SPA112:BE-SPA-SSL 인증서 인식 문제

식별된 날짜

2017년 1월 30일

해결된 날짜

해당 없음

영향을 받는 제품

SPA112	1.4.2

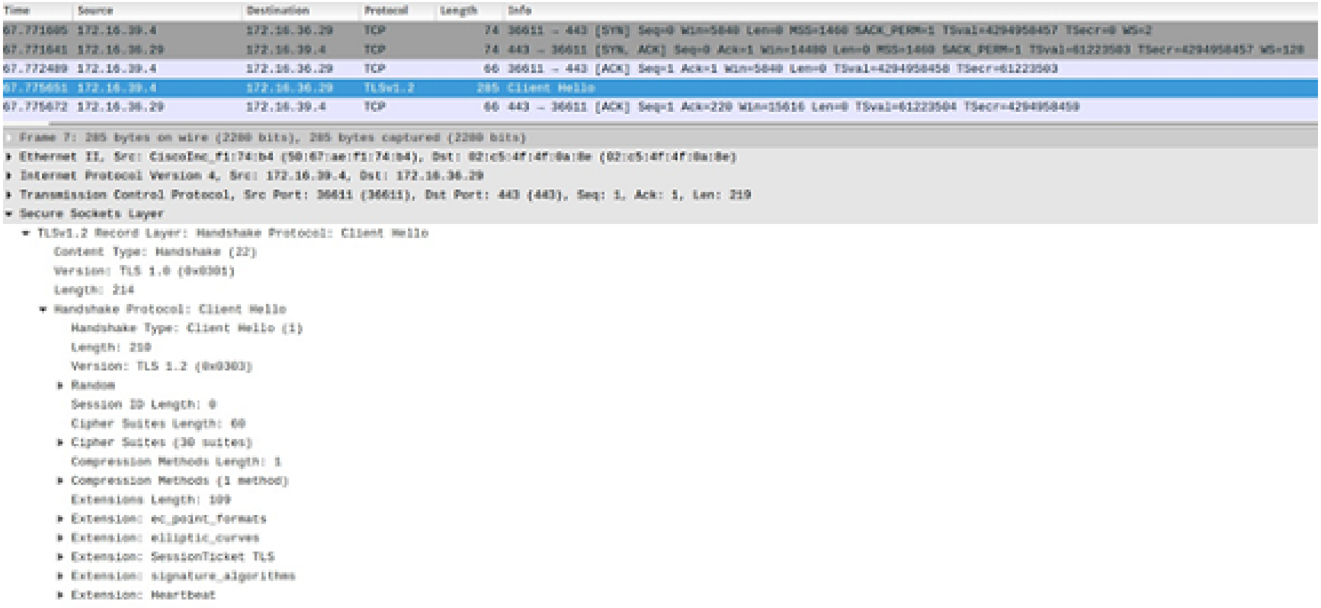
문제 설명

SPA에서 받은 요청은 SNI(서버 이름 표시)를 지원하지 않습니다. Transport Layer Security 단계에서 Name Indication SNI를 지원하지 않으면 Client Hello에 서버 이름 정보가 포함되지 않습니다.

다음 이미지에서는 다음과 같은 경우 서버에서 받은 TLS CLIENT Hello 메시지의 스크린샷을 볼 수 있습니다.

1. SNI가 지원되지 않습니다(SPA에서 요청 접수).

참고:이 경우 Handshake Protocol Client Hello에는 server_name 확장이 없습니다.

