

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

SPA1 12	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。

```
Time      Source          Destination      Protocol  Length  Info
07.771600 172.16.39.4     172.16.36.29    TCP       74      36611 → 443 [SYN] Seq=0 Win=65535 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=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=220 Win=35616 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: 280
    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.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。

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 (00:10:00: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
  
```

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。

9	87.779299	172.16.36.29	172.16.36.4	TLSv1.2	1554	Server Hello
10	87.779333	172.16.36.29	172.16.36.4	TLSv1.2	1448	Certificate
11	87.782182	172.16.36.4	172.16.36.29	TCP	66	39611 → 443 [ACK] Seq=229 Ack=1449 Win=8736 Len=0 TSval=4294958468 TSecr=61223595
13	87.784148	172.16.36.4	172.16.36.29	TCP	66	39611 → 443 [ACK] Seq=736 Ack=7691 Win=65537 Len=0 TSval=4304888468 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: 3082932b30829213a003020102020168300604092a864886... [id-at-commonName=172.16.36.29,id-at-organizationName=ESCAUX,id-at-countryName=BE]
        Certificate Length: 784
        Certificate: 3082930c308291f74a003020102020168300604092a864886... [id-at-commonName=00000000,id-at-organizationName=ESCAUX,id-at-countryName=BE]
        Certificate Length: 792
        Certificate: 30829314308291f7ca003020102020900000c57c508329376... [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: 329
      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: 041823c9663f2e79ba44da876d908b3fe49f248d63a083...
          EncryptedMasterSecret: 00000000
  
```

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。

