Bip - Bug #339

Client side ssl not working

2014-06-10 16:02 - Pierre-Louis Bonicoli

Status:	Rejected	**Start date:**	2014-06-10
Priority:	Normal	**Due date:**	
Assignee:	Pierre-Louis Bonicoli	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			
Patch Available:		**Branch:**	
Found in Versions:		**Security:**	
Confirmed:	No	**Help Needed:**	

Description

kick wrote on irc:

> I copied my working config file from my bip 0.8.8-2
> and I've got ssl handshake problems..
> I'm using a ubnutu trusty for bip 0.8.9-1
> I have a bip.pem set, with good owner and permissions.

Error in client:

> connexion a échoué. Erreur : (336151568) error:14094410:SSL routines:SSL3_READ_BYTES:sslv3 alert handshake failure

bip.log contains:

> 139638493165216:error:1408A0C1:SSL routines:SSL3_GET_CLIENT_HELLO:no shared cipher:s3_srvr.c:1358:ERROR: Error in SSL handshake.

bip 0.8.8-2, sslv3

```
openssl s_client -ssl3 -connect edited.bip.server:7778
CONNECTED(00000003)
depth=0 C = fr, O = Sexy boys, OU = Bip, CN = Bip
verify error:num=18:self signed certificate
verify return:1
depth=0 C = fr, O = Sexy boys, OU = Bip, CN = Bip
verify return:1
---
Certificate chain
 0 s:/C=fr/O=Sexy boys/OU=Bip/CN=Bip
   i:/C=fr/O=Sexy boys/OU=Bip/CN=Bip
---
Server certificate
-----BEGIN CERTIFICATE-----
EDITED XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
-----END CERTIFICATE-----
subject=/C=fr/O=Sexy boys/OU=Bip/CN=Bip
issuer=/C=fr/O=Sexy boys/OU=Bip/CN=Bip
---
```

```
No client certificate CA names sent
---
SSL handshake has read 2318 bytes and written 364 bytes
---
New, TLSv1/SSLv3, Cipher is DHE-RSA-AES256-SHA
Server public key is 4096 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol  : SSLv3
    Cipher    : DHE-RSA-AES256-SHA
    Session-ID: EDITED XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
    Session-ID-ctx:
    Master-Key: EDITED XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
    Key-Arg   : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    Start Time: 1402406408
    Timeout   : 7200 (sec)
    Verify return code: 18 (self signed certificate)
```

bip 0.8.8-2, tls1

```
openssl s_client -tls1 -connect server.bip.edited:7778
CONNECTED(00000003)
depth=0 C = fr, O = Sexy boys, OU = Bip, CN = Bip
verify error:num=18:self signed certificate
verify return:1
depth=0 C = fr, O = Sexy boys, OU = Bip, CN = Bip
verify return:1
---
Certificate chain
 0 s:/C=fr/O=Sexy boys/OU=Bip/CN=Bip
   i:/C=fr/O=Sexy boys/OU=Bip/CN=Bip
---
Server certificate
-----BEGIN CERTIFICATE-----
Edited XXXXXXXXXXXXXXXXXXXXXXX
-----END CERTIFICATE-----
subject=/C=fr/O=Sexy boys/OU=Bip/CN=Bip
issuer=/C=fr/O=Sexy boys/OU=Bip/CN=Bip
---
No client certificate CA names sent
---
SSL handshake has read 2454 bytes and written 423 bytes
---
New, TLSv1/SSLv3, Cipher is DHE-RSA-AES256-SHA
Server public key is 4096 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol  : TLSv1
    Cipher    : DHE-RSA-AES256-SHA
    Session-ID: Edited XXXXXXXXXXXXXXXXXXXXXXX
    Session-ID-ctx:
    Master-Key: Edited XXXXXXXXXXXXXXXXXXXXXXX
    Key-Arg   : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
```

```
    TLS session ticket lifetime hint: 60 (seconds)
    TLS session ticket:
    0000 - 0d b9 57 57 8b b7 cd bf-70 3c 72 79 d0 f4 6f 81   ..WW....p<ry..o.
    0010 - e4 30 64 d1 97 96 62 05-8c ed 45 8e d8 36 d6 52   .0d...b...E..6.R
    0020 - 37 65 b5 7d 6d 19 5c 8e-22 ab 31 4c a5 b9 ac 6a   7e.}m.\.".1L...j
           Edited XXXXXXXXXXXXXXXXXXXXXXX
    0080 - f7 cc ab e5 18 cc 33 28-b0 7a 12 46 3f 21 ba 1b   ......3(.z.F?!..
    0090 - c0 9b 4c 8b 61 3a 4d d4-78 e8 77 91 80 b9 ab a1   ..L.a:M.x.w.....

    Start Time: 1402406391
    Timeout   : 7200 (sec)
    Verify return code: 18 (self signed certificate)
---
```

