

SPA112: Problem mit der BE-SPA-SSL-Zertifikaterkennung

Identifiziertes Datum

30. Januar 2017

Auflösungsdatum

K/A

Betroffene Produkte

SPA 112	1,4/2

Beschreibung des Problems

Die vom SPA empfangene Anfrage unterstützt die Servernamenanzeige (SNI) nicht. Ohne die SNI-Unterstützung für die Name Indication in der Sicherheitsphase des Transportebene enthält der Client Hello keine Informationen zum Servernamen.

In den folgenden Bildern wird der Screenshot der TLS CLIENT Hello-Nachricht angezeigt, die der Server beim Empfang erhält:

1. SNI wird nicht unterstützt (Anfrage vom SPA erhalten)

Hinweis: In diesem Fall gibt es im Handshake Protocol Client Hello keine Erweiterung `server_name`.

```
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=228 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: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 wird unterstützt (Anfrage über Browser)

Hinweis: In diesem Fall ist die Erweiterung server_name im Handshake Protocol Client Hello vorhanden.

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 (90:10:0b: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: 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

Nach der Auflösung wird die Anforderung an den virtuellen Standardhost weitergeleitet, der über ein anderes Zertifikat verfügt, das von einer anderen CA signiert wurde. An dieser Stelle tritt der Fehler "Unknown CA" (Unbekannte CA) in der Verhandlungsphase auf. Mit einem anderen Ergebnis, je nachdem, ob die Anforderung Informationen über den Servernamen enthält oder nicht:

1. Ohne SNI (Anfrage vom SPA erhalten) enthält das Zertifikat das falsche Zertifikat.

| | | | | | | |
|----|-----------|--------------|--------------|---------|------|--|
| 9 | 67.779290 | 172.16.36.29 | 172.16.39.4 | TLSv1.2 | 1504 | Server Hello |
| 10 | 67.779333 | 172.16.36.29 | 172.16.39.4 | TLSv1.2 | 1448 | Certificate |
| 11 | 67.782182 | 172.16.39.4 | 172.16.36.29 | TCP | 66 | 30612 → 443 [ACK] Seq=220 Ack=1449 Win=8736 Len=0 TSval=4294950469 TSecr=61223005 |
| 15 | 67.784168 | 172.16.36.29 | 172.16.36.29 | TCP | 66 | 30614 → 443 [ACK] Seq=750 Ack=7691 Win=14857 Len=0 TSval=4294950469 TSecr=61223005 |

[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: 3082032b30820213a00302010202010300000002a864896... [id-at-commonName=172.16.36.29,id-at-organizationName=ESCAUX,id-at-countryName=BE]
 - Certificate Length: 784
 - Certificate: 3082030c308201f4a00302010202010300000002a864896... [id-at-commonName=00000000,id-at-organizationName=ESCAUX,id-at-countryName=BE]
 - Certificate Length: 792
 - Certificate: 30820314308201fca00302010202010300000002a864896... [id-at-commonName=0001254,id-at-organizationName=ESCAUX,id-at-countryName=BE]

2. Wenn SNI unterstützt wird (Anfrage vom Browser empfangen), enthält das Server Hello

das entsprechende Zertifikat.

The image shows a Wireshark packet capture of a TLS handshake. The top section is a packet list with columns for No., Time, Source, Destination, Protocol, Length, and Info. Packet 22 is selected, showing details for the TLSv2.2 Handshake (22) protocol. The details pane shows the following structure:

- Handshake Type: Server Hello (2)
- Length: 83
- Version: TLS 1.2 (0x0303)
- 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, renegotiation_info, ec_point_formats, session_ticket_TLS
- Handshake Layer - Handshake Protocol: Certificate
- Content Type: Handshake (22)
- Version: TLS 1.2 (0x0303)
- Length: 5170
- Handshake Protocol: Certificate
- Handshake Type: Certificate (11)
- Length: 1046
- Certificate Length: 1046
- Certificate (5336 bytes)
- Certificate Length: 5336
- Certificate: 302349736293F48323252022893388888824804... (hex)
- Signature: sha256WithRSAEncryption
- Padding: 0
- Signature: 603617e6d87191fa1134f84c3a876d30b6b47e48b97...

At the bottom, there is a hex dump of the certificate data, showing hexadecimal values and their corresponding ASCII characters.

Aktueller Status

Der Verbesserungsantrag zur Unterstützung von SNI wurde bereits mit der CDETS-ID eingereicht: CSCve12309.