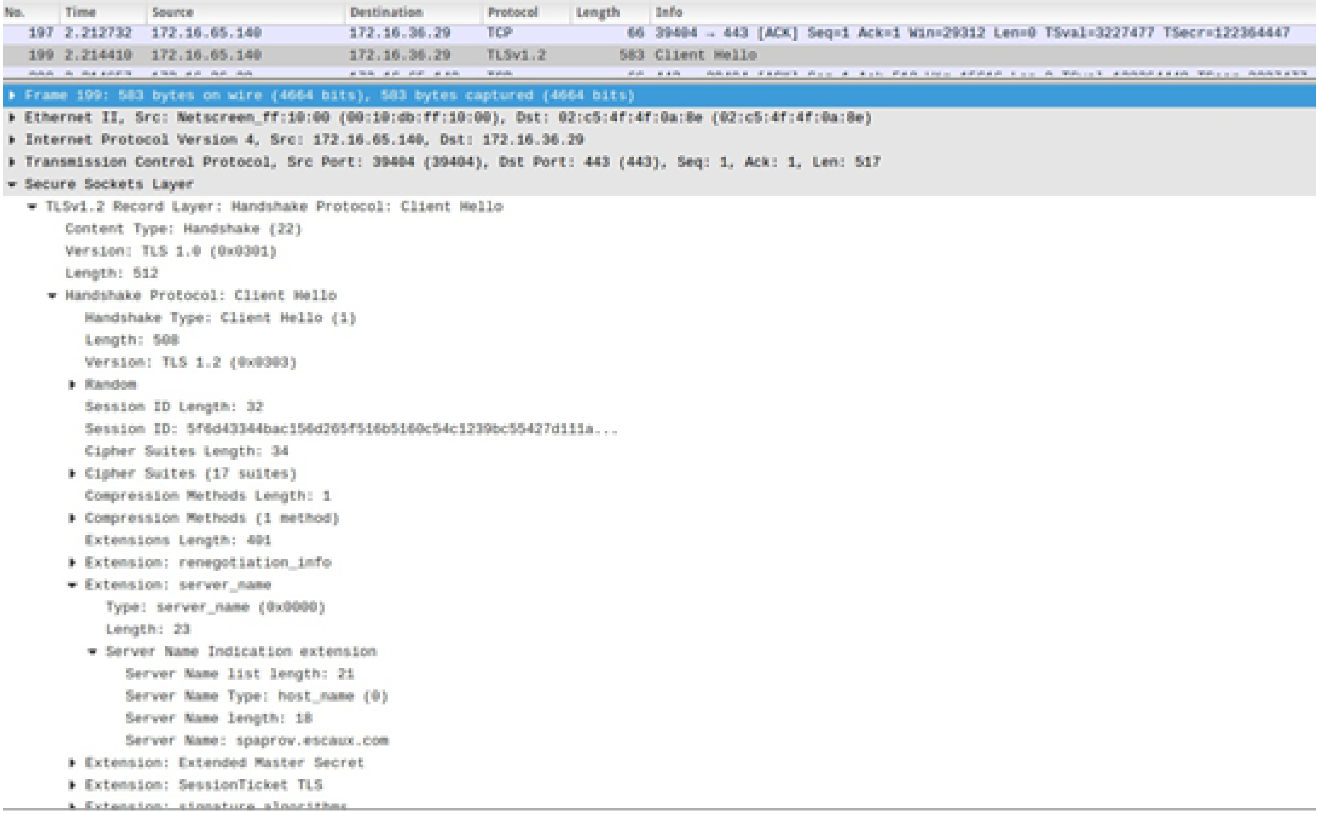


```
Time        Source         Destination    Protocol  Length  Info
67.771605   172.16.39.4    172.16.36.29   TCP       74 36611 → 443 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=4294958457 TSecr=0 WS=2
67.771641   172.16.36.29   172.16.39.4    TCP       74 443 → 36611 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=61223503 TSecr=4294958457 WS=128
67.772489   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
67.775651   172.16.39.4    172.16.36.29   TLSv1.2   285 Client Hello
67.775672   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: CiscoInc_f1:74:b4 (58:67: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: 210
        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. SNI가 지원됨(브라우저를 통해 요청)

참고:이 경우 server_name 확장명은 Handshake Protocol Client Hello에 있습니다.

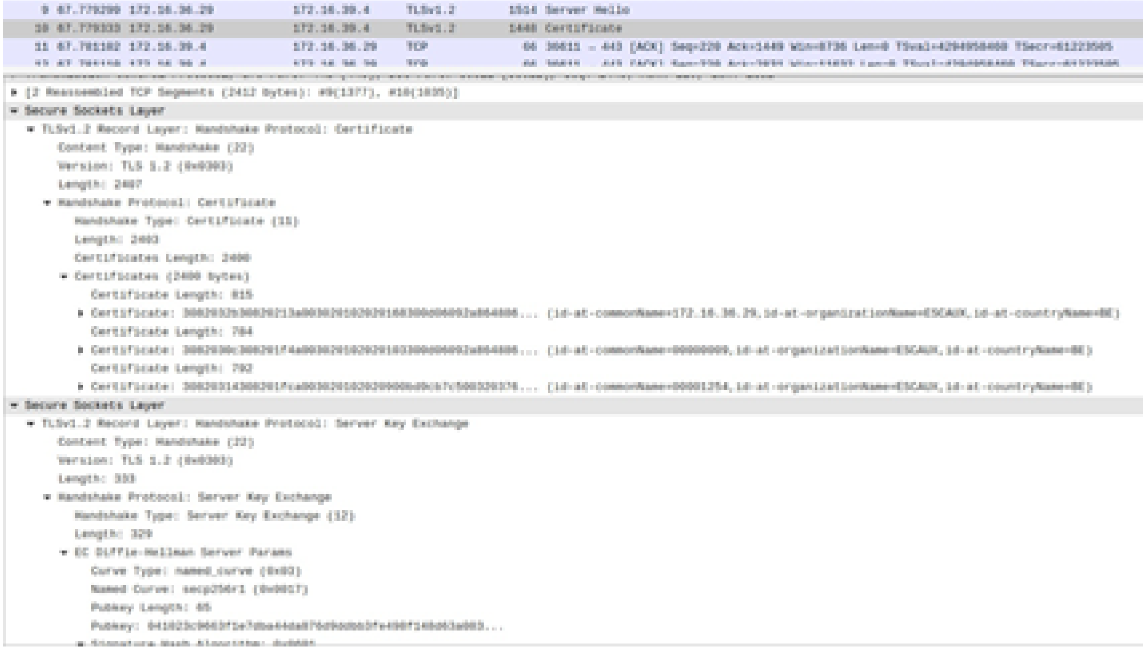


