

SPA112:BE-SPA-SSL憑證識別問題

識別日期

2017年1月30日

解決日期

不適用

受影響的產品

SPA1 12	1.4.2

問題描述

從SPA收到的請求不支援伺服器名稱指示(SNI)。 如果傳輸層安全階段不支援名稱指示SNI，則客戶端Hello不包含伺服器名稱資訊。

在以下影像中，您會看到伺服器在以下情況下收到的TLS CLIENT Hello消息的螢幕快照：

1.不支援SNI (收到來自SPA的請求)

附註：在這種情況下，握手協定客戶端Hello中沒有server_name擴展。

```
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
07.775651 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=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.支援SNI (通過瀏覽器請求)

附註：在這種情況下，握手協定客戶端Hello中存在server_name擴展。

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:10:90 (90:10:00:ff:10:90), 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
  
```

解析後，請求會被轉發到預設虛擬主機，該虛擬主機具有由其他CA簽名的不同證書。這是協商階段發生未知CA錯誤的地方。根據請求是否包含server_name資訊，結果不同：

1.如果沒有SNI (從SPA收到的請求) ，則證書包含錯誤的證書。

```

9 87.779299 172.16.36.29 172.16.36.4 TLSv1.2 5504 Server Hello
10 87.779303 172.16.36.29 172.16.36.4 TLSv1.2 1448 Certificate
11 67.782182 172.16.36.4 172.16.36.29 TCP 66 30611 → 443 [ACK] Seq=229 Ack=1449 Win=8736 Len=0 TSval=4294958468 TSecr=61223595
12 67.784168 172.16.36.4 172.16.36.29 TCP 66 30611 → 443 [ACK] Seq=736 Ack=7851 Win=65557 Len=0 TSval=4294958468 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: 3082932b30829213a003020102020160300004092a864896... [id-at-commonName=172.16.36.29,id-at-organizationName=ESCAUX,id-at-countryName=BE]
        Certificate Length: 784
        Certificate: 3082930c308291f74a003020102020160300004092a864896... [id-at-commonName=00000000,id-at-organizationName=ESCAUX,id-at-countryName=BE]
        Certificate Length: 792
        Certificate: 30829314308291f74a003020102020900000c57c508326376... [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: 041823c966072e79ba44da876d9000d7e490748d63a083...
          Encrypted_Mach_Altname: 00000000000000000000000000000000
  
```

2.如果支援SNI (從瀏覽器接收請求) ，則伺服器Hello證書包含正確的證書。

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=1[4242]00 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	44303 -> 443 [ACK] Seq=1268 Ack=1386 Win=3213 Len=0 Tls=1[7879]4 TSecr=33424200
41	12.250690	172.16.36.17	172.16.36.29	TLSv1.2	392	Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request
42	12.250623	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_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 (0x0303)
Length: 1376
Handshake Protocol: Certificate
Handshake Type: Certificate (13)
Length: 1368
Certificates Length: 1366
Certificates (1366 bytes)
Certificate Length: 1343
Certificate: 308204873082030FA08020102020001000000020040... (341x-9-at-ens1Address@desec.com, 10-at-comonbaterpaprov.esecur.com, 10-at-organization@NewDevOps, 10-at-organization@scam SA, 10-at-34ca3)
SignedCertificate
SignatureAlgorithm (sha256WithRSAEncryption)
Padding: 0
encrypted: 008078e087191Fac518d8Ac3d87d82066A47e408c67...

```

當前狀態

支援SNI的增強請求已通過CDETS ID提交：CSCve12309。