SPA112: Problem mit der BE-SPA-SSL-Zertifikaterkennung

Identifiziertes Datum

30. Januar 2017

Auflösungsdatum

K/A

Betroffene Produkte

SPA 112	1,4/2

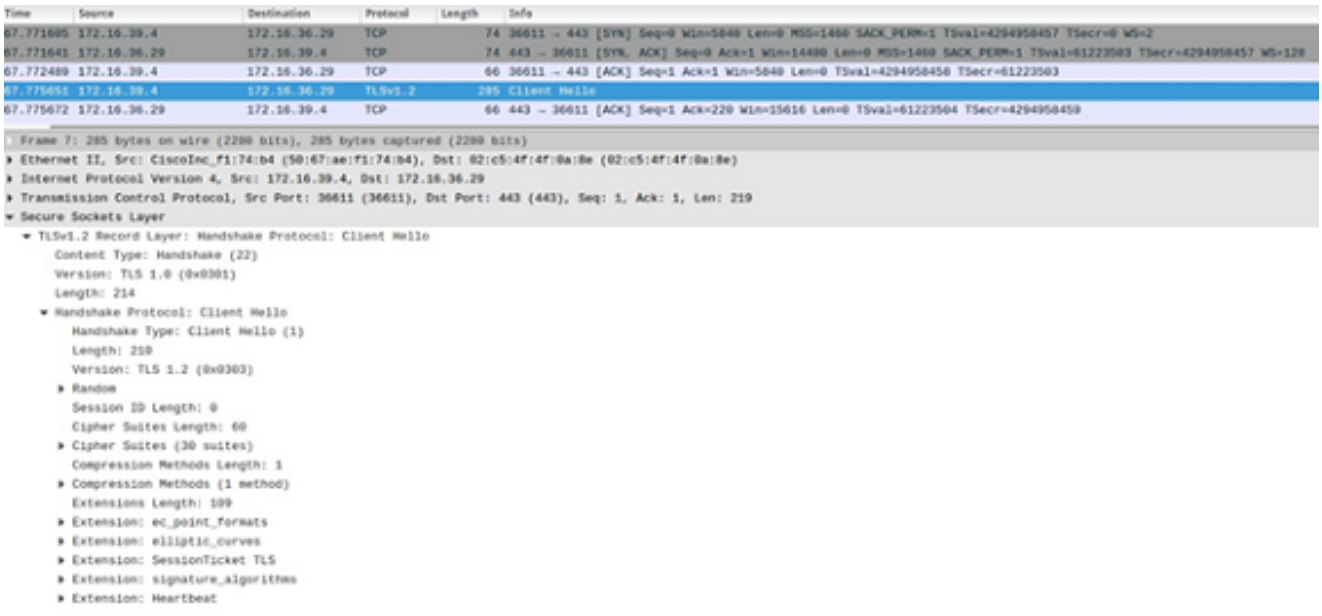
Beschreibung des Problems

Die vom SPA empfangene Anfrage unterstützt die Servernamenanzeige (SNI) nicht. Ohne die SNI-Unterstützung für die Name Indication in der Sicherheitsphase des Transportebene enthält der Client Hello keine Informationen zum Servernamen.

In den folgenden Bildern wird der Screenshot der TLS CLIENT Hello-Nachricht angezeigt, die der Server beim Empfang erhält:

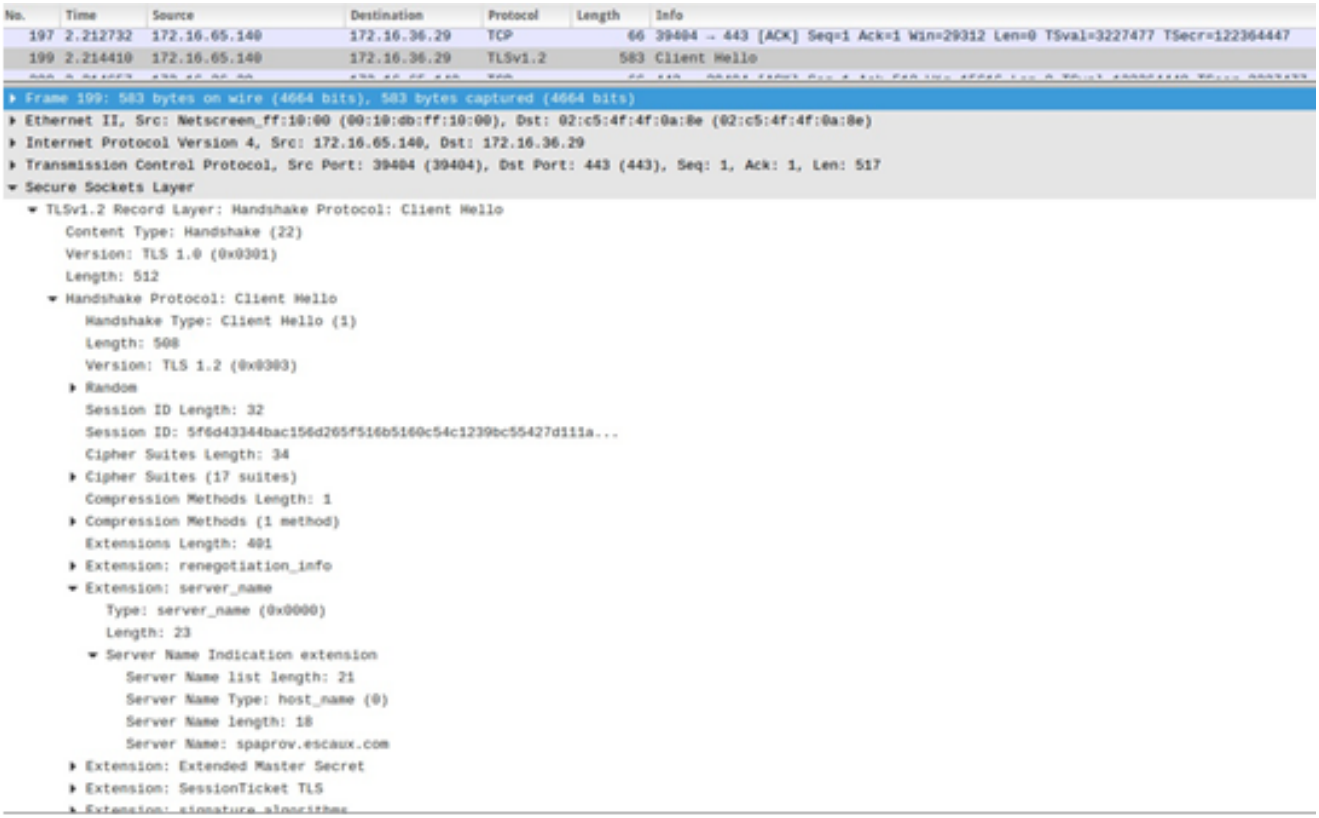
1. SNI wird nicht unterstützt (Anfrage vom SPA erhalten)