bip 0.8.9-1, sslv3

```
openssl s_client -ssl3 -connect edited:7778
CONNECTED(00000003)
140228681320096:error:14094410:SSL routines:SSL3_READ_BYTES:sslv3 alert handshake failure:s3_pkt.c
:1260:SSL alert number 40
140228681320096:error:1409E0E5:SSL routines:SSL3_WRITE_BYTES:ssl handshake failure:s3_pkt.c:596:
---
no peer certificate available
---
No client certificate CA names sent
---
SSL handshake has read 7 bytes and written 0 bytes
---
New, (NONE), Cipher is (NONE)
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol  : SSLv3
    Cipher    : 0000
    Session-ID:
    Session-ID-ctx:
    Master-Key:
    Key-Arg   : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    Start Time: 1402406211
    Timeout   : 7200 (sec)
    Verify return code: 0 (ok)
---
```

bip 0.8.9-1, tls1

```
openssl s_client -tls1 -connect edited:7778
CONNECTED(00000003)
140587600295584:error:14094410:SSL routines:SSL3_READ_BYTES:sslv3 alert handshake failure:s3_pkt.c
:1260:SSL alert number 40
140587600295584:error:1409E0E5:SSL routines:SSL3_WRITE_BYTES:ssl handshake failure:s3_pkt.c:596:
---
no peer certificate available
---
No client certificate CA names sent
---
```

```
SSL handshake has read 7 bytes and written 0 bytes
---
New, (NONE), Cipher is (NONE)
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol  : TLSv1
    Cipher    : 0000
    Session-ID:
    Session-ID-ctx:
    Master-Key:
    Key-Arg   : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    Start Time: 1402406299
    Timeout   : 7200 (sec)
    Verify return code: 0 (ok)
```

History

#1 - 2014-07-14 17:23 - Pierre-Louis Bonicoli

- Status changed from New to Feedback

I couldn't reproduce.

Test environment:

- server: bip 0.8.9-1 (Ubuntu 14.04 - Trusty)
- client1: Weechat 0.4.3-3 (Debian unstable)
- client2: Weechat 0.4.2-3 (Ubuntu 14.04 - Trusty)
- self-signed certificate generated with XCA using template [default] CA

Openssl s_client command runs without any error on both clients.

```
pilou@client1$ apt-cache policy openssl |grep Ins
  Installed: 1.0.1h-3

pilou@client1$ openssl s_client -tls1 -connect bip.local:7778
CONNECTED(00000003)
depth=0 C = FR, L = PARIS, O = piloucorp, CN = bip.local, emailAddress = root@test.eu
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 C = FR, L = PARIS, O = piloucorp, CN = bip.local, emailAddress = root@test.eu
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:/C=FR/L=PARIS/O=piloucorp/CN=bip.local/emailAddress=root@test.eu
   i:/C=FR/L=PARIS/O=piloucorp/CN=bip.local/emailAddress=root@test.eu
---
Server certificate
-----BEGIN CERTIFICATE-----
[...]
-----END CERTIFICATE-----
subject=/C=FR/L=PARIS/O=piloucorp/CN=bip.local/emailAddress=root@test.eu
issuer=/C=FR/L=PARIS/O=piloucorp/CN=bip.local/emailAddress=root@test.eu
---
No client certificate CA names sent
---
SSL handshake has read 2575 bytes and written 429 bytes
---
New, TLSv1/SSLv3, Cipher is DHE-RSA-AES256-SHA
Server public key is 4096 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol  : TLSv1
```

```
    Cipher    : DHE-RSA-AES256-SHA
    Session-ID: [...]
    Session-ID-ctx:
    Master-Key: [...]
    Key-Arg   : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 60 (seconds)
    TLS session ticket: [...]

    Start Time: 1405350395
    Timeout   : 7200 (sec)
    Verify return code: 21 (unable to verify the first certificate)
```

Bip configuration:

```
client_side_ssl = true;
# contains certificate and key
client_side_ssl_pem = "/etc/bip.pem";
```

Certificate:

```
$ openssl x509 -in /tmp/bip.pem -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=FR, L=PARIS, O=piloucorp, CN=bip.local/emailAddress=root@test.eu
        Validity
            Not Before: Jul 14 00:00:00 2014 GMT
            Not After : Jul 13 23:59:59 2015 GMT
        Subject: C=FR, L=PARIS, O=piloucorp, CN=bip.local/emailAddress=root@test.eu
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                [...]
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Subject Key Identifier:
                96:7C:F9:BD:E7:A9:6C:50:C4:28:9C:C4:3B:AE:E7:72:93:6B:45:95
            X509v3 Key Usage:
                Digital Signature, Non Repudiation, Key Encipherment
            Netscape Cert Type:
                SSL Server
            Netscape Comment:
                xca certificate
    Signature Algorithm: sha1WithRSAEncryption
    [...]
```

Weechat configuration:

```
# .weechat/weechat.conf
[network]
# contains certificate but not the key
gnutls_ca_file = "/tmp/bip.pem"
```

```
# .weechat/irc.conf
[server]
freenode.addresses = "bip.local/7778"
freenode.ssl = on
freenode.ssl_dhkey_size = 1024
freenode.password = "pilou:XXX:testnetwork"
freenode.nicks = "bip_pilou"
```

#2 - 2014-07-24 01:56 - Pierre-Louis Bonicoli

- Status changed from Feedback to Rejected

- Found in Versions deleted (0.8.9)

Reporter was not able to reproduce too, kick wrote on irc:

```
I restarted an installation on a trusty container, and I could log in with ssl. Strange...
I must have done a mistake previously....
```