

# SPA112: Problema de reconhecimento de certificado BE-SPA-SSL

## Data de identificação

30 de janeiro de 2017

## Data de resolução

N/A

## Produtos afetados

SPA1 12	1.4.2

## Descrição do problema

A solicitação recebida do SPA não suporta a indicação de nome do servidor (SNI). Sem o suporte SNI de indicação de nome na fase de segurança da camada de transporte, o Hello do cliente não contém as informações de nome do servidor.

Nas imagens a seguir, você tem a captura de tela da mensagem de saudação do CLIENTE TLS recebida pelo servidor quando:

1. SNI não é suportado (solicitação recebida do SPA)

**Note:** Nesse caso, não há extensão `server_name` no Handshake Protocol Client Hello.

```
Time    Source                Destination            Protocol  Length  Info
07.771695 172.16.39.4          172.16.36.29          TCP      74      36611 -> 443 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=4294958457 TSecr=0 WS=2
07.771641 172.16.36.29         172.16.39.4          TCP      74      443 -> 36611 [SYN, ACK] Seq=0 Ack=1 Win=14400 Len=0 MSS=1460 SACK_PERM=1 TSval=61223503 TSecr=4294958457 WS=128
07.772489 172.16.39.4          172.16.36.29          TCP      66      36611 -> 443 [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSval=4294958458 TSecr=61223503
07.775651 172.16.39.4          172.16.36.29          TLSv1.2  285     Client Hello
07.775672 172.16.36.29         172.16.39.4          TCP      66      443 -> 36611 [ACK] Seq=1 Ack=220 Win=15616 Len=0 TSval=61223504 TSecr=4294958459

...
Frame 7: 285 bytes on wire (2280 bits), 285 bytes captured (2280 bits)
  Ethernet II, Src: CiscoInc_f1:74:b4 (50:67:ae:f1:74:b4), Dst: 02:c5:4f:4f:0a:8e (02:c5:4f:4f:0a:8e)
  Internet Protocol Version 4, Src: 172.16.39.4, Dst: 172.16.36.29
  Transmission Control Protocol, Src Port: 36611 (36611), Dst Port: 443 (443), Seq: 1, Ack: 1, Len: 219
  Secure Sockets Layer
    TLSv1.2 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 214
    Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 250
      Version: TLS 1.2 (0x0303)
      Random
      Session ID Length: 0
      Cipher Suites Length: 60
      Cipher Suites (30 suites)
      Compression Methods Length: 1
      Compression Methods (1 method)
      Extensions Length: 109
      Extension: ec_point_formats
      Extension: elliptic_curves
      Extension: SessionTicket TLS
      Extension: signature_algorithms
      Extension: heartbeat
```

2. O SNI é suportado (solicitação feita através do navegador)

**Note:** Nesse caso, a extensão server\_name está presente no Handshake Protocol Client Hello.

```

No.    Time    Source                Destination           Protocol    Length  Info
-----
197    2.212732 172.16.65.140        172.16.36.29         TCP        66      39404 -> 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3227477 TSecr=122364447
199    2.214410 172.16.65.140        172.16.36.29         TLSv1.2    583     Client Hello
-----
* Frame 199: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits)
* Ethernet II, Src: Netscreen_ff:10:00 (00:10:0b:ff:10:00), Dst: 02:c5:4f:4f:0a:8e (02:c5:4f:4f:0a:8e)
* Internet Protocol Version 4, Src: 172.16.65.140, Dst: 172.16.36.29
* Transmission Control Protocol, Src Port: 39404 (39404), Dst Port: 443 (443), Seq: 1, Ack: 1, Len: 517
* Secure Sockets Layer
  * TLSv1.2 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 512
  * Handshake Protocol: Client Hello
    Handshake Type: Client Hello (1)
    Length: 508
    Version: TLS 1.2 (0x0303)
    * Random
      Session ID Length: 32
      Session ID: 5f6d43344bac156d265f516b5160c54c1239bc55427d111a...
      Cipher Suites Length: 34
    * Cipher Suites (17 suites)
      Compression Methods Length: 1
    * Compression Methods (1 method)
      Extensions Length: 491
    * Extension: renegotiation_info
  * Extension: server_name
      Type: server_name (0x0000)
      Length: 23
      * Server Name Indication extension
        Server Name list length: 21
        Server Name Type: host_name (0)
        Server Name length: 18
        Server Name: spaprov.escaux.com
    * Extension: Extended Master Secret
    * Extension: SessionTicket TLS
  * Extension: signature_algorithm
  
```

Após a resolução, a solicitação é encaminhada ao host virtual padrão, que tem um certificado diferente, assinado por uma CA diferente. É aqui que ocorre o erro de CA desconhecido na fase de negociação. Com um resultado diferente, dependendo se a solicitação estava contendo as informações de server\_name ou não:

### 1. Sem SNI (solicitação recebida do SPA), o certificado contém o certificado errado.

```

0 87.779290 172.16.36.29        172.16.36.4          TLSv1.2    1554    Server Hello
28 87.779330 172.16.36.29        172.16.36.4          TLSv1.2    1448    Certificate
11 87.781182 172.16.36.4         172.16.36.29         TCP        66      30615 -> 443 [ACK] Seq=229 Ack=1449 Win=8736 Len=0 TSval=429495469 TSecr=61223505
49 87.784110 172.16.36.29        172.16.36.4          TCP        66      30614 -> 30615 [RST] Seq=750 Len=0 Win=0 Len=0 TSval=429495469 TSecr=61223505
-----
* [2 Reassembled TCP Segments (2412 bytes): #0(1377), #1(1035)]
* Secure Sockets Layer
  * TLSv1.2 Record Layer: Handshake Protocol: Certificate
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 2407
  * Handshake Protocol: Certificate
    Handshake Type: Certificate (11)
    Length: 2403
    Certificates Length: 2400
  * Certificates (2400 bytes)
    Certificate Length: 815
    * Certificate: 308202b30820213a003020102030100300004002a04806... [10-at-commonName=172.16.36.29,10-at-organizationName=ESCAUX,10-at-countryName=BE]
    Certificate Length: 784
    * Certificate: 3082030c308201f4a003020102020103000004002a04806... [10-at-commonName=00000009,10-at-organizationName=ESCAUX,10-at-countryName=BE]
    Certificate Length: 792
    * Certificate: 30820314308201fca00302010202000004002a04806... [10-at-commonName=00001254,10-at-organizationName=ESCAUX,10-at-countryName=BE]
  * Secure Sockets Layer
  * TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 353
  * Handshake Protocol: Server Key Exchange
    Handshake Type: Server Key Exchange (12)
    Length: 329
  * EC Diffie-Hellman Server Params
    Curve Type: named_curve (0x03)
    Named Curve: secp256r1 (0x0007)
    Pubkey Length: 65
    Pubkey: 041023c9603f2e73ba44a876b0b0b3fe40f14b03a0b3...
  * Signature: SHA1withRSA
  
```

### 2. Com o SNI suportado (solicitação recebida do navegador), o Server Hello, Certificate contém o certificado correto.

