eole-annuaire - Tâche #11341

Désactiver le SSLv3 sur l'annuaire

04/20/2015 03:33 PM - Joël Cuissinat

Status:	Fermé	**Start date:**	12/01/2015
Priority:	Normal	**Due date:**	
Assigned To:	Laurent Flori	**% Done:**	100%
Target version:	Sprint 2015 49-51 - Équipe MENESR	**Estimated time:**	3.00 hours
		Spent time:	1.33 hour

Description

Associated revisions

Revision 77946995 - 12/01/2015 12:16 PM - lolo

Correction de la liste des suites de chiffrement
fixes: #11341 @1h

History

#1 - 11/30/2015 09:34 AM - Laurent Flori

- Assigned To set to Laurent Flori

#2 - 12/01/2015 10:14 AM - Scrum Master

- Status changed from Nouveau to En cours

- Start date set to 12/01/2015

#3 - 12/01/2015 12:35 PM - Anonymous

- Status changed from En cours to Résolu

- % Done changed from 0 to 100

Appliqué par commit 7794699522aacdbf2c02fda9af901c7ec08a139f.

#4 - 12/04/2015 04:44 PM - Joël Cuissinat

- Remaining (hours) changed from 3.0 to 0.5

- Avant (2.5.1) :

```
root@scribe:~# openssl s_client -connect localhost:636 -ssl3
   [ ... ]
New, TLSv1/SSLv3, Cipher is AES256-SHA
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol  : SSLv3
    Cipher    : AES256-SHA
    Session-ID: 0C2D17F9F30FABC2C6A54711237117D1704A2F29D3036476B8BCFCCC44D39248
    Session-ID-ctx:
    Master-Key: 75DC04526CCCD80A14FD38490C51F83AA529066BC9346EF1787C7DADB8A0ED3F493B1172080A0CBF4176CD1FF7
B51B01
    Key-Arg   : None
    PSK identity: None
    PSK identity hint: None
```

```
    SRP username: None
    Start Time: 1449242571
    Timeout   : 7200 (sec)
    Verify return code: 19 (self signed certificate in certificate chain)
```

- Après (2.5.2) :

```
root@scribe:~# openssl s_client -connect localhost:636 -ssl3
CONNECTED(00000003)
139631814735520:error:1408F10B:SSL routines:SSL3_GET_RECORD:wrong version number:s3_pkt.c:339:
---
no peer certificate available
---
No client certificate CA names sent
---
SSL handshake has read 5 bytes and written 7 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: 1449243671
    Timeout   : 7200 (sec)
    Verify return code: 0 (ok)
---
```

#5 - 12/04/2015 05:01 PM - Joël Cuissinat

- Status changed from Résolu to Fermé

- Remaining (hours) changed from 0.5 to 0.0