

SPA112: BE-SPA-SSL Certificate Recognition Issue

Date Identified

January 30, 2017

Date Resolved

N/A

Products Affected

SPA1 12	1.4.2

Problem Description

Request received from the SPA does not support the Server Name Indication (SNI). Without the Name Indication SNI support on the Transport Layer Security phase, the Client Hello does not contain the server name information.

In the following images, you have the screenshot of the TLS CLIENT Hello message received by the server when:

1. SNI is not supported (Request received from the SPA)

Note: In this case, there is no server_name extension in the Handshake Protocol Client Hello.

```
Time      Source          Destination      Protocol  Length  Info
07.771605 172.16.39.4     172.16.36.29    TCP       74      36611 -> 443 [SYN] Seq=0 Win=5040 Len=0 MSS=1460 SACK_PERM=1 TSval=4294958457 TSecr=0 WS=2
07.771645 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=5040 Len=0 TSval=4294958458 TSecr=61223503
07.775655 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=229 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: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. SNI is supported (request made via the browser)

Note: In this case, the server_name extension is present in the 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 (90:10:0b: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: 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

After the resolution, the request is forwarded to the default virtual host, which has a different Certificate, signed by a different CA. This is where the Unknown CA error occurs in the negotiation phase. With a different result depending on if the request was containing the server_name information or not:

1. Without SNI (request received from the SPA), the Certificate contains the wrong certificate.

9	67.779290	172.16.36.29	172.16.39.4	TLSv1.2	1504	Server Hello
10	67.779333	172.16.36.29	172.16.39.4	TLSv1.2	1448	Certificate
11	67.782182	172.16.39.4	172.16.36.29	TCP	66	30612 → 443 [ACK] Seq=220 Ack=1449 Win=8736 Len=0 TSval=4294950469 TSecr=61223005
15	67.784168	172.16.36.29	172.16.36.29	TCP	66	30614 → 443 [ACK] Seq=220 Ack=1449 Win=8736 Len=0 TSval=4294950469 TSecr=61223005

[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 (13)
 - Length: 2403
 - Certificates Length: 2400
 - Certificates (2400 bytes)
 - Certificate Length: 815
 - Certificate: 3082032b30820113a00302010202010300000001a054896... [id-at-commonName=172.16.36.29,id-at-organizationName=ESCAUX,id-at-countryName=BE]
 - Certificate Length: 784
 - Certificate: 3082030c308201f4a00302010202010300000001a054896... [id-at-commonName=00000000,id-at-organizationName=ESCAUX,id-at-countryName=BE]
 - Certificate Length: 792
 - Certificate: 30820314308201f1a00302010202010300000001a054896... [id-at-commonName=0001254,id-at-organizationName=ESCAUX,id-at-countryName=BE]

2. With SNI supported (request received from the browser), the Server Hello, Certificate

contains the right certificate.

The image shows a Wireshark packet capture of a TLS handshake. The top section is a packet list with columns for No., Time, Source, Destination, Protocol, Length, and Info. Packet 20 is the Server Hello message. The bottom section is the packet details pane for packet 20, showing the following structure:

- Handshake Type: Server Hello (2)
- Length: 65
- Version: TLS 1.2 (0x0303)
- Random (8)
- Session ID Length: 0
- Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc030)
- Compression Method: null (0)
- Extensions Length: 21
- Extensions: server_name, renegotiation_info, ec_point_formats, session_ticket (0)
- Handshake Protocol: Certificate
- Handshake Type: Certificate (1)
- Length: 1048
- Certificate Length: 1048
- Certificate (1048 bytes)
- Certificate Length: 1048
- Certificate: 3023497362303F46032052022803300000024004... (hex)
- Signature Algorithm: sha256WithRSAEncryption
- Padding: 0
- Signature: 603617e6d07191fa11b0f84c3db70d30b6b7e40b97...

Current Status

Enhancement request to support SNI has already been filed with CDETS ID: CSCve12309.