

SPA112 : Problème de reconnaissance de certificat BE-SPA-SSL

Date d'identification

30 janvier 2017

Date de résolution

S/O

Produits affectés

SPA1 12	1.4.2

Description du problème

La demande reçue du SPA ne prend pas en charge l'indication de nom de serveur (SNI). Sans la prise en charge SNI de l'indication de nom dans la phase de sécurité de la couche transport, le client Hello ne contient pas les informations de nom de serveur.

Dans les images suivantes, vous avez la capture d'écran du message Hello du CLIENT TLS reçu par le serveur lorsque :

1. SNI n'est pas pris en charge (demande reçue du SPA)

Note: Dans ce cas, il n'y a aucune extension server_name dans l'Hello du client de protocole de connexion.

```
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: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: 200
        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 est pris en charge (demande effectuée via le navigateur)

Note: Dans ce cas, l'extension server_name est présente dans l'Hello du client de protocole de connexion.

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) on interface 0
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: 5f6d4334bac156d265f516b5160c54c1239bc55427d111a...
        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
```

Après la résolution, la demande est transmise à l'hôte virtuel par défaut, qui a un certificat différent, signé par une autre autorité de certification. C'est là que l'erreur d'autorité de certification inconnue se produit dans la phase de négociation. Avec un résultat différent selon que la requête contenait ou non les informations nom_serveur :

1. Sans SNI (demande reçue du SPA), le certificat contient le mauvais certificat.

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=4294958469 TSecr=61223505
13	67.781188	172.16.36.4	172.16.36.29	TCP	66	30611 → 443 [ACK] Seq=756 Ack=7691 Win=65537 Len=0 TSval=4294958469 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: 3062032b30620213a03020102020160306004092a864896... [id-at-commonName=172.16.36.29,id-at-organizationName=ESCAUX,id-at-countryName=BE]
        Certificate length: 784
        Certificate: 3062030c306201f74a003020102020103300004092a864896... [id-at-commonName=00000000,id-at-organizationName=ESCAUX,id-at-countryName=BE]
        Certificate length: 792
        Certificate: 30620314306201fca003020102020900000c57c500320376... [id-at-commonName=00001254,id-at-organizationName=ESCAUX,id-at-countryName=BE]
  TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 323
    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: 041623c0660f2e70bae4da876b900003fe490f24b03a083...
```

2. Avec SNI pris en charge (demande reçue du navigateur), le certificat Hello du serveur contient le certificat approprié.

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 -> 44303 [ACK] Seq=1268 Win=1816 Len=0 Tls=104242200 TSecr=787953
38	12.250586	172.16.36.29	172.16.36.17	TLSv1.2	3324	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	44303 -> 443 [ACK] Seq=288 Ack=1386 Win=32132 Len=0 Tls=104242200 TSecr=334242200
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 (0x0303)
Random
Session ID Length: 0
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0x0303)
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 (0x0303)
Length: 1376
Handshake Protocol: Certificate
Handshake Type: Certificate (13)
Length: 1368
Certificate Length: 1366
Certificates (1366 bytes)
Certificate Length: 1343
Certificate: 30820487386263FA803020102020013000000020046... (3416 9-ut-ew11AM@ress@gr@descom.com,10-ut-com@com@aters@p@rov.ec@com,10-ut-@r@get@at@ons@001@New@Dev@l@p@ent,10-ut-@r@get@at@on@Name@@@com SA,10-ut-1@ac@1)
SignedCertificate
SignatureAlgorithm: sha256WithRSAEncryption
Padding: 0
encrypted: 008078e0b07191fa5134b0ac3ab57d29664a7e409c67...

```

État actuel

La demande d'amélioration de support SNI a déjà été déposée avec l'ID CDETS : CSCve12309.