

# 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
07.775651 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
36	12.250487	172.16.36.17	172.16.36.29	TLSv1.2	273	Client Hello
37	12.250500	172.16.36.29	172.16.36.17	TCP	66	443 -> 44303 [ACK] Seq=1268 Win=1816 Len=0 Tls=014242200 TSecr=787953
38	12.250506	172.16.36.29	172.16.36.17	TLSv1.2	334	Server Hello, Certificate
39	12.250421	172.16.36.29	172.16.36.17	TLSv1.2	213	Server Key Exchange
40	12.250884	172.16.36.17	172.16.36.29	TCP	66	4433 -> 443 [ACK] Seq=288 Ack=1386 Win=32132 Len=0 Tls=0178764 TSecr=334242200
41	12.250886	172.16.36.17	172.16.36.29	TLSv1.2	392	Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request
42	12.250923	172.16.36.17	172.16.36.29	TLSv1.2	589	Application Data

```

Handshake Type: Server Hello (2)
Length: 63
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
Certificate Length: 1366
+ Certificates (1366 bytes)
Certificate Length: 1343
+ Certificate: 308204873062636FA803026102623991308000024046... (343x-9-at-ens1Address@desicon.com,10-at-comobakerspaprov.ecicon.com,10-at-organization@New-Dev@pewt,10-at-organization@scam SA,10-at-34633)
+ signedCertificate
+ signedCertificate (sha256WithRSAEncryption)
padding: 0
encrypted: 008078e087195Fac518d8Ac3d87d2966Aa7e408c67...

```

## 当前状态

支持SNI的增强请求已向CDETS ID提交：CSCve12309。