SPA112:BE-SPA-SSL证书识别问题

确定日期

2017年1月30日

解决日期

不适用

受影响的产品

SPA112	1.4.2

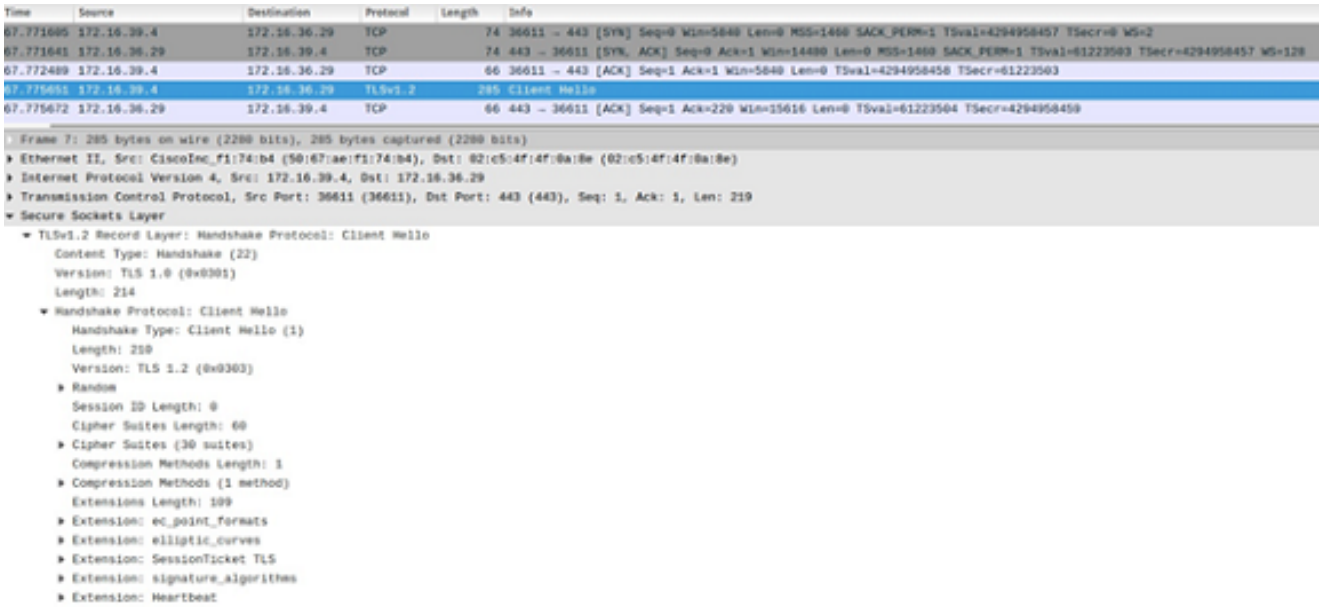
问题说明

从SPA收到的请求不支持服务器名称指示(SNI)。 如果在传输层安全阶段没有名称指示SNI支持，客户端Hello将不包含服务器名称信息。

在以下图像中，您拥有服务器在以下情况下收到的TLS CLIENT Hello消息的截图：

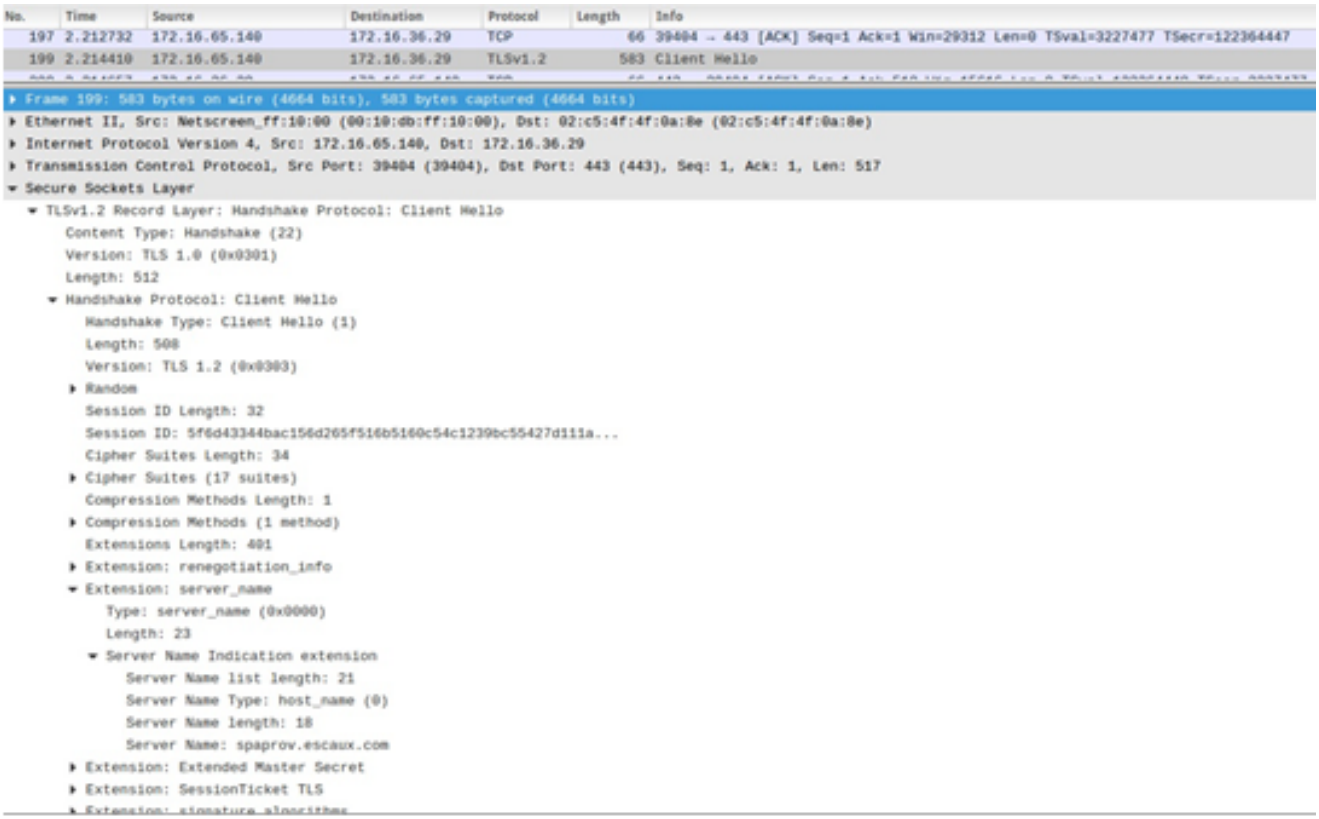
1.不支持SNI（从SPA接收请求）

注意：在这种情况下，握手协议客户端Hello中没有server_name扩展。