```
No.   Time       Source            Destination      Protocol  Length  Info
  197 2.212732   172.16.65.140     172.16.36.29     TCP           66  39404 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3227477 TSecr=122364447
  199 2.214410   172.16.65.140     172.16.36.29     TLSv1.2      583  Client Hello

▸ Frame 199: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits)
▸ Ethernet II, Src: Netscreen_ff:10:00 (00:10:db: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: 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
```

해결 후 요청은 다른 CA에 의해 서명된 다른 인증서가 있는 기본 가상 호스트로 전달됩니다 .협상 단계에서 알 수 없는 CA 오류가 발생하는 위치입니다.요청에 server_name 정보가 포함되어 있는지 여부에 따라 다른 결과가 표시됩니다.

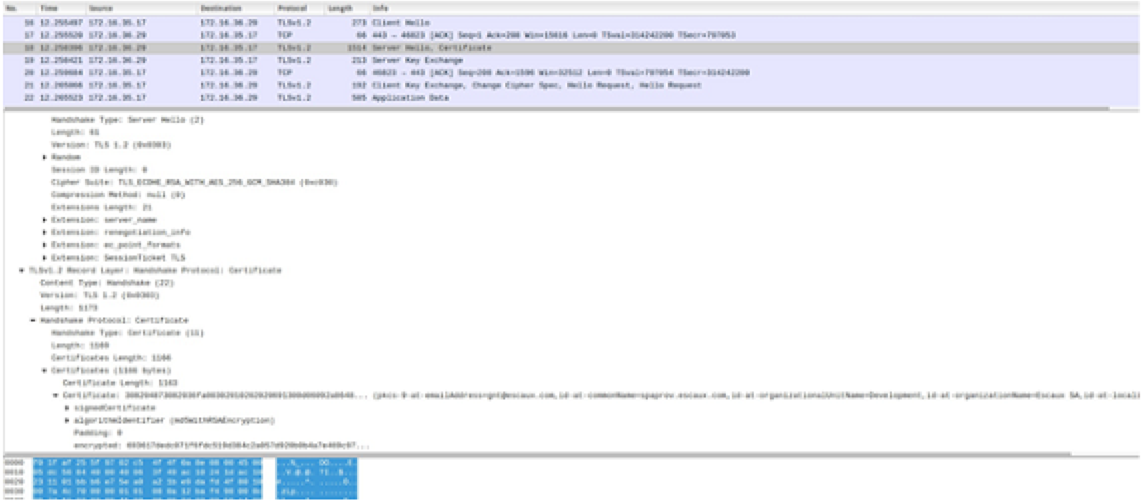
1. SNI가 없는 경우(SPA에서 받은 요청) 인증서에 잘못된 인증서가 포함되어 있습니다.



