

# SPA112:BE-SPA-SSL証明書認識の問題

## 指定日

2017年1月30日

## 解決日

N/A

## 影響を受ける製品

SPA1 12	1.4.2

## 問題の説明

SPAから受信した要求は、サーバ名表示(SNI)をサポートしていません。 Transport Layer Security(TLS)フェーズでName Indication SNIがサポートされていない場合、Client Helloにはサーバ名情報が含まれません。

次の図では、次の場合にサーバが受信するTLS CLIENT Helloメッセージのスクリーンショットがあります。

### 1. SNIはサポートされない ( SPAから要求を受信 )

注：この場合、Handshake Protocol Client Helloにserver\_name拡張はありません。

```
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
07.771641 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
07.775652 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=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: 82: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. SNIがサポートされる ( ブラウザを介した要求 )

注：この場合、server\_name拡張がHandshake Protocol Client Helloに存在します。

```

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 (90:10:00: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

```

解決後、要求は別の証明書を持つデフォルトの仮想ホストに転送され、別のCAによって署名されます。ここで、ネゴシエーションフェーズでUnknown CAエラーが発生します。要求にserver\_name情報が含まれているかどうかに応じて、異なる結果が得られます。

1. SNI (SPAから受信した要求) がない場合、証明書に誤った証明書が含まれています。

```

9 67.779299 172.16.36.29        172.16.36.4         TLSv1.2    1504    Server Hello
10 67.779333 172.16.36.29        172.16.36.4         TLSv1.2    1448    Certificate
11 67.781282 172.16.36.4        172.16.36.29        TCP        66      30612 -> 443 [ACK] Seq=229 Ack=1449 Win=8736 Len=0 TSval=4294958469 TSecr=61223005
45 47 304168 475 48 36 0  475 48 36 36  370    68 30614  443 14741  Seq=708  Acc=1634  Win=14832  Len=0  TSval=4764008468  TSecr=61579406

* [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: 3062032b30620213a003020102020100300000002b064896... [id-at-commonName=172.16.36.29,id-at-organizationName=ESCAUX,id-at-countryName=BE]
        Certificate Length: 784
        * Certificate: 3062030c306201f4a003020102020100300000002b064896... [id-at-commonName=00000000,id-at-organizationName=ESCAUX,id-at-countryName=BE]
        Certificate Length: 792
        * Certificate: 30620314306201fca0030201020200000000c7c50032037e... [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: 48
          Pubkey: 041023c0603f2a70a64da8760b0bd3fe40f14003a063...
          * Signature Hash Algorithm: null

```

2. SNIがサポートされている場合 (ブラウザから要求を受信した場合)、Server Hello, Certificateに正しい証明書が含まれています。

No.	Time	Source	Destination	Protocol	Length	Info
36	12.250487	172.16.36.17	172.16.36.29	TLSv1.2	378	Client Hello
37	12.250509	172.16.36.29	172.16.36.17	TCP	66	443 -> 443 [ACK] Seq=1268 Win=1816 Len=0 Tls=014242200 TSecr=787953
38	12.250586	172.16.36.29	172.16.36.17	TLSv1.2	334	Server Hello, Certificate
39	12.250621	172.16.36.29	172.16.36.17	TLSv1.2	213	Server Key Exchange
40	12.250684	172.16.36.17	172.16.36.29	TCP	66	443 -> 443 [ACK] Seq=1268 Ack=1386 Win=3212 Len=0 Tls=014242200 TSecr=934242200
41	12.250686	172.16.36.17	172.16.36.29	TLSv1.2	392	Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request
42	12.250629	172.16.36.17	172.16.36.29	TLSv1.2	589	Application Data

```

Handshake Type: Server Hello (2)
Length: 33
Version: TLS 1.2 (0x0302)
Random
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
Extensions: renegotiation_info
Extensions: ec_point_formats
Extensions: session_ticket_TLS
TLSv1.2 Record Layer: Handshake Protocol: Certificate
Content Type: Handshake (22)
Version: TLS 1.2 (0x0302)
Length: 1376
Handshake Protocol: Certificate
Handshake Type: Certificate (13)
Length: 1368
Certificate Length: 1366
Certificates (1366 bytes)
Certificate Length: 1343
Certificate: 308204873082030FA08020102020001000000020040... (343x-9-at-ens1ADDRESS@descon.com,10-at-comonbaterpaprov.escon.com,10-at-organization@NewDevOps,10-at-organization@escon SA,10-at-343x3)
SignedCertificate
SignatureAlgorithm: sha256WithRSAEncryption
Padding: 0
encrypted: 008070e007195Fac51b40Ac4b7f020604a7e400c07...

```

## 現在のステータス

SNIをサポートするための拡張要求は、CDETS ID:CSCve12309