Hinweis: In diesem Fall gibt es im Handshake Protocol Client Hello keine Erweiterung server_name.



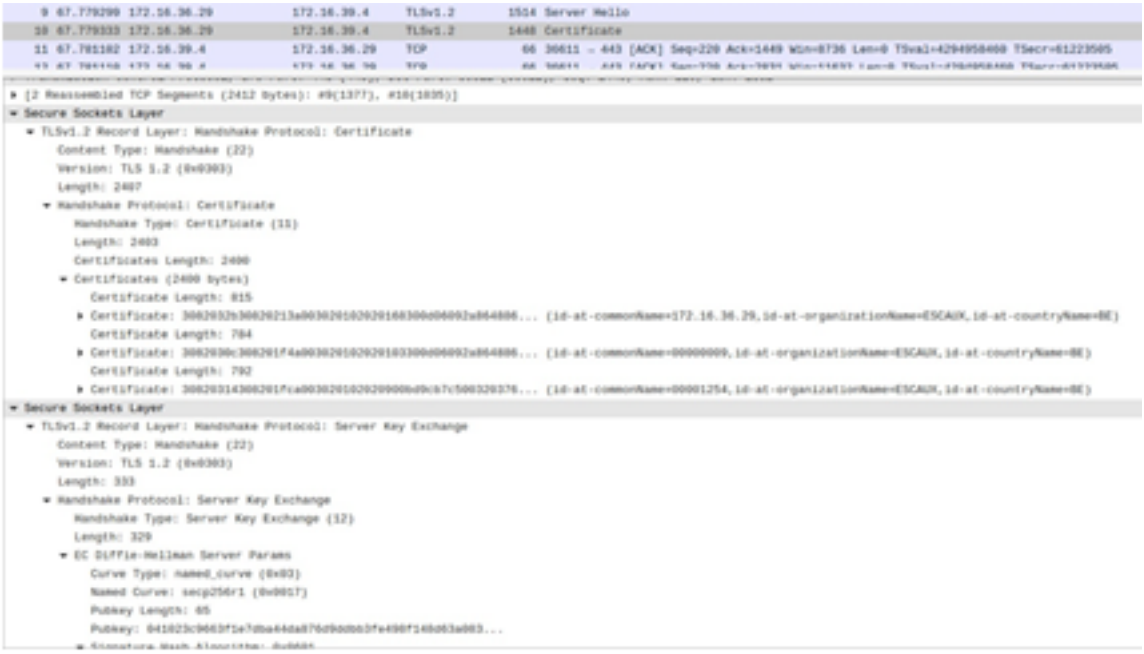
2. SNI wird unterstützt (Anfrage über Browser)

Hinweis: In diesem Fall ist die Erweiterung server_name im Handshake Protocol Client Hello vorhanden.



Nach der Auflösung wird die Anforderung an den virtuellen Standardhost weitergeleitet, der über ein anderes Zertifikat verfügt, das von einer anderen CA signiert wurde. An dieser Stelle tritt der Fehler "Unknown CA" (Unbekannte CA) in der Verhandlungsphase auf. Mit einem anderen Ergebnis, je nachdem, ob die Anforderung Informationen über den Servernamen enthält oder nicht:

1. Ohne SNI (Anfrage vom SPA erhalten) enthält das Zertifikat das falsche Zertifikat.



2. Wenn SNI unterstützt wird (Anfrage vom Browser empfangen), enthält das Server Hello

das entsprechende Zertifikat.

Aktueller Status

Der Verbesserungsantrag zur Unterstützung von SNI wurde bereits mit der CDETS-ID eingereicht: CSCve12309.