

SPA112: Problema de reconocimiento de certificado BE-SPA-SSL

Fecha identificada

30 de enero de 2017

Fecha de resolución

N/A

Productos afectados

SPA1 12	1.4.2

Descripción de problemas

La solicitud recibida del SPA no admite la indicación de nombre de servidor (SNI). Sin la compatibilidad con la SNI de indicación de nombre en la fase de seguridad de la capa de transporte, la Hello del cliente no contiene la información del nombre del servidor.

En las siguientes imágenes, tiene la captura de pantalla del mensaje TLS CLIENT Hello recibido por el servidor cuando:

1. No se admite SNI (solicitud recibida del SPA)

Nota: En este caso, no hay extensión server_name en el protocolo de intercambio de señales de cliente Hello.

```
Time      Source          Destination      Protocol  Length  Info
07.771600 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=14480 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=4294958458

...Frame 7: 285 bytes on wire (2280 bits), 285 bytes captured (2280 bits)
* Ethernet II, Src: CiscoEnc_f1:74:b4 (50:67:ae:f1:74:b4), Dst: 02:c5:4f:4f:8a:8e (02:c5:4f:4f:8a: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. Se admite SNI (solicitud realizada a través del explorador)

Nota: En este caso, la extensión server_name está presente en el protocolo de intercambio de señales de cliente 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	563	Client Hello

Frame 199: 563 bytes on wire (4664 bits), 563 bytes captured (4664 bits)

- Ethernet II, Src: Netscreen_ff:10:00 (90:10:0b:ff:10:00), Dst: 02:c5:4f:0a:8e (02:c5:4f: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: 401
 - 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_algorithms

Después de la resolución, la solicitud se reenvía al host virtual predeterminado, que tiene un certificado diferente, firmado por una CA diferente. Aquí es donde ocurre el error de CA Desconocida en la fase de negociación. Con un resultado diferente dependiendo de si la solicitud contenía o no la información de nombre_servidor:

1. Sin SNI (solicitud recibida del SPA), el certificado contiene el certificado incorrecto.

9	67.779299	172.16.36.29	172.16.36.4	TLSv1.2	1554	Server Hello
10	67.779333	172.16.36.29	172.16.36.4	TLSv1.2	1448	Certificate
11	67.781182	172.16.36.4	172.16.36.29	TCP	66	30611 → 443 [ACK] Seq=229 Ack=1449 Win=8736 Len=0 TSval=429495869 TSecr=61223595
13	67.781188	172.16.36.4	172.16.36.29	TCP	66	30611 → 443 [ACK] Seq=756 Ack=7691 Win=6557 Len=0 TSval=429495869 TSecr=61223595

[2 Reassembled TCP Segments (2412 bytes): #9(1377), #10(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: 3062932b30629213a03020102020160306004092a864886... [id-at-commonName=172.16.36.29, id-at-organizationName=ESCAUX, id-at-countryName=BE]
 - Certificate Length: 784
 - Certificate: 3062930c306291f74a00302010202010300004092a864886... [id-at-commonName=00000000, id-at-organizationName=ESCAUX, id-at-countryName=BE]
 - Certificate Length: 792
 - Certificate: 30629314306291fca00302010202000000c57c500329376... [id-at-commonName=00001254, id-at-organizationName=ESCAUX, id-at-countryName=BE]

2. Con SNI admitido (solicitud recibida del navegador), Server Hello, Certificate contiene el certificado correcto.