```
    9 67.779299 172.16.36.29       172.16.39.4      TLSv1.2      1514 Server Hello
   10 67.779333 172.16.36.29       172.16.39.4      TLSv1.2      1448 Certificate
   11 67.781182 172.16.39.4        172.16.36.29     TCP            66 38611 → 443 [ACK] Seq=220 Ack=1449 Win=8736 Len=0 TSval=4294958460 TSecr=61223505

▸ [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: 3082032b30820213a003020102020168300d06092a864886... (id-at-commonName=172.16.36.29,id-at-organizationName=ESCAUX,id-at-countryName=BE)
          Certificate Length: 784
        ▸ Certificate: 3082030c308201f4a003020102020163300d06092a864886... (id-at-commonName=00000009,id-at-organizationName=ESCAUX,id-at-countryName=BE)
          Certificate Length: 792
        ▸ Certificate: 30820314308201fca003020102020900bd9cb7c500320376... (id-at-commonName=00001254,id-at-organizationName=ESCAUX,id-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: 333
    ▾ 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 (0x0017)
          Pubkey Length: 65
          Pubkey: 041023c9663f1e7dba44da876d9bdbb3fe498f148d63a083...
        ▸ Signature Hash Algorithm: 0x0601
```

2. SNI가 지원되는 경우(브라우저에서 받은 요청), Server Hello, Certificate에 올바른 인증서가 포함됩니다.



```
No.   Time        Source         Destination    Protocol  Length Info
   16 12.255497   172.16.35.17   172.16.36.29   TLSv1.2      273 Client Hello
   17 12.255520   172.16.36.29   172.16.35.17   TCP           66 443 → 46823 [ACK] Seq=1 Ack=208 Win=15616 Len=0 TSval=314242200 TSecr=797053
   18 12.258396   172.16.36.29   172.16.35.17   TLSv1.2    1514 Server Hello, Certificate
   19 12.258421   172.16.36.29   172.16.35.17   TLSv1.2      213 Server Key Exchange
   20 12.258684   172.16.35.17   172.16.36.29   TCP           66 46823 → 443 [ACK] Seq=208 Ack=1506 Win=32512 Len=0 TSval=797054 TSecr=314242200
   21 12.265068   172.16.35.17   172.16.36.29   TLSv1.2      192 Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request
   22 12.265523   172.16.35.17   172.16.36.29   TLSv1.2      505 Application Data

        Handshake Type: Server Hello (2)
        Length: 61
        Version: TLS 1.2 (0x0303)
      ▸ Random
        Session ID Length: 0
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
        Compression Method: null (0)
        Extensions Length: 21
      ▸ Extension: server_name
      ▸ Extension: renegotiation_info
      ▸ Extension: ec_point_formats
      ▸ Extension: SessionTicket TLS
  ▾ TLSv1.2 Record Layer: Handshake Protocol: Certificate
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 1173
    ▾ Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 1169
        Certificates Length: 1166
      ▾ Certificates (1166 bytes)
          Certificate Length: 1163
        ▾ Certificate: 308204873082036fa003020102020900913000000092a0548... (pkcs-9-at-emailAddress=gnt@escaux.com,id-at-commonName=spaprov.escaux.com,id-at-organizationalUnitName=Development,id-at-organizationName=Escaux SA,id-at-locali
          ▸ signedCertificate
          ▸ algorithmIdentifier (md5WithRSAEncryption)
            Padding: 0
            encrypted: 6036l7dedc071f6fdc510d384c2a057d920b0b4a7e408c07...

0000  70 1f af 25 5f 07 02 c5  4f 4f 6a 8e 08 00 45 00   ...%_... OO....E.
0010  05 ac 58 04 40 00 40 06  3f 40 ac 10 24 1d ac 10   ..V.@.@. ?I...$..
0020  23 11 01 bb b6 e7 5e a0  a2 5b e9 da fd 4f 80 10   #.....^. .[...O..
0030  00 7a 4c 70 00 00 01 01  08 0a 12 ba f8 98 00 0c   .zLp.... ........
```

현재 상태

CDETS ID로 SNI 지원 개선 요청이 이미 제출되었습니다.CSCve12309.