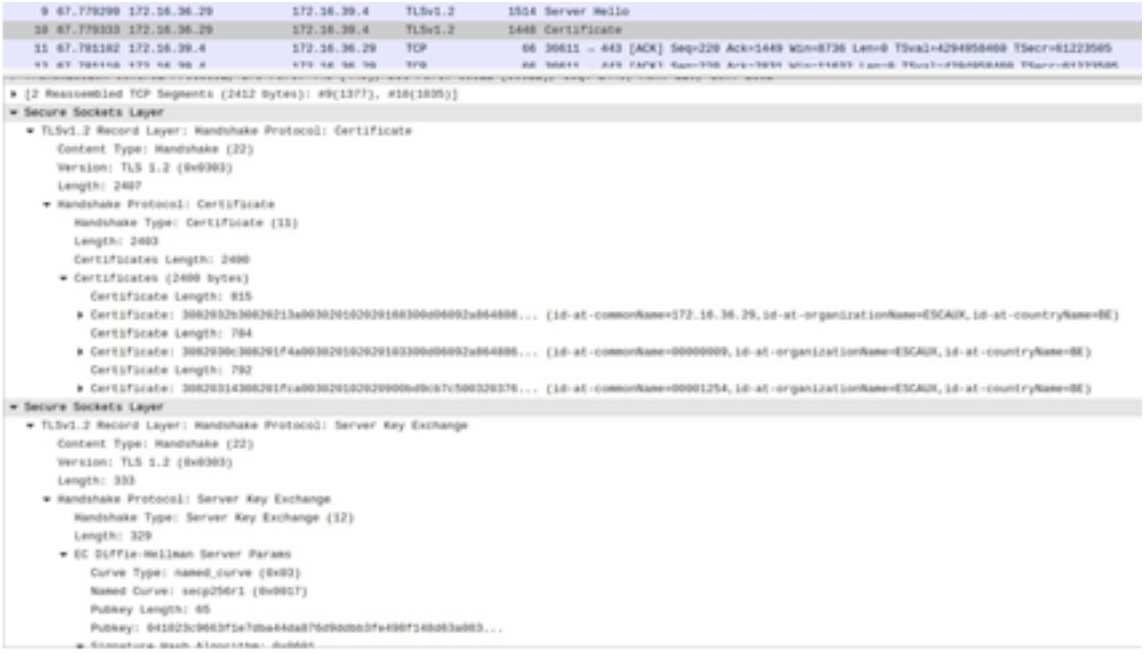
2.支持SNI（通过浏览器发出的请求）

注意：在这种情况下，server_name扩展出现在握手协议客户端Hello中。



解决后，请求将转发到默认虚拟主机，该虚拟主机具有不同的证书，由不同的CA签名。这是协商阶段发生未知CA错误的地方。结果不同，具体取决于请求是否包含server_name信息：

1.如果没有SNI（从SPA接收的请求），证书包含错误的证书。



2.支持SNI（从浏览器接收请求），服务器Hello，证书包含正确的证书。

当前状态

支持SNI的增强请求已向CDETS ID提交：CSCve12309。