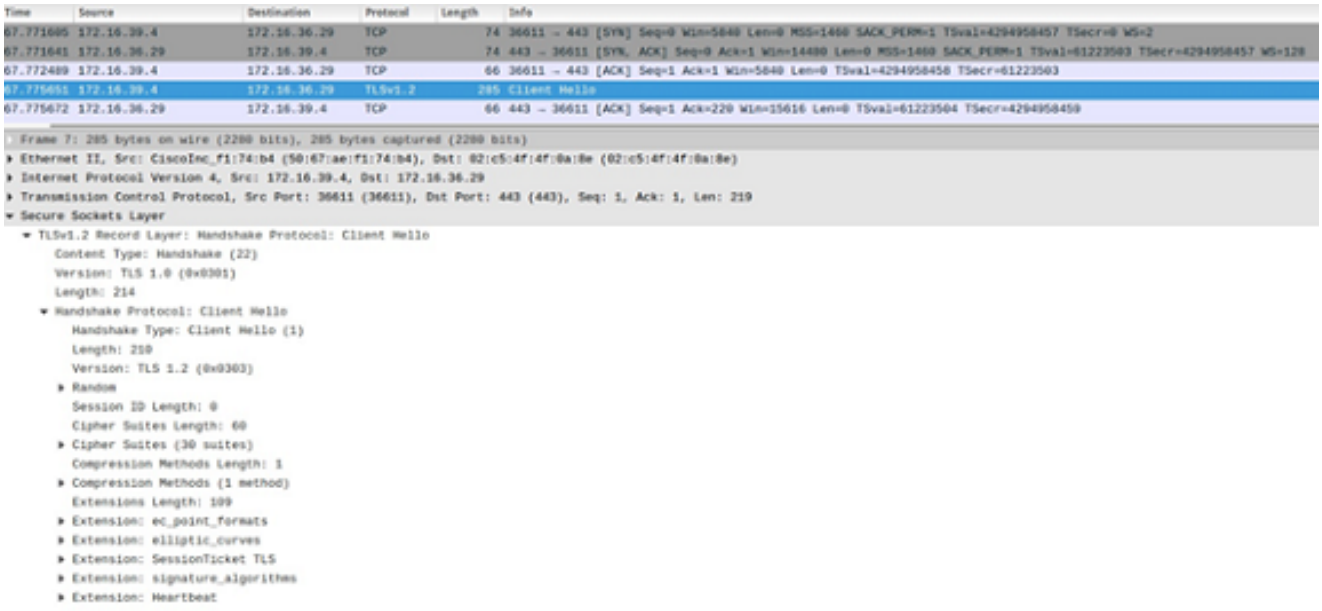
問題の説明

SPAから受信した要求は、サーバ名表示(SNI)をサポートしていません。 Transport Layer Security(TLS)フェーズでName Indication SNIがサポートされていない場合、Client Helloにはサーバ名情報が含まれません。

次の図では、次の場合にサーバが受信するTLS CLIENT Helloメッセージのスクリーンショットがあります。

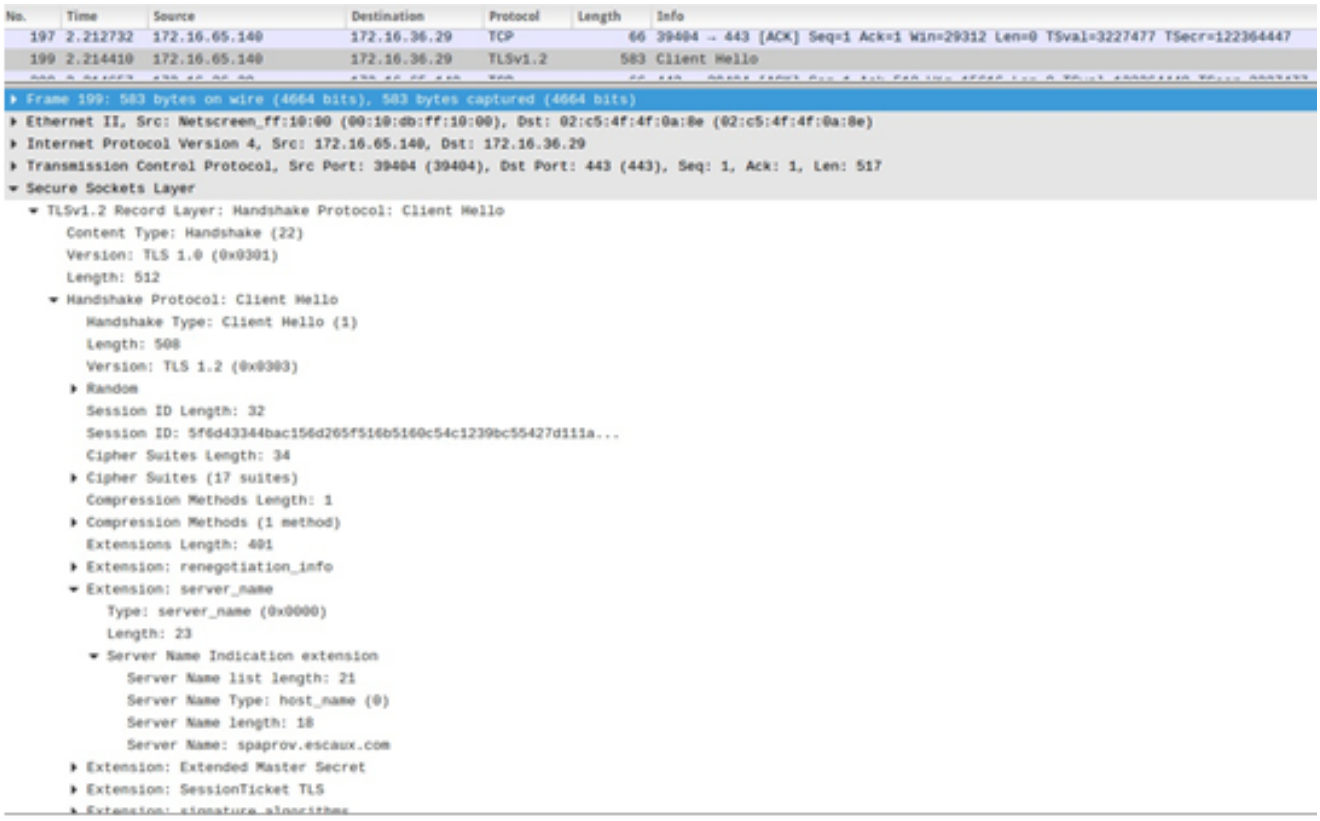
1. SNIはサポートされない（SPAから要求を受信）

注：この場合、Handshake Protocol Client Helloにserver_name拡張はありません。



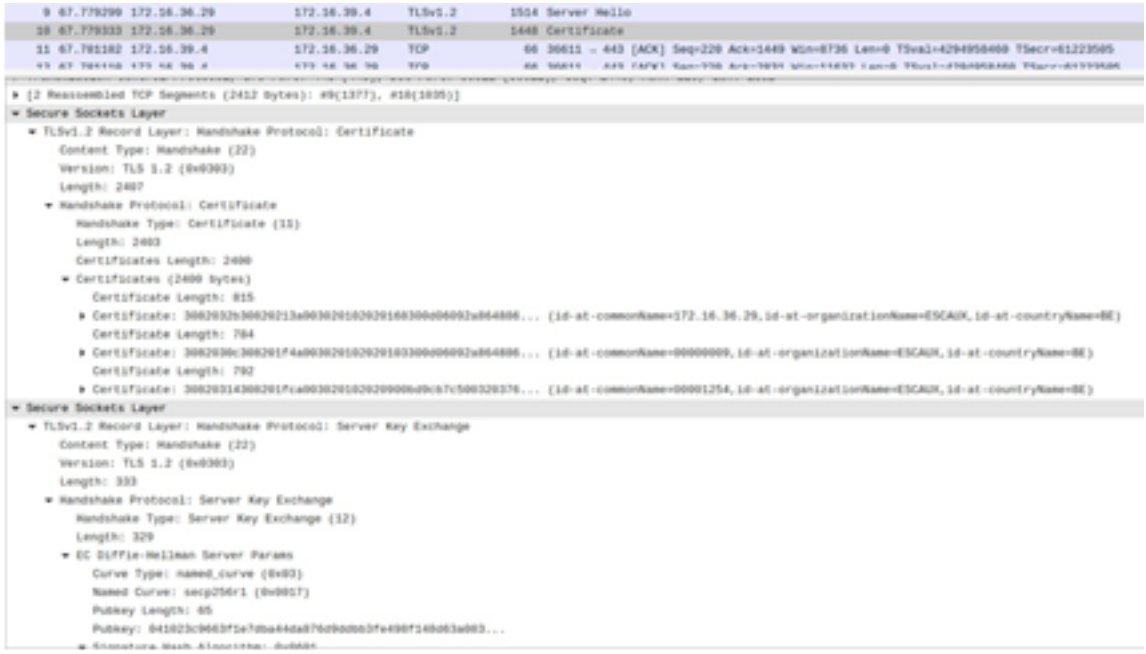
2. SNIがサポートされる（ブラウザを介した要求）

注：この場合、server_name拡張がHandshake Protocol Client Helloに存在します。



解決後、要求は別の証明書を持つデフォルトの仮想ホストに転送され、別のCAによって署名されます。ここで、ネゴシエーションフェーズでUnknown CAエラーが発生します。要求にserver_name情報が含まれているかどうかに応じて、異なる結果が得られます。

1. SNI（SPAから受信した要求）がない場合、証明書に誤った証明書が含まれています。



2. SNIがサポートされている場合（ブラウザから要求を受信した場合）、Server Hello, Certificateに正しい証明書が含まれています。

現在のステータス

SNIをサポートするための拡張要求は、CDETS ID:CSCve12309