

SPA112: BE-SPA-SSL certificaatherkenning

Datum geïdentificeerd

30 januari 2017

Datum opgelost

N.v.t.

Producten getroffen

SPA1 12	1.4.2

Beschrijving van probleem

Een verzoek dat van de SPA is ontvangen, ondersteunt de servernaamindicator (SNI) niet. Zonder de SNI-ondersteuning van de Naam in de Security fase van de Vervoerlaag bevat de Client Hallo niet de informatie over de servernaam.

In de volgende afbeeldingen hebt u het screenshot van het TLS CLIENT Hallo-bericht van de server ontvangen wanneer:

1. SNI wordt niet ondersteund (verzoek van de SPA ontvangen)

Opmerking: In dit geval, is er geen server_name extensie in het Handshake Protocol Client Hallo.

```
Time      Source            Destination        Protocol  Length  Info
07.771085 172.16.39.4      172.16.36.29      TCP       74      36611 → 443 [SYN] Seq=0 Win=5648 Len=0 MSS=1460 SACK_PERM=1 TSval=4294958457 TSecr=0 WS=2
07.771041 172.16.36.29     172.16.39.4       TCP       74      443 → 36611 [SYN, ACK] Seq=0 Ack=1 Win=14400 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=5648 Len=0 TSval=4294958458 TSecr=61223503
07.775655 172.16.39.4      172.16.36.29      TLSv2.2    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=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: 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: 219
      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 wordt ondersteund (verzoek ingediend via de browser)

Opmerking: In dit geval, is de server_name extensie aanwezig in de Handshake Protocol Client Hello.

```

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 (00:10:0b: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: 5f6d43344bac156d265f516b5160c54c1239bc55427d111a...
        Cipher Suites Length: 34
      * Cipher Suites (17 suites)
        Compression Methods Length: 1
      * Compression Methods (1 method)
        Extensions Length: 491
      * 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
  
```

Na de resolutie wordt het verzoek doorgestuurd naar de standaard virtuele host, die een ander certificaat heeft, ondertekend door een ander CA. Dit is waar de Onbekende CA-fout optreedt in de onderhandelingsfase. Met een ander resultaat afhankelijk van of het verzoek de server_name informatie bevatte of niet:

1. Zonder SNI (verzoek van de SPA ontvangen) bevat het certificaat het verkeerde certificaat.

```

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      30611 -> 443 [ACK] Seq=229 Ack=1449 Win=8736 Len=0 TSval=4294958469 TSecr=61223505
13     87.784168  172.16.36.4         172.16.36.29        TCP        66      30611 -> 443 [ACK] Seq=758 Ack=7601 Win=14837 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 (2400 bytes)
        Certificate Length: 815
        * Certificate: 3062032b30620213a03020102020100300000002b064896... [id-at-commonName=172.16.36.29,id-at-organizationName=ESCAUX,id-at-countryName=BE]
          Certificate Length: 784
        * Certificate: 3062030c306201f74a003020102020100300000002b064896... [id-at-commonName=00000000,id-at-organizationName=ESCAUX,id-at-countryName=BE]
          Certificate Length: 792
        * Certificate: 30620314306201f7ca003020102020100300000002b064896... [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: 041823c0660f2e70ba4e4a876b90003fe490f24b063a083...
          * Extension: ec_point_formats: 0x0000
  
```

2. Wanneer SNI wordt ondersteund (verzoek van de browser ontvangen), bevat het Server Hello, Certificaat het juiste certificaat.

No.	Time	Source	Destination	Protocol	Length	Info
36	12.250487	172.16.36.17	172.16.36.29	TLSv1.2	278	Client Hello
37	12.250509	172.16.36.29	172.16.36.17	TCP	66	443 -> 44303 [ACK] Seq=1268 Win=1816 Len=0 TlsV1=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	44303 -> 443 [ACK] Seq=288 Ack=1386 Win=32132 Len=0 TlsV1=787954 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	12.250623	172.16.36.17	172.16.36.29	TLSv1.2	589	Application Data

```

Handshake Type: Server Hello (2)
Length: 64
Version: TLS 1.2 (0x0303)
Random
Session ID Length: 0
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (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: 308204873082030FA08020102020001000000020040... (JKS - 9-ut-ews1@address@domain.com, 10-ut-comobaberspaprov.address.com, 10-ut-organization@NameDev@pext, 10-ut-organization@Name SA, 10-ut-10ca3)
SignedCertificate
SignatureAlgorithm: sha256WithRSAEncryption
Padding: 0
encrypted: 008078e007195Fac518d08Ac3d57d2966A47e408c67...

```

Huidige status

Een verzoek om ondersteuning van SNI is al bij CDETS-id ingediend: CSCve